A Comparative Analysis of Various Multistep Login Authentication Mechanisms

Navpreet Kaur
Department of Information Technology
Chandigarh Engineering College, Landran
(Punjab, India)

Mandeep Devgan
Department of Information Technology
Chandigarh Engineering College, Landran
(Punjab, India)

ABSTRACT

Due to advancements and improvements in internet and communication systems, more people are relying on internet to store their confidential information. Earlier the idea of Static passwords was being used but most of the users try to use easily guessable, weak passwords or keywords from their personal information, which makes it easy for the intruders to guess their passwords in few combinations using Brute Force attack. Thus idea of using Multi-Factor Authentication has been introduced in the world of internet to harden the security of network and make it difficult for the attackers to crack systems. In this mechanism, users are required to provide some extra information along with their login Id and password. Most popular is using One-Time Passwords that are generated randomly and valid only for single login and even for short duration of time (usually 30 to 60 seconds). One-Time Passwords can be generated either online or offline via various mechanisms. In this paper, review of various Multi-step Authentication schemes has been performed to compare various authentication mechanisms.

Keywords

Multi-factor Authentication, One-Time Passwords (OTP) , Static Passwords, Short Message Service (SMS), Time-based One Time Passwords (TOTP) and Image-based Authentication.

1. INTRODUCTION

The internet and mobile communications have been developing and related application or services for managing money and personal information are increasing in number day by day. Thus, now-a-days people rely more on internet to store the confidential and important data. However, there is a risk that private data may be wiretapped. Therefore, it is necessary to authenticate users and in order to keep this web data safe on cloud almost every client and server implement cryptographic techniques to encrypt this sensitive data, as well as verify entities at the other end of the connection [1].Thus if more confidential data is to be stored online, it is necessary that the network security should stay up to date with modern attacks. However, online users continue to use weak and easily guessable passwords like birth dates, partner names, children names etc. and they are typically only letters. Also, if the user sends the same password every session, an attacker can easily masquerade as a user, because the attacker may succeed in getting the user's password through internet. So, it is becoming clear that passwords are not sufficient means to protect the online accounts [2].Various authentication schemes are being in use today to harden the security of online data or information. Authentication also plays an important role when the transactions are related to money i.e. in financial transactions. One of the common authentication scheme used in financial services or transactions is using a hardware token like smartcards, credit/debit cards etc., but using these cards to authenticate the user identity is also not very sure in providing the security to the transactions. They are vulnerable to some frauds like swindlers (attackers) make use of skimmers that are devices used to capture data from the magnetic stripe of the card issued by the bank or any financial institution [11]. Multi layering of multi factor authentication is also important in hardening the security of financial services [12]. Some of the most popular authentication mechanisms are as follows:

1.1 Usernames and Passwords

The traditional and oldest method for providing authentication is using usernames and passwords. Most of the websites use this method to provide security to their client's personal data. The username is used to identify which online account does user or client wants to access and passwords are used to prove the identity of that legitimate user [2]. Passwords are stored on server side in encrypted form or using hash functions, also the username and passwords transmit in encrypted form over the secure connection. Thus if any intruder get access over the network, there is no worry about leakage of important information as it will not reveal any information about actual password.

Even though it looks secure but in practical it is not as secure as an attacker can get original password of a client using brute force attack after a few combinations. Also, the user continues to use easy and guessable passwords, so it is recommended to use complex passwords or changing it repeatedly after short period of times. These single static passwords are also very vulnerable to social engineering i.e. people may ask for passwords or can also guess them correctly. Some surveys carried out on various places have revealed that how easy it is to get people reveal their passwords very easily. Any attacker can also use these passwords to access their personal accounts otherwise one need to change their passwords repeatedly [9]. A few emphasis have been given on usage of complex passwords like it's length should be minimum 8 characters, should have at least one numeric and one special symbol etc. But due to various vulnerabilities and attacks like phishing, man in the middle attack, brute force etc on static passwords, a need of hardening the security of online data and information stored by the users has been raised. Thus, after a few researches in the field of online security, a method has been proposed. In which the authentication of legitimate users have to be performed not only in a single step through a password but is to be performed in various steps by asking for more information about the user by the server. This gives rise to the introduction of Multi-step or Multi-factor authentication scheme.

