Secure Two Factor Authentication Framework based on Deep Learning

Talal Eid Alanzi[1], **Dr. Mohammed Naif Alatawi**[2]

[1]Department of Information Security, Tabuk University, Tabuk, KSA

[2]Supervisor, Department of Information Security, Tabuk University, Tabuk, KSA

Abstract: ***Nowadays, many web sites make use of log in capabilities to permit users to get entry to protected information. From old days username and password has been the usual for accomplishing this. The hassle with this is that human beings generally tend to apply vulnerable password and frequently the equal password for more than one domain. Shared passwords between more than one domain, specifically vulnerable passwords, present high security risks, from this an attacker may take advantage of this to have unauthorized control for one or numerous of a user's accounts. This research intends to propose an efficient two-factor authentication for web page. The research presents drawbacks issues of two-factor web authentication based on multimodal biometric authentication.***

Keywords: authentication; biometric; two-factor authentication; unauthorized control; vulnerable passwords; Web authentication

1. Introduction

For the time being, Web has becoming the predominant interface for users to perform their own daily tasks and businesses via Internet or a private/global network. Users use their computer devices or smartphones to check and access their emails and bank accounts, perform bills payments and online shopping, retrieve personal information, etc., all these tasks are performed using a web browser. Web authentication is considered as the first defense mechanism to ensure security of web accounts and personal data.

In common, a user authenticates himself to a web page located on a remote server device, as he/she should enter his/her identity (i.e., username and password) in the logging page. Password is considered the defacto technique for authentication (Zimmermann & Gerber, 2020). However, text password as an authentication method could not give efficient protection as the method is prone to several types of attacks such as surfing attack (Binbeshr et al., 2020), password guessing attack (Han et al., 2020), MITM attack (Al-shareeda et al., 2020) and so forth. To enhance authentication and security of web pages and applications, and allow management of users' passwords, a built-in password manager was provided by web browsers (Oesch&Ruoti, 2020). However, independent password manager cannot provide efficient security defense because of insecure dynamic web environments locally and globally.

On the other hand, authentication using text passwords have been exceedingly utilized by almost all online applications and websites (Lyastani et al., 2020). However, it is popular this authentication method is insecure for different reasons such as simple text password are preferable by users due to its memorability; thus, they are vulnerable to dictionary attacks (Mohammadinodoushan et al., 2021); besides, they might be stolen by malicious attacks such keystroke logger's application (Makura et al., 2020). Phishing attack is another well-known threat to authentication using text passwords (Agaste et al., 2020), as a user might be convinced to use a phoney website and enter their login cardinalities.As depicted in Figure 1, authentication techniques can be categorized into three main categories, namely: (i) knowledge-based authentication, (ii) token-based authentication, and (ii) biometric-based authentication. In fact, biometric-based authentication is considered the securest and most reliable authentication technique since it depends on the personal characteristic of the end-user only (Saini et al., 2020). The widespread biometric methods utilized in authentication are scanning the fingerprint (Chanukya&Thivakaran, 2020), scanning retina (Srivastava, 2020). scanning face (Pramana et al., 2020), keystroke (Pramana et al., 2020). However, scanning the retina and figure are the most widely used biometric method being in authentication using smartphones (Saini et al., 2020).

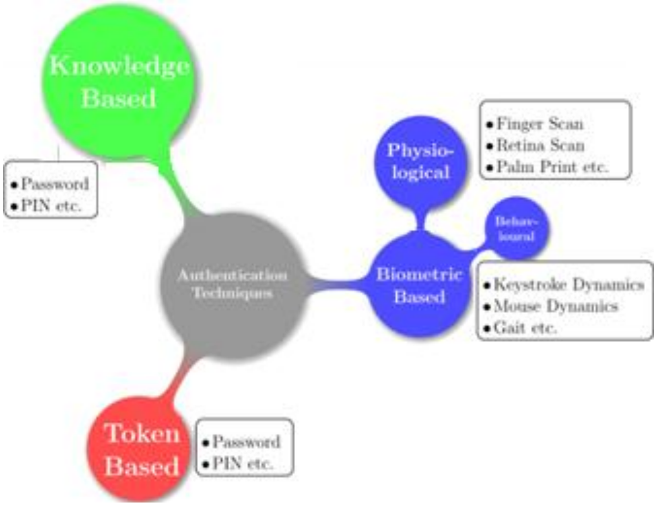


Figure 1: Taxonomy of Authentication Techniques

2. Research Problem

1) Recent years have testified many outbreaks of sensitive and personal data breaches and password leaks that happened on prominent websites and online applications Facebook, Yahoo!, and Gmail. Stealing these passwords imperil millions of users' information security not only on those online applications/ websites

but also on other websites because of password reusability (Florencio &Herley, 2007; Dastane, 2020). To make matters worse, MITM and phishing attacks are usually used by attackers to steal users' passwords.

