

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/332435177>

Password-Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites

Chapter · January 2019

DOI: 10.4018/978-1-5225-8100-0.ch008

CITATIONS

5

READS

8,206

2 authors:



Rahul Singh Chowhan

Jai Narain Vyas University

23 PUBLICATIONS 46 CITATIONS

SEE PROFILE



Rohit Tanwar

University of Petroleum & Energy Studies

52 PUBLICATIONS 187 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Conference Paper [View project](#)




Journal Paper [View project](#)

Chapter 8

Password–Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites

Rahul Singh Chowhan

 <https://orcid.org/0000-0001-6567-4979>
Agriculture University Jodhpur, India

Rohit Tanwar

University of Petroleum and Energy Studies, India

ABSTRACT

Over the years, passwords have been our safeguards by acting to prevent one's data from unauthorized access. With the advancement of technologies, the way we have been using passwords has changed and transformed into much more secure yet more user friendly than they were ever been in the past. However, the vulnerabilities identified and observed in this traditional system has motivated industry and researchers to find some alternate where there is no threat like stealing, hacking, and cracking of password. This chapter discusses the major developed password-less authentication techniques in detail and also puts an effort to explain the in-depth details along with the working principle of each of the technique through a use-case diagram. It would be of great benefit and contribution to the callow trying to explore research opportunities in this area.

DOI: 10.4018/978-1-5225-8100-0.ch008

Password-Less Authentication

INTRODUCTION

Over the years, passwords have been stolen, cracked and hacked. Fraudulent agencies can buy user information and credentials online on social media sites. Many cases have been seen worldwide like Facebook data leak, Yahoo Security Breach, LinkedIn Data Breach, DropBox User Accounts leak etc. Another reason could be to increase in the variety of applications and platforms that could force the user to remember more and more passwords (Cortopassi, M., Edward, E., 2013). As technology and its users keep on increasing with the demand-branding, publicity and efficiency of the application, there is an increase in secure channels to communicate and store passwords. Although, password-based login is more prevalent in today's time but because of the drastic increase in internet-connected devices and user's possessing more online accounts than ever before has made password-less authentication a more relevant alternative for secure logging-in to online accounts (Rabkin, A., 2008). It becomes difficult to memorize passwords and that would lead users to keep one password for most of the application causing them prone to hackers. This is the reason that could actively lead to an increase in security breaches and easier for hackers to capture data. This has also fostered the applications that keep a store of all user accounts and passwords associated with respective accounts that user uses locally. At this end, the password management scheme seems to be a promising and reliable factor to store tricky passwords for accessing cross-platform systems with single sign-on. The layman user thinks them as time savvy and less tedious as they keep the bulky password at one place. But the user does not understand how these applications might work behind the walls in the backend to share their sensitive information across the internet. Though, along with acceptance of terms during the installation process or registration process, the user may unknowingly allow the application to share the sensitive information (Luke, Hok-Sum H., Matthew W. T., 2015). This time the trustworthiness of a user can be tested by blindly allowing these kinds of applications to access secure accounts. The password occurrence per user stays common and relative to each other which would also cause hackers to guess passwords by using hit and try the method. This hit-and-trial method causes severe problems like gaining remote access to obtain user information stored either on a client machine or server. After facing and accepting all the challenges we are at the step of no more password breaches with a promise of more secure authentication and no password memorization at all (Chiasson, S., Elizabeth, S., Alain, F., Robert, B., Paul, C. V. O., 2012). Passwordless authentication is a critical investment on security which serves various benefits as under:

Password-Less Authentication

1. **Enhanced User Experience:** New age users need not to remember the use of puzzles and questions like “What is your first pet dog name?”, “Which was your high school?” etc. This not only reduces the signup time but also eliminates users to go through a tedious registration process for new apps. They have much interactive interface and facilities than the password-based authentication.
2. **Improved Security:** With no use of passwords we have more secure improvised security with zero passwords to remember.

Security is the main dimension of any software development application which involves various processes of authentication, verification, authorization, and integrity. The user, as well as developer of the application, could not overlook these aspects while using and developing the application. Increase in security breaches in the past decade has forced the developers to come up with more secure strategies and authentication handling mechanisms (Mahaffey, K. P., et.al. 2016). One such authentication mechanism is the use of passwordless authentication. In this authentication service, users are no more required to remember tricky passwords for different applications that they use in daily life. This type of authentication does not require passwords to login into any application. The password-less authentication has become the talk of town making passwords obsolete day by day. This new age enterprise model ensures the effortless security based on these enhanced user authentication mechanism (Fox, A., Steven, D., G., 1996). This kind of authentication showcases various options for securely logging for users.

DIFFERENT TECHNIQUES OF PASSWORD-LESS AUTHENTICATION

The working of various password-less authentication modalities are as follows:

1. **Magic Link Login Authentication:** In day-to-day life user logs in to various accounts so rather than asking users to enter passwords, just get the username to generate a transient authorization code for the session-full login. Simultaneously, this code is acknowledged to mail id for the associated username provided by the user. Later with the time-bound access of magic link user needs to click the link to verify its identity for accessing the account based services. In the back end, once the user logs in to the associated account this authorization code is then exchanged with the session key to let user access account as long the session times out (Lee, W., Simon, SH., P., Chasing, L., Jinho, K.,

Password-Less Authentication

Byeong-Soo J., 2014). This same key is stored at user device as well. The magic link authentication down the line believes that mail server is safe enough to authenticate the user's identity as the user cannot regulate the backend security at mail databases. The general flow in passwordless magic link login system may follow as:

- The user is asked to fill up the username
- On click of submitting, two API calls are used
- First to begin the verification process that generates an authentication code, this will be sent to the registered user's mail id.
- Second to compare the authentication code previously generated and another which is obtained with user's navigation from mail to app/account.
- After a successful comparison, the user is navigated to the app and the matched authentication code is exchanged with the secure session key for longer access to the account.
- The magic link is now disabled.

