Computers, Materials & Continua
DOI:10.32604/cmc.2022.020624
Article

Tech Science Press

IoT Devices Authentication Using Artificial Neural Network

Syed Shabih Ul Hasan[1], Anwar Ghani[1], Ikram Ud Din[2], Ahmad Almogren[3,*] and Ayman Altameem[4]

[1]Department of Computer Science and Software Engineering, International Islamic University Islamabad, 45000, Pakistan
[2]Department of Information Technology, The University of Haripur, 22620, Haripur, Pakistan
[3]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh, 11633, Saudi Arabia
[4]Chair of Cyber Security, Department of Natural and Engineering Sciences, College of Applied Studies and Community Services, King Saud University, Riyadh, 11543, Saudi Arabia
[*]Corresponding Author: Ahmad Almogren. Email: ahalmogren@ksu.edu.sa
Received: 31 May 2021; Accepted: 09 July 2021

Abstract: User authentication is one of the critical concerns of information security. Users tend to use strong textual passwords, but remembering complex passwords is hard as they often write it on a piece of paper or save it in their mobile phones. Textual passwords are slightly unprotected and are easily attackable. The attacks include dictionary, shoulder surfing, and brute force. Graphical passwords overcome the shortcomings of textual passwords and are designed to aid memorability and ease of use. This paper proposes a Process-based Pattern Authentication (PPA) system for Internet of Things (IoT) devices that does not require a server to maintain a static password of the login user. The server stores user's information, which they provide at the time of registration, i.e., the R-code and the symbol, but the P-code, i.e., the actual password, will change with every login attempt of users. In this scheme, users may draw a pattern on the basis of calculation from the P-code and R-code in the PPA pattern, and can authenticate themselves using their touch dynamic behaviors through Artificial Neural Network (ANN). The ANN is trained on touch behaviors of legitimate users reporting superior performance over the existing methods. For experimental purposes, PPA is implemented as a prototype on a computer system to carry out experiments for the evaluation in terms of memorability and usability. The experiments show that the system has an effect of 5.03% of the False Rejection Rate (FRR) and 4.36% of the False Acceptance Rate (FAR), respectively.

Keywords: Implicit authentication; behavioral authentication; artificial neural network; processed pattern authentication

1 Introduction

Accounts whether they may be of emails, social networking websites, website administrators, personal computers, or networks, are mostly protected by passwords. Textual passwords are common in use methods of authentication. Memorization of powerful passwords is burdensome, thus,

people normally choose short passwords or even simple dictionary words. The worst situation is that users may use the same username and password for multiple accounts for their easement, that make it more vulnerable, where the exposure of one password can lead to security breaches of all accounts associated with it [1,2]. Each Internet of Things (IoT) device and account must have a distinct password for security, if in case the attacker gets success for breaking a password, he cannot breach the other accounts. According to a study in [3], a security team at an organization ran a password cracker and amazingly cracked about 80% of the employees' passwords in less than a minute. It is advised that users must use long and complicated passwords that contains special characters, letters (upper- and lower-case letters), and numbers, to protect their devices from different attacks. In general, it's very hard to memorize complex and lengthy passwords. Consequently, for logging into different accounts users prefer to save the passwords by writing on paper that raises the likelihood for the violation of security by different attackers [4].

To tackle the weaknesses of traditional passwords, Graphical password techniques were introduced. Graphical passwords such as OP-Grid [5], PassTag [6], and Passpositions [7] make cell phones more adaptable than the conventional, because a wide scope is offered for symbols over password techniques based on text. They are therefore being introduced in smart devices. The authentication process having multi-factors, e.g., "Something you Process", is used by researchers while presenting their schemes against attacks, such as shoulder surfing attack [8]. In such multi-factor authentication, users remember the equation/formula and the values of variables are given to them at the time of authentication. A user puts these values in the formula and processes/calculates the outcome in his/her brain, which is then entered as a password. The values of variables may change; therefore, the password changes every time it is entered. Hence, an attacker may know the password, which restricts user to login with that password.

With the adoption of the Android mobile operating system, a substitute to PIN authentication, known as pattern authentication system, on mobile devices has been implemented and widely deployed. A user generates a hidden authentication pattern on a 3×3 grid with his finger and then redesigns it for verification, as shown in Fig. 1.

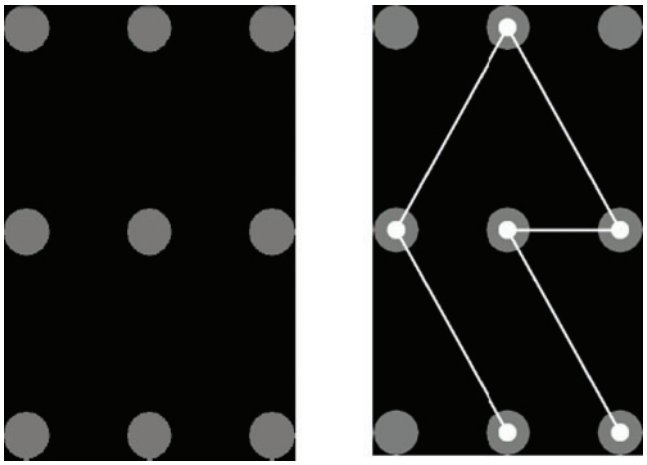

Figure 1: Standard layout of authentication system through pattern [9]

Compared to PIN/Password, authentication through pattern keeps the brain to learn the information and accumulates in a better way. The pattern might remember in the form of an image,

thus manipulate the impact of illustrated supremacy [10]. Patterns are exposed to a hazardous environment, even if a user selects complex or lengthy ones, as in the case of shoulder surfing attack, where the adversary is capable to know what you have drawn as a pattern. Some of the attacks are discussed below.