2) Besides, nowadays, text-based passwords are growing to be the prevailing form for most user identification, business, and services attempt to protect their users account and sensitive information through providing new or enhanced authentication methods using trending security technologies.
3) Therefore, authentication using text password is obviously inadequate and inefficient; therefore, two-factor authentication (2FA) has been mightily recommended and used to enhance web authentication security process, and therefore, enhance overall security. Along with the advancement of smartphone devices in the past decade, many smart phone devices assisted 2FA methods to ensure high level of security and privacy, as the smartphones has become the second authentication factor in addition to the text or pin passwords. In practice, Short Message Service (SMS) based-authentication (e.g., (Mulliner et al., 2013)) and soft token based-authentication (e.g., (Das &Samdaria, 2014)) TFA methods that leverage cellphones especially smartphones devices have been used.

3. Research Objectives

This study aims to propose an efficient two-factor authentication method. To achieve this aim, the following objective has been formulated:

1) To explore and synthetically analyze the existing authentication method.
2) To implement a user-friendly web application to provide efficient user authentication.
3) To adopt an efficient two-factor authentication method based on biometric features (i.e., face scanning); and
4) To evaluate the effectiveness of the proposed method.

4. Research question

The main research question is" Does the two-factor authentication provide efficient authentication". The following sub-question are directly derived from the main question:

1) What are the challenges and shortcomings of the existing wen authentication methods?
2) Does the biometric- based authentication enhance web authentication?
3) Does the proposed authentication method work efficiently?

5. Literature Review

In usual, 2FA requires the presentation of two or more authentication elements including: (i) what the end-user knows such as text password, (ii) what end-user has such as secure toke), and (iii) what a user is such as biometric features. Indeed, the use of 2FA as opposed to 1FA usually provides a high level of authentication. For instance, text password might be integrated with security tokens (i.e., RSA SecurID), which utilize one-time passwords or biometric features like fingerprint of face scan. With the advancements of smart phone, a new class of 2FA methods and tools transforms a personal computer devices and smart phones into a token device through either SMS (Ali et al., 2020), an interactive and real-time telephone call (Dutson et al., 2019), or using a mobile application (AlQahtani et al., 2020). Several mobile device-supported authentication methods such as (Derhab et al., 2020; Petrov et al., 2020) were used to protect a user and his/her sensitive data from either password stealing on an untrusted access or web/phishing attacks. In those methods, smart phones devices are supposed to be trustworthy and can perform specific computing tasks like hashing. Parno et al. (2006) proposed Phoolproof, which is a public-key based method for support security of bank transactions system. End-user has to select a bank site from the whitelist on mobile device, after that, he/she wait to exchange information between the mobile device and personal computer device (PC). Besides, Mannan et al. (2011) proposed authentication model, called MP-Auth, to detect keylogger and phishing attacks using mobile devices, through transferring authorized users' passwords to mobile device and re-encrypting the username and password.

The study for Reese et al. (2018) explains the following are the primary contributions of this work: First, created a novel user behavior model that covers four phases of user-authentication system interaction. This model is intended to guide the design of future usability studies and provide researchers and others responsible for developing authentication systems with a more nuanced understanding of authentication system functionality. Second, we performed a usability comparison of some of the most popular two-factor authentication methods. Unlike earlier authentication usability tests, we had people utilize the system for two weeks and collected time data as well as SUS metrics on the systems under test. drawing various conclusions about the usability and acceptance of two-factor authentication from this research, including the fact that many users want extra security for their sensitive online accounts and are willing to utilize multiple kinds of two-factor authentication. also propose that security researchers employ risk communication theory to better assist consumers in making secure decisions. Other study interested in showing the the benefits of using two factor authentication such as Gordin et al. (2019) , the study presented the benefits of this new style of authentication, which also synthesizes the TOTP authentication forms used by major cloud providers. On addition, the paper proposes a solution to this problem by offering a practical approach for implementing two-factor authentication in the OpenStack cloud. The online authentication form has been updated for this purpose, and a new authentication module has been created. The current document also covers the complete process of adding a TOTP user, as well as producing and transmitting the secret code to the user in QR format. The research closes with OpenStack tools that were utilized to simplify the above-mentioned process. On the other hand, the study of Alharbi et al. (2019) offers a novel two-factor authentication framework for the OTP- SMS approach to prevent various attacks, including Man in The Middle (MITM) and third-party assaults. The suggested framework is built on the usage of Blockchain technology, which