Figure 1. API Call 1 (for authentication key)

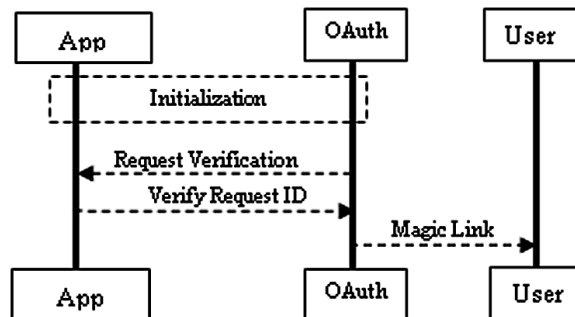
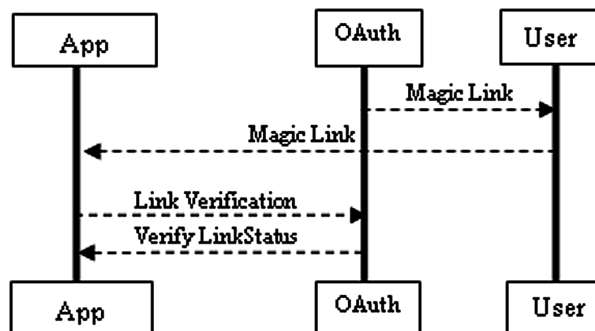


Figure 2. API Call 2 (to get authenticated)



Password-Less Authentication

Figure 3. Working: Getting magic authentication link on Email

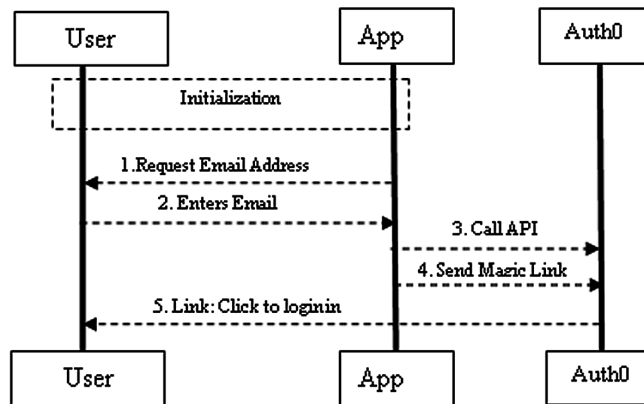
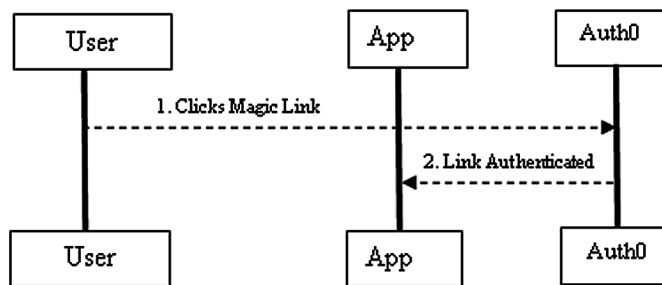


Figure 4. Working: Authenticated login to the user account



Now with this scheme of authentication has a challenge to face if mailbox or mail client of the user is compromised. This will open the access to the user account to someone using the mail id (Popp, N., David, M., Loren, H., 2011). Then with the help of a magic link, someone else might access the account as long as the validity of the link exists. However, there persist many solutions to this problem, which are as shown in Box 1.

2. **Token-Based Login (OTP Based):** The OTP is the most commonly used form of two-factor authentication for secure access of network. At cryptographic level, the multi-factor authentication differentiates this terminology into “what user has”, “what user knows” and “what user is” in terms of cryptography (Bychkov, E., 2012). The token-based mechanism works similar to magic link authentication. In this rather than using email id link the registered mobile number of the user is used to authenticate it. As well as they provide an authentication token which is solely enough to authenticate the user. Nowadays,

Password-Less Authentication*Box 1.*

Solution 1: Maintain a blacklist of the magic link that can be canceled by the app owner.

Solution 2: Forming a Revision Index, i.e. the link with the latest revision would be allowed.

Solution 3: Short span of Magic Links i.e. quick expiry say 5 minutes to login.

Solution 4: Rebuild the link in two pieces so user logging would be authenticated by the first split sent to mail and second one sent in response to the request by the user.

many organizations make use of OTP in the combination of Username & Static password. As the name is One Time Password that means it is valid for single time interaction, single session, a single transaction or single authentication. These are more secure than the user created static password mainly for two reasons (M'Raihi, D., Salah M., Mingliang P., Johan R., 2011). First, they are different and dynamic for different users that mean the brute force attacker has more guesses to break and second they are of short life span validity minimizing the risk of replay attacks. Cryptographically, they are tokens generated by a counter with a combination of token key and a current counter value which is unique and secure notion followed by server and token manager in synchronization. They can not only be used for simple user account login but also for 3D secure transactions and payment gateways, which often requires a tricky combination of alphanumeric and special characters with various validation. Like a typical 3D secure transaction would ask its user to create a password with at least two special characters, a minimum of four digits and six characters which may not include spaces and tabs (Steeves, D., J., Mwende, W., S., 2007). There is absolutely no limit to adding up a validation to not allow compromise on user information. But it becomes difficult for a layman user to remember this kind of password which may end up in a recreation of it in next login. The static passwords are more gullible to Password Guessing Probability (PGP) attack than One Time Password or One Time Code. This has become the most common password-less authentication service to protect various network devices like Firewall, Router, Switches VPN Users, etc. that enterprises prefer to use. The One Time Password is also known as Pass Code as it helps the user to get authenticated by Authentication Manager (Curry, S., M., Donald, W., Loomis, Christopher W., F., 2000). In general, an Authentication Manager is the software that generates and validates a user before allowing login securely. It matches the OTP sent to the user and the Pass Code saved with it. The steps for the general flow of token-based authentication are as follows:

- a. User visits the login page & inputs the registered phone number and submits

Password-Less Authentication

- b. A token, 4 or 6 digit PIN, is generated by the authenticator at server side which is associated with the registered number after submission
- c. On submit, Open Authorization (OAuth) will send the token to the user's mobile number.
- d. The GUI on app/site asks for that 4 or 6 digit PIN to be filled by the user.
- e. Second API call compared the previously generated PIN with the PIN entered by the user on GUI.
- f. If both PIN matches, the user is securely authenticated to access the associated account.

OTP Tokens can be generated synchronously as well as asynchronously based on which they are classified into two main categories.

3. **Certificate/Counter Based Security Token Authentication:** This type of authentication is also called as HOTP (Hash Message Authentication Code based One Time Password). It happens between the client's token and token generated by the authentication server. Regardless of Time Based Token i.e.