1.2 Multi-factor authentication

Multi-factor Authentication is a method of computer access control which a user can pass successfully presenting various authentication stages. In this, instead of asking just single piece of information like passwords, users are asked to give some additional information which makes it more difficult for any intruder to fake the identity of the actual user. This additional information can include various factors like finger prints, biometric authentication, security tokens etc. It has emerged an alternative way to improve the security by requiring the user to provide with more than one authentication factor rather than only a single password. Authentication factors are of these kinds:

1. *Knowledge* – something that the user knows, e.g., a username and a password;
2. *Possession* – something the user has, e.g., a hardware token(as a security token);
3. *Inherence* – something verifies the user is, e.g., fingerprints [10].

Multi factor authentication can be performed in various ways, most common of them is using login credential with some additional information but a different technique also include authentication in which usage pattern of input data is used in determining the authenticity of user like the time taken by user to input his details, or the pressure exerted by the user's finger on the touch screen of the Smartphone may be calculated to find whether the login is done by the authenticate user or by any other attacker[13]. Mostly all the websites and online services are now-a-days implementing multi-step authentication to provide security to their customers. More recently, an increasing number of service providers like Google, Face book, Drop box, Twitter, LinkedIn etc. have also begun to provide their users with the option of enabling multi-factor authentication; this is motivated by the increase in number of hacking passwords. Multi layering of authentication is also becoming popular these days in which authentication is provided at various levels. Different kind of authentication technique is provided at each level like knowledge based biometric authentication etc. individually at each level [12]. As a general, in multi-step users are required to provide some required information along with the login credentials of the user. Most of the information that has been used in this authentication is like:

- A digital Certificate
- An RSA token code
- PIN from a paper or from a card i.e. One-time PIN
- Google Authentication
- A Smartphone
- A USB token/Security token
- A verification code received via SMS or email

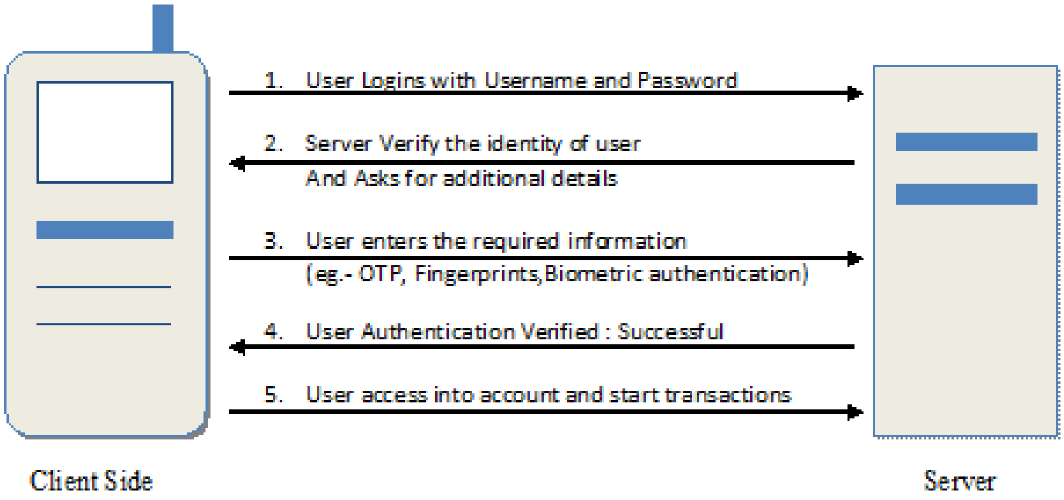

1. User Logins with Username and Password
2. Server Verify the identity of user
And Asks for additional details
3. User enters the required information
(eg.- OTP, Fingerprints,Biometric authentication)
4. User Authentication Verified : Successful
5. User access into account and start transactions
Client Side
Server

