ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 2, April 2022, pp.292-303

Proposing a security system for the VPN through design and implementation of a scheme for android and IOS mobiles based on two-factor authentication

Dr.Ahssan Ahmed Mohammed Lehmoud[1], Dr.Nawfal Turki Obeis[2], Ahmed Fakhir Mutar[3,4]
[1] Babylon Education Directorate, Iraq
[2] College of Information Technology, University of Babylon, Iraq
[3]Al-Mustaqbal University College, Iraq
[4] Babylon Education Directorate, Iraq

ABSTRACT

A virtual private network (VPN) is a network, but a virtual network means that it creates a virtual bridge between the user and the server located somewhere across the world, and this network is private because to connect the connection with it you must have an account and password. The idea of VPN arose to protect its communications from industrial espionage, because there are very easy ways to penetrate a network and steal the information circulating in it. Data transmission encryption protocols and tunneling systems are used in order to secure the transfer of information between two points back and forth, so their data is encrypted and protected. Hacking the VPN is a very dangerous thing because of the importance and privacy of the data. Therefore, special systems must be provided for the VPN to suit the network's work scenarios with high security. In our work, we proposed a private authentication system for the VPN network that provides high security with fast execution and reliability based on two factors authentications: Using the varieties of authentications method, robust VPNs screen everybody who will tries to sign in. An authentication system was designed based on a special user interface that provides an easy environment for choosing two passwords in two different stages of registration and authentication. The proposed system was implemented on Android and iOS devices. The proposed system was evaluated through experiments with 720 participants with 3600 system entry processes, then the proposed system was tested in terms of its ability to break and resistance to different types of attacks. Where it was tested by 1900 attacks at different times with participants who were randomly selected from the main sample of participants during the implementation period of 30 days through using the modern types of mobile devices.

Keywords: VPN, Security, Network, Authentication, Mobile

Corresponding Author:

Dr.Ahssan Ahmed Mohammed Lehmoud
Babylon Education Directorate
Babylon, Iraq
ahssan_ahsan@bab.epedu.gov.iq

1. Introduction

With the tremendous progress of the information revolution in its various aspects, the expansion of the work area and the generalization of the electronic network, this growth has grown more and more during times of quarantine and social distancing. Where computer networks have developed in our current world in a very large way, which is reflected in the reality of companies to provide adequate protection for their systems, including international remittance companies, energy saving companies, banks, e-marketing and advertising agencies, technical solutions companies for offices and others[1].

In order to prevent incidents of penetration, data theft and manipulation, and information security problems, it is necessary to provide protection systems for companies that deal with remote users, such as the VPN[2].

VPNs attitudes at virtual private networks with describes how to create the secure networks connections when implement public networks. VPN encrypts user internet traffic with mask user online identity, making it as very difficult for others to be track user online activity with steal user data, as an encryption is real-times[3].

VPNs mask your IP address by allowing the network to forward it through a specially configured and remotely configured server under the management of the VPN host. This is means that if user browse the Internet by VPN, a server of VPN becomes user data source[4]. This is means that user internet service providers (ISPs) with others 3rd parties can't know what a websites user visits or what a data user send or as well as receive over the internet. VPNs work such as the filters that turns every user data in a obfuscate data. Also when any party were to gain access to this data, it would be of no use[5].

VPN servers basically act as proxy servers for you on the Internet. Because demographic data comes from a server in another country, it is not possible to determine your actual location. In addition, most VPN services do not store logs of your activity, on the other hand, some service providers log your behavior, but they do not pass this information to third parties. This means that any possible history of your behavior as a user remains permanently hidden[6].

User can count on his VPN server for do single or more tasks. And a VPNs server by self should be hack protected. Here a feature of user can trust from any comprehensive VPNs solutions:

1- Encrypt user IP address: For a master jobs at the VPN is to be hiding a user IP address from his ISP with other 3rd parties. This is allow for user to be sending with receiving the information through online case and without any risk at being seen by anyone other than himself and user VPNs service provider [7].

2- Protocol encrypts: VPNs should also prevent any traces of your usage, such as a history of your browsing, history of search, or cookies, from remaining. The encryptions processes of cookies are particularly very important, that is because of it prevents 3rd parties at accessing confidential information like a personal data, financial information's also, and another contents at websites[8].

3- Disconnect: If a user VPNs connection unexpectedly drops, user secure connections will be also disconnected. A perfect VPNs can detect the unexpected stop as well as terminate pre-selected all program, reduce a possibility of data being compromised[9].

4- Two-factor authentication: In this point use the varieties of authentications methods, robust VPNs screen anyone who will trying for sign in. Like user may to be asked for input the password and then the coding will be sending to user mobile device. In this case makes more difficulty from any uninvited 3rd parties for gain accesses to user secure connections. This is what we will focus on and build our proposed system of authentication to ensure a secure connection as well as provide information security to users[10-12].

Finally, the work results explain the proposed authentication system can efficiently eliminate of attack types and provide more detectability to attackers.

The structures of our paper is systematic by follows. Section 2 investigates a related works on VPN authentications systems with security for the last three years. Section 3 provide the work at a proposed system for structure of two procedures of registration of user data and authentication of system. Section 4 provide of discussion and analysis with usability experiment for work. Ultimately, we state our concluding remarks in Section 5.

2. Related works

There are numbers of works designed with done based for provide security for VPN such as Sami, M. A. (2017), he introduces a secure communication for data of shared at communication infrastructure through communication between 2 departments. Via analysis proposed project they find that a VPN as more efficient solution at Bangladesh[13].