(1) Shoulder surfing is the latest weapon used by hackers as this technique depends upon observation for example sneaking over the shoulder or recording his login or other information by using a hidden camera. This type of attack is an effective way to steal the authentication data, i.e., pattern, as it requires no extra knowledge or software. Pretty much every "keen" customer's gadget today incorporates a camera, from savvy watches to shrewd TVs, glasses, telephones, and MP3 players. Researchers at Black Hat [11] exhibited that how these cameras can keep an eye on individuals tapping, for example, passwords or patterns into mobile and tablet consoles.
(2) Pattern authentication methods require users to touch the display screens for login and thus are vulnerable to smudge attacks. An attacker can retrieve the pattern of the users etc. through examining the marks remain over the display screen [12].
(3) In password guessing attack, a hacker can guess a user's pattern password using his stolen cell phone devices as well as the data caught during the registration or authentication phase [13].

We all have different "living credentials" such as fingerprints, facial expressions, optical elements, voice tones, and behavioral attributes. User behavior is one way to represent the identity of an individual [14]. It identifies whether the current user is a valid one by collecting and training the features of the sample data in order to carry out authentication. The key characteristics of behavioral authentication are as follows:

- It is an entirely back-end application, ensuring that the whole data collection and authentication process doesn't require users to do something that sounds user-friendly.
- Additional hardware support is not required, it only needs a smartphone with common sensors and a touch screen.
- It does not overlap with other methods of authentication.
- It is hard to conceal but only possible if the attacker can accurately mimic the actions of the owner.

"Something user process" is an authentication factor [15], which is a formula-based authentication that requires the formula processing by the user that the server provides related to the numbers or images. This study suggests a multi-factor behavioral pattern lock system. First, by using authentication factor "something you process" the user shall compute the values for pattern. Second, the pattern will be drawn and validated if the user's touch dynamics features match the features saved in the system. Following are the primary benefactions of the study:

- Built-in effective, reliable authentication framework.
- Use the concept of "something you process" authentication factor that allows users to enter new patterns on each login session, hence, improving protection in opposition to shoulder surfers, smudge and guessing attacks.
- Proposed multi factor behavior authentication method using "something you process" factor, the drawn pattern by the user is checked, i.e., whether it is correct or not, later on by using the login behavioral features of the user, will conclude the correctness of drawn pattern.

2 Related Work

With a major increase in the IoT environment, researchers have begun to use the accessible sensual data from IoT devices to modeling the behaviors of humans. Machine learning algorithms are workable to improve the protection applications related to the touch screens of mobile phones [16]. Behavioral biometrics using machine learning classifiers are more widely used for implicit and continuous authentication [17]. In the research on continuous authentication that was based on gesture behavior of the user [18], 30 features were extracted by the authors from the retrieved data by touch screens and using SVM and K-nearest-neighbors (KNN) algorithms a validation model was developed based on sliding gestures (top and bottom). The equivalent error rate (EER) of their proposed system lies between 0% and 4%. To improve the accuracy, multi stoke features is missing for big touch screen devices like tablets. Bo et al. [19] suggested utilizing the SVM to construct a classification model based on touch behavior biometrics for the users of smartphones. The developed classification model updates the SVM model by introducing new observed features through self-learning to enhance the accuracy of classification. The results show that the proposed authentication scheme is fast and accurate with regards to identification. The authors in [20] proposed neuro-fuzzy inference system (ANFIS) classifier for the security of smartphones with pattern passwords. ANFIS is used as behavioral features to construct a classification model. Some of the features like touch pressure and touch stroke interval were not considered in the proposed scheme. Alpar et al. [21] suggested Levenberg-Marquardt ANN (LM-NN). ANN was trained by touch location data. The outcomes indicate that the authentication of LM-NN is stronger and quicker as compared to other classification algorithms. The limitation in the system is the amount of epochs required to train the networks. The intervals would have been narrower if the number of repetitions is increased, resulting in a higher FRR and lower FAR. Zhou et al. [22] suggested ANN back propagation (BPNN) to enhance the security of smartphones. Using thumb stroke behavior, BPNN is used to build an authentication method. The proposed classifier offers an improvement in security and usability compared to the keystroke dynamics model. On the usability and security model, this scheme is limited to reduce the complexity of a password. In order to build an enhanced pattern, the password authentication method uses touch locations as biometrics. Researchers did not perform the feature reduction, section, and transformation of data prior to model training.

In some cases, machine learning algorithms are merged or combined with a traditional technique. For example, a scheme in [23] created an authentication classifier using a combination of SVM and RBF. The SVM-RBF classifier is designed on the basis of multiple facial attributes extracted from smartphone users. The outcomes indicated that the created classifier (SVM-RBF) is highly stable, uses slight space and the greater performance under various conditions. This solution lacks the ability to adjust to attribute changes of the user, such as aging. Changing attributes of the user especially facial hair change are missing in this scheme. In [24], the authors used three separate algorithms to construct three classifiers, for user authentication, i.e., SVM, DTW and KNN. These algorithms focus on creating a classification scheme for the identification of smartphones users that is based on user's physical activities. The verification and testing were carried out in order to choose the best classifier among the three classifiers. The results indicate that SVM's general performance in authenticating individuals in five distinct positions on smartphones is higher as compared to DTW and KNN. This approach only considers the behavior patterns but neglects the background features. This study did not examine motion and physiological sensors along with contextual authentication knowledge. Liang et al. [25] suggested a Convolutional neural network (ConvNet) to predict user actions of the tap series and device usage.