Fig 1: Multistep Authentication Process

1.4 One-Time Passwords

A One-Time Password (OTP) is a password or code which is valid only for one login session or transaction on a computer system or any digital device. OTPs were introduced just to avoid the shortcomings that are associated with static passwords. Even they are valid for a small period of time and they automatically expires after the given time span. The most important advantage of OTPs, in contrast to static passwords, is that they are not vulnerable to replay attacks [1].It means that a potential intruder or attacker who manages to record an OTP that was already used by a user to login into the service will not be able to reuse it since it will be no longer valid. Also, OTPs are very difficult for humans to memorize [9]. Another advantage is that a single OTP code cannot be used to login on multiple systems. Many Techniques have been introduced today to generate and deliver these one-time passwords and most of them use Time-based One Time Passwords. Some of the OTP generation techniques are:

- Based on **Time-synchronization** between authenticating server and the client providing the login details. In Time-based One Time Password generation method, time is an important part in password algorithm as the generation of new password is based on current time rather than on previous password or any secret key. Mobile phones or similar mobile devices which runs software that is proprietary, open source or freeware is used to generate these times synchronized pass codes. An example of time synchronised passwords is Time-based One-Time Passwords (TOTP) [9].

- Based on **Mathematical Algorithms** in which each new One-time Passwords are generated from the past OTPs used. In this unique passwords are generated from a certain secret key or seed value using hash function.

Table 1: Login Table to the main Server with OTP's

Username	One Time Password	Token	Status
Alia	328461	1	Valid
John	647552	0	Expired
Tom	673837	1	Valid
Jenny	896321	0	Expired

2. LITERATURE REVIEW

Uymatiao, Mariano Luis T., and William Emmanuel S. Yu [2] (2014) have worked on Time-based OTP through secure tunnel (TOAST). They have collectively developed a mobile TOTP scheme using TLS seed exchange and encrypted offline keystroke. The main objective of this research is to build upon existing cryptographic standards and web protocols to design an alternative multi-factor authentication cryptosystem for the web. It involves seed exchange to a software-based token through a login-protected Transport Layer Security (TLS/SSL) tunnel, encrypted local storage through a password-protected keystroke (BC UBER) with a strong key derivation function, and offline generation of one-time passwords through the TOTP algorithm. Authentication occurs through the use of a shared secret (the seed) to verify the correctness of the one-time password used to authenticate.

Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin and Jean-Pierre Seifert [3] (2014) have worked on SMS-based One Time Passwords that were introduced to counter phishing and other attacks against various internet services like in Banking Services. Now days, these OTPs are used for authentication and authorization in various other applications. But they are also prone to very heavy attacks especially to Smartphone Trojans. Thus, they collectively study the security architecture of SMS OTP systems and study attacks. Also, they proposed a mechanism to secure SMS OTPs against common attacks and specifically against Smartphone Trojans.

Michiel Appelman, Yannick Scheelen[4] (2012) have analysed on Google's 2-step verification login system. In which, Google asked for a verification code in combination with username and password. This unique verification code can be generated via three methods i.e. verification code can be sent via email or to the mobile phone through voice call or a text message. Another way is Google introduces a special Smartphone application that generates verification codes on users Smartphone that are valid only for 30 seconds of time.

Subashini K., and G. Sumithra [5] (2014) have worked on Secure multimodal mobile authentication using one time password. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc.

Himika Parmar, Nancy Nainan, and Sumaiya Thaseen [8] (2012) have collectively analyse on phishing attack and provides the need to prevent such phishing attacks. Thus based upon all this proposes not to use passwords and to authenticate a user without a text password. They proposed an authentication service that is image based and eliminates the need of text passwords. In which a user will receive OTP through the instant messaging service available in internet after image authentication. The OTP then can be used by user to access their personal accounts. It integrates Image based authentication and HMAC based one time password to achieve high level of security in authenticating the user over the internet.

Nitin Mujal, R. Moona [11] (2009) described a secure and cost effective transaction model for financial services. As with the advent of the e-commerce, it has become much easier for the intruders or attackers to sit in non-descriptive location and quietly siphon away the money from the service users. Thus also the financial service outlets like Automated Teller Machine (ATM), Point of sale (PoS) terminal have also been an easy target. As the users are forced to trust a service outlet to be authentic but actually they can be spoofed and also a spoofed outlet can collect the account information of the users and can use the same to do financial transactions. These outlets are also very expensive to implement. Thus a secure and cost effective model has been proposed to overcome various securities and cost related issues of financial service models. It is cost effective such that financial services can also reach to the rural population and contribute to rural development. It relies on public key infrastructure (PKI) architecture to provide ensures about both cost and security issues.