Figure 5. API Calling in Token Based Login

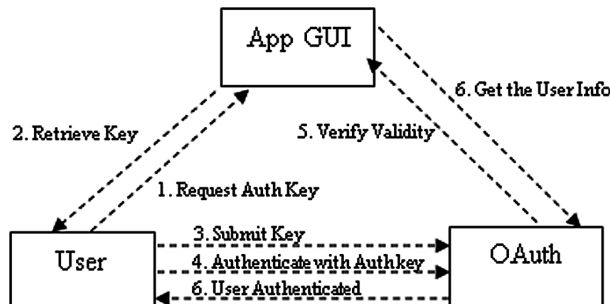
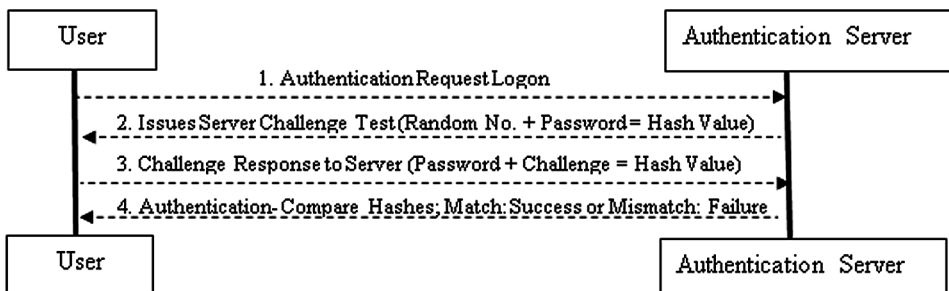


Figure 6. Working: Requesting and Obtaining Token on Registered Phone Number



Password-Less Authentication

Figure 7. New User: Authenticating new user by adding it to the connection

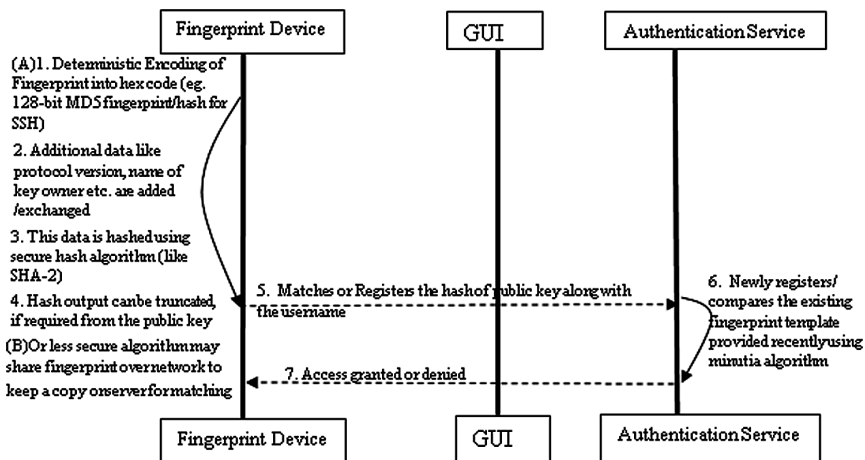
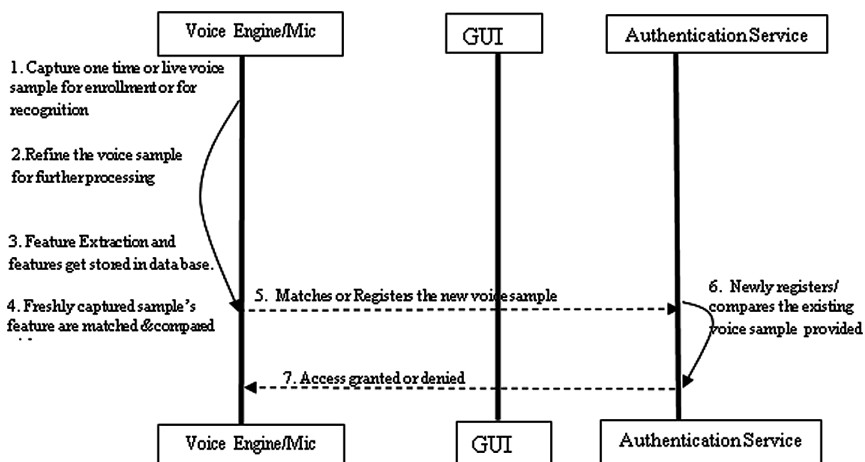


Figure 8. Registered User: Authenticating previously registered user



TOTP which changes on its own after every few seconds, this requires the user to tap on token button asking for next token in counter (Shaw, J., Richard H., Mike A., James N., et. al., 2003). In this, the server maintains the windows of token numbers so if the user taps twice or enter an expired token it will not be authenticated (Giobbi, John J., David, L., B., and Fred S. H., 2011). The major drawback of counter-based token authentication is that if the user taps multiple times on the token generator button and is not authenticated for any of them. Then it may accidentally manage to get over the window of numbers and user

Password-Less Authentication

has to start all over again by resetting the whole authentication process. The changing value of the counter called a moving factor, which gets incremented after usage. Both the parties that are getting involved in the authentication process needs to remember the last used value of the counter. In this process, the client and server may get desynchronized due to a network issue. If the client has sent the token and incremented its moving value and due to an error in connection if the server never received it, then on a comparison of counter value at the server will result into the process of manual resynchronization (Khan, M. A., Hasan, A., 2008). As there is a lack of single synchronization technique, the communication takes place in unidirectional only.

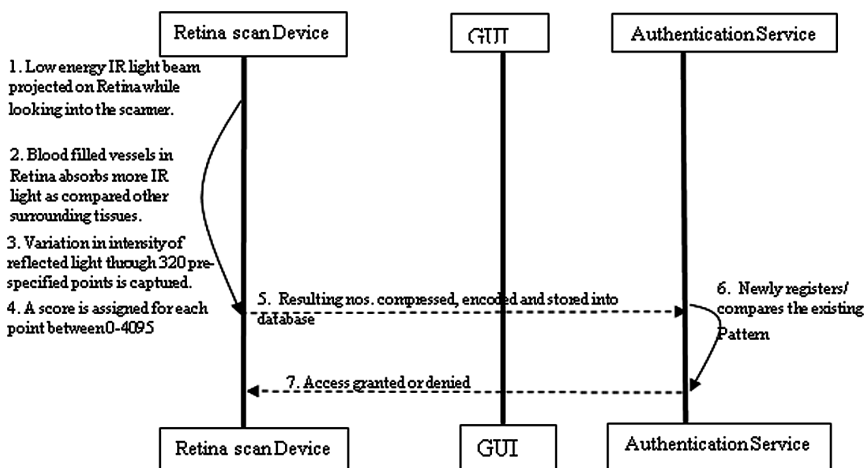
Mathematical notation of HOTP Cryptographic function:

$$HOTP(K, C) = Trunc(HMAC - SHA - 2(K, C))$$

where; K is shared key and C is counter

4. **Time-Based OTP (TOTP):** This is a transient passcode that authenticates the access of user accounts. It is temporary in nature and is generated using the current time as one of its parameters making each password unique and strong to compromise. In general, they are used with traditional login system of username/password for two-factor authentication. Even though the username

