BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Semiconductor Science and Information Devices
https://ojs.bilpublishing.com/index.php/ssid

ARTICLE

The Role of Multi-factor Authentication for Modern Day Security

Joseph Williamson Kevin Curran*

School of Computing, Engineering & Intelligent Systems, Ulster University, UK

ARTICLE INFO

Article history
Received: 26 April 2021
Accepted: 21 May 2021
Published Online: 25 May 2021

Keywords:
Multi-factor authentication
Cybersecurity
2FA

ABSTRACT

Multi-factor Authentication (MFA) often referred to as Two-factor Authentication (2FA), which is a subset of MFA, is the practice of implementing additional security methods on top of a standard username and password to help authenticate the identity of a user and increase the security of data. This chapter will investigate the problem with username and password logins, the different types of authentication, current best practice for multi-factor authentication and interpretations about how the technology will grow in the upcoming years.

1. Introduction

Multi-factor authentication (MFA) is an increasingly common security measure being implemented in online services to help validate the identity of the user wanting to access the content provided. On top of a traditional username and password MFA is an authentication method which requires the user to enter some form of additional code or data that only they possess. Current MFA methods require two or more authentication methods from a user. The authentication methods used are

- Something the user has
- Something the user knows
- Something the user is

A common example of MFA usage in an everyday activity is using an ATM machine with a bank card (something the user has) and PIN (something the user knows). Examples of something the user include various biometric data such as fingerprints or iris scans. Each variation of MFA implementations will have different strengths and weaknesses which will be covered in the next chapter. Multi-factor authentication is one of the most reliable ways to protect online accounts from attackers [1]. With MFA enabled on an account if a hacker has obtained the username and password details, they will be unable to access said account as they will not be able to receive or use the MFA data. It is therefore a quick way for a company to increase the security of their users accounts without giving the user more information to remember.

Despite the rise in usage of MFA, passwords remain the most frequently used methods of user authentication [2]. Two common problems with using only passwords for authentication are that users will create simple, easy to remember passwords and they will reuse passwords. These two factors cause various problems regarding security of user accounts as they leave themselves vulnerable to basic password cracking attacks. From analysis of common passwords, it has been found that there are ten common

**Corresponding Author:*
Kevin Curran,
School of Computing, Engineering & Intelligent Systems, Ulster University, UK;
Email: kj.curran@ulster.ac.uk

DOI: https://doi.org/10.30564/ssid.v3i1.3152

practices for creating a password. These patterns are Appending, Prefixing, Inserting, Repeating, Sequencing, Replacing, Reversing, Capitalizing, Special-format and Mixed patterns [3]. By knowing this one of the most common password cracking techniques used by attackers is a dictionary attack. This method in its most basic sense attempts using every word in the dictionary as a password. However more complicated attacks will use a pattern-based dictionary attack. These attacks consist of using the same dictionary words ran through functions to alter them, so they also test against variations of the words using the ten common practices for creating a password. Although the performance of a pattern-based dictionary attack is much slower than a simple dictionary attacks the upside is that a much greater number of passwords can be cracked using this method [3].

Table 1. Number of possible passwords per character in password using all letters (upper and lower case), digits and symbols (including space) on a keyboard

Number of Characters used	Number of password combinations
1	69 (69^1)
2	4761 (69^2)
3	328509 (69^3)
4	22667121 (69^4)
5	1564031349 (69^5)
6	107918163081 (69^6)
7	7446353252589 (69^7)
8	513798374428641 (69^8)

One of the most well know methods for password cracking is a brute force attack. A standard brute force attack simply tries every combination of characters starting from single letters until the correct password is found. Often when a machine is compromised by a brute force attack it will join a botnet, which is a network of infected machines that are all controlled in a group. This allows for a single person often called the "bot master" to control all the devices in the network to carry out distributed attacks. Similarly, to dictionary attacks there are various methods of brute force attacks which differ in complexity. There is the standard botnet attack of trying all possible character combinations. Letter frequency analysis which uses letters based on the frequency they occur in words. Markov model which represents the probability of two letters appearing beside each other in a string. Finally, there is targeted brute force attacks which uses both letter frequency analysis and the Markov model and apply other outside logic [4].The danger with a brute force attack is that assuming it is given the right character set and unlimited time it will be able to crack the password. Although brute force attacks can guarantee a 100% success rate, it is extremely inefficient as for every extra character added to a strong password the time it would take for it to crack it grows exponentially, this can be seen in Table 1 which shows how for each additional character added to a password the number of combinations grows exponentially and therefore the time to crack also increases at the same rate.