M.M. Mohammed, M. Elsadig (2013) provided a multi-layer of multi factors authentication model for Online Banking Services. The security risks of internet banking have always been a matter of concern for the service providers as well as for the users. Various online environments like internet banking, electronic transactions and financial services have been analyzed to identify the characteristics and issues of existing authentication methods in order to present a user authentication level system model that is suitable for different online services. Multi-factor Authentication has been integrated with multi layer authentication techniques in order to produce a standard layered multi factor authentication model suitable for different online banking services suitable based on risk assessment criteria. The proposed model includes 5 levels such that each level contains one or combination of various authentication factors such as knowledge-based, possession based, or biometric based factors. The standard model is compared to multi layering guidelines and it shows improvement and fulfilment of authentication needs.

Hojin Seo, Huy Kang Kim [13] (2011) proposed a novel approach to prevent e-financial incidents by analyzing the input patterns of mobile banking users such as how long it takes by the user to input data into a mobile phone, and the normal finger pressure levels when user inputs through a touch screen. This can help in distinguishing the differences between the legitimate user's usage pattern and an attacker's usage pattern. This proposed method shows high accuracy and is effective in preventing e-financial incidents.

3. LOGIN AUTHENTICATION SCHEMES

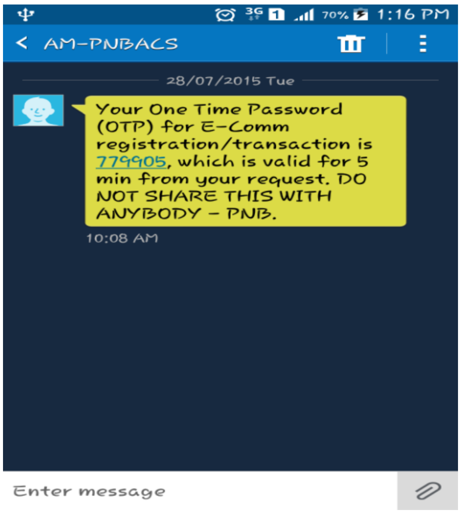
3.1 Short Message Service based One Time Passwords

In previous system, the security of online data was based on system authorization and authentication processes. The most simplest way of authenticating a user is through usernames and passwords. Though the various well-known security issues, passwords are most-popular method for end-user authentication. Guessing and offline Brute force attacks are very common due to their limited entropy. According to Ashlee Vance, 20% of passwords can be covered by a list of only 5000 passwords [10]. Thus, multifactor authentication or usage of complex passwords becomes necessity for hardening the security of internet.

Short Message Service (SMS) based One Time Passwords is a two factor authentication. It is the simplest scheme of generating one time codes. In this scheme, the onetime code is generated on the server side and is being sent over the network to the registered mobile number via SMS. Authentication occurs when the server recognises that the user enters in the correct code for login [2]. The phone number of the user must be registered with the service that provides SMS OTPs for authentication [3].Whenever a user tries to login into his account with username and password, he will receive a unique code on his phone number and will enter this code to get access to his account. The user can receive the OTP either as a text message or via an automated call using text-to speech conversion. Also, Google has started offering OTP to mobile and landline phones for all Google accounts. Additionally, OTP is also restricted to a very short period of time and will expire automatically. There is no additional software or hardware requirement in authentication system that uses SMS based OTPs to authenticate or authorize a valid user which shows that this is the simplest way of delivering OTPs as SMS enabled devices are almost available with every person using internet these days.SMS based One Time Passwords is the most simplest and widely used mechanism in providing Multistep authentication scheme. It is most popular in banking and credit-debit card transactions.

The major advantage of SMS based OTP system is that it is compatible with any SMS-enabled mobile phone. Since the only thing a SMS-based system needs to provide to the server is the user's phone number[2].Also, very few steps are involved in this technique and is the simplest way of generating one time passwords and even simpler in transmission of the unique codes. It also keeps the cost very low as a large customer already owns a mobile phone for purposes other than generating One Time Passwords. Because of these advantages most of the banking transactions like internet banking, Master/Visa credit or debit card transactions, enables an extra layer of security by providing an extra One Time Passwords (OTP) SMS verification.

