Foundation University Journal of Engineering and Applied Sciences
Vol. 3, Issue 2, 2022.
DOI: 10.33897/fujeas.v3i2.690

Research Article

Behavioral Authentication for Smartphones backed by "Something you Process"

Nouman Imtiaz[1], Abdul Wahid[2], Syed Shabih Ul Hasan[3], Habib Akbar[3], Adeel Ahmed[3*]

[1]Shandong University, China
[2]Qingdao University, China
[3]Department of Information Technology, The University of Haripur, KPK, Pakistan
[*]Corresponding Author: Adeel Ahmed. Email: adeel@uoh.edu.pk

Abstract:

Authentication of smartphone devices has been never so important nowadays. Machine learning techniques are not far behind to touch the new milestones of the latest and ever updating world. However, totally depending on machine learning will give you the scenarios of false user being accepted as true one and a true user being rejected as the false one, which can be devastating in some cases. Fifth factor of authentication "Something You Process" eradicates most of the cases of the false acceptance and false rejection, if used with the mentioned techniques. The novel approach applied here is the fifth factor combined with machine learning system and Behavioral authentication. The fifth factor is anti-shoulder surfing since the arithmetic operation is hidden by hand placed on the screen. After placing hand on the screen in such a way that it hides the code from others, the system shows the arithmetic operation and the processed calculation is performed in user's mind. The pattern which is shown to the user is public, but machine learns the touch dynamics of the user along with his different postures including lying posture. The focus has been on the aspect of something that can be another layer or line of defense which can save the user's authentication process. It results in decrement of false acceptance or false rejection upon unlocking of a smartphone device. This study deals with the postures of standing, sitting, and lying. The data is collected and the features are extracted in all of these positions.

Keywords: Machine learning; Behavioral authentication; Smartphone devices; Smartphones; Pattern lock; Something you process; Shoulder surfing

1. Introduction

Human living standards have totally changed with the gadgets around them, amongst which the most impactful and life changing gadget is the smartphone. It has literally brought the whole world in our hand. The range of usage of smartphone is crossing the limits in all of the aspects of life. This importance also gives it a very huge responsibility of being safe and secure. The secure authentication of a mobile phone should be of the utmost value and strength which can pass the test of time from all types of threats and attacks. Nowadays various authentication methodologies are used by the smartphone users throughout the world which include passwords, PIN, biometrics and patterns. Every technique has its own advantages and disadvantages Bier, A, et al., (2017). Pattern techniques are very widely used in the smartphone users of different platforms.

Jose, T, et al., (2019) These techniques have been used and proposed since quite some time such as PassGo Tao, et al., (2008) and Graphical Password Design and Analysis Jermyn, A, et al., (1999) where the user registers and draws the graphical password for registration and authentication respectively. Any biometric-based authorization platform's core attribute is that the calculated qualities must be sufficiently unique to each person. Higher precision is associated with greater individuality or uniqueness. Morphological attributes are thought to be more identifiable for both validation and recognition, while behavior patterns are only thought to be completely different for verification Yampolskiy, R, et al., (2008).

Studies have shown that the smartphones users opt for using pattern rather than other techniques of authentication like PIN, passwords or other biometrics for unlocking their cellphones Andriotis, G, et al., (2016), Ye, G, et al., (2017). Biometric techniques are also becoming popular and its usage is getting more and more but still patterns are widely used and they are also used as the backup of the biometric authentication. User who is using the biometric technique has to register a pattern as well, in case of too many invalid entries of the biometric authentication. The percentage of pattern authentication users for unlocking smartphones is about 40% Van, B, et al., (2014). In short, the pattern lock is one of the most widely used methods for unlocking smartphones.

According to daily life observations and studies performed on the security analysis of the pattern lock, it is quite clear that these techniques are rather vulnerable to attacks like shoulder surfing and other different sorts. This has been one of the oldest problems in the human performed authentication that users tend to make a simpler pattern or password which is easy to remember but liable to be cracked, guessed or shoulder surfed. In terms of pattern lock, user mostly opts for a simpler pattern Ullenbeck, S, et al., (2013), Cha, S, et al., (2017) and leaves the patterns lines enabled for the shoulder surfer to easily see and know it in the first go.