Another common password cracking method used by attackers is through rainbow tables. Rainbow tables are a representation of plaintext passwords and their hash values [5]. They work checking if the hash value from the table matches any of the final hash values. If it does, it begins by entering the plain text values for that hash, if the hash produced by entering the plain text value matches then the plain text password has been found, if it fails it reduces the hash to a new plain text value and tries again. This process repeats until a successful password is found. Figure 1 visualises this process in the form of a block diagram. Rainbow tables are much faster than brute-force attacks as the values are already stored. The trade-off for this is that a large amount of disk space is required [6].

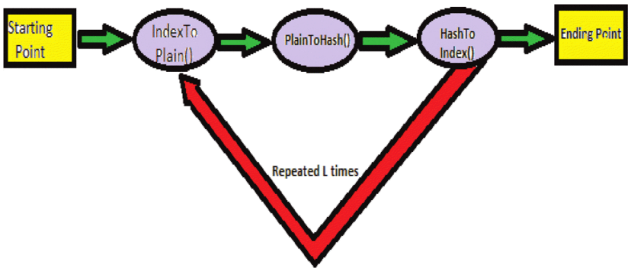

Figure 1. A Block Diagram of a Rainbow Table [6]

These password cracking methods and others are part of the problem with only using password authentication for online services. A computer cannot tell if a password has been cracked using any of the aforementioned methods. They will simply allow access to any user who enters a correct password. By using multi-factor authentication alongside a username and password the system can validate the legitimacy of the user's identity (if the users MFA methods have not been compromised) and avoid some of the flaws of only using passwords for authentication. With the issues in simple username and password systems explored and how MFA can help cover their flaws a deep dive on MFA itself can be undertaken. The following sections of this report will explore the different types of MFA

DOI: https://doi.org/10.30564/ssid.v3i1.3152

used today and the positives and negatives of each type, the best practice for implementing MFA into services, current security issues with MFA and its adoption, future developments and a conclusion of the topics discussed throughout the report.

2. Types of Authentication

Multi-factor authentication can be broken down into three main types. They are knowledge factors, possession factors and inherent factors. It is the combination of two or more of these features together that gives multi-factor authentication its strength, with each additional factor used the identity of the user should verify the integrity and identity of the user. In this section these different factors will be analysed individually based on their rigidity and real-world examples will be considered.

2.1 Knowledge Factors

Starting with knowledge factors (these are things that only the user should know), popular methods for authentication via knowledge include passwords, PINs and questions. Passwords as already mentioned have various problems, there is large amounts of different cracking methods available, users reuse passwords so when compromised on one service hackers will often try the same password on other services, many passwords are not complex enough and when passwords are complex users often write them down or save them in files. Use of a password manager can help avoid some of these issues. A password manager automatically creates strong passwords and auto fills them for a user. This means all a user must do is remember one master password and the rest are automatically created by the password manager service. However, if the user creates a weak master password and it is cracked it can lead to access of all the users accounts and login details.

PINs or personal identification numbers are most commonly used in card transactions or to unlock mobile phones/tablets. A pin should be four to twelve digits in length, but it is recommended that they should be no more than six digits in length [7]. In general, a PIN is used in the same way as a password it is entered into a system and compared with a reference PIN and if they have the same value, it will be accepted. In the same way PINs used for different applications should be different since if you use the same PIN across multiple platforms, they are only as secure as the weakest one [8]. The advantage of a PIN is that they're shorter and therefore easier for people to remember. In a standard 4-digit PIN there is 10000 (10^4) possible different combinations. This makes the use of a PIN less than ideal for online activity as it could easily be cracked by a brute force attack, but for physical use such as with ATM machines or mobile phones a PIN is usually secure enough to stop attacks as when the PIN is entered incorrectly a certain number of times a mobile device will lock out for a period of time or the card will get shredded by the ATM machine. The nature of PINs used in these examples makes them part of multi-factor authentication as an attacker will require both the bank card or phone and the PIN number to access the information [8].