Figure 9. Server Verifying the User using HOTP



Password-Less Authentication

and password of user accounts are compromised the TOTP will unauthenticated the false access to accounts (M'Raihi, D., Mihir B., Frank H., David N., Ohad, R., 2005). There exist many ways of TOTP which include: Hardware Security Token, Mobile apps, and Text Messages. The TOTP is often 8 digits long numeric code valid for 30 or 60 seconds and changes frequently that means the brute force attacker will almost run out of time to break through new credentials every time (Conklin, A., Glenn, D., Diane, W., 2004). It is generated from a shared Private Key and the Current Time Zone using HMAC (Hash-based Message Authentication Code) so they are also called as HOTP (M'Raihi, D., Salah, M., Mingliang, P., Johan, R., 2011). There is a slight difference between HOTP and TOTP which are stated in Table 1.

Mathematical notation of TOTP Cryptographic function:

$$TOTP = HOTP(K, T)$$

$$HOTP(K, T) = Trunc(HMAC - SHA - 2(K, T));$$

where, K is shared key and T is no. of time stamps between initial courier time (T_0) and current system time

T is given as:

$$T = floor((current\ time - T_0) / X);$$

where X is time stamps (sec)

By default $T_0 = 0$ and $X = 30sec$

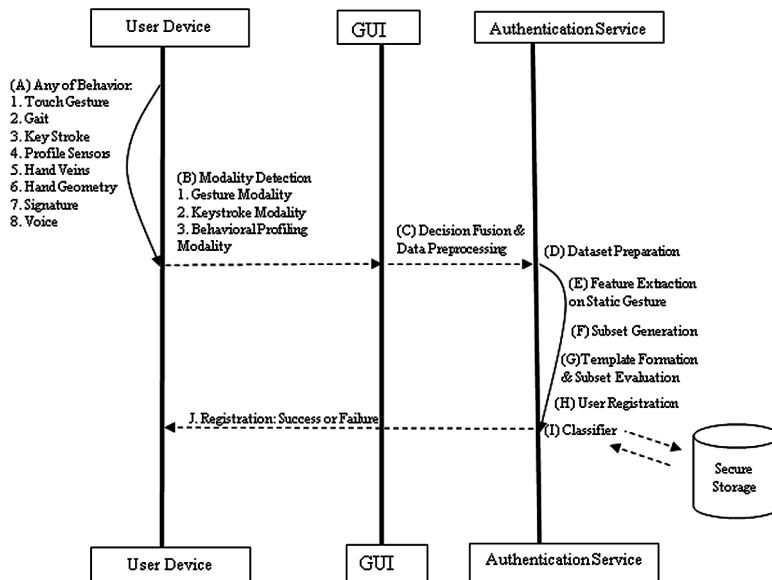
The only condition with TOTP is that the device generating TOTP must be in sync with Standard Time Zone of that area. It is generated on both ends i.e. on the server and client app so it is always available with the client allowing them to enter Zero Wait Zone eliminating the network dependency in case of OTP (Soare, C., Andrei., 2012). So in this to utilize the higher level of security the user has to be fast enough to enter the generated token before the timer times out. It is also called a combination of “something you know” i.e. Password and “Something you have” i.e. a device with TOTP. The diagram below shows the communication mechanism and authentication of the user using TOTP:

Password-Less Authentication

Table 1. Comparison of HOTP and TOTP

HOTP (HMAC Based One Time Password)	TOTP (Time-Based One Time Password)
Relies on Shared Key and Counter (moving factor), Counter values are generated based on the shared key	Relies on Share key and Counter but counter values changes with the function of time (every 30 or 60 sec)
Event-based OTP algorithm is used i.e. the moving factor is an event counter	Time-based OTP algorithm is used i.e. short-lived OTP values for enhanced security are used
The counter is subsequently incremented whenever a new OTP is generated	The counter values are incremented with a timeout of an OTP
Pass Token is valid for an unknown amount of time	Passcodes are valid only for short duration of time (can also be called as Extension of HOTP that involved time)
Requires more maintenance but no synchronization between user device and server	Requires less maintenance but high-level synchronization because of the factor of time
Published as IETF RFC 4226	Published as RFC 6238
An example can be Yubikey, Google Authenticator	Example Google Authenticator
Less Expensive as the counter is cheaper to implement for authentication purpose	More Expensive because accurate time devices are required for authentication

Figure 10. Verifying the user using TOTP authentication



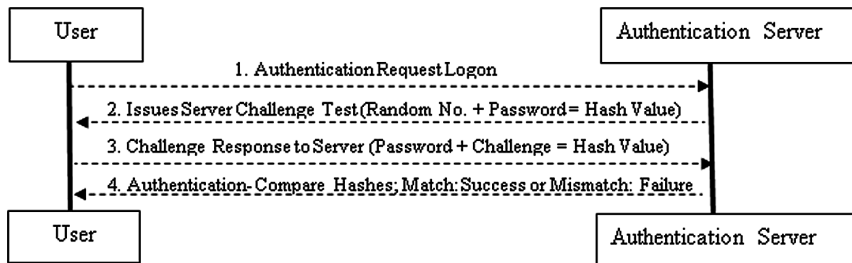
Password-Less Authentication

There exist few drawbacks with both the techniques like a major issue with HOTP is user can get locked in the self loop by multiple tapping of a token button. Another problem could be related to session validity, the authentication is valid until the user uses the token. Once it is used it will not be reused again. Whereas in the case of TOTP, the session is only authentic until the timer times out after that user needs to re-sync the whole process again. Both of the protocols suffer from the common issue of storing the shared secret key on the user's local device that makes it susceptible to attacks (Abukeshipa, A., SM., Tawfiq, SM., B., 2014).