Licensed Under Creative Commons Attribution CC BY

increases security and improves the authentication process environment. The suggested framework sends an encrypted OTP created by a smart contract to the application/website, together with its hash value, to complete the authentication process. made a comparison between our proposed framework and two alternative Blockchain-based OTP-SMS security frameworks. The framework has been found to be secure against MITM and third-party attacks, as well as having a lower computation time and complexity than competing frameworks. Blockchain is one of the most technology which provides high security system, some study interested in using this technology in the authentication such as Putri et al. (2020) , it propose a two-factor authentication framework based on the Ethereum blockchain, with a decentralized application (dApp) as the token creation method. Following the results of the system analysis, the team was able to create a two-factor authentication solution without the use of third parties. Second, the token system has been collision-tested and can create up to 3164 distinct tokens in one second. Third, a security approach for preventing an MITM attack on the token. Because all the checks are done via dApp user authentication, the attacker is unable to gain access. Also, Bao et al. (2021) Based on the advantages of blockchain with decentralization and anonymity, a novel biometric identity authentication technique is suggested. First and foremost, the fuzzy extractor for biometric information is utilized in the authentication process, which addresses the issue of permanent unavailability caused by biometric template leaking. The Fabric architecture is then utilized to create a blockchain in which the hash value of the random key obtained using the fuzzy extractor is stored, which solves the problem of centralized storage that plagues traditional identity authentication mechanisms. A two-factor identity authentication technique is realized using blockchain and fuzzy extractor. The study ran practical simulations on our suggested algorithm, and we were able to demonstrate the security of our system by assessing simulated enemy attack and resistance under harsh conditions. Meanwhile, our efficiency analysis demonstrates that our strategy is available. scalability and reliability are more important to improve the performance of the system, the study for Déncs-Fazakas et al. (2020) provides a two-factor authentication scheme for multi-site large companies where scalability and reliability of authentication, processing, and storage are critical. To provide data parallelism, fault tolerance, and distributed data storage, our solution is built on the Apache Spark framework, which is enhanced with Apache Cassandra, Kafka, and a MySQL database. For the electronic payments, the study of Hassan et al. (2021) proposes a multi-authentication method for electronic payments. The multi-factor authentication system suggested here combines password, biometric, and OTP verification for more reliable user authentication. The suggested system is divided into three phases: registration, authentication, and transactions. Our proposed solution has been found to improve security efficacy for a variety of assaults and authentication layers that rely on passwords. Other study such as Elshamy et al. (2021) suggested, a two-factor authentication-based dual-security cryptosystem for VoIP voicemail, followed by Baker Map and RC6 encryption. There are two security system types proposed: one uses biometric voiceprint encryption with a pin code, and the other uses dual-biometric encryption with voiceprint and fingerprint. Parameters were used to evaluate the suggested security solutions for both function quality and real-world applicability. A genuine VoIP call manager, VoIP terminals, and a fingerprint scanner were used in an experiment. In addition, the new cryptosystems were developed and tested using Visual Basic and MATLAB. To assure efficiency with varying signal-to-noise ratios, an orthogonal frequency division multiplexing (OFDM) simulation system was built (SNR). Based on a cost-benefit study of both encryption systems, the first is more cost-effective than the second due to the lack of a fingerprint-reading device, while the second is more secure due to the combined biometric print requirements. Also, the study of Alsoliman et al. (2021) provides a Vision-Based Two-Factor Authentication and Localization Scheme for Autonomous Vehicles in this study. The method uses the cars' light sources and cameras to create a "Optical Camera Communication (OCC)" channel, which serves as an auxiliary channel between vehicles for visually authenticating and localizing message transmitters who use Radio Frequency (RF) channels. also evaluate potential threats to the proposed strategy, as well as mitigating solutions. Other study such as Sain et al. (2021) Starting with Single-Factor Authentication (SFA) and progressing through Two-Factor Authentication (TFA), this paper will describe the progression from single authentication to Multi-Factor Authentication (MFA) (2FA). This study aims to analyze and evaluate the most popular authentication mechanisms in terms of accuracy, cost, and implementation feasibility. also, the study recommends a few authentication strategies for CPS that use Multifactor Authentication. The e-services authentication is more important topic in authentication filed, more study interested in it such as Quadry et al. (2021) proposes the creation of an e-services authentication mechanism that is immune to a variety of attacks, including a stolen verifier attack. The paper will also cover the following topics: 1) The suggested approach was evaluated for the level of security it provides against known authentication attacks. 2) The proposed scheme's concept execution. Also, the study of Jan et al. (2021) suggested a lightweight and robust authentication strategy for network-enabled healthcare devices (IoMT) that addresses all the recent literature's highlighted flaws. Formally, using BAN logic and ProVerif2.02, and informally, using pragmatic example, the proposed protocol's security has been assessed. Simultaneously, the performance analysis result at the end of the study reveals a delicate balance of security and performance that is typically missing in current protocols.