Questions, also known as security questions, are a method of authentication where the user is required to answer one or more questions about themselves and these answers are then stored by the service. The next time the user wants to access the service they will be prompted to answer on or more of their questions correctly to authenticate themselves. Good security questions should meet the following criteria [9].

- The question should be appropriate for many people
- The answer should be easy to remember
- There should only be one right answer
- The answer should be difficult to guess

Despite these guidelines for creating good security questions two problems with them are that users will forget their answers and also answers can be guessed. Findings show that users forget 16% of their answers in half a year and acquaintances to users could guess 17% of their answers [10]. People are also sharing more than ever online through social media and many common answers for security questions can be found through a quick search, so the answers become public knowledge. Questions to fit large quantities of people also cause problems as common answers will occur see Figure 2 for some example questions, in the case of "What was the name of your first pet?" a search of common pet names can be done and names from the returned lists can be tried. Just like with passwords and PINs it is important that only a limited number of attempts at answering these questions can be made so that situations like this can be limited.

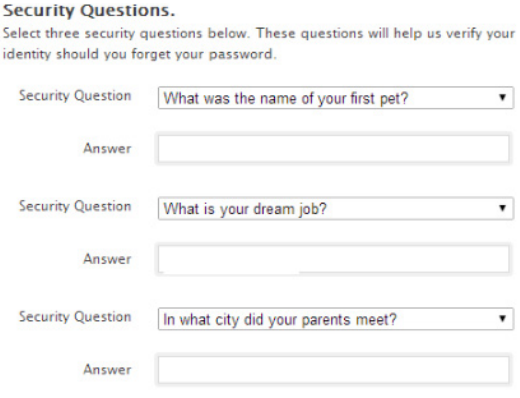

Figure 2. Apple ID security questions [11]

DOI: https://doi.org/10.30564/ssid.v3i1.3152

From analysing these three different knowledge factors a pattern can be noticed, as extra security is added to increase the difficulty for hackers, the difficulty for a user to remember the data also increases.

2.2 Possession Factors

A possession factor can be defined as something only the user has, popular authentication methods via possession tokens including connected, disconnected and contactless. The main advantage of these tokens is that the only thing the user needs to remember to have the token when they need to authorise themselves.

A connected token usually comes in one of two forms, a smart card or a USB key. A smart card is a normal card with an integrated circuit. Smart cards perform authentication by interacting through a smart card read that allows the circuit in the card to interact with the device. An example of a smart card is a bank card in this case for authentication to be completed the additional measure of a PIN code is needed. A USB key is simply a USB device that when plugged into a device via a USB port authenticates any connected services. Yubico is an example of a USB key. It adheres to Fast Identity Online stands and is used by 9 of the top 10 internet companies [12]. Their USB keys require that you press a small button located on the key, which can be seen in Figure 3, while it is plugged in to authenticate your access.

Figure 3. Yubikey 5 USB key

Like connected tokens, disconnected tokens also usually come in two different forms, a key fob (see Figure 4) or a soft token. In each case the token generates a code that the user must enter on the service they are using to confirm their identity. The authentication code is generated using a Time-based One Time Password (TOTP) algorithm which uses a key and the current time to create the unique code [13]. Software tokens much more common in today's age as many can be accessed through mobile applications such as Symantec VIP or Google Authenticator.

Figure 4. RSA SecurID 700 Authenticator

Another example of a disconnected token is SMS authentication, this simply works by receiving the code on a phone through a text message and then entering said code to authenticate the user's identity. This possession factor authentication, although beneficial over no authentication, has become arguably a method of attack for hackers wanting to access accounts rather than a secure authentication method [14]. The attack method to gain SMS authentication codes is called SIM swapping. It involves the attacker getting the individuals phone number and convincing a phone shop staff member to port the number to a burner phone or SIM card [16]. They attempt to reset the password for the user's account and "verify" their identity through the authenticator code sent to the burner phone.