In the different choices and procedures of authentication one of the emerging techniques is of Behavioral Authentication which is based on the behavior of the user. This technique has been strengthened with the upgrade of machine learning. The machine learns through the behavioral biometrics such as touch sensor dynamics and gait etc. Different machine learning categories are shown in Figure 1. These biometric behaviors are measured by different sensors which are present in the machine by default. Most of the time the touch dynamics which are recorded, need the user to draw a shape or a pattern on the screen of the smartphone. For the authentication to be accurate through behavior depends on the gesticulations and not all of them are suitable for authentication to be accurate for the legal user Song, Y, et al., (2015). The combination of behavior authentication with pattern has been an improvement in the aspect of security but along with the peak attack and other different attacks there is quite room for improvement. Along with the threats there has been another aspect which needs to be addressed which is the False Acceptance Rate and False Rejection Rate.

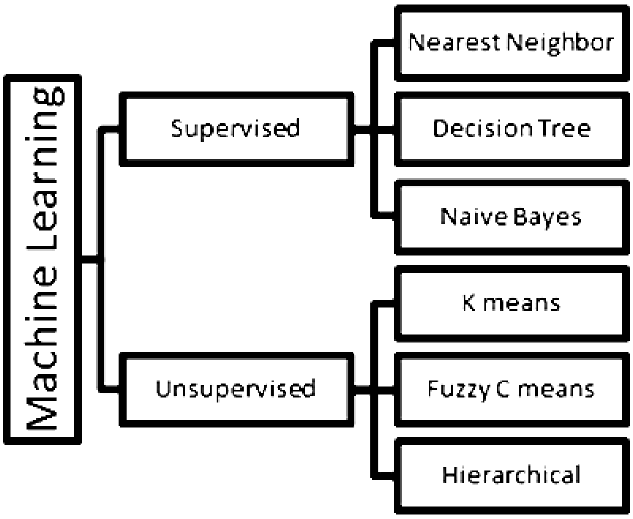


Figure 1: Machine learning categories

2. Background

There are millions of smartphones used all over the world and this number is increasing. Smartphones are not only used for just having calls or for messaging, but people are also carrying out their life activities like education, business, security, defense, awareness, socio political life, health etc. through them. It's obvious that there would be large amount of data of utmost importance which is to be secured through a strong authentication process. The machine-learning-based intelligent authentication approaches features in the multi-dimensional domain for achieving cost-effective, more reliable, and situation-aware device validation He, Fang, et al.

There are constant and real threats towards the authentication and unlocking of smartphones. These threats include Shoulder surfing attack, Phishing attack, Brute force attack, Guessing attack. Shoulder surfing is a type of attack where an adversary attempts to obtain sensitive information, such as passwords or PINs, by watching the victim enter it on their device. To perform shoulder surfing on a mobile device, an adversary may take the following steps:

1. Identify a potential target: The adversary may look for someone using their mobile device in a public place, such as a coffee shop or on public transportation.
2. Position themselves strategically: The adversary may position themselves behind or beside the target to get a clear view of the device screen while it is in use.
3. Observe the target's actions: The adversary may watch as the target enters sensitive information, such as a password or PIN.
4. Record the information: The adversary may use a camera or simply remember the information they observed to use later to access the device or sensitive information.

Behavioral Authentication is the technique which grants authentication through constant measure of behavior at the back of the biometric authentication system which will again put the burden on password or pattern system Aviv, J, et al., (2017), Khan, H, et al., (2018), Oakley, J, et al., (2018).

Biometric authentication involves analyzing physical or behavioral characteristics unique to an individual, such as their fingerprints, face, voice, or even their touch dynamics. For touch-based authentication, the system may capture data on how a user interacts with their device's touch screen, such as the pressure applied, the angle of touch, the duration of contact, and the frequency of taps. This data can then be used to create a unique profile for the user, which can be compared against future interactions to verify their identity.