5. **Challenge Response Authentication Mechanism (CRAM):** This is the family of protocols with characteristics of one entity sending challenges to other entity. On receiving the appropriate answer from the second entity the authenticated access is allowed. It is a way to prove the user identity over an insecure communication channel without giving any information to an eavesdropper. It is the two-step scheme for verifying the user connected in the network from HTTP that makes use of one way hash functions which makes it infeasible to find the input of function by using a generated hash. The two steps include user authentication and digest authentication. Like most smart card systems make use of CRAM which requires two entities: user smart card and password (Mizrah, L., L., 2011). Another example is the use of CAPTCHA which recognizes the auto-registration, prevent spam and determine human inputs. In cryptography, Key Agreement mechanism like CRAM-MD5, Secure Shell CRS, Zero-Knowledge Proofs based on RSA are secure CRAM. The major drawback with this scheme is sending of same challenge more than once. If the server throws the same challenges again and again then it will make the system gullible to replay attack (Rhee, K., Jin Kwak, S. K., and Dongho W., 2005). The attacker might record the hash of the previous authentication and can simply replay the hash to gain the secure access without knowing the password. The working of CRAM is shown in a diagram below:
6. **Fingerprint/Thumbprint Authentication:** Most of the app developers expect users to form a complicated combination of passwords that are unique and unguessable on first sight. Though it is need of time to having an easy yet secure authentication pass-code mechanism. This must be secure, unique, cannot be forged, and provides quicker access to app or service. One such way is using a fingerprint of the user that is easy to do as everyone possesses a smart-phone and also nothing to remember like in password-based authentication schemes (Morales, A., Travieso, C. M., Ferrer, M. A., Alonso, J., B., 2011).

Password-Less Authentication

Figure 11. Authentication using CRAM



Authentication using fingerprints is not a novice concept it has been in the market a couple of decades before in laptop, automatic suitcase and electronic doors etc. but now it has been fanned more with the prevalence of mobile gadgets. Though fingerprint scanning is a better option for identity verification and detecting duplicates but it is not secure enough for proving the authenticity of a person. In the year 2013, Apple released TouchID based fingerprint authentication for Apple iPhone users that have boomed the biometric market with similar features in Android and Samsung. For Apple users, it could be used for two purposes of unlocking the phone and authenticate app store. This form of authentication allows to user scan fingerprint by placing their finger on a mobile device. The verification process happens by analysis of special features of prints called minutiae. This is basically the lines on fingers that terminates and bifurcate by creating distances and angles (Yi, C., Dass, S. C., Jain A. K., 2005). This measurement is unique for every person and based on which a unique key pair is generated locally using a pattern matching algorithm on the user device while at the server a new user is registered that has a mapping with a unique key pair of fingerprint. A new session is initialized and the user gets authenticated to securely login to an associated account.

The fingerprint of the user is never sent over the network. In fact, when a user signs up using fingerprint authentication, a unique key pair, secret key, and the public key is generated on the user device. The user is created, the public key is assigned and the private key is saved in a key store and all this happens locally on the user device. Not only this much but fingerprints are also used biometric attendance system, a collection of forensic evidence during criminal investigations, to control access to devices like smartphone, laptops etc. The most important part of fingerprint scanning and authentication is quality control which decides the ridges, valleys and required details of minutia points on fingers accurately. There is no problem called as forgetting passwords, creating a strong combination of alphanumeric cum special characters and as well as no fear of losing them. Swipe-and-PIN was also a promising alternative for payments using e-wallets (Rassan, Iehab, AL., Shaher,

Password-Less Authentication

H. Al., 2013). These used magnetic strips to store user's personal data like credit card number and the user is asked to swipe the card and insert the associated PIN to complete the transaction. But many of security breaches with the merchants have been recorded on checkout machines in the US. This has coined more secure and new technologies like Chip-and-PIN, Chip-and-Signature, and Swipe-and-PIN.

Any key management technique involves key generation, key modification and key sharing for establishing in secure message communication over a network.

The process is shown in Fig(12).

7. Authentication Using Face Recognition (Selfie Authentication Service):

User is capable of open the camera application within the device which captures the current face in real-time. This captured face is then compared with the file stored in the device media to get the genuine access of the device. Upcoming face recognition technologies are capable of providing high-level of confidence to oversee facial variances due to age effects like wrinkles and more (Avital, A. 2017). This enables more live detection and determination of the user in case if the user is using a steady photo for insecure login. The facial recognition software tools recognize the facial data points and liveness detection for accurate authentication. Face recognition algorithms have evolved from primitive models to advanced models making use of Neural Networks, Machine Learning algorithm and many more for authentic unlocking of the device or access of account. The access control system of face authentication involves capturing devices, image processing entity and recognition algorithm (Bowyer, Kevin W., Chang, K., Flynn, P., 2006).

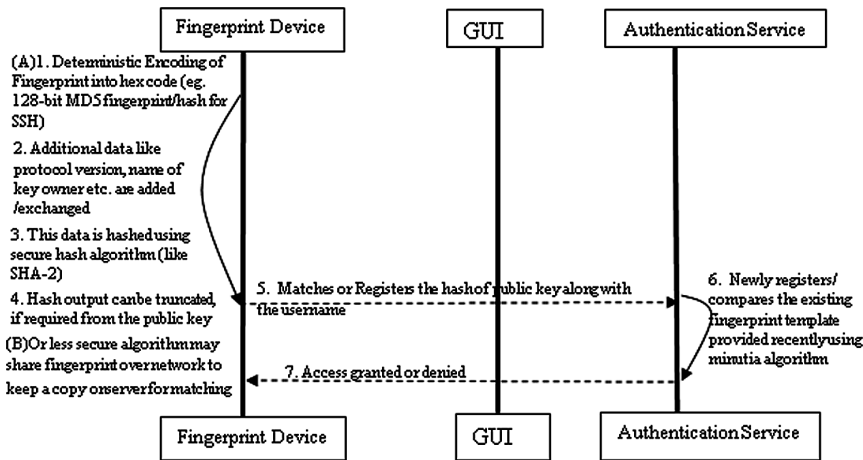
Nowadays, the high definition spatial cameras are used for surveillance at public places. They can help in tracking fugitive criminals, missing people and observing many suspicious activities without even been noticed by the subject. Thought they work differently in comparison with the authenticated facial login mechanism (Atick, Joseph, J., Griffin P., A., Redlich, A. N., 2000). Many authentication devices can configure with multiple authentication feature, this way make use of additionally added security layer for a much advanced level of user authentication.