The problem with SMS-based OTP is that it is only as good as the mobile network of the user. If the network is slow, the user may be delayed from logging into account or even the received unique code may be expired [2]. Thus, a user would either be delayed to get access to the service or may request to send a new one time password. Also, several attacks against GSM and 3G networks have shown that confidentiality for SMS messages cannot necessarily be provided[3].The one time passwords sent via SMS are always transmitted in plaintext which is more vulnerable to man-in-the middle attack. As SMS-OTP relies on single mode of communication between the users and the related web services and thus it is an in-band authentication.



28/07/2015 Tue

Your One Time Password (OTP) for E-Comm registration/transaction is 779905, which is valid for 5 min from your request. DO NOT SHARE THIS WITH ANYBODY - PNB.

10:08 AM

Fig 2: SMS-OTP received on Mobile Phone

Because of single stream communication, fraudsters or attackers may attack in-band authentication with Man-in the Middle attack or Phishing. Man in the Middle attack attacks on the mobile device and sniffs all the SMS messages being sent to the user to a server that is controlled by the fraudster. Through phishing attack, the attacker will steal the Login Id or username and password of the user. Now, the only thing remaining is the one time passwords that are received on the mobile phone of the user via Short Message Service (SMS). Then, as a part of Man in the Middle attack, the attacker infects the user's mobile device and insists the user to download a malicious application which is responsible of forwarding all the text messages to the server controlled by the attacker. Now, the attacker can login with the stolen login credentials of the user and for next step the verification code will be received on the fake server created by the fraudsters.

3.2 RSA SecurID

The RSA SecurID authentication System consists of a token that can be hardware (e.g.- a USB dongle) or a software (a soft token) which is given to the computer user and it is used to generate one time unique passwords that lasts for a maximum of 60 seconds time span. Generation of this one time password is done using encoded-random key that is known as seed. This seed is unique for each token and is loaded into their corresponding to RSA SecurID server. Tokens are also available On-Demand, in which token codes or unique passwords can be sent to the user via email or text SMS, which eliminates the need of a provision of token to the user. In this authentication scheme, seed is the secret key used to generate unique passwords. It also allows token to be used as Smart Card-like device to store certificates securely [7].

(a)

(b)

Fig 3: RSA SecurID hardware token: (a) older style, Model SD600, (b) New style Model SID800 with smartcard functionality

While RSA SecurID authentication mechanism provides stronger layer of security to a network as well as it protects the network from replay attack. But it is more vulnerable to man-in-the-middle attacks when used alone. If the intruder manages to block the legitimate user from authenticating him to the server until the next code will be valid, the attacker will be able to login to the server. Also, the difficulty may occur in this system if the authentication server's clock becomes out of sync with the clock built into the authentication tokens. However, the security of this system can be improved using mechanisms for encryption/ authentication such as SSL.

Hard Tokens are on the other hand can be physically stolen (like they can be stolen by social engineering attacks) from the authenticated end users. Also the user will not report immediately after the theft of the security token. The user will at least wait for one day before reporting the device as missing. This will give intruder a plenty of time to breach the protected system. However this could only occur if the unique username and password of account is known.

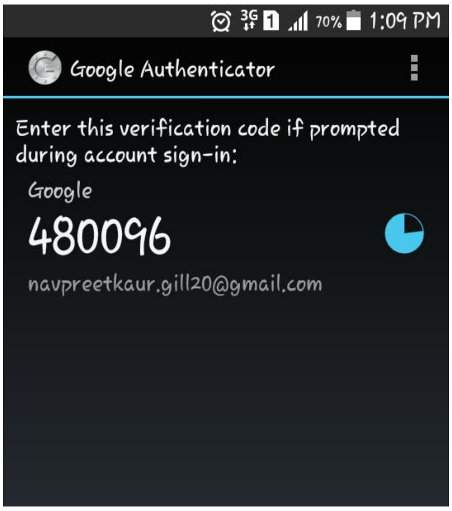
3.3 Google Authenticator

Google introduces 2-step verification or authentication scheme in September 2010 for Google Applications users. After enabling this service user have to provide an extra verification code after logging into their Google accounts. This verification code could be received by a Short Message Service (SMS) text message or voice over text message, or even through a token or code generating application developed by Google. Google's 2-step verification requires something you have (like smart phone with Google authenticator installed to generate verification code) and something you know (that is the password of your Google account) that is required to access into your account [4]. The verification code could be retrieved via a token generator on a Smartphone. These token based verification codes are generated using a time-based algorithm.