The sensor data was collected on various applications as users interact with the system and by the use of sensor data formulated on ConvNet, SVM, and KNN a classification model is constructed. As a comparison ConvNet performs better than SVM and KNN. To achieve consistent and better performance, the CovNet model with more layers was not considered. Olade et al. [26] proposed a scheme of protection required to approve a user's identity utilizing a variety of familiar characters tics which distinguish the user from other users in a virtual and augmented reality environment. Identifying the task comes first, followed by identifying the individual in the identification process. Machine learning was used to test 65,241 datasets regarding the movements of hands, head and eyes in order to develop a continuous biometric authentication system and achieved an accuracy of 98.6%. This technique focuses only on specific age group. For machine learning, Artificial Neural Network (ANN) is considered among the strongest algorithms for machine learning that has gained considerable attention from researchers and shows up in various forms [27].

The authentication schemes discussed here in the literature review are limited to specific age group [26], or are not compatible with large screen mobile devices [18]. The features like touch pressure and touch stroke intervals were missing in [19]. The proposed authentication system in this research have tried to overcome the flaws discussed in the literature review. The concept of "something user process" is used, which lets the user to enter a different pattern for each login session, hence increasing security against guessing attacks, smudge attacks, and shoulder surfer attacks. Something you process enhanced the security that even the attacker mimics the behavioral features of the user, but cannot find the trace the exact pattern as the pattern is different at every login attempt.

3 PPA

This proposed technique addresses the weaknesses in pattern lock method by the implementation of the authentication's fifth factor and introduces Processed Pattern Authentication (PPA). As described earlier for login purpose this authentication factor requires the processing of predefined formula by the users. It uses a graphical pad comprising 10 graphical boxes, each having a combination of symbols and numbers used in the authentication process, as shown in Fig. 2. Each graphical box in the graphical pad has 10 symbols representing numbers from 1 to 10. The user after calculating two digits of the process-code to get the pass-code will draw a pattern from one graphical box to another having the user's symbol and the pass-code digit. During registration, user's selected numbers is referred to as R-code (Registration code), and the server's given along with mathematical operation symbol to the user for processing along the R-code is referred to as P-code (Process-code), whereas the resulting password is referred to as Pass-code.

The PPA comprises three components, i.e., the P-code Indicator, Pattern Checker, and Feature Extraction and Evaluation. The P-code Indicator displays two random numbers between 1 and 5 along with two alphabets for the addition and subtraction operations, which will appear every time during user authentication. The communications between user and authentication system is secured by Secure Socket Layer Protocol (SSL) [28]. After processing, the user will get two numbers and draw a pattern connecting two graphical boxes (having its symbol and the resulting Pass-code digits) in the graphical pad. The pattern checker module checks the validity of the drawn pattern by the user. The pattern checker authenticates users on the condition that if the outcomes of the arithmetic operation between the R-code and P-code is accurately in position with the resultant pattern drawn by users. Once a user draws the pattern and finds it correct by the Pattern Checker, meanwhile by using machine learning model the pattern drawing behavior of user is examined. The PPA was installed on the user android smartphones, where the users

were asked to use the PPA authentication pattern lock system around 30 to 40 times to obtain the training samples. A total of 29008 pattern samples were obtained from 35 users. The PPA has two phases, registration and authentication, subsections coming next provide description about the phases.

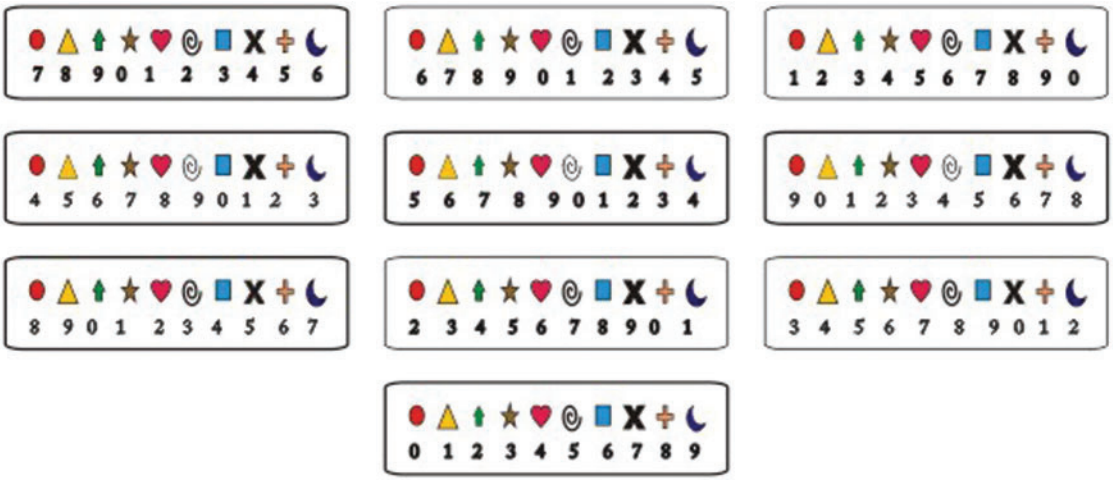

Figure 2: Graphical pad interface PPA

3.1 Phase of Registration

In registration phase, following steps are performed by the user in a sequence:

- Chooses a username
- Selects a symbol (from the given sets of symbols)
- Selects an R-code (minimum of 2 digits)
- Once the three required credentials are selected, the registration phase concludes

A user inputs three things in the registration phase, i.e., username, symbol, and R-code. The server will keep the user R-code and symbol information against the username. Let us suppose that Ali is the user name and the triangle is the symbol. Let the R-codes chosen by the user are 7 and 6. The user will click on the box that has 7 triangles, as shown in Fig. 3. The same will be done for the second number 6. When the user sees the pairing of his/her chosen symbol and the R-code digit, he/she can click anywhere in that box, which makes it nearly impossible for a shoulder surfer to guess any one of them.