Zhang, J. (2018, December), they introduce a new algorithm for a self-correlation randomness detection for VPN traffic in a field at VPN protocol recognition[14].

Iqbal, M., & Riadi, I. (2019), they introduce an attempt to produce the VPN utilizing a network of OpenVPN designing at laboratory of research within Informatics University of Ahmad Dahlan. To be produce attempt gives as a positive results by perform a VPN, which proofed through a data sniffing that can't discover a password with user name sent in network[15].

Juma, M., Monem, A. A., & Shaalan, K. (2020) , they introduce for development of the hybrid system based on end user for end one as a VPN security structure realized through integrating of a IPv6, IPSec and OpenSSL to make smart secure IoT objects[16].

Uddin, M. R., Evan, N. A., Alam, M. R., & Arefin, M. T. (2021, March), they introduce a modified of the present VPNs to perform at a new of environment. They simulat of generic routing encapsulation through IPsec of VPN Tunneling based of IP v6 network. The proposed work was simulated through utilizing of GNS3 network simulator[17].

El Kirafi, M., Rahimi, I., & Both, C. (2021), they introduce of how a blueeld1 smartNIC, through NVIDIA Mellanox which DPU is developed. As how can enable a transparent and scalable of security solution advantage of IDS/IPS to be support a numerous VPNs communication[18].

3. Our Proposed Structure

We will explain the structure of our proposed scheme with the operation workflow of user authentication for a VPN system, then introduce an advanced strategy that is dynamically modifies, to comply the different security requirements as acclimate the proposed work is to several scenarios of the security levels.

In order to counter different types of attacks, we designed a scheme to provide security for VPN based on authentication with two types of passwords at different phases. It is implemented in two procedure: registration and authentication.

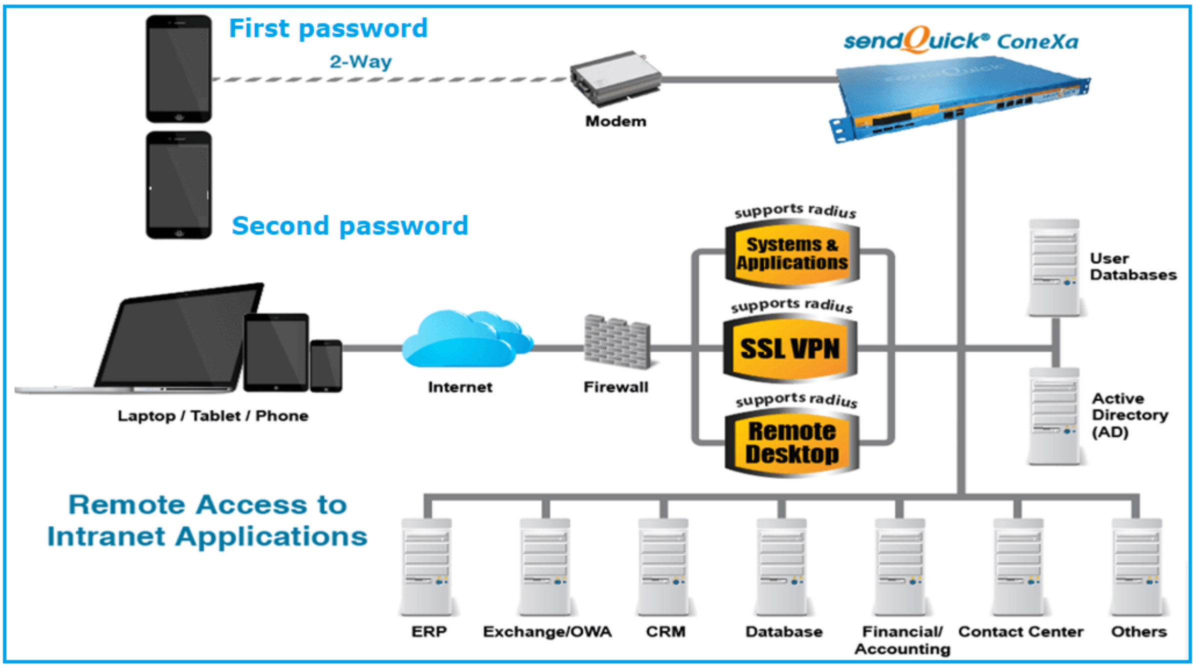

Figure 1. Illustrate two-factor authentication

3.1. Registration procedure

The red circle in the following figures introduce the actions that implement in the system, and the green circle means actions performed by user in our work.