Contactless authentication allows the user to authenticate their identity using a device they possess that does not need to contact a reader but just needs to be in close proximity. Two common technologies involved in contactless authentication are Radio-frequency Identification (RFID) and Near Field Communication (NFC), NFC being based off RFID technology standards. An example of RFID in use is through ID cards or badges. In this scenario the card is usually used to allow access to a room or building, the user holds the card up to the reader, see Figure 5, and if they have the correct access level the door will open allowing them to enter.

Figure 5. A wireless RFID reader

A common use of NFC authentication is to make contactless payments using a mobile device, to do this the device must be able to transmit data through NFC and also have a supporting app that enables payments to be completed for example Apple Pay, Google Pay or other mobile banking apps. Then the user holds their device close to the reader and it authenticates a payment. NFC differs from RFID in that it can provide two-way data transfer. NFC can however be vulnerable to attacks; two such methods

 DOI: https://doi.org/10.30564/ssid.v3i1.3152

are eavesdropping and man-in-the-middle attacks. Eavesdropping is where the attacker makes use of an antenna to intercept the radio signals that are being transmitted [17]. A man-in-the-middle attack occurs when an attacker acts as if it is one of the legitimate parties in the NFC communication and can therefore intercept all data communicated between to two legitimate parties.

These different possession factors all make increasing the security for a user much easier as they only need to remember to carry the device they are using for authentication with them when they want to access their data. However, should the user forget or lose their authenticator they will be unable to access the accounts unless they go through a recovery process, they will then also need to replace their authenticator.

2.3 Inherent Factors

Inherent factors of authentication cover features about the user, the most widespread methods of inherent authentication use biometric methods however behavioural methods can also be used. This section will focus on various biometric methods. Biometric authentication does not require the user to bring or remember anything to authenticate themselves, they just need to interact with some form of interface. Methods for biometric authentication include fingerprint scanning, face recognition and retina scans. The most common example of each of these methods is for unlocking mobile devices.

Fingerprint authentication is the most used biometric authentication method with more than one billion smartphones shipped in 2018 containing them. This can be observed in Figure 6 which shows the percentage of phones shipping with a fingerprint scanner each year.

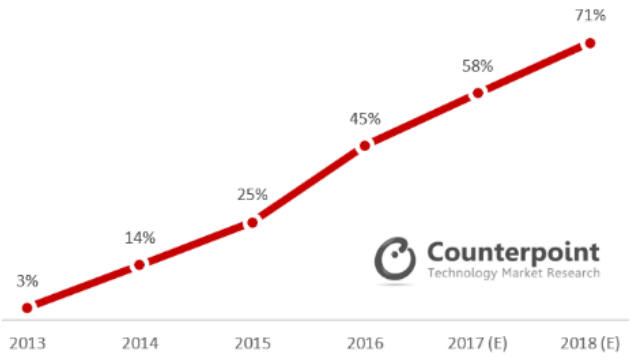

Figure 6. Global Smartphone Fingerprint Sensor Penetration

Fingerprint authentication works using the minutiae algorithm. It works by storing the ridges of fingerprints as dots in a co-ordinate system. The user sets it up by doing an initial scan of their fingerprint ensuring to press and get as many areas of the fingerprint as possible. Then when it comes to authentication the user places their registered finger on the scanner and if the ridges match up with the co-ordinate system the user will be authenticated and allowed access. The use of fingerprint scanners has high reliability compared to other biometric authentication methods. This is most likely due to the technology being much more established and that no two people have an identical fingerprint.

Face recognition works in a similar way to minutiae algorithm but instead of plotting ridges on a co-ordinate system it looks at the facial features (Figure 7), two features that are deemed particularly important are the distance between a person's eyes and the distance from a person's forehead to their chin [18]. Facial authentication can also double as a contactless authentication method as the user does not need to make physical contact for the authentication to occur, instead it is a camera that reads the users facial features and compares it to an internal database of the features it is looking for and if it is a match the authentication is verified. Facial recognition also has a high reliability with Apple saying that the chance of a stranger being able to unlock a device using their Face ID is roughly one in one million.