6. Research Methodology

In this section, the methodology being used to achieve the thesis stated objectives and to answer the thesis questions is explained. Figure 2 summarizes the stages of the methodology being used in this thesis.

Licensed Under Creative Commons Attribution CC BY

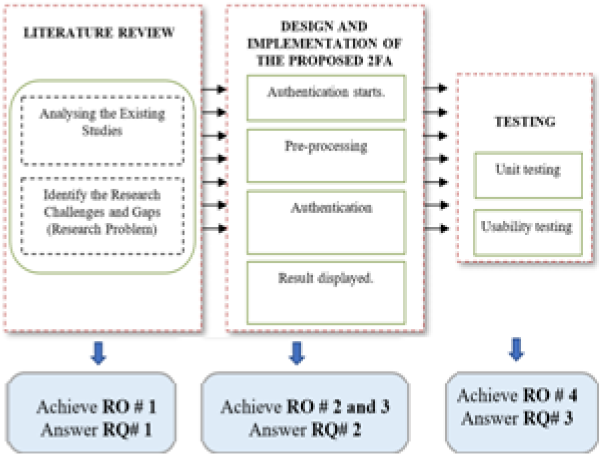

LITERATURE REVIEW
Analysing the Existing Studies
Identify the Research Challenges and Gaps (Research Problem)
DESIGN AND IMPLEMENTATION OF THE PROPOSED 2FA
Authentication starts.
Pre-processing
Authentication
Result displayed.
TESTING
Unit testing
Usability testing
Achieve RO # 1 Answer RQ# 1
Achieve RO # 2 and 3 Answer RQ# 2
Achieve RO # 4 Answer RQ# 3

Figure 2: Research Methodology

In the first stage, the existing literature is explored and analyzed. First, comprehensive review of the web authentication, methods being used is conducted. Then, the prior studies will be synthetically analyzed to highlights the shortcomings and gaps they are suffering from. Besides, the proposed solution will be outlined in this stage.

The second stage, the proposed 2FA solution is proposed. As the proposed 2FA method and its phases will be defined in detail, the requirements, design, and implementation of 2FA solution will be provided indeed. Figure 3 illustrates the main step of proposed 2FA method.

The third stage, the proposed solution will be tested through unit testing and usability testing.

To apply the project idea in operate two factor authentication; it must be achieved two phases; the first phase is text message authentication, and the second phase is face authentication using deep learning algorithm. The figure below shows the two phases.

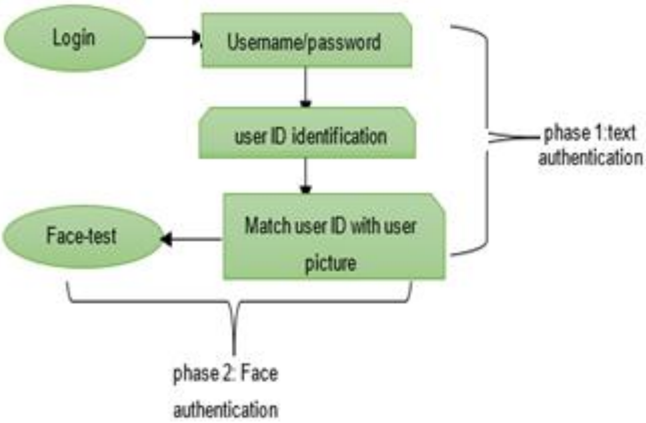

Login
Username/password
user ID identification
phase 1:text authentication
Face-test
Match user ID with user picture
phase 2: Face authentication

Figure 3: Methodology: two factor authentication

Phase 1: Text authentication; In this step the user inserts username and password then the system will send message authentication to user phone by SMS message.

Phase 2: Face authentication; in this step deep learning algorithm is used to apply the face authentication idea using Artificial Neural Network (ANN) algorithm.