We can summarize our work with a set of points and algorithms where the new connecter or user must register in the system. The registration procedure will show in the following figure

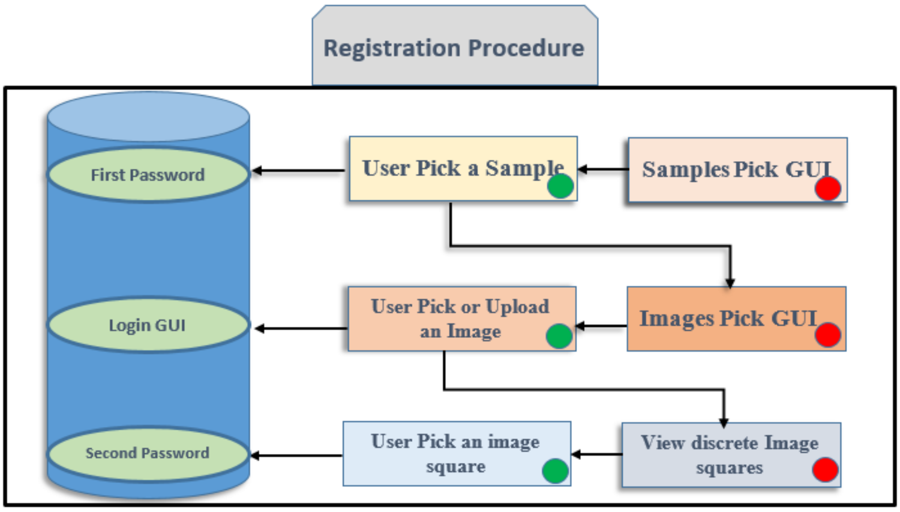

Figure 2. Illustrate the registration procedure

At the registration stage for the first time, the users will required for choose 2 password, as a 1st exercise sample password will be chosen through a special GUI for this purpose, as shown in the figure 3.

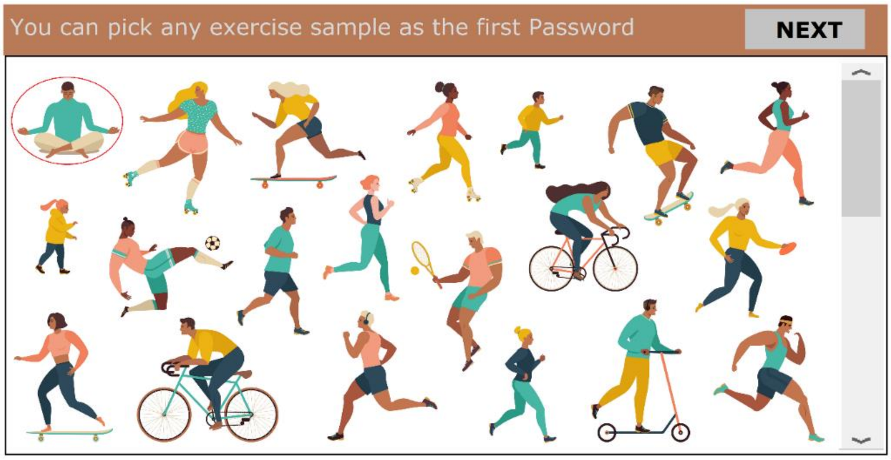

Figure 3. Screenshot of GUI for pick first password

The figure 3 is a screenshot for GUI and shows the user suppose pick a yoga exercise sample to be a first password. The user must keep in his memory the exercise sample form he chose during the registration procedure, as it is considered the most important in terms first password of achieving authentication.
After that the user will be choosing the sports fields as illustrate in the following figure based on GUI

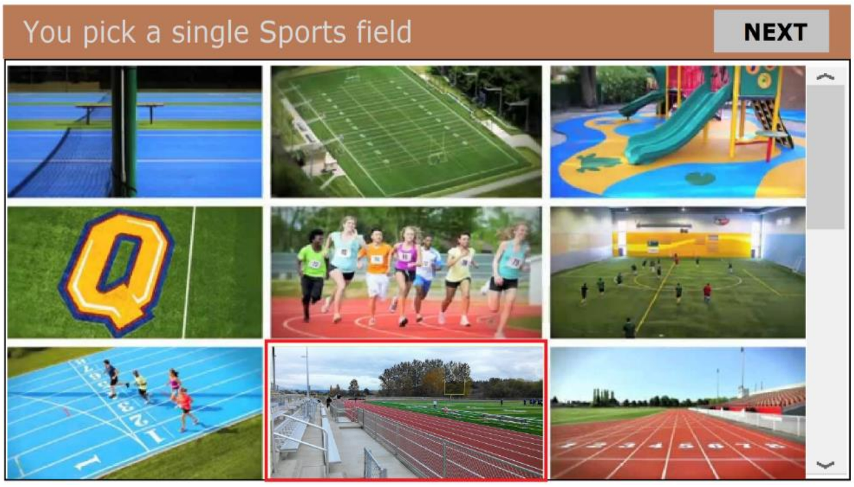

Figure 4. Choose the single sports field from database.

Then we divide the selected sports field image into a matrix with 10 * 7 cells, by pick any cell from image matrix as desired by the user to represent the second password. The following figure illustrate screenshot for GUI based for second password.