And application that performs this verification code generating is called as Google Authenticator. Google authenticator is a software-based OTP generation scheme based on Time-based One Time Passwords (TOTP). It implements TOTP; security token from RFC 6238 in mobile apps made by Google or may be referred to as 'Two-Step Verification'. Google Authenticator uses an offline scheme of TOTP, where it's user's device which generates one-time passwords for the user rather than the server. Authenticator provides a six to eight digit one time unique password which user must provide in contrast with username and password to get access or login to Google services or other sites. It is an open source project that is available for android, iOS and BlackBerry devices. The application generates one-time time-based code using open-standards, including HMAC-based One-Time password (HOTP) algorithms and Time-based One-Time password (TOTP) algorithms. The generated Token or code is six digits in length and is valid for a 30 second timeframe [4].

Before the application could generate the unique tokens, it has to be linked with user's Google account either using Quick Response (QR) code which is created by Google and has to be scanned by the user Smartphone, or by using a secret-key provided by Google [4].Once the account is linked to the device, the app can generate a token for 30 seconds time span, after which a new token will be generated.

When a user has enabled his Google applications with Google's 2-step verification, his login process will be protected through an extra layer of security. Firstly, the user will as usual has to enter his username or login id and password and then in second step, he will enter the 6-digit verification code generated by the application Google Authenticator installed on the users Smartphone [4]. But, before the application could generate verification codes, it has to be linked to users Google account. This can be done via two methods. Firstly, link can be made using Quick Response (QR) code which is generated by Google in the browser and has to be scanned by the Smartphone device. Another method is by using a secret key provided by Google. Once the account and Google Authenticator are linked to each other, the Application would generate security token or verification code that are valid not more than 30 seconds time span i.e. it will automatically expires after 30 seconds and a new code will be generated.



Google Authenticator

Enter this verification code if prompted during account sign-in:

Google

480096

navpreetkaur.gill20@gmail.com

Fig 4: Verification Code generated by Google Authenticator

The major advantage of this system is that it generates tokens offline i.e. it can also generate verification codes even if there is no network connectivity. Also it ensures that only the rightful owner is given access to the account. The Time-based One Time Password (TOTP) generated verification codes based upon a synchronize time between the Google services and the users mobile device provides a robust login system that is not prone to attacks. But the major drawbacks of this system comes down to two things: seed transmission and seed storage[2].When it comes to transfer the seed to the mobile phone, Google relies on QR codes in which the seed travels in plaintext during transmission. This is more vulnerable to be attacked by any intruder. Also secret seed and login credentials of user are stored on Android device in plaintext so can be accessible to anyone easily and can be used to enrol the same seed on multiple devices. Thus, retrieving the secret code to link the Google account with Google application or Authenticator and the verification codes can be easily done by performing Structured Query Language (SQL) query on the right databases. This would allow the user to use any of these devices to authenticate to same online account from various devices.

3.4 Time-based OTP Authentication via Secure Tunnel

Time-based OTP Authentication via Secure Tunnel (TOAST) is a Smartphone app that obtains its secret seed from the server through a secure tunnel- TLS/SSL, stores this seed value on the Smartphone using a password protected keystroke, and then uses the seed to generate all time one time unique codes. Mainly three entities are involved in TOAST: a client who wants to login to the service, a server that listens for authentication requests, and a Smartphone with this app installed that possess by the client[2].Firstly the client or user has to register on the website of the service and then tends to download and install the Smartphone app. Then a secret seed will be generated by the server and shared with the client through secure TLS tunnel. This seed is stored on the mobile and will generate unique one time code offline every time the user wants to login. Whenever a user wants to access the service, the client may begin logging onto the account using his/her username, password and six-digit code generated by the phone. It uses the existing cryptographic standards and web protocols to increase the time and effort needed to crack a given system. It makes use of Blowfish algorithm for encryption or decryption and SHA-1 for generating one-time codes from a number of random keys.