Working Principle of Face Recognition Authentication

- a. Draw connections of data points of the face on highly accurate, secure and sophisticated machine learning algorithm to generate the biometric template of the face.
- b. Compares the newly generated biometric template with the previously stored template.
- c. Securely authenticates the match based on accuracy score.

Password-Less Authentication

Figure 12. Authentication using Thumb/Fingerprint



8. **Voice Recognition Based Login (Voiceprints):** It does the comparison of voiceprints stored on the device with the voice of a person trying to authenticate it. Due to rapid growth in the fraud cases related to the banking system wherein the victim is contacted through telephonic means, banking systems are investing more in authentication using voice. It is because of the higher accuracy being achieved in this technology day by day that most of the security-related problems are looking for a solution using voice recognition (Hunt, A. K., Thomas B. S., 1992).

Speech recognition and Speaker recognition are two subsets of voice recognition having slightly different focused domains. While speaker recognition is intended to authenticate the human using its voice features but not interested in understanding the meaning of words uttered by the person but the speech recognition does this also wherein the words are further used to command or to control something (Yuanchun, shi., Xie, Weikai., Xu, Guangyou., Shi, Runtong., et. al. 2003).

Voice Recognition is further divided into two types; recognition and identification as follows:

- a. **Recognition:** It is the term used when an unknown user raises a claim in his/her voice using some ID. The system then matches the voice prints of newly received samples with the voice prints saved in a database for that particular ID and assigns some matching score. If the score is above some threshold value then the claim is accepted and authentication is granted otherwise not. Since the comparison is done with a single database entry, this process is comparatively easy.

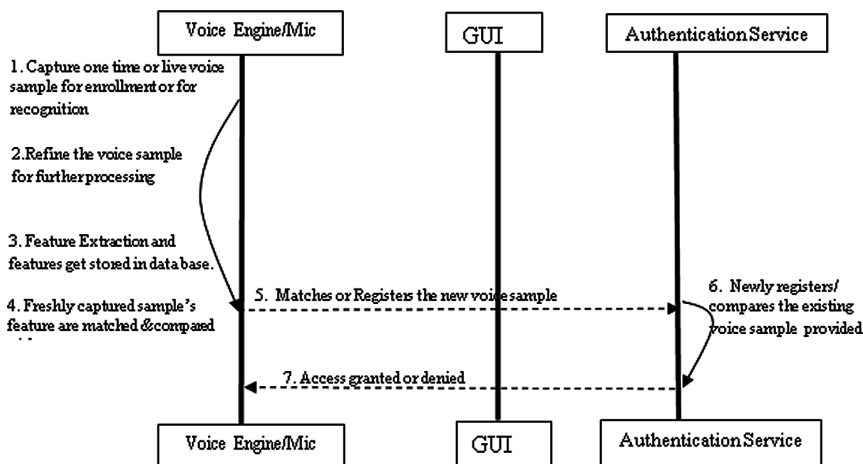
Password-Less Authentication

- b. **Identification:** It is the term used when an unknown person raises a claim in his/her voice and with no ID. The challenge is to identify the person now out of all the registered users if a successful match is there. The given voice sample's prints are matched with existing voice prints and assigned some matching scores. All the scores are then ranked. The topmost ranker's matching score is compared for threshold restrictions. If succeeded then it is authenticated otherwise not (Dimitri K., Maes S. H. 2000).

here are so many factors that affect the voice sample and hence increase challenges of the voice-based authentication system; like surrounding noise, physical and mental fitness of the speaker, accent of the speaker and so on. Because of these challenges, it is the area of interest of many of the researches these days.

9. **Retinal Scan Authentication:** The human retina that is situated in the back segment of the eye is a thin tissue made out of neural cells. In light of the unpredictable structure of the vessels that supply the retina with blood, every individual's retina is one of a kind. The system of veins in the retina is complex to the point that even indistinguishable twins don't share a comparative example (Shanley, C. W., Jachimowicz, K., Lebby, M., S., 1994). It might happen that retinal patterns got modified in few diseases like as of diabetes, glaucoma or retinal degenerative issue; the retina normally stays unaltered from birth until death. Retina-scan innovation first launched in the 1980s is outstanding however most likely it has gain very low popularity of all the biometric advancements.

Figure 13. Authentication using Voice



Password-Less Authentication

Moreover, the retina-examine technique is still in a model improvement stage and still financially inaccessible.

Retinal Scan technology depends on the vein design in the retina of the eye. The rule behind the innovation is that the veins at the retina give a one of a kind example, which might be utilized as a non-alterable identifier. Since infrared waves are assimilated quicker by veins in the retina than by encompassing tissue, it is utilized to enlighten the eye retina. Investigation of the upgraded retinal vein picture at that point happens to discover trademark designs. Retina-check gadgets are utilized solely for physical access applications and are normally utilized in situations that require high degrees of security, for example, abnormal state government military needs.

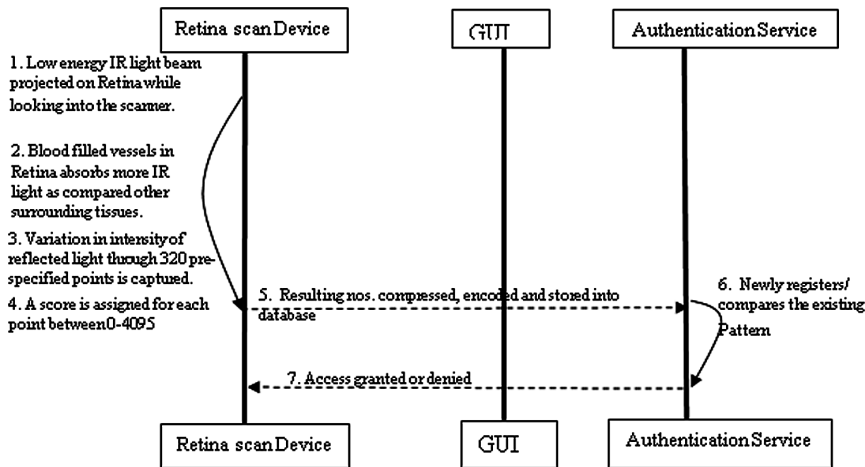
Unlike this in iris authentication technology, the identification task is completed by get-together at least one itemized pictures of the eye with a modern, high-goals advanced camera at unmistakable or infrared (IR) wavelengths, and after that utilizing a specific PC program called a matching engine to compare the subject's iris image and the pictures already stored in a database. The engine is able to compare a large number of pictures every second with a level of accuracy similar to customary fingerprinting or computerized finger scanning (Britz, D., Robert R. M., 2012).