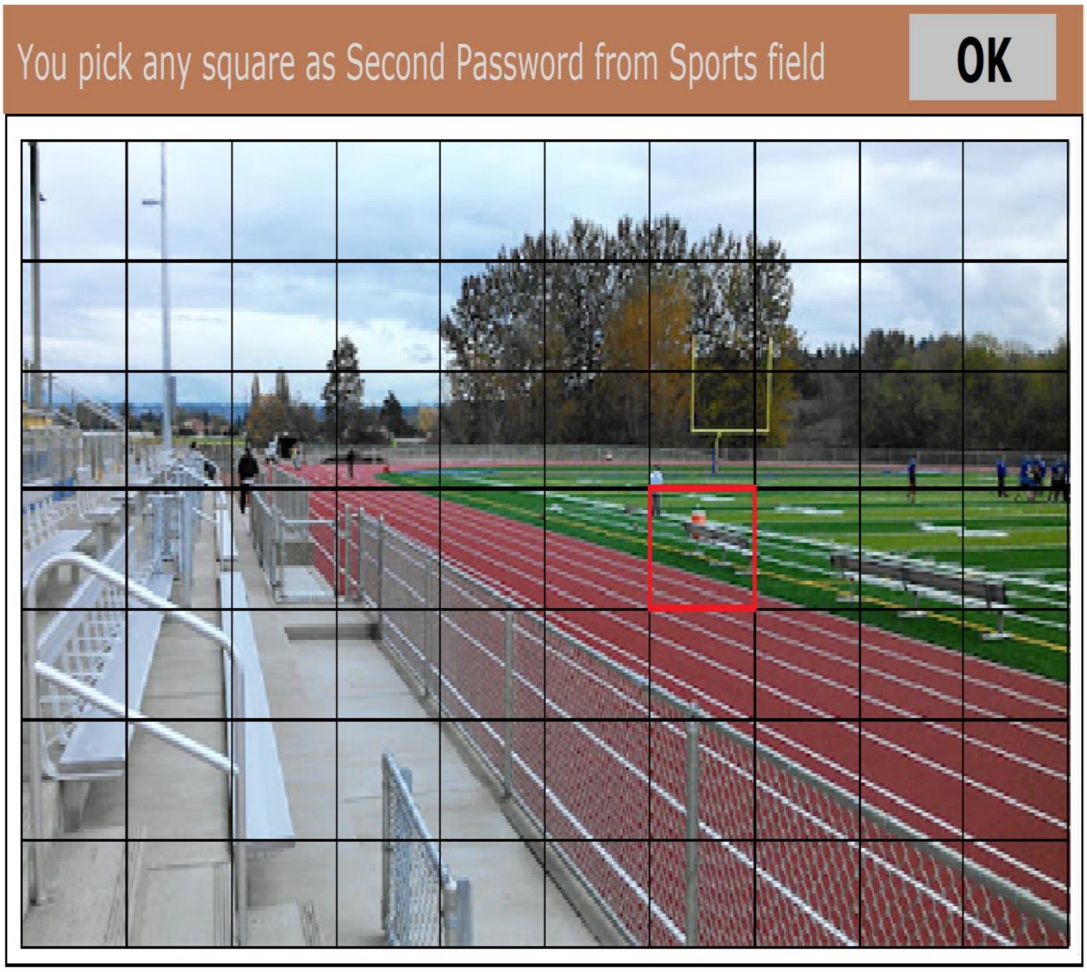

Figure 5. Illustrating a chosen of second password for sports field image

The following algorithm is explanation of the steps of the authentication procedure of our proposed work.

```
Algorithm
Input   :  The name of user implemented in registration(NoU)
           The exercise sample picked from user in registration(ESU)
           The exercise image picked from user in registration(EIU)
           The cell picked from exercise image(CEI)
Output:  Save a registration of user within system database
Step 1 If NoU not match with database table then
Step 2 Save (NoU, ESU, EIU, CEI) within system database
Step 3 Return (the registration was done in success)
Step 4 Else return (the registration was faild try again)
Step5 End- condition
```

3.2. Authentication procedure

The second procedure or user login authentication. Where the proposed system creates a user login indicator as a first step in order to comply coordinate value with the first password as a method for implicitly login. The following figure illustrate the authentication procedure.

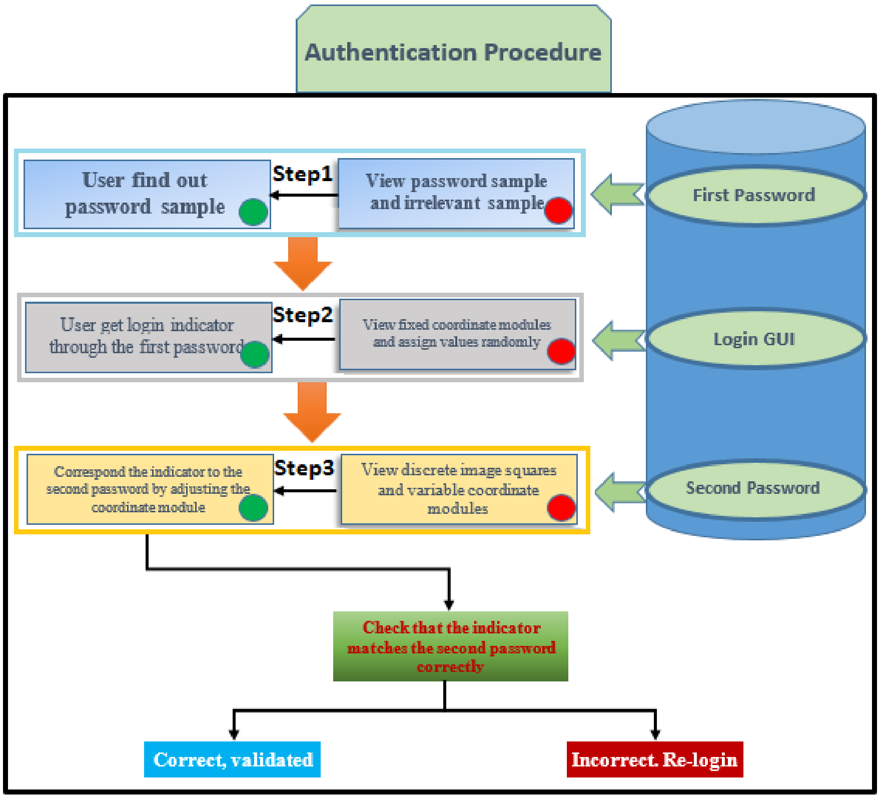
Authentication Procedure
User find out password sample
Step1
View password sample and irrelevant sample
First Password
User get login indicator through the first password
Step2
View fixed coordinate modules and assign values randomly
Login GUI
Correspond the indicator to the second password by adjusting the coordinate module
Step3
View discrete image squares and variable coordinate modules
Second Password
Check that the indicator matches the second password correctly
Correct, validated
Incorrect. Re-login

Figure 6. Illustrate the authentication procedure

Dependent in the figure 6 the red circle introduce the actions that implement in the system as well as the green circle means actions performed by user in our proposed work.