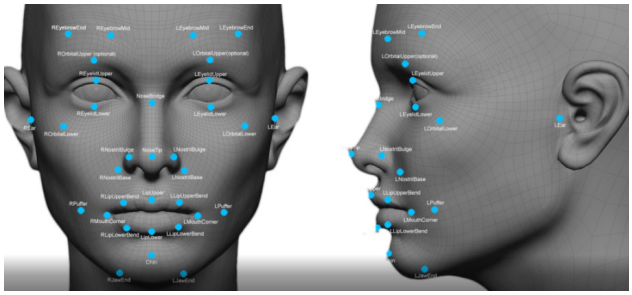

Figure 7. An example of facial features used for authentication [19]

Retina scanners are an authentication method that looks at the user's retina. The main method for authentication via retinal scans is using the blood vessel pattern in the retina, these patterns are unique for every person [20]. Like facial recognition authentication this method can also be considered a contactless authentication method as the user has their eye scanned by a camera and the blood vessel patterns are matched to those stored in the system database. The initial image scanned by the retinal scanners is broken down in various stages to make the matching of the patterns faster. This breakdown can be seen in Figure 8.

DOI: https://doi.org/10.30564/ssid.v3i1.3152

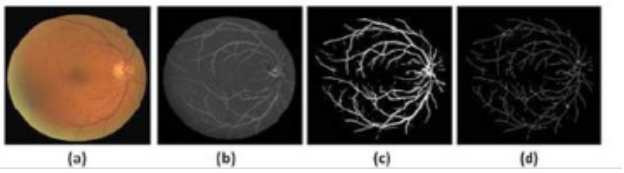

Figure 8. Breakdown of a retina scan. a) Original retina image. b) Enhanced image. c) Segmented blood vessels. d) Thinned blood vessels. (Mazumdar, J., 2018)

Inherent factors although strong methods of authentication are not without their complications. With many people worrying about how the data they put online are being used, this concern only increases with the collection of biometric data. A common issue that users of biometric authentication can also face is that if the scanner is dirty, or in the case of fingerprint scanners the user's finger is wet or dirty, the scanners can give a false rejection of authentication. In most cases if this happens a certain number of times the system will lock a legitimate user out.

3. Best Practice

With the various authentication methods investigated in the previous section it is important to consider what the current best practice for using multi-factor authentication is. For service providers the first step in providing best practice is to implement multi-factor authentication in any form. Despite some of the security issues with various types of MFA using it in conjunction with a username and password will significantly increase the validity of a user login and make it much harder for attackers to gain access.

For service providers that already have multi-factor authentication implemented into their software applications the best practice for them should be to not make multi-factor authentication an optional feature but rather to enforce it upon its users. By leaving the responsibility of enabling multi-factor authentication down to the users companies controlling data will end up in situations where some users will never activate MFA methods for their account, this results in a situation where the company has to deal with user accounts of varying security levels. This would make it harder for the company to manage their security as it will be harder to identify potential threats to their data. Companies could however give users the option to choose which methods of MFA they want to use, by providing multiple options for users. This would allow them to use the authentication methods they are most familiar with, for example a company providing biometric authentication should probably include another form of authentication that users can use instead if they do not have the necessary equipment to authenticate via biometrics.

In many cases today services with MFA enabled only allow users to enable one additional method of authentication as well as username and password when accessing their accounts. This is known as two-factor authentication (2FA) which has become standard practice for software and services that have MFA features. However, there is no standards or guidelines that enforce the use of only two factors for authentication. Therefore, companies that care about their user's security could implement solutions that require a minimum of three or more factors to authenticate. This could lead to frustrations from users who need to confirm via all the authentication methods but for each additional authentication factor that is made mandatory it increases the difficulty for an attacker to gain unauthorised access.