All together for iris recognition to give precise and reliable outcomes, the subject must be inside a couple of meters of the camera. Some control systems must be executed to guarantee that the caught picture is a genuine face, not a fantastic photo. The encompassing lighting must not create reflections from the cornea (the gleaming external surface of the eyeball) that darken any piece of the iris. The subject must stay stationary, or almost stationary, regarding the camera, and must not be antagonistic to the procedure. Certain kinds of contact focal points and glasses can darken the iris design (Nichols, T J., Thompson, D. L., 2005).

Iris scan likewise discovered across the board selection in Government's drives relating to Aadhar and UID. Aadhar is being made required by numerous associations. As Aadhaar enlistments cross the 1 billion checks, the utilization of Aadhaar for occupant verification and eKYC is relied upon to quickly spread widely in services provided by the government and private firms. The requirement for a biometric methodology that works dependably is basic for the utilization of Aadhaar, a key segment of the administration's Janardhan Aadhaar Mobile (JAM) drove activities. The iris is generally acknowledged as a more secure and dependable methodology to recognize and confirm individuals. The iris works over a more extensive populace, overall age gatherings and occupations. This verification benefit empowers an Aadhaar holder to distinguish himself/herself utilizing the picture of his iris picture. It is expected by the market experts that retina/iris scan technology market is set to grow from \$676.6 million in 2016 to \$4.1 billion by 2025. In future everything starting from your bank account to air travel ticket will get unlocked through this

Password-Less Authentication

Figure 14. Authentication using Retina



technique. However few smart-phones are coming enabled with technology at present (Bolle, R. M., Sharon L. N., et. al. 2004).

10. **Behavioral Biometric Authentication:** Behavioral biometrics is described as identifying, measuring and recording some patterns in the behavior of human and utilizing them to authenticate that human in real time or because of retrospection. Instead of concentrating on a result of an activity, it centers on how a client does the predetermined action. For example, while asking for entering username and password, it doesn't look whether they are entered correctly or not rather it notices their typing speed (slow or fast), whether the mouse was used for changing cases or with the keyboard (Banerjee, S. P., Damon L. W., 2012). Digital devices like cell phones, tablets and wearable gadgets, etc. are the prime data providing sources of behavioral biometrics. Improvement in size, connectivity, efficiency and configuration of sensors is supportive in the growth of this technology. Most of the consumer devices are equipped with advanced sensors. It is very easy to get data related to the behavior of an individual through a smartphone or similar devices having accelerometer and gyrometer (Wayman, J., Jain, A., Maltoni, D., Dario M., 2005). Advanced and smart algorithms are available now that can analyze, interpret and utilize that data to fight against fraud authentication. For additional security and preventing biometric data from mischievous attacks, it is preferred to encrypt the acquired data before storing into database. After data acquisition, few points are nominated as match points by specific software. These points are then processed by an algorithm which is responsible for converting the

Password-Less Authentication

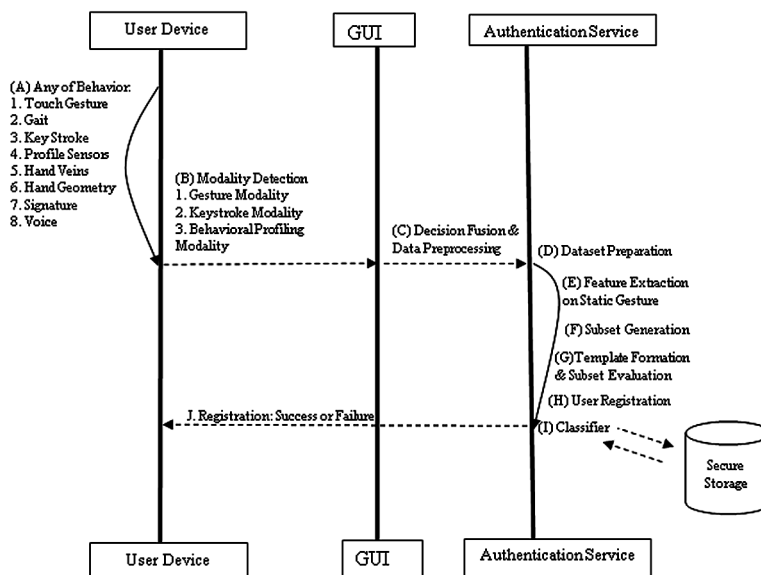
extent of matching in some numerical value. The value stored in the database is compared with the input provided by the user for biometric and then the decision of granting or denying access is taken accordingly.

The most positive fact in favor of this technology is its compatibility with the existing hardware. What it requires additionally is some specific software only. Because of this, the technique is cheaper and easy to deploy. The market is already in transition from traditional biometric system to behavioral biometrics. The leading market analyst Technavio expect that the annual growth rate of the behavioral biometric market will be 17.34% in the duration of 2016 to 2020. With the rise in deploying services on an online platform, the high demand for tamper-proof authentication technology is getting voice raised (Yuxin, M., Wong, D. S., Schlegel, R., 2012). It is the time now when moving from traditional authentication approaches like physical signatures to PIN and then to fingerprint recognition recently, behavioral biometrics seems to become as next popular part of our digital life in future.

CONCLUSION AND FUTURE SCOPE

This has increased the number of possibilities with new vendors to come up with a more secure and less tedious single point authentication solution for future customers.

Figure 15. Authentication using Behavior Biometrics



Password-Less Authentication

They can right away reach to sort out customer problems with their voice, face or the way they interact with their authentic devices. They may also be provided with multiple modalities like two-factor biometric authentications without any direct PINs and password sharing. These various credential free authentications without any interrogations and having to prove who they are, allow customers to be choice-free from the side of service providers. Due to its vast benefits, the market for face authentication, iris authentication, Voice authentication and etc. is expected to have a huge growth by 2021.