3.2 Authentication Phase

The steps for the authentication process are as follows.

- User enters his/her username.
- Graphical pad appears on the screen having different boxes with symbols and numbers.
- P-code Indicator will display two random numbers between 1–5 along with two alphabets either ‘U’ or ‘R’. ‘U’ represents the addition and R means the subtraction.
- User will add or subtract the P-code digits given by the server taken from the R-code to generate the two Pass-code digits.

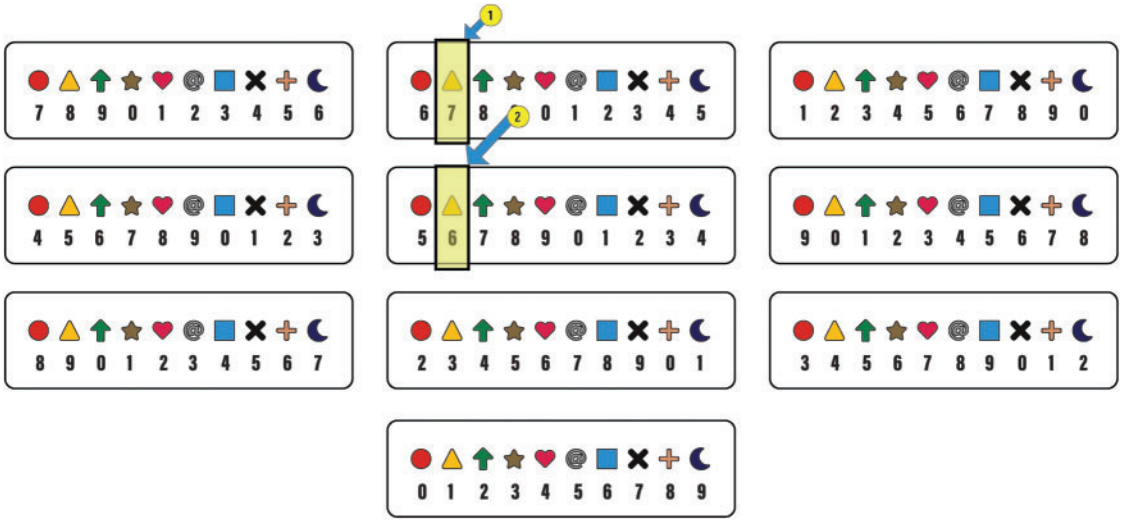

Figure 3: Registration example

- User will draw the pattern between those specific boxes in the graphical pad that have resultant Pass-code digits under the registered symbol.

Suppose a user's R-codes are 1 and 4 and the symbol is a triangle. When he/she enters the username for authentication, the P-code Indicator will show the two process code digits to be added or subtracted from the two R-code digits. Let us suppose the first process code for the first R-code digit 5U, i.e., add 1 with 5, and the second process code for the second R-code digit is 2R, i.e., subtract 2 from 4. The resulting Pass-code digits are 6 and 2. The user will draw a pattern by connecting the nodes of two graphical boxes that have 6 and 2 written below the triangle symbol, as shown in Fig. 4.

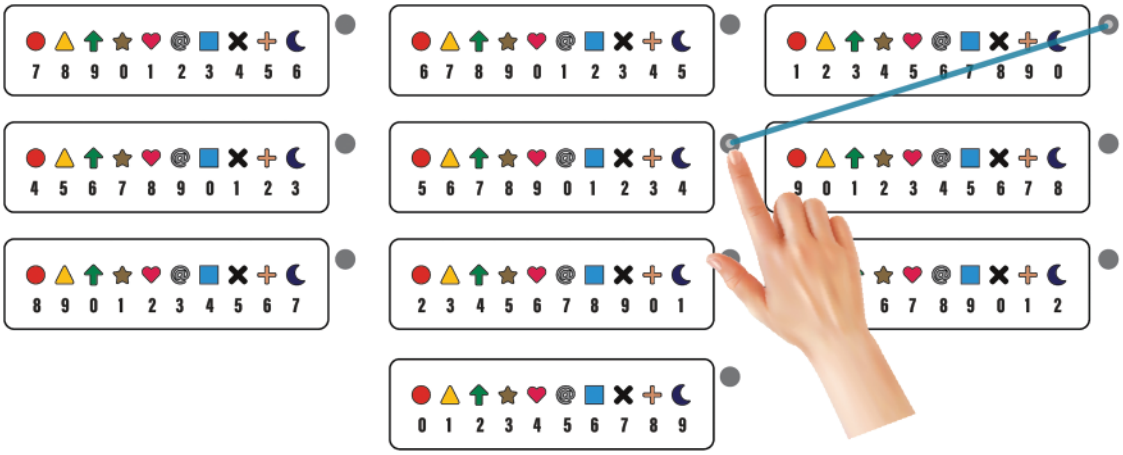

Figure 4: Login example

4 Feature Extraction

The PPA is a two-factor authentication technique, i.e., firstly authenticates the user according to the values drawn as a pattern, and secondly how he/she draws the pattern. Latest smartphones have numerous installed sensors that are built-in them wherefrom the desirable sensor(s) is selected that is capable of representing behavioral characteristics of the user, while the PPA pattern is being drawn. A collection of smartphone sensors that have been used in various researches [29,30] is shown in Tab. 1.

Table 1: Embedded smartphone sensors

Name of the sensor	Functionality
Linear Accelerometer	Computes the force of acceleration applied on the smartphone except force of gravity.
Accelerometer	Computes the force of acceleration applied on the smartphone including force of gravity.
Magnetometer	Computes the geomagnetic ambient field on three axes (x, y, z).