The following figure is an example of authentication of first password as shown a screenshot at set of exercise samples with selected single sample as first password that is a yoga sample. The remaining 69 samples are randomly shown by samples database, which were created and stored as a 200 unrepeated exercise samples within proposed database work

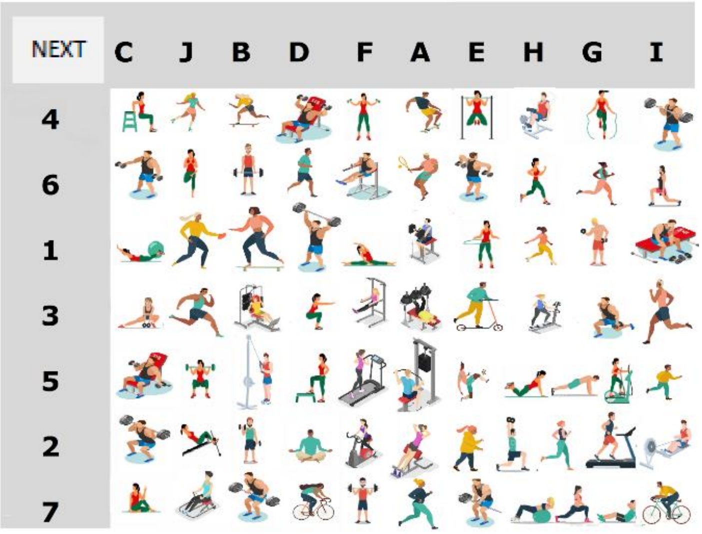

Figure 7. A GUI of passing a sign in indicator.

Consequently, by randomly generated for the samples when implement any login that cause a different of the login indicator, which is introduce in the first step at authentication procedure. Thereafter, the coordinate of x-axis with y-axis of exercise samples that were illustrate in left and top of figure 7 applied to allocate a value to any sample. A user require to be identify his x-axis / y-axis values and first password. Based on example in figure 7 a yoga exercise sample is a first password for user selected with a number 2 as the x-axis and with D letter as the y-axis. Considering at each login implemented in system will change the coordinates of x,y as well as the position of first graphical password, which ability to change a login signal randomly, which is introduce second step of authentication procedure. Means at first and second authentication steps, that a user isn't needed make any action. Therefore, different malicious attacks can’t take out the login indicator or first graphical password.

Thus, the user requires to remember the x-axis and y-axis that was selected via the sample of first graphical password when generated a current login indicator, as well as required to match it with user second password to be activate authentication with unlock the system.

The third step of authentication procedure that happen after the user presses the next button in the system GUI, which shown as new GUI at the screen triggered. The following figure illustrate the third step of authentication procedure and designed in proposed word a swappable coordinate.

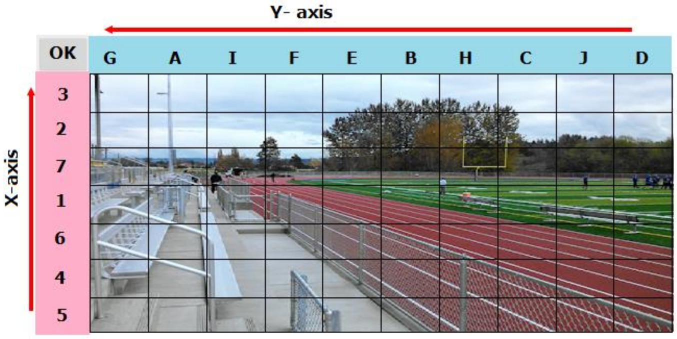

Figure 8. Illustrate an input an initial status at sign in password for sports field image.

In our work, the user has complete freedom to move and swapped between the coordinates. He can pass his fingers to swapping the coordinates from top to left or right and vice versa as well, and the divided background image remains fixed and does not move while swapping coordinates. There are ten columns (A to J) as a range of top coordinate and seven row for left coordinate (1 to 7). Thus, the cell has been specified by the user in the figure 5 is considered as a second password that has coordinates (H,1) as in the figure 8.

In the event that the user moves his fingers with two shifts on the x-axis to the up and four shifts on the y-axis to the left, he gets new coordinates (D,2) for same selected cell, as shown in the following figure.