7. Improvement as Per Reviewer Comments

Analyze and understand all the provided review comments thoroughly. Now make the required amendments in your paper. If you are not confident about any review comment, then don't forget to get clarity about that comment. And in some cases there could be chances where your paper receives number of critical remarks. In that cases don't get disheartened and try to improvise the maximum.

A. Face recognition using neural network

Many of our services have become applied using electrical tools that based on inserting the user information in an electrical way, resulting in the need to protect this information and control the services using security technical such as face recognition to protect your details from any theft or loss. Face recognition is a modern technology that is used to identify a person's ID and protect his or her personal information from attack or error.

Face recognition technology has many effective advantages, including the ability to recognize anyone because it is not based on any specific features or conditions, such as skin color or eye color, so this technology can recognize people of all shapes and sizes. Simple to set up, test, and use.

This project is interested in implementing face recognition technology using Artificial Neural Networks; Artificial neural networks are one of the primary tools used in machine learning. They are brain-inspired systems, as the "neural" part of their name implies and are designed to mimic how humans learn. The system will be trained for all of the important information in this technique, and it will then be used to quickly identify the information. The Back propagation Neural Network (BPNN) performs the recognition; it is a method used in artificial neural networks to calculate a gradient that is required in the calculation of the network's weights. It is frequently used to train deep neural networks, which are neural networks with more than one hidden layer. In this project, the MATLAB program will be used to put the idea into action because it has a plethora of tools and features that aid in the recognition of face images.

The system has four main features which are shown in Figure.: provide face image, pre-processing, Feature Extraction, and Face Recognition.

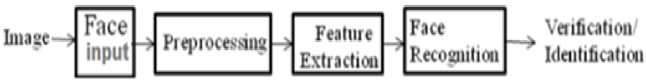


Figure 4: Structure of Face Recognition System

Face input: insert given image

Pre-processing: This step serves as pre-processing for face recognition. Using pre-processing techniques, unwanted noise, blur, varying lighting conditions, and shadowing effects can be removed.

Feature Extraction: In this step features of face can be extracted using feature extraction algorithm

Licensed Under Creative Commons Attribution CC BY

Face Recognition: Once feature extraction is complete, the next step is to analyze the representation of each face; this final step is used to recognize the identities of the faces in order to achieve automatic face recognition; for the recognition, a face database must be built. face detection, pre-processing, and feature extraction are performed before comparing its feature to each face class stored in the database.

8. Project Result and Discussion

For the first authentication, the user must insert correct username and password then the system will request the user to insert ID to show the picture user ID. Each user has ID that used to connect his information with picture which used in the second authentication. The Figure5 shows how we apply the first authentication in our project.

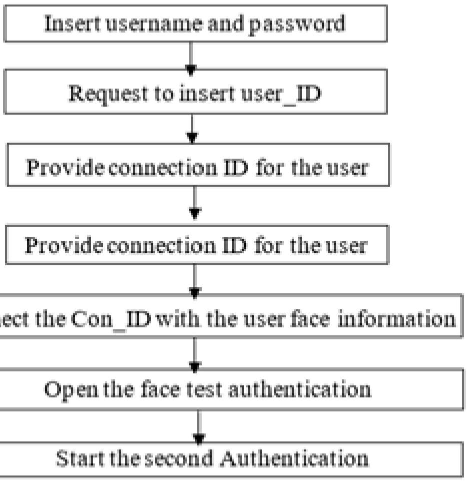
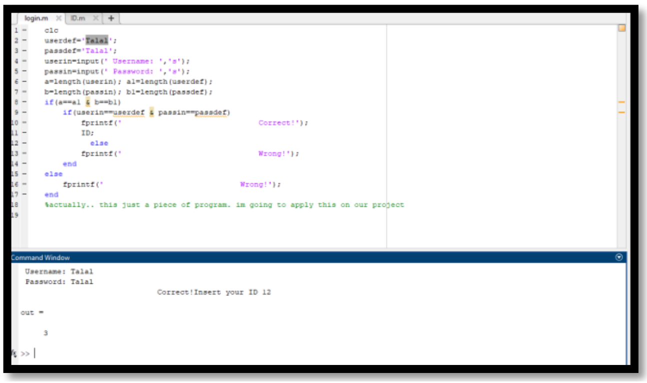

Insert username and password
Request to insert user_ID
Provide connection ID for the user
Provide connection ID for the user
Connect the Con_ID with the user face information
Open the face test authentication
Start the second Authentication

Figure 5: First authentication steps

First authentication code



```
clc
userdef='Talal';
passdef='Talal';
userin=input(' Username: ','s');
passin=input(' Password: ','s');
a=length(userin); a1=length(userdef);
b=length(passin); b1=length(passdef);
if(a==a1 & b==b1)
    if(userin==userdef & passin==passdef)
        fprintf('                              Correct!');
        ID;
          else
        fprintf('                              Wrong!');
    end
else
    fprintf('                              Wrong!');
end
%actually.. this just a piece of program. im going to apply this on our project
```

```
 Username: Talal
 Password: Talal
                              Correct!Insert your ID 12

out =

     3

>> 
```

Figure 6: First authentication code

After inserting correct information will access to the second Authentication. The second Authentication is biometric authentication using face recognition. The Figure7 shows the main interface of the face Authentication system.