The installation of PPA was done on the participants mobile phones who were asked to unlock a device using the pattern of PPA. After accomplishing successful log-in of the user that formulated on his PPA pattern input, later on the information is saved regarding the drawing of pattern by the user that is collected using the touch sensors in the form of training sample; else, rejection for the drawn pattern. The pattern authentication can appear being a classification issue.1 and 0 are marked as Legal users and illegitimate users respectively. SVM, Random Forest, and Neural Networks have been introduced by several research studies as classification algorithms [31,32] to solve the classification problems. The proposed scheme for two-class classification chose to consider Artificial Neural Network. The analysis of neural network simulations in biological neural networks highly inspire the mathematical model related to artificial neural network (ANN). Like human brains, the ANN strives to construct the way for the quick processing of data. Tab. 2 lists various features derived from touch and sensors of the user's smartphone while using the PPA authentication system.

An overview of the PPA is shown in Fig. 5. Two components make up the system. The smartphone is installed on PPA. Using the PPA technique when the pattern is drawn by the user (see Fig. 5a), the Pattern checker module checks if the pattern is right (see Fig. 5b), then it switches to the next level (i.e., Fig. 5c) of the user's authentication algorithm.

Table 2: The set of extracted features

Feature symbol	Feature name
T_{dr}	Time between touch down and release of pattern nodes
T_{ap}	Average touch pressure while drawing the PPA pattern
M_{xp}	Maximum touch pressure while drawing the PPA
M_{np}	Minimum touch pressure while drawing the PPA
S_{ss}	Speed of finger sliding between PPA nodes
S_{sa}	Angle of finger sliding between PPA nodes
Avg_{ax}	Each sensor's average x value
Avg_{ay}	Each sensor's average y value
Std_p	Touch pressure's standard deviation

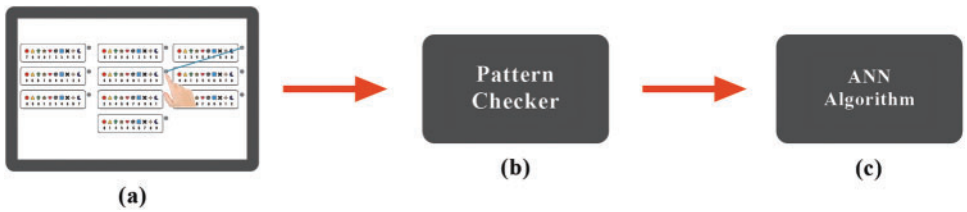

Figure 5: Three stages of PPA (a) smartphone login screen (b) pattern checker module (c) user authentication algorithm

4.1 Initialize Setting

The neural network is constructed in this step by specifying the design of the network (input units, output units). Features that are extracted from the touch and sensors of smartphone are utilized in training the neural network.

4.2 Training Set Generation

The quality of learning is considered essential for the neural network, as it's providing the capability to the network in order to address the changes in the environment. For this objective numerous learning algorithms were developed. On the basis of the features (listed in Tab. 2) gathered from various users, ANN is trained, the data that is gathered is used as training data and la-belled as valid users (1).

4.3 Creation of Neural Network

In this stage, a multi-layer network that contains multiple hidden layers is fed with the training set created from the previous phase. The direction of flow of the data is always forward because it always flows from input layer to output layer.

4.4 Network Initialization

This phase stipulates the accessible weights using an equation of weighting on every connection: $w(t+1) = w(t) + \mu\Omega w(t)$. Both the weights $w(t+1)$ and $t+1$ are equivalent as the learning rate times measured change in the weight.

4.5 Training Process

To get the desired output, for the purpose of input dealing, training the network is must. For network training, several kinds of learning algorithms are used in the literature. The kinds may categorize into two algorithms, i.e., supervised and unsupervised. In supervised algorithms, the network training is done by provision of training examples that include the matching of patterns (input to output). In unsupervised learning algorithms, the training of the network is done first then features are gained from internal data. Some reinforcement algorithms are also used that combine both supervised and unsupervised techniques, wherein the weights for the network are raised or reduced for honor or penalty [33]. A popular method for training artificial neural network is the back-propagation algorithm [34]. As a supervised learning algorithm it is beneficial for feed-forward networks. It is possible to implement the back-propagation algorithm in two phases, i.e., forward and backward pass. The addition of input to the neural network in the forward pass and is propagated to measure the output through all neurons in the layers. The error determination for each output neuron is done in the last step. The concealed weights among neurons are modified in the backward pass. The hidden layer errors for neurons are measured and returned to the neurons. In this study, by finding convolution of inputs with their corresponding weights, the net inputs are determined. The outputs are defined by applying the net output activation function. To classify the succession among the activation value (zero and one) logistic function is being utilized. The activation value is assumed to be the same as the input layer's output. The anticipated output is determined in the way that: comparing all the with the values that were saved, the desired output value becomes '1' in the case of equality, and it stays as '0' otherwise (see Fig. 6).