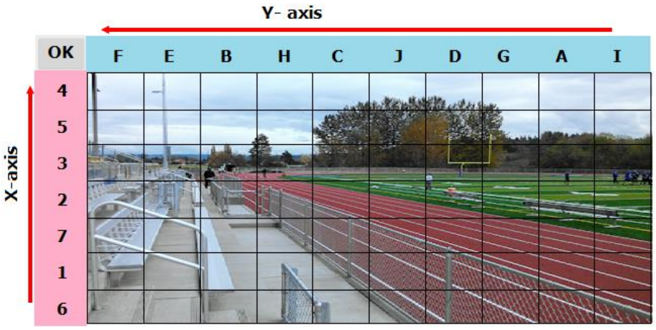

Figure 9. Illustrate the shifting of coordinates (x-axis,y-axis) by figure of user

When the coordinates (x-axis,y-axis) values of the first and second passwords are matched, the authentication procedure takes place. In the mentioned example, authentication was completed successfully based on matching the coordinates.

This is because the user has swiped the coordinates, which causes the values corresponding to each cell in the image to constantly change, and this leads to the dispersal of malicious attacks and the inability to get any scheduling idea of the first and second passwords as well as login indicator.

The fourth step at authentication procedure that the explicit user or the attacker will be deleted when he enters one of the wrongly used passwords for three consecutive times. This step is to address the problem of attempts or guesswork that is used by hacking or attacking methods by monitoring the registration screen or losing the victim's device or other methods of penetration. In the event that the authentication process fails on a real user and he has been deleted from the system due to a wrong in entering one of the passwords, he is required to re-register as a new user of the system. The following algorithm is explanation of the steps of the authentication procedure of our proposed work.

```
Algorithm
Input :The name of user (NoU)
       The cell corresponding of sing in indicator (CCSI)
       The no. for users sing in (NUS)
Call   :The names of user from DB storage (NDB)
       The cell within image from DB storage (CDB)
Output: The login process is successes or failed
Begin
  1.  If NoU = NDB then
  2.      The system will generates an indicator of login
  3.      Put NUS as 1
  4.      While
  5.          If CCSI = CDB then
  6.              Returns(Success)
  7.          ElseIf NUS that tried > three time then
  8.              Delete NDB from DB
  9.              Returns(Failed)
  10.         Else increase NUS by 1
  11.             End- condition
  12.         End- condition
  13.     Repeat until CCSI = CDB with NUS <= 3
  14. Else return(Failed)
  15. End-condition
```

4. Trial of security at proposed system

Based on the real tests of our proposed system and how it resistances to various attacks, all this will be evaluated in the following paragraphs

4.1. Trial setup

Our proposed system has been implemented and tested on mobile systems for both android and iOS, 200 exercise samples were entered for the system and 60 wallpapers were saved in the system database as a sports field's image. The system also allows easy entry of the new user's personal photos during the registration process to be stored in the databases and to help in a reminder during the authentication process.

therefore, based on attacks of smudge and attacks of shoulder surfing attack, The system avoided them by ordering all users to make a single exercise sample as a 1st password. As for the attacks of screen recording, the new users were required to make various numbers of exercises samples as 1st password to them.

A sample of 360 users who use the latest types of mobile phones were randomly selected out of 720 participants over the course of 30 days of testing.

Where the mechanism of the system's work was clarified, including registration and authentication of the participants before testing the system, and the system was trained by them. Then they were randomly divided into two groups, where the first group contains 60 attackers of the proposed system and the second is for the 300 regular users, and they were trained on their tasks assigned to them before the test.

After that, we tested the proposed system for 24 hours, monitoring and recording events, and we noticed that the attacker needs to know all exercise samples for the first of passwords, and this did not happen because the user was restricted to only three attempts.

4.2. The implementation of proposed system

1- Attacks of shoulder-surfing : After the participants were divided into two groups (attackers and regular users), they were distributed in groups of 30 sets, and each set contained 12 participants represented by 10 regular users and two participants as attackers using two types of attack, where the first type was used by cameras and the second by the naked eye. The attack was carried out with 6 attacks for each regular user (that is, each attacker has 3 attacks), to be 60 attacks on each set, and the total number of attacks is 1800 attacks on the whole system.

2- Attack of smudge: This type of attack is different from the rest attacks, as it does not depend on monitoring or observation, but rather on analysis. By analyzing the traces of the fingerprints of the regular user remaining on the screen of the device, In this case, the attacker can break the system. The system was tested according to this type of attack, where we chose 20 participants randomly from the main sample of the 300 participants and they were distributed to 10 sets, each set with two participant as a one regular user and the other as an attacker. The test was conducted and each user performed a new registration and authentication process to the system, then each attacker was given the device to perform the attack and password-defeat by 10 attempts, therefore record all the data required. In the final the total smudge attacks on the entire system was 100 attacks.

4.3. Trial results and analysis

During the 30-days period in which the tests were conducted on the proposed system with the participation of 360 users and 1900 attacks on the system, 1800 attacks of shoulder surfing and 100 attacks of smudge attack. Consequently, recorded all the required data like the time it takes for each regular user needs in the registration process for the first time, the time regular user needs to perform the authentication process, the distance traveled for the movement of the fingers in choosing the samples for the first and second password, as well as the distance traveled by the movement of the x and y axes. Interviews were conducted from the participants who played the role of the attackers, their data that they recorded during the attacking operations was reviewed. The collected results indicate that none of the mentioned attacks succeeded and did not break the proposed system.

Some of the reasons for the fail offensive at the attacks of shoulder surfing on the system will be summarizing in following

1- The time taken for registration and authentication is very short as the surveillance cameras were not able to capture every detail accurately.

2 - The attackers could not visually see the minute details of the registration and authentication processes

3 - The movement of the fingers on the screen played a major role in obscuring a lot of details during the recording, which created a blocking area for the naked eye as well as for the camera.