Main advantages of TOAST authentication system are that it works offline for OTP generation i.e. can even work without network coverage. Secondly, the seed is not exposed in the plaintext form during enrolment which means the secret seed is generated at the server end and is transmitted over the network through TLS/SSL secure tunnel [2]. Lastly, the seed is stored inside the phone once transmitted and it is too stored in encrypted form and is password-protected using UBER Keystroke. Once the TOAST starts generating OTPs, it is self-reliant and will continue to operate reliably independent even of network conditions. But it also has some drawbacks or vulnerabilities that include no secure initial authentication setup during the transfer of secret seed.

3.5 Generation of secure One Time Password based on Image Authentication

The Image-based Authentication (IBA) is based on Recognition Technique. It is almost similar to text one time passwords as in this also the user is provided a shared secret as an evidence of his/her identity. However, text-based OTPs use alphanumeric characters to represent the secret and IBA uses visual information. When the user registers for the first time on the website, they are required to select a set of images that are easy to remember such as natural scenery, automobiles etc [8]. Every time a user login into the website or service, they are provided a grid of images randomly generated. Then, the user can identify the images previously selected by them. The user is authenticated by correctly identifying the password images. The category of images is stored by the authentication system on Image Identification Set (IIS). When a user login, the IIS for that user is only retrieved and is being used to authenticate that particular user. The human is more adept in retrieving or recalling a previously seen image rather than a previously seen text. In a study conducted at University of California at Berkeley, Image-based authentication (IBA) systems have been found as more user-friendly than usually used text-password systems.

Main advantage of IBA is that it is more secure and requires less memory. Image-based authentication also prevents from social engineering attacks, as it is easier to verbally describe the text password to the attacker but rather in case of image passwords nobody can reveal practically describe the passwords. Although graphical passwords may be shared via taking photos, taking screen shots or even through drawing but it obviously require more time than text passwords. Also, idea of using images as one time passwords makes it difficult for the attacker to intrude using Brute Force attack.[8] But this also facilitates to data manipulation and interpretation to a greater extent than the alphanumeric characters does. This complexity, however, makes IBA harder to implement and deploy, requiring environments with increased computational power and graphical capabilities. This prevents it to be used by most of the services of websites because of complexity.

Hotspots: The major drawback in case of security in Image-based authentication is Hotspots. Hotspots are the specific areas in an image that have a higher probability of being selected by most of the users as a part of their passwords. If any attacker can accurately predict the hotspots in that image, a dictionary of images can be built basis on these hotspots. Thus, hotspots are meant to be problematic in Image-based authentication.[8]

4. DISCUSSIONS

We now discuss some findings that are explored by the study and highlighted items for further references.

Adoption: Multi-step or Multi-factor authentication technologies are adopted at different rates, depending upon their context, complexity and motivation. Mostly, in the work environments, the verification codes generated by security tokens are popular way of adopting multifactor authentication. In personal context or financial transactions, one time passwords received via SMS or email is generally popular [10]. The adoptability rate of Smartphone applications is little as a reason of complexity in their implementation.

Usability: Today, in the world of internet everybody is trying to harden the security of their data and every web service is trying in order to provide extra layer of security to their users so that it becomes difficult for the attacker to breach in to the account of the user [10].

Firstly, the most popular multi-factor authentication is using SMS-based OTP authentication. It is used in financial areas mostly like in banking transaction, internet banking, Google two-step authentication via SMS, Mater or Visa Debit-Credit card transactions, online payments on E-commerce websites etc.

Google Authenticator is a Smartphone based application that generates unique codes for accounts. It is used with only Google associated accounts like Gmail accounts. Image-based authentication scheme is also now becoming popular in various web service providers like in HDFC, ICICI bank use images as one-time unique codes in their online transactions like internet banking.