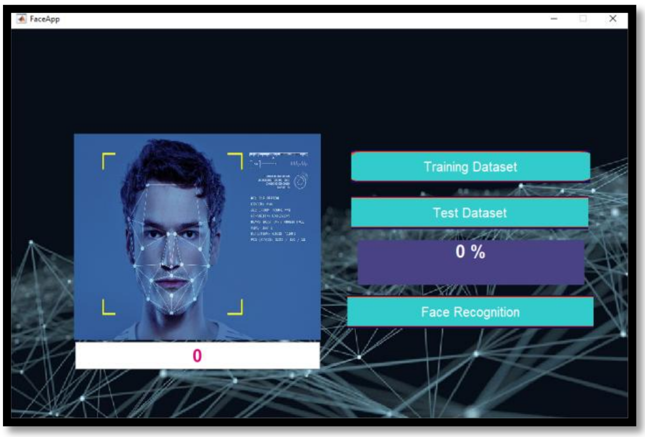
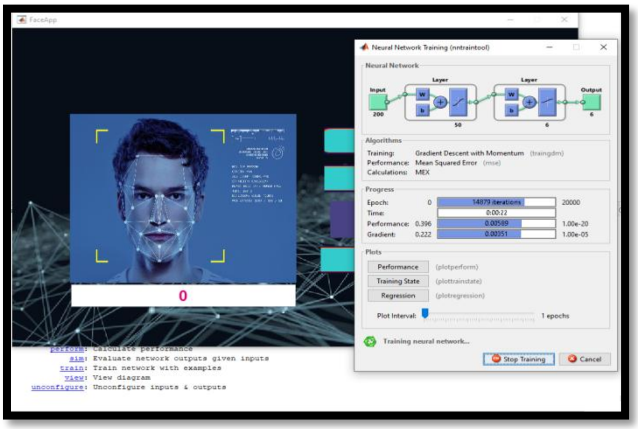


Figure 7: The face Authentication system

For the second Authentication, the system training dataset which includes the users who registers in the system, the training system based on ANN machi leaning method then will test the system to show the accuracy and evaluate the system. The Face Recognition button allow the user to select the picture of user which match with the user ID to approve the user authentication and allow access the system. Figure 8 show the model using ANN in MATLAB program. Figure8 shows the test and evaluate the system and the Figure 9 shows how the system face recognition.



Algorithms
Training: Gradient Descent with Momentum (traingdm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress
Epoch: 0 14879 iterations 20000
Time: 0:00:22
Performance: 0.396 0.00589 1.00e-20
Gradient: 0.222 0.00351 1.00e-05

Plots
Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)
Plot Interval: 1 epochs

Training neural network...

```
    perform: Calculate performance
        sim: Evaluate network outputs given inputs
      train: Train network with examples
       view: View diagram
unconfigure: Unconfigure inputs & outputs
```