The analyzes of the smudge attack indicated that no attacker was able to break the system, because the remaining fingerprints at mobile screen be completely several at each sing in operation according to an attackers opinion. This is due to the fact that the locations of the first password and the login indicator alteration by random any time of users logs in. This procedure is reflected in the fingerprints at a device screen any times, therefore no fixed remaining traces left at device screen. Which leads to not obtaining any useful information for the attacker.

4.4. Usability testing

Our proposed system can be evaluated based on the following set of metrics

1- Timeout for the registration process (for a new user or a practicing user with a skill): The time taken for the registration procedure for the first time for new participants was calculated separately from the authentication time. Where the most time-out was 46 minutes and 35 seconds, and after several practices, the time decreased to nearly half, where the highest time was 25 minutes and 21 seconds. While the times of skilled participants were much less. The following figure illustrate Variation in time taken for the participants.

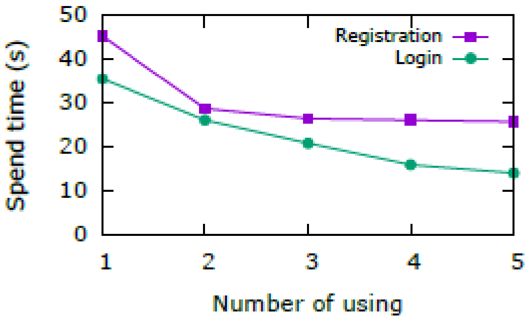

Figure 10. Timeout for registration and sign in process

2- The predilections of users for various strategies from security. The proposed work provides a soft path to be permit a user's for their system by set the security levels within different strategies via alteration the samples number. In the start we imposed on participants to implement a registration procedure. The results indicate a 60% of users chosen one sample for authentication procedure of them, while a rate reduced through a number of selection samples increase. After that we investigated a user's priorities of selecting a samples number at various strategies. The Statistics we obtained are illustrate in the following figure, which found they users consider a security is a very significant factor in the case of an authentication procedure is applied based on sensitive applications like a safe deposit box and bank system.

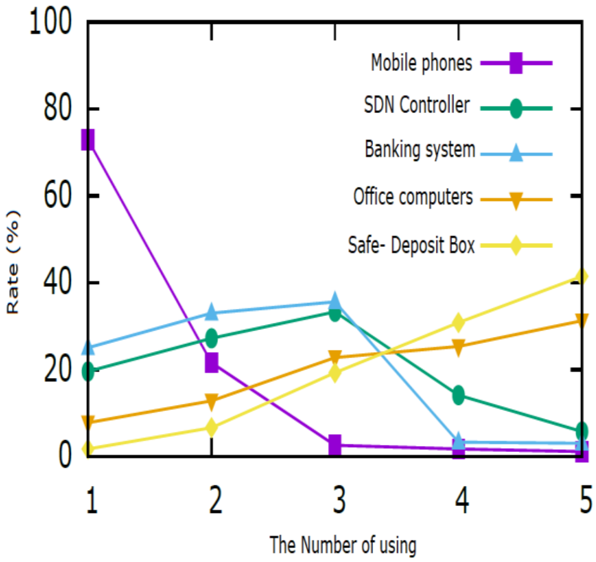

Figure 11. Illustrate the number of samples based on various strategies

3- The exercises samples number that allowed to picked for any user. Chosen direction at hotspot guessing: based on the proposed system testing, which checked user's priority of choosing exercises samples. Therefore recorded the total number of any exercise sample chosen through users. 505 from of 720 users chosen a one sample, 166 users chosen two samples, 92 users chosen three samples, 33 users chosen four samples, and 4 chosen five samples. Where is the sum of the test results?

$$Tn = 505 * 1 + 166 * 2 + 92 * 3 + 33 * 4 + 4 * 5$$
$$Tn = 505 + 332 + 276 + 132 + 20$$
Tn = 1265 samples options.

The following figure illustrate the distribution of chosen exercises samples by random ordered, which appear as relatively evenly. One sample was chosen 20 times as well as 6 samples isn't be chosen. Conformities to the test's results, we can consider that a hotspot guessing can't arrange the efficient attack because there isn't happen the characteristic sample which is chosen oftentimes morethan other samples.

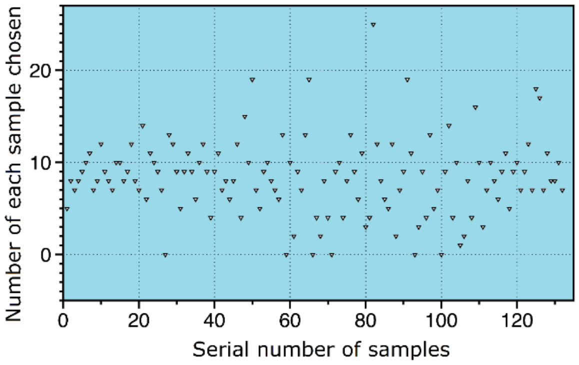

Figure 12. Illustrate the number of chosen samples

4- Our proposed system via comparisons biometric authentication systems. A proposed system as well insert user's priorities for system with several present biometric systems in several popular application strategies. In this work we chosen 5 strategies at higher security requirements. Then we calculated a rate of users chosen beneath various strategies. The following figure illustrate our proposed work has widely high opportunity to be selection in the strategies, which request higher security.