2.1 Smartphone Pattern Lock

It is a graphical representation made by the user on the screen of the phone which makes a pattern by joining different points. Studies have shown that pattern is relatively more used than PIN or password Andriotis, G, et al., (2016), Ye, G, et al., (2017). Mostly it is a 3x3 setup resembling to the numbers from 1 to 9. A little bit more secure aspect of pattern is that if the user opts for the lines not to be shown. If it is shown, then the adversary can easily know the pattern by just giving a single peak. There are approximately close to 4 million possible patterns Aviv, J, et al., (2010), Cho, J, et al., (2017). Yeet al. (2018), which used an image processing algorithm to detect the fingertip activity on the video and is based on the security of android pattern lock. Zhou et al. (2018) converted sound waves as lock pattern using the defendant's device's speaker and microphone. Hong et al. (2015) presented a similar model which includes ten waving gestures for the process of authentication to be completed securely. The FAR and FRR of this system are 4% and 7% respectively.

Behavior Authentication – This mode of authentication relies upon the human behavior with the examples like touch dynamics, gait along with the postures and movement of the body. As smartphones have sensors present in them by default, so along with the touch screen this makes the behavior authentication practical.

2.2 Smartphone Authentication

The authentication mechanisms used commonly, have commonality of ease of use but can be compromised in threating scenario. Different types of authentication types are shown in Figure 2. PIN and passwords are notoriously set as weak which can be easily guessed, smudged or shoulder surfed. On the other hand, biometrics like fingerprint or face recognition are now regularly used but fingerprint recognition is unprotected against smudge attack Lee, H, et al., (2017). Face recognition gives problems with angles and lighting. There would always be another mode of authentication. The weaknesses shown in this mode of authentication are in terms of figure of the gesticulations Alpar, O, et al., (2017) and the False Acceptance and False Rejection cases. The proposed focuses on these grief weaknesses and aim to exterminate them by techniques like open pattern, operation hiding and something you process.

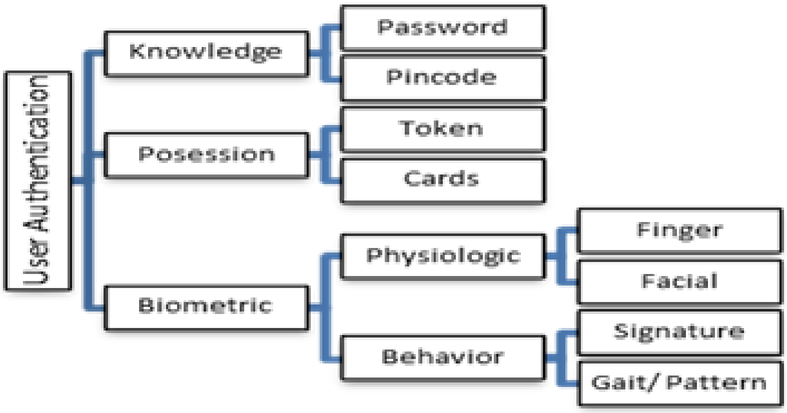


Figure 2: Type of authentications

The valuable aspect of uniting behavioral authentication with pattern is to get rid of gesture problems, memorizing problems. While operation hiding with hand will prevent shoulder surfing and lastly something you process will provide the solution of any false acceptance or rejection case. Signatures and forms have been the better recognized movements, and signals were immune to shoulder surfing attacks, according to the research Yangt, Y, et al., (2016). It is also studied that smartphone users seem to visit certain locations at specific times on certain days in a week. It was also known that smartphone users are most likely to call or email a known number rather than an unfamiliar number, implying that the smartphone phones are in their hands Jakobsson, M, et al., (2009).

3. Hazard Model

The scenario is assumed where the adversary is in proximity presumably familiar or unfamiliar person. In both cases adversary can pose a threat. Non expert threat of shoulder surfing can be performed by naked eye while sitting near to the user or in the other case when authentication process is recorded. In such cases adversary procuring the mobile can easily lead to unlocking of it, as the pattern can be easily learned through abovementioned techniques.

The adversary is also well acquainted of the error rates while performing Behavioral authentication and knows that there would be chance of false acceptance so can keep on attacking. Such educated attempts not just only watch the pattern but in the recorded shoulder surfing attack, the behavior can also be impersonated. Applying the proposed system, such hazards can be easily avoided. An internet poll of 260 people was performed to help evaluate their authorization actions. They discovered that only 42.7 percent of participants activated authorization on their smartphones, and that 57 percent of those who could not install authorization stated discomfort as a justification who doesn't use a lock feature.