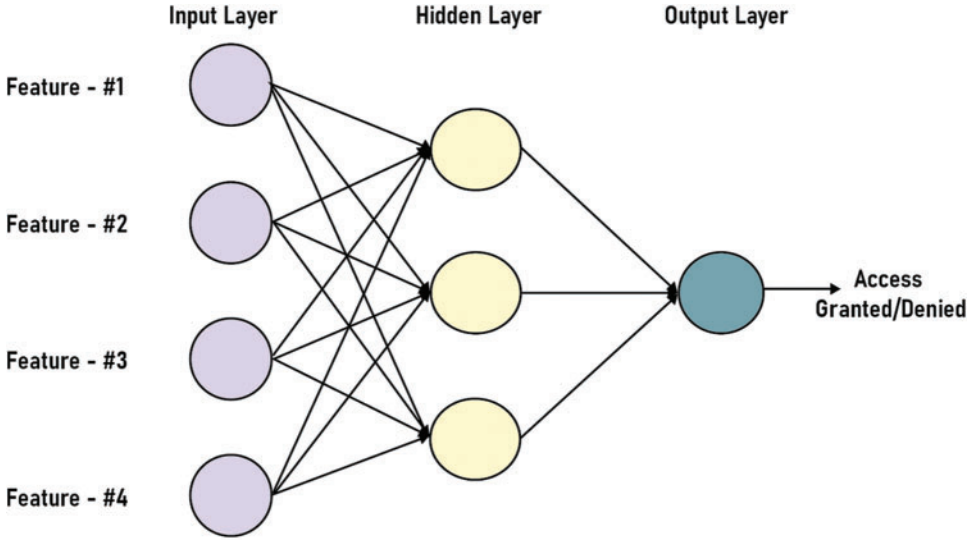

Figure 6: Structure of ANN

The prediction method for errors is carried out as follows:

$$O_{e\gamma} = D_0 p - N_0 p \tag{1}$$

where $O_{e\gamma}$ is the error of the output layer, D_0p represents desired output, and N_0p is the output of the network. Backward pass input layer errors are calculated as:

$$I_{e_\gamma} = Iw - O_{e\gamma} \tag{2}$$

where I_{e_γ} represents the input layer, Iw is the weight of the input layer and $O_{e\gamma}$ is the output layer error. The input and hidden layers' weights are modified in a sequence. The computed errors are measured in contradiction of the preset error value that changes the algorithm of the back propagation. Following is the Mean Square Error (MSE) function:

$$MSE = \frac{(Do_P - N_0p)^2}{2} \tag{3}$$

where N_0p is the network output and Do_P is the desired output. In case the error exceeds the highest acceptable value or if the network is fully trained and the error value is zero, the algorithm stops.

4.6 Recognition Process

After finalizing the training process, the network becomes ready for the process of behavior recognition. For calculating the final values of the output layer, maximum percentage value of same layer is extracted. For instance, if the percentage is 15, then this indicates that the behavior while drawing the pattern is original at 15% and not identical at 85%.

5 Experimental Results

To evaluate the viability of the projected system, a thorough user study was conducted. Data from 25 volunteers were collected. For the evaluation of predictive output, the ANN classifier is trained consuming the test data set. Total 30 students from University of Haripur (12 females and 16 males) voluntarily participated in this study. The presentation with animations was given to them to explain the concept of the proposed authentication system. The participants created their accounts after choosing their required credentials of the registration phase. They were asked to get login into their smartphones using the proposed system. The false reject rate (FRR) and false accept rate (FAR) are the significant parameters regarding the performance for mobile-based behavior authentication systems. The FRR recognizes and denies mobile phone access to authorized users as unauthorized users (Eq. (4)), where the FAR treats unauthorized users as authorized ones (Eq. (5)). This paper analyzes the proposed authentication system for both efficiency and accuracy.

$$FRR = \frac{No.\ of\ authorized\ user\ access\ denied}{No.\ of\ login\ attempts\ by\ authorized\ users} \tag{4}$$

$$FAR = \frac{No.\ of\ unauthorized\ access\ approvals}{No.\ of\ login\ attempts\ by\ unothorized\ user} \tag{5}$$

The outcomes indicate the FAR 4.36 and FRR 5.03. The accuracy of classification, i.e., ratio of correctly classified instances, can be determined by the following equation.

$$Classification\ accuracy = \frac{True\ positive + True\ negative}{Total\ instances} \tag{6}$$

The accuracy in the example is 0.75% and the error rate is 0.25%. Thus, a high percentage of instances can be correctly labelled by the model.

6 Comparative Analysis

In this section, the proposed authentication system has been evaluated against different known attacks. Furthermore, a comparative analysis of the proposed authentication scheme has been presented with the existing authentication schemes.

6.1 Shoulder Surfing & Smudge Attacks

Shoulder surfing being a real threat to authentication systems is of two types, i.e., weak and strong shoulder surfing attacks. In the first one, an attacker directly observes the authentication mechanism, whereas in the latter one, the attacker uses any hardware device, i.e., recording camera [35]. Textual passwords are slightly unprotected and are easily attackable that's why they are considered to be the weakest link in authentication chain [36,37]. In the proposed authentication scheme by using small arithmetic operations (addition and subtraction) a user draws a unique pattern on every login session and thus makes it challenging for the attacker (shoulder surfer) to capture. If the shoulder surfers try to authenticate, a new P-code indicator will be shown at the screen and she/he will not be able to process the Pass-code without the R-code digits. If the attacker captures the user's pattern via the camera, the P-code indicator will be different in the next login session. The participants were divided into two groups, 16 of them acted as the attackers (shoulder surfer and smudge attacks) and 14 acted as users. The attackers were fully prepared regarding the two attacks. In the video or by looking over the user's back, the attackers need to notice the user's P-code indicator and hand movement. When drawing the authentication pattern to conduct skilled attacks, in practicing the user's behavior the attackers can watch the videos as much as possible to. A total of 1650 samples were used for the test set. An attacker first has to assume the values of R-code to process with the server given P-code indicator values. Even if the user knows the values and patterns still there is a need of drawing the resultant pattern in accordance with the behavior of the user. The outcomes indicate that when the PPA pattern is drawn by the attacker, in the sitting position, the attack's success rate was 3%, while in walking, the shoulder surfing and smudge attack are not possible.