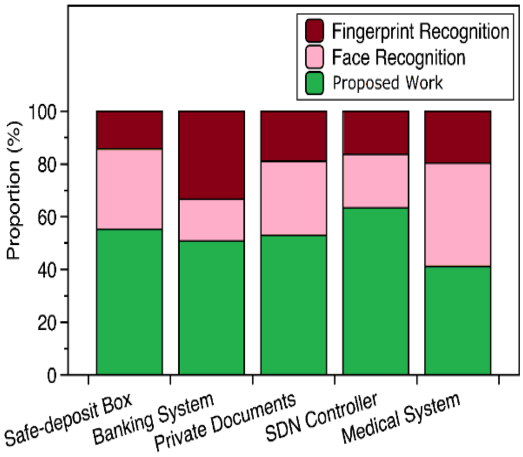

Figure 13. Illustrate a Comparison our work via biometric authentication systems.

5. Conclusions

Ultimately, a new VPN authentication system has been designed and implemented to provide strong security to users who operate on the VPN environment. The proposed system has the ability to prevent various attacks. In this work, two passwords were used based on graphical password (the exercise samples and Sports field's images) with the coordinates used. The user based on the vertical and horizontal movement of the x and y axes, which leads to converting the password content into a sign-in indicator to enter the system, which complicates the attacker's authentication guessing process. The proposed system achieved two fundamental goals, high security and rapid usability. Also, we permit a user's to upload there any graphical from his device as a samples. Therefore, we set a graphical samples presentation style at registration procedure for randomly. All of these goals to decrease a security danger imparted via chosen trend. The proposed system was implemented on the different platforms (android and iOS), as well as the system was tested to evaluate its performance in three comprehensive trials, where 720 participants were involved with 3600 logins to the system during a period of 30 days.

The results of the experiments we conducted on the proposed system indicate that the VPN environment provides a high security with ease of use. In addition, the security of our work was theoretically analyzed by us, after which we proposed a work structure that allows the user to choose a password dynamically during the registration process in the system as a step to meet the different security requirements and use it in various environments.

Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

References

[1] S. N. Xayrullaevna, K. D. Pakhritdinovna, and B. G. Anvarovna, "Digitalization of the economy during a pandemic: Accelerating the pace of development," *JCR,* vol. 7, pp. 2491-2498, 2020.

[2] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *The journal of supercomputing,* vol. 76, pp. 9493-9532, 2020.

[3] D. W. Jolley, "If You Only Knew the Power of the Dark Web! Finding Intellectual Freedom, Privacy, and Anonymity Online," 2021.

[4] S. Miller, K. Curran, and T. Lunney, "Detection of Virtual Private Network Traffic Using Machine Learning," *International Journal of Wireless Networks and Broadband Technologies (IJWNBT),* vol. 9, pp. 60-80, 2020.

[5] K. M. A. Kamal and S. Almuhammadi, "Vulnerability of Virtual Private Networks to Web Fingerprinting Attack," in *Advances in Security, Networks, and Internet of Things*, ed: Springer, 2021, pp. 147-165.

[6] N. Hassan and R. Hijazi, *Digital Privacy and Security Using Windows: A Practical Guide*: Apress, 2017.

[7] P. Papadopoulos, N. Kourtellis, and E. P. Markatos, "Exclusive: How the (synced) cookie monster breached my encrypted vpn session," in *Proceedings of the 11th European Workshop on Systems Security*, 2018, pp. 1-6.

[8] A. Reed, M. Scanlon, and N.-A. Le-Khac, "Forensic analysis of epic privacy browser on windows operating systems," in *European Conference on Cyber Warfare and Security*, 2017, pp. 341-350.

[9] S. Fisher, "How do authoritarian states react when targeted by the use of information as a foreign policy tool?: case studies of Russia and North Korea," Rutgers University-Graduate School-Newark, 2018.

[10] D. Dasgupta, A. Roy, and A. Nag, *Advances in user authentication*: Springer, 2017.

[11] J. Abbott and S. Patil, "How mandatory second factor affects the authentication user experience," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1-13.

[12] T. A. Waasalage, "WIFI Password Management with Two Factor Authentication," 2021.

[13] M. A. Sami, "DATA COMMUNICATION SECURITY AND VPN INSTALLATION: BANGLADESH PERSPECTIVES," Jahangirnagar University Dhaka, Bangladesh 28, 2017.

[14] J. Zhang, "Research on Key Technology of VPN Protocol Recognition," in *2018 IEEE International Conference of Safety Produce Informatization (IICSPI)*, 2018, pp. 161-164.

[15] M. Iqbal and I. Riadi, "Analysis of security virtual private network (VPN) using openVPN," *International Journal of Cyber-Security and Digital Forensics,* vol. 8, pp. 58-65, 2019.

[16] M. Juma, A. A. Monem, and K. Shaalan, "Hybrid end-to-end VPN security approach for smart IoT objects," *Journal of Network and Computer Applications,* vol. 158, p. 102598, 2020.

[17] M. Uddin, N. A. Evan, M. R. Alam, and M. Arefin, "Analysis of Generic Routing Encapsulation (GRE) over IP Security (IPSec) VPN Tunneling in IPv6 Network," in *International Conference on Ubiquitous Communications and Network Computing*, 2021, pp. 3-15.

[18] M. El Kirafi, I. Rahimi, and C. Both, "DPU implementation of a scalable and transparent security solution for numerous VPN connections," 2021.