REFERENCES

- Abukeshipa & Barhoom. (2014). *Implementing and Comprising of OTP Techniques (TOTP, HOTP, CROTP) to Prevent Replay Attack in RADIUS Protocol*. Academic Press.
- Atick, J. J., Griffin, P. A., & Norman Redlich, A. (2000). *Continuous video monitoring using face recognition for access control*. U.S. Patent 6,111,517.
- Avital, A. (2017). *Authentication using facial recognition*. U.S. Patent 9,547,763.
- Banerjee, S. P., & Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research*, 7(1), 116–139. doi:10.13176/11.427
- Bolle, R. M., Nunes, S. L., Pankanti, S., Ratha, N. K., Smith, B. A., & Zimmerman, T. G. (2004). *Method for biometric-based authentication in wireless communication for access control*. U.S. Patent 6,819,219.
- Bowyer, K. W., Chang, K., & Flynn, P. (2006). A survey of approaches and challenges in 3D and multi-modal 3D+ 2D face recognition. *Computer Vision and Image Understanding*, 101(1), 1–15. doi:10.1016/j.cviu.2005.05.005
- Britz, D., & Miller, R. R. (2012). *Method and apparatus for eye-scan authentication using a liquid lens*. U.S. Patent 8,233,673.
- Bychkov, E. (2012). *Extended one-time password method and apparatus*. U.S. Patent 8,132, 243.
- Chen, Y., Dass, S. C., & Jain, A. K. (2005). Fingerprint quality indices for predicting authentication performance. In *International Conference on Audio-and Video-Based Biometric Person Authentication* (pp. 160-170). Springer. 10.1007/11527923_17

Password-Less Authentication

Chiasson, Stobert, Forget, Biddle, & Van Oorschot. (2012). Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing*, 9(2), 222-235.

Conklin, D., & Walz. (2004). Password-based authentication: a system perspective. In *System Sciences*. Proceedings of the 37th Annual Hawaii International Conference on, 10.

Cortopassi, M., & Endejan, E. (2013). *Method and apparatus for using pressure information for improved computer controlled handwriting recognition data entry and user authentication*. U.S. Patent 8,488,885.

Curry, S. M., Loomis, D. W., & Fox, C. W. (2000). *Method, apparatus, system, and firmware for secure transactions*. U.S. Patent 6,105,013.

Fox, A., & Gribble, S. D. (1996). Security on the move: indirect authentication using Kerberos. *Proceedings of the 2nd annual international conference on Mobile computing and networking*, 155-164. 10.1145/236387.236439

Giobbi, J. J., Brown, D. L., & Hirt, F. S. (2011). *Personal digital key differentiation for secure transactions*. U.S. Patent 7,904,718.

Hunt, A. K., & Schalk, T. B. (1992). *Simultaneous speaker-independent voice recognition and verification over a telephone network*. U.S. Patent 5,127,043.

Kanevsky, D., & Maes, S. H. (2000). *Apparatus and methods for providing repetitive enrollment in a plurality of biometric recognition systems based on an initial enrollment*. U.S. Patent 6,092,192.

Khan, M. A., & Hasan, A. (2008). Pseudo-random number based authentication to counter denial of service attacks on 802.11. Wireless and Optical Communications Networks, 2008. In *WOCN'08. 5th IFIP International Conference*. (pp. 1-5). IEEE.

Lee, Park, Lim, Kim, & Jeong. (2014). Server authentication for blocking unapproved WOW access. *2014 International Conference on Big Data and Smart Computing (BIGCOMP)*, 155-159. 10.1109/BIGCOMP.2014.6741427

Luke & Taylor. (2015). *Apparatus, method, and article for authentication, security and control of power storage devices, such as batteries*. U.S. Patent 9,182,244.

M'Raihi, Machani, Pei, & Rydell. (2011). *Top: Time-based one-time password algorithm*. No. RFC 6238.

Password-Less Authentication

M'Raihi, Machani, Pei, & Rydell. (2011). *TOTP: Time-based One-Time Password algorithm*. No. RFC 6238.

M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). *An Hmac-based One-Time Password algorithm*. No. RFC 4226.

Mahaffey, Richardson, Salomon, Croy, Walker, Buck, ... Golombek. (2016). *Multi-factor authentication and comprehensive login system for client-server networks*. U.S. Patent 9,374,369.

Meng, Y., Wong, D. S., & Schlegel, R. (2012). Touch gestures based biometric authentication scheme for touchscreen mobile phones. In *International Conference on Information Security and Cryptology* (pp. 331-350). Springer.

Mizrah, L. L. (2011). *Two-channel challenge-response authentication method in random partial shared secret recognition system*. U.S. Patent 8,006,300.

Morales, A., Travieso, C. M., Ferrer, M. A., & Alonso, J. B. (2011). Improved finger-knuckle-print authentication based on orientation enhancement. *Electronics Letters*, 47(6), 380–381. doi:10.1049/el.2011.0156

Nichols, T. J., & Thompson, D. L. (2005). *User authentication in medical device systems*. U.S. Patent 6,961,448.

Popp, M'raihi, & Hart. (2011). *One-time password*. U.S. Patent 8,087,074.

Rabkin, A. (2008). Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. *Proceedings of the 4th symposium on Usable privacy and security*, 13-23. 10.1145/1408664.1408667

Rassan & Shaher. (2013). Securing mobile cloud using fingerprint authentication. *International Journal of Network Security & Its Applications*, 5(6), 41.

Rhee, K., Kwak, J., Kim, S., & Won, D. (2005). Challenge-response based RFID authentication protocol for distributed database environment. In *International Conference on Security in Pervasive Computing* (pp. 70-84). Springer. 10.1007/978-3-540-32004-3_9

Shanley, C. W., Jachimowicz, K., & Lebby, M. S. (1994). *Remote retinal scan identifier*. U.S. Patent 5,359,669.

Shaw, Holway, Alex, Nikolai, Joyce, Hilsenrath, & Speers. (2003). *Method and system for facilitating secure transactions*. U.S. Patent Application 10/032,535.

Password-Less Authentication

Shi, Y., Xie, W., Xu, G., Shi, R., Chen, E., Mao, Y., & Liu, F. (2003). The smart classroom: Merging technologies for seamless tele-education. *IEEE Pervasive Computing*, 2(2), 47–55. doi:10.1109/MPRV.2003.1203753

Soare, C. A. (2012). Internet banking two-factor authentication using smartphones. *Journal of Mobile. Embedded and Distributed Systems*, 4(1), 12–18.

Steeves & Snyder. (2007). *Secure online transactions using a CAPTCHA image as a watermark*. U.S. Patent 7,200,576.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). *An introduction to biometric authentication systems*. In *Biometric Systems* (pp. 1–20). London: Springer.