Regarding the technologies used for best practice, the inherent factors will provide the most reliable method for authentication as the user does not have to remember any information or carry anything with them in order to access their data. They are also the hardest methods for attackers to crack so they are much more secure than knowledge factors and possession factors. Despite their strength inherent factors will not be suitable for every situation as users may not have the required technology to use them. If this is the case, a possession factor should be used. Out of possession factors the two most secure to use are the connected and disconnected tokens excluding SMS authentication. These methods that have the added benefit of being easy for users to set up as mobile authenticator apps are very common and can be used on a wide variety of platforms. As stated previously the best option for security is to use a combination of two or more of these inherent and possession authentication methods.

4. Future Development of MFA

As mentioned in the best practice chapter of the report, one of the main future developments will be to make multi-factor authentication more of an adopted approach to security and user identification. This could come in the form of making multi-factor authentication in one form or another a mandatory security measure when accessing certain online services that may contain a lot of private data such as email services or social media. Although many of these online services do contain the ability to activate MFA it is very much up to the user to go out of their way to use them. For example, for a user to activate MFA on a Facebook account they must navigate to their settings, go to "security and login" and then manually activate MFA for their account. It could become a standard for websites to either enforce users to use MFA for their accounts or to

 DOI: https://doi.org/10.30564/ssid.v3i1.3152

do regular reminders that their service has MFA functionality and what the benefits of using it are for the user. Also new users to such services could be prompted to activate MFA upon account creation.

Another area of future development will be in the form of inherent factors. Although authentication in biometric forms are very common with modern mobile devices the trend has not quite carried over to desktop computers. While the hardware and software technologies exist, they have thus far failed to reach the mass market of users. With a Microsoft representative stating that although fingerprint scanning is present within enterprises the main issue is that it isn't prevalent [21]. The main way this could be implemented for both companies and consumers are including the scanning technologies in newly developed laptops and desktops. This is becoming an emerging trend in the computer market with the implementation of Windows Hello for Windows powered devices and Touch ID for MacBooks. However currently on the Windows side it is limited in the number of devices that support it and only MacBooks introduced after 2018 have touch ID functionality. With the increased uptake of these features for new laptops and raised awareness of how to implement the features on existing devices using webcams and USB fingerprint readers inherent factors of authentication should rise in popularity due to their ease of use and fast authentication times.

Behavioural methods of authentication are also likely to be an increasing method of user authentication. They are a subset of inherent factors where how the user interacts with a system is used to authenticate their identity. These methods include keystroke dynamics, which is identifying a user based on how they interact with a keyboard e.g. typing speed, key press time, rhythm of typing, mouse movements and other typing behaviours. These methods of authentication allow for the user to be authenticated in a continuous manner so would not interrupt the user [22]. The issue with these methods of authentication however again follows the problems of more common biometric authentication, users do not want everything about them to be known by companies and biometrics can feel particularly invasive. Users will want to be sure about how their data are being stored, used and who will be able to have access to it. However, if they can see or be taught about the benefits of these authentication methods such as how they would be extremely hard if not impossible for an attacker to crack then it is possible that these methods of continuous authentication could be implemented into all modern software where users are required to login for access.

5. Conclusions

It is clear that despite the issues with some authentication methods, multi-factor authentication being used in one form or another is much more secure than only using a username and password. With users becoming increasingly aware of security issues and the importance of protecting their online data, their first steps in increasing the security of their accounts should be to enable multi-factor authentication.

This chapter investigated the problem with username and password logins, the different types of authentication, current best practice for multi-factor authentication and interpretations about how the technology will grow in the upcoming years.

As security becomes a more pressing concern for companies wanting to protect user data, and with governing bodies starting to regulate security standards it seems inevitable that multi-factor authentication will become standard for confirming a user's identity. The first step is for companies to implement MFA options for their users. As the technologies continue to develop and become more reliable and secure, the implementation of multi-factor authentication methods should only increase year by year allowing it to become as normal to technology users as usernames and passwords are today.

References

[1] Archana, B. S., Chandrashekar, A., Bangi, A. G., Sanjana, B. M. and Akram, S. (2017) Survey on usable and secure two-factor authentication.