Figure 8: Training the model

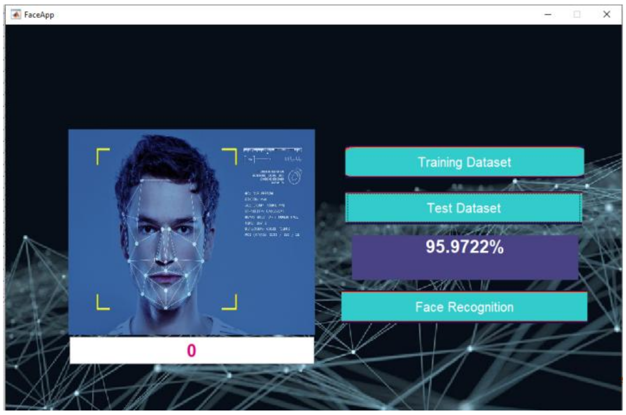


Figure 9: Test and evaluate the system

Licensed Under Creative Commons Attribution CC BY

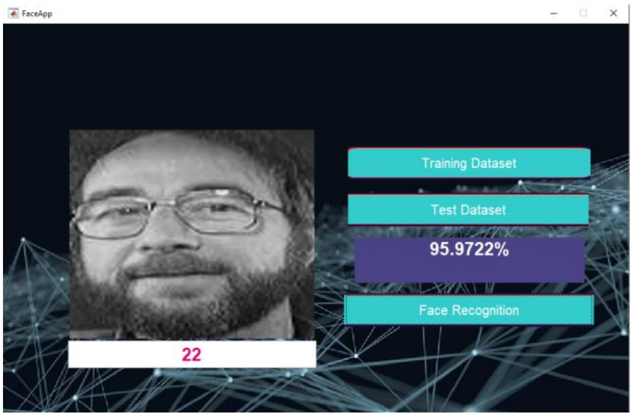


Figure 10: Face recognition Result

9. Conclusion

Two-factor authentication is a security mechanism that double-checks the user's identity. When a user attempts to sign into an account, he or she will be prompted to enter a username and password - this is the first verification layer. Two-factor authentication functions as an additional step in the process, a second security layer that uses a face recognition system to re-confirm the user's identity. Its goal is to make attackers' lives more difficult and to reduce fraud risks. The project provides many benefits because it based on two factor authentication; it makes the system Stronger security. using this system Increase productivity and flexibility because when using two factor authentication allow the users access to system in safety way. Two-factor authentication reduces the number of time-consuming password resets that help desks are required to perform. Users can reset their own passwords in a secure manner with 2FA. Increased employee productivity is the result for businesses.

10. Acknowledgment

Thanks for my doctor who supervise my idea to achieve this work, and I thanks my family for all support and love.

References

[1] Agaste, S., Bhamare, A., Sadre, A., Honrao, S., & Patil, A. A. (2020). Password Security System With phishing website detection System.

[2] Ali, F. A. B. H., Hanza, M. Z. B. M., & Sukri, M. A. B. M. (2020). Two Factor Authentication by Using SMS for Web Based Application. International Journal of Information Technology, 9(6).

[3] AlQahtani, A. A. S., Alamleh, H., Gourd, J., & Alnuhait, H. (2020). TS2FA: Trilateration System Two Factor Authentication. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-4). IEEE.

[4] Al-shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020). Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. International Journal of Engineering and Management Research, 10.

[5] Binbeshr, F., Kiah, M. M., Por, L. Y., & Zaidan, A. A. (2020). A Systematic Review of PIN-entry Methods Resistant to Shoulder-surfing Attacks. Computers & Security, 102116.

[6] Chanukya, P. S., & Thivakaran, T. K. (2020). Multimodal biometric cryptosystem for human authentication using fingerprint and ear. Multimedia Tools and Applications, 79(1), 659-673.

[7] Das, M. L., & Samdaria, N. (2014). On the security of SSL/TLS-enabled applications. Applied Computing and informatics, 10(1-2), 68-81.

[8] Dastane, O. (2020). The Effect of Bad Password Habits on Personal Data Breach. *International Journal of Emerging Trends in Engineering Research*, 8(10).

[9] Derhab, A., Belaoued, M., Guerroumi, M., & Khan, F. A. (2020). Two-factor mutual authentication offloading for mobile cloud computing. *IEEE Access*, 8, 28956-28969.

[10] Dutson, J., Allen, D., Eggett, D., & Seamons, K. (2019). Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. *In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 119-128). IEEE.

[11] Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *In Proceedings of the 16th international conference on World Wide Web* (pp. 657-666).

[12] Han, W., Xu, M., Zhang, J., Wang, C., Zhang, K., & Wang, X. S. (2020). TransPCFG: Transferring the Grammars From Short Passwords to Guess Long Passwords Effectively. *IEEE Transactions on Information Forensics and Security*, 16, 451-465.

[13] Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 268-285). IEEE.

[14] Makura, S. M., Venter, H. S., Ikuesan, R. A., Kebande, V. R., & Karie, N. M. (2020). Proactive forensics: keystroke logging from the cloud as potential digital evidence for forensic readiness purposes. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 200-205). IEEE.

[15] Mannan, M., & Van Oorschot, P. C. (2011). Leveraging personal devices for stronger password authentication from untrusted computers. *Journal of Computer Security*, 19(4), 703-750.

[16] Mohammadinodoushan, M., Cambou, B., Philabaum, C. R., & Duan, N. (2021). Resilient Password Manager Using Physical Unclonable Functions. *IEEE Access*, *9*, 17060-17070.