Moreover, 46.8% of those who locked the smartphone partially or fully admitted that activating them would be inconvenient Harbach, M, et al., (2014).

Another experiment was conducted with 28 individuals so to achieve a deeper understanding of users' behaviors and reactions regarding smartphone security. In order to substantiate their conclusions, they performed an online survey of 2,518 smartphone consumers to augment their individual studies. According to the findings of the poll, 42% of participants said they won't lock the devices. Furthermore, 33.6 percent of those who did not secure their phones did so due to the reason they thought it was uncomfortable Egelman, S, et al., (2014).

4. Related Work

Y. Sheng et al. (2005) used Decision Tree which is a method that uses pattern recognition and is a type of' Learning by Example' procedure. The algorithm used in this system was for the purpose of granting authentication to the users on the basis of keystroke patterns. This system can be implemented on mobile internet of thing devices. This system proposes that the only corresponding Decision Tree cannot be able to resolve the grant of authentication through keystroke patterns. They performed training with 43 users and allowed each user to type common combination of string having 37 characters. In results, their study attained 9.62 % FRR and 0.88% FAR.

A. Buriro et al. (2019)opted for a system of authentication named AnswerAuth in which the data was captured through the sensors of the smartphone which are already present in it. These sensors extract features from that data collected by the sensors. They tested their AnswerAuth system with compilation of data of more than 10,000 patterns. Amongst these patterns there were 120 extracted from each sensor from participants which were 85 in number. The procedures used for classification were 6 that are Bayes, Naïve Bayes, kNN, random forest, SVM and J48. The results gathered from these were Random Forest with the top scores in aspect of True Acceptance rate which was close to 100 percent.

L. Fridman et al. (2015) for continuous authentication through multi modal decision fusion proposed this system and used the classification of Naïve Bayes. As it is on the basis of Bayesian Theorem, this system came up with the FAR of 0.004 and FRR of 0.01 and the timeline of the user authentication given, was of 30 seconds. Identifying the user with Behavioral characters has also been used and X. Wang et al. (2017) showed through their study about the recognizing of a user with his Behavioral features and characters. It was proposed for numerous devices which would recognize a particular user but will not pinpointing the user as to keep the user anonymous.

Mario Frank et al. (2013) in this study showed the application of Behavioral Biometric in order to attain authentication with the data gathered from the touchscreens. The analytics of touch screen were gathered from the features like median velocity, mean length, trajectory length, velocity, direction, duration, phone orientation and finger orientation. The results showed that the recognition of user through very restricted usage of touch screen is also conceivable. The rejection chance of legal user is 0-4% and it is similar in the false acceptance.

Shakir Ullah Shah et al. (2009) presented the new factor of authentication, which was something you process, the factors that were there before this one was "Something you Know" (Password, Pin code), "Something You are", "Something you have". This factor was the first which involved the process of processing to enter the password, Pin code or pattern. This technique is said to be one of the formidable against shoulder surfing attack. As this method ensures the password or pin code is random and keeps on changing with the condition of user's ease. Crouse et al. (2015) previously presented same algorithms of multi - factor authorization methods commonly incorporate facial expression and voice methods.

Gait is a technique for identifying individuals based on how user walks Derawi, M, et al., (2010), Mantyjarvi, J, et al., (2005). In a few of the pioneering approaches, used an elevated accelerometer attached to the individuals' belts at the back to test gait ways. Another gait-based authorization has recently been seen to work well on wrist wearing gadgets Cola, G, et al., (2016). It had a 2.9 percent ERR for 15 participants. Signature models demonstrate control of the ability users autograph with a stylus on smart phones. Among the first tries to create sign verification work on smartphone was by Narayanaswamy et al. (1999). They applied a mix of international and national characteristics. Signs' total spatial as well as temporal properties are captured by global characteristics.

Stroke and dimension pertaining functions make up the local characteristics. The database of 542 authentic and 325 fake signs, they obtained a 3 percent Equal Error Rate. There has been research in which approaches for authorizing clients dependent on the 3D sign formed in the space have also been proposed Ketabdar, H, et al., (2012), Ketabdar, H, et al., (2010). Sae-Bae