6.2 Comparison

Tab. 3 presents the proposed work's comparison with the projects using ANN in different ways to provide security for smartphones' authentication. The findings describe their proposed work. This article proposed a method that provides the security in the registration phase and a multi-factor security in the authentication phase.

The proposed technique is time consuming in the beginning. By the time, users get familiar with the technique, which is then results in less time consumption. The techniques which are easy to use and are less time consuming are vulnerable to different attacks. Our proposed scheme has two line of defense, i.e., the P-code will be different on every login attempt, hence a new pattern will be drawn by the user on every login, and secondly the behavioral features properties of every user. Tab. 4 shows the fastest, slowest and average login time taken by the participants.

Table 3: Related work comparison

Reference	Algorithm	Registration security	Findings	Average login time	Constraint
[20]	ANFIS	No	The ANFIS produces the lowest error rate	12.3 s	The proposed architecture considers limited of features
[21]	ANN-LMNN	No	In both optimization and authentication, ANN-LMNN provides better efficiency	7.3 s	The ANN has the chance of being stuck in the local minima
[22]	ANN-BPNN	No	The ANN gives better results than other classifiers	6.3 s	The proposed research could not alleviate the password complexity of the system's protection and usability.
[25]	ConvNe	Yes	ConvNet has the highest accuracy in predicting the behavior's action of the user than the compared algorithms.	6.03 s	To get the many-features-hierarchy, the CovNet contains too many layers
Proposed PPA scheme	ANN	Yes	Two factor authentications using ANN for behavior features	5.8 s	User joins only two nodes for authentication

Table 4: Login time

Login	Average time
Fastest login	5.8 s
Slowest login	12.37 s
Average	8.23 s
After 5 logins	6.02 s
After 15 logins	5.03 s

7 Conclusion

With the growing tendency of network services and applications, users can access such applications through various IoT gadgets. Therefore, as to ensure users digital property, there is need of validation each time they attempt to reach their personal data or accounts. Textual passwords or PIN methods are commonly used by most of the users to be authenticated. People use small passwords because complex passwords are not easy to remember or they even use one password for various accounts. Thus, attackers can easily guess the passwords. Some of those attacks do not require any special technique or software, e.g., shoulder surfing and smudge attacks, to steal information. Graphical passwords are more secure than the textual ones and are difficult to crack. The graphical authentication system is more user friendly and removes the difficulty of remembering complex passwords. Cracking the graphical passwords through guessing is so

challenging for the attacker, dictionary or brute force attacks. The proposed authentication scheme combines the behavior authentication and "something you process" authentication factors in a graphical box. It has two lines of defense, i.e., a unique pattern indicator, which shows a different value to the user at every login attempt, and a pattern checker that verifies the pattern correctly. Later, it authenticates users on the basis of touch behavior features. For authentication purpose, the sequence of position is not considered in the proposed method. The future work can include physiological and moving sensors for user identification in the IoT environment.

Funding Statement: This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Cyber Security.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Thavalengal and P. Corcoran, "User authentication on smartphones: Focusing on iris biometrics," *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 87–93, 2016.

[2] F. Masood, A. Almogren, A. Abbas, H. A. Khattak, I. U. Din *et al.,* "Spammer detection and fake user identification on social networks," *IEEE Access*, vol. 7, pp. 68140–68152, 2019.

[3] K. Gilhooly, "Biometrics: Getting back to business," *Computerworld*, vol. 9, pp. 4, 2005.

[4] S. Azad, M. Rahman, M. N. Ranak, B. K. Ruhee, N. N. Nisa *et al.,* "Vap code: A secure graphical password for smart devices," *Computers & Electrical Engineering*, vol. 59, no. 7, pp. 99–109, 2017.

[5] S. S. Ul Hasan, A. Ghani, M. Bilal and A. Jolfaei, "Multi-Factor pattern implicit authentication," *IEEE Consumer Electronics Magazine*, early access, pp. 1, 2021.

[6] J. K. Han, X. Bi, H. Kim and S. S. Woo, "PassTag: A graphical textual hybrid fallback authentication system," in *Proc. of 15th ACM Asia Conf. on Computer and Communication Security*, Taipei Taiwan, pp. 60–72, 2020.

[7] G. C. Yang, "Passpositions: A secure and user-friendly graphical password scheme," in *IEEE 4th Int. Conf. on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Indonesia, pp. 1–5, 2017.

[8] S. S. Hasan, S. Ullah, S. Afzal, M. A. Khan, M. A. Khan *et al.,* "Servers voice graphical authentication," in *IEEE 12th Int. Conf. on Fuzzy Systems and Knowledge Discovery*, Zhangjiajie, China, pp. 2582–2586, 2015.

[9] A. De Luca, A. Hang, F. Brudy, C. Linder, H. Hussmann *et al.,* "Touch me once and I know its you! Implicit authentication based on touch screen patterns," in *Proc. of SIGCHI Conf. on Human Factors in Computing Systems*, Austin, Texas, USA, pp. 987–996, 2012.

[10] C. Baadte and B. Meinhardt-Injac, "The picture superiority effect in associative memory: A developmental study," *British Journal of Developmental Psychology*, vol. 37, no. 3, pp. 382–395, 2019.

[11] S. A. Kumar, R. Ramya, R. Rashika and R. Renu, "A survey on graphical authentication system resisting shoulder surfing attack," in *Advances in Artificial Intelligence and Data Engineering*, vol. 1133. Springer, pp. 761–770, 2021.

[12] J. Zheng and S. K. Chigurupati, "M-pattern: A novel scheme for improving the security of android pattern unlock against smudge attacks," *ICT Express*, vol. 5, no. 3, pp. 192–195, 2019.