Multi-factor authentication's most important use is in financial services like in online banking or internet banking etc for providing security to the users so that only the authenticate or the legitimate user can process their financial transaction. As security risks are of great concern for the servers providing these services as well as for the users [12]. In this we rely on the public key infrastructure for authentication and key generation [11]. Another way of providing authentication in financial transactions like mobile banking is through analyzing user's usage pattern to input data into mobile and pressure of finger determine whether the user using the mobile device is legitimate or not [13].

Future scope: Various OTP generating mechanism are provided with more security day by day. New ideas may be introduced to remove any remaining points of vulnerability still remaining in systems in use today. There is a need to further harden existing authentication schemes such that they are easier to use but more complex to crack.

5. CONCLUSION

In this article by reviewing the pros and cons of various available login authentication schemes, firstly we reported on already available multi-step authentication mechanisms, how they work, how they are used, where and why. A few popular multistep authentication schemes include: one time pass code or passwords received via SMS, one time codes generated by security token i.e. RSA SecurID, Smartphone applications for generating verification code like Google authenticator and TOAST, using images as verification passwords i.e. Image-based authentication. Almost every kind of authentication system discussed above is widely used today to provide security to the users. One Time Passwords are an efficient technique to generate passwords randomly each time for user. OTP prevent users from replay or eavesdropping attacks. These passwords are valid only for given timeframe thus there is no threat that they can be reused by an intruder to login to user account as they are invalid after one time use. One Time Passwords can be generated either online or offline but offline generation is better as it can also be generated even if there is no network connectivity and it also prevents from the man in the middle attack. Thus it will be better for the services or websites to use offline method of generating one time unique codes like Google Authenticator or TOAST as they provide more confidentiality and authentication to the user on internet.

6. REFERENCES

[1] Singh, S., The Code Book: The Secret History of Codes and Code-breaking. Fourth Estate, 1999.

[2] Uymatiao, Mariano Luis T., and William Emmanuel S. Yu. "Time-based OTP Authentication via Secure Tunnel(TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystroke." 4th*IEEE International Conference on Information Science and Technology(ICIST)*, 2014,Pp. 225-229,IEEE,2014.

[3] Muliner, C., Borgaonkar, R., Stewin, P.,Seifert, J., "SMS-based One-Time Passwords: Attacks and Defense", volume 7967,Pp. 150-159 Springer-Verlag Berlin Heidelberg 2013.

[4] Appelman, M., Scheelen, Y., "Analysis of Google's 2-step Authentication",University of Amsterdam, May 2012, www.scribd.com/doc/95267199/Analysis-of-Google-s-2-StepVerification#scribd

[5] Subashini, K., and Sumithra, G., "Secure multimodal mobile authentication using one time password." 2nd *International Conference on Current Trends in Engineering and Technology (ICCTET)*, 2014, pp. 151-155. IEEE, 2014.

[6] Takasuke Tsuji, Akihiro Shimizu, "A One-Time Password Authentication Method", January 2003, www.kochi-tech.ac.jp/library/ron/2002/g5/M/1055124.pdf

[7] Wikipedia-RSA SecurID, http://en.wikipedia.org/ wiki/ RSA_SecurID, 2015.

[8] Parmar,H., Nainan, N.,Thaseen, S.,"Generation of Secure One time passwords based on Image Authentication System", Pp. 195-206, 2012.© CS & IT-CSCP 2012.

[9] Kalaikavitha, E.,Gnanaselvi, J., "Secure Login using Encrypted One Time Password(OTP) and Mobile based Login Methodology", International Journal of Engineering and Science, Vol. 2, Pp. 14-17, Issue 10(2013).

[10] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, Greg Norcie, "A Comparative Usability Study of Two-Factor Authentication", Cornell University Library, 31 January 2014.

[11] Munjal N., Moona R., "Secure and Cost effective Transaction Model for Financial Services", *International Conference on Ultra Modern Telecommunications and Workshops*, 2009, Pp. 1-6, IEEE, ICUMT'09.

[12] Mohammed M.M., Elsadig M., "A multi-layer of multi factors authentication model for online banking services", *International Conference on Computer, Electrical and Electronics Engineering (ICCEEE)*, Pp 220-224, August 2013.

[13] Hojin Seo, Huy Kang Kim, "User Input Pattern-based Authentication Method to Prevent Mobile e-Financial Incidents", Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW), Pp 382-387, May 2011.