[2] Bošnjak, L., Sreš, J. and Brumen, B. (2018) Brute-force and dictionary attack on hashed real-world passwords.

[3] Tatli, E. I. (2015) Cracking More Password Hashes With Patterns.

[4] Gautam, T. and Jain, A. (2015) Analysis of brute force attack using TG — Dataset.

[5] Theocharoulis, K., Papaefstathiou, I. and Manifavas C. (2010) Implementing Rainbow Tables in High-End FPGAs for Super-Fast Password Cracking.

[6] Kumar, H., Kumar, S., Joseph, R., Kumar, D., Shrinarayan Singh, S. K., Kumar, P. and Kumar H. (2013) Rainbow table to crack password using MD5 hashing algorithm.

[7] British Standards Institution. (2017) BS ISO 9564-1:2017 Financial services. Personal Identification Number (PIN) management and security. Basic principles and requirements for PINs in card-based systems. BSI Standards Limited.

[8] PayPal. (2014). Password and PIN security. Avail-

DOI: https://doi.org/10.30564/ssid.v3i1.3152

able: https://www.paypal.com/us/webapps/mpp/security/secure-passwords. Last accessed 7th November 2019.

[9] Rouse, M. (2015). knowledge-based authentication (KBA). Available: https://searchsecurity.techtarget.com/definition/knowledge-based-authentication. Last accessed 7th November 2019.

[10] Schechter, S., Brush, A.J.B. and Egelman, S. (2009) It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions.

[11] How-To Geek. (2014). Security Questions Are Insecure: How to Protect Your Accounts. Available: https://www.howtogeek.com/185354/security-questions-are-insecure-how-to-protect-your-accounts/. Last accessed 7th November 2019.

[12] FIDO Alliance. (2013). FIDO U2F Security Key. Available: https://fidoalliance.org/showcase/fido-u2f-security-key/. Last accessed 8th November 2019.

[13] Sudar, C., Arjun, S. K. and Deepthi, L. R. (2017) Time-based one-time password for Wi-Fi authentication and security.

[14] Muppidi, S. (2017) Companies Need More Than Two-Factor Authentication to Keep Users Safe. Harvard Business Review Digital Articles, 2-4.

[15] Kugler, L. (2019) The Trouble with SMS Two-Factor Authentication. Communications of the ACM, 62 (6), 14-14.

[16] Ghosh, S., Goswami, J., Kumar, A. and Majumder, A. (2015) Issues in NFC as a form of contactless communication: A comprehensive survey.

[17] Haselsteiner, E. and Breitfuß K. (2007). Security In Near Field Communication (NFC) Strengths and Weaknesses. In: Goje, Amol C., Gornale, Shivanand S. and Yannawar, Pravin L. Proceedings of the 2nd National Conference on Emerging Trends in Information Technology (eIT-2007). New Delhi: L.K. International Publishing House Pvt. Ltd. 74.

[18] Symanovich, S. (2019). How does facial recognition work? Available: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html. Last accessed 9th November 2019.

[19] Elets News Network. (2018). From July 1, authenticate Aadhaar through face recognition. Available: https://egov.eletsonline.com/2018/01/from-july-1-authenticate-aadhaar-through-face-recognition/. Last accessed 9th November 2019.

[20] Mazumdar, J. (2018). RETINA BASED BIOMETRIC AUTHENTICATION SYSTEM: A REVIEW. International Journal of Advanced Research in Computer Science. 9. 711-718. 10.26483/ijarcs.v9i1.5322.

[21] Kapko, M. and Finnegan, M. (2018). What is Windows Hello? Microsoft's biometrics security system explained. Available: https://www.computerworld.com/article/3244347/what-is-windows-hello-microsofts-biometrics-security-system-explained.html. Last accessed 11th November 2019.

[22] Dasgupta, D., Roy, A. and Nag, A. (2016) Toward the design of adaptive selection strategies for multi-factor authentication. Computers & Security, 63 85-116.

 DOI: https://doi.org/10.30564/ssid.v3i1.3152