[17] Mulliner, C., Borgaonkar, R., Stewin, P., & Seifert, J. P. (2013). SMS-based one-time passwords: attacks and defense. *In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 150-159). Springer, Berlin, Heidelberg.

[18] Oesch, S., & Ruoti, S. (2020). That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers. In *USENIX Security Symposium*.

[19] Parno, B., Kuo, C., & Perrig, A. (2006). Phoolproof phishing prevention. *In International conference on financial cryptography and data security* (pp. 1-19). Springer, Berlin, Heidelberg.

Licensed Under Creative Commons Attribution CC BY

[20] Petrov, P., Dimitrov, P., Stoev, S., Dimitrov, G. P., & Bulut, F. (2020). Using the Universal Two Factor Authentication Method in Web Applications by Software Emulated Device. *International Multidisciplinary Scientific GeoConference: SGEM*, 20(2.1), 403-410.

[21] Pramana, M. D., Lestyea, A., & Amiruddin, A. (2020). Development of a Secure Access Control System Based on Two-Factor Authentication Using Face Recognition and OTP SMS-Token. *In 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* (pp. 52-57). IEEE.

[22] Saini, B. S., Singh, P., Nayyar, A., Kaur, N., Bhatia, K. S., El-Sappagh, S., & Hu, J. W. (2020). A Three-Step Authentication Model for Mobile Phone User Using Keystroke Dynamics. *IEEE Access*, 8, 125909-125922.

[23] Srivastava, R. (2020). Score-Level Multimodal Biometric Authentication of Humans Using Retina, Fingerprint, and Fingervein. International Journal of Applied Evolutionary Computation (IJAEC), 11(3), 20-30.

[24] Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. International Journal of Human-Computer Studies, 133, 26-44.

[25] Reese, K. R. (2018). Evaluating the usability of two-factor authentication. Brigham Young University.

[26] Gordin, I., Graur, A., & Potorac, A. (2019, October). Two-factor authentication framework for private cloud. In 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC) (pp. 255-259). IEEE.

[27] Alharbi, E., & Alghazzawi, D. (2019). Two factor authentication framework using otp-sms based on blockchain. Transactions on Machine Learning and Artificial Intelligence, 7(3), 17-27.

[28] Putri, M. C. I., Sukarno, P., & Wardana, A. A. (2020). Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 6(2), 74-85.

[29] Déncs-Fazakas, L., Kail, E., & Fleiner, R. (2020, November). Two-factor, continuous authentication framework for multi-site large enterprises. In 2020 IEEE 20th International Symposium on Computational Intelligence and Informatics (CINTI) (pp. 173-178). IEEE.

[30] Hassan, M. A., & Shukur, Z. (2021, January). A Secure Multi Factor User Authentication Framework for Electronic Payment System. In 2021 3rd International Cyber Resilience Conference (CRC) (pp. 1-6). IEEE.

[31] Elshamy, E. M., Hussein, A. I., Hamed, H. F., Abdelghany, M. A., & Kelash, H. M. (2021). Voice over internet protocol voicemail security system using two factor authentication and biometric prints with new efficient hybrid cryptosystem. Multimedia Tools and Applications, 80(7), 9877-9893.

[32] Bao, D., & You, L. (2021). Two-factor identity authentication scheme based on blockchain and fuzzy extractor. Soft Computing, 1-13.

[33] Sain, M., Normurodov, O., Hong, C., & Hui, K. L. (2021, February). A Survey on the Security in Cyber Physical System with Multi-Factor Authentication. In 2021 23rd International Conference on Advanced Communication Technology (ICACT) (pp. 1-8). IEEE.

[34] Alsoliman, A., Levorato, M., & Chen, A. (2021, February). Vision-Based Two-Factor Authentication & Localization Scheme for Autonomous Vehicles. In Third International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021 (part of NDSS).

[35] Quadry, K. M., Govardhan, A., & Misbahuddin, M. (2021). Design, Analysis, and Implementation of a Two-factor Authentication Scheme using Graphical Password. International Journal of Computer Network & Information Security, 13(3).

[36] Jan, S. U., Ali, S., Abbasi, I. A., Mosleh, M. A., Alsanad, A., & Khattak, H. (2021). Secure Patient Authentication Framework in the Healthcare System Using Wireless Medical Sensor Networks. Journal of Healthcare Engineering, 2021.

[37] Albawi, S., Mohammed, T. A., & Al-Zawi, S. (2017, August). Understanding of a convolutional neural network. In 2017 International Conference on Engineering and Technology (ICET) (pp. 1-6). Ieee.

Licensed Under Creative Commons Attribution CC BY