[13] M. Wazid, S. Zeadally and A. K. Das, "Mobile banking: Evolution and threats: Malware threats and security solutions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 56–60, 2019.

[14] Y. Sun, Q. Gao, X. Du and Z. Gu, "Smartphone user authentication based on holding position and touch-typing biometrics," *Computers, Materials Continua*, vol. 61, no. 3, pp. 1365–1375, 2019.

[15] S. S. H. Naqvi and S. Afzal, "Operation code authentication preventing shoulder surfing attacks," in *IEEE 3rd Int. Conf. on Computer Science and Information Technology*, Chengdu China, vol. 4, pp. 32–35, 2010.

[16] G. Shin, D. Kim, S. Kim and M. Han, "Unknown attack detection: Combining relabeling and hybrid intrusion detection," *Computer, Materials & Continua*, vol. 66, no. 3, pp. 3289–3303, 2021.

[17] M. Abuhamad, T. Abuhmed, D. Mohaisen and D. H. Nyang, "Autosen: Deep learning-based implicit continuous authentication using smartphone sensors," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5008–5020, 2020.

[18] M. Frank, R. Biedert, E. Ma, I. Martinovic and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2012.

[19] C. Bo, X. Y. Li Zhang, Q. Huang and Y. Wang, "Silentsense: Silent user identification via touch and movement behavioral biometrics," in *Proc. of 19th Annual Int. Conf. on Mobile Computing and Networks*, New York, pp. 187–190, 2013.

[20] O. Alpar, "Intelligent biometric pattern password authentication systems for touchscreens," *Expert Systems with Applications*, vol. 42, no. 17, pp. 6286–6294, 2015.

[21] O. Alpar and O. Krejcar, "Pattern password authentication based on touching location," in *Int. Conf. on Intelligent Data Engineering and Automated Learning*, Wroclaw, Poland, Springer, pp. 395–403, 2015.

[22] L. Zhou, Y. Kang, D. Zhang and J. Lai, "Harmonized authentication based on thump stroke dynamics on touch screen mobile phones," *Decision Support Systems*, vol. 92, pp. 14–24, 2016.

[23] P. Samangouei, V. M. Patel and R. Chelleppa, "Facial attributes for active authentication on mobile devices," *Image Vision Computing*, vol. 58, no. 2, pp. 181–192, 2017.

[24] M. E. ul Haq, M. A. Azam, U. Naeem, Y. Amin and J. Loo, "Continuous authentication of smartphone of smartphone users based on activity pattern recognition using passive mobile sensing," *Journal of Network and Computer Applications*, vol. 109, pp. 25–35, 2018.

[25] Y. Liang, Z. Cai, J. Yu, Q. Han and Y. Li, "Deep learning based interface of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, pp. 8–14, 2018.

[26] I. Olade, C. Fleming and H. Liang, "BioMove: Biometric user identification from human kinesiological movements for virtual reality systems," *Sensors*, vol. 20, no. 10, pp. 2944, 2020.

[27] A. A. Bello, H. Chiroma, A. Y. Gital, L. A. Gabralla, M. A. Shafii *et al.,* "Machine learning algorithms for improving security on touch screen devices: A survey, challenges and new perspectives," *Neural Computing and Applications*, vol. 32, no. 17, pp. 1–28, 2020.

[28] E. Mbunge and T. Rugube, "A robust and scalable four factor authentication architecture to enhance security for mobile online transaction," *International Journal of Scientific & Technology Research*, vol. 7, no. 3, pp. 139–143, 2018.

[29] Y. Ku, L. H. Park, S. Shin and T. Kwon, "Draw it as shown: Behavioral pattern lock for mobile user authentication," *IEEE Access*, vol. 7, pp. 69363–69378, 2019.

[30] A. Sagbas, S. Korukoglu and S. Balli, "Stress detection while keyboard typing behaviors by using smart phone sensors and machine learning techniques," *Journal of Medical Sciences*, vol. 44, no. 4, pp. 1–12, 2020.

[31] S. H. Ebenuwa, M. S. Sharif, M. Alazab and A. Al-Nemrat, "Variance ranking attributes selection techniques for binary classification problem in imbalance data," *IEEE Access*, vol. 7, pp. 24649–24666, 2019.

[32] J. Zhao, Q. Hu, G. Liu, X. Ma, F. Chen *et al.,* "Adversarial fingerprinting authentication for deep neural networks," *Computer Communications*, vol. 150, no. 7553, pp. 488–497, 2020.

[33] T. Hachaj and P. Mazurek, "Comparative analysis of supervised and un supervised approaches applied to large scale in the wild face verification," *Symmetry*, vol. 12, no. 11, pp. 1832, 2020.

[34] E. S. Alkronz, K. A. Moghayer, M. Meimeh, M. Gazzaz, B. S. Abu-Naseer *et al.,* "Prediction of whether mushroom is edible or poisonous using back-propogation neural network," *International Journal of Academic and Applied Research*, vol. 3, no. 2, pp. 1–8, 2019.

[35] M. Ali, A. Baloch, A. Waheed, M. Zareei, R. Manzoor *et al.,* "A simple and secure reformation-based password scheme," *IEEE Access*, vol. 9, pp. 11655–11674, 2021.

[36] H. M. Sun, S. T. Chen, J. H. Yeh and C. Y. Cheng, "A shoulder surfing resistant graphical authentication system," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 180–193, 2016.

[37] B. A. Azad, P. Laperdix and Nikiforakis, "Less is more: Quantifying the security benefits of debloating web applications," in *Proc. of 28th USENIX Security Symp.*, Santa Clara, USA, pp. 1697–1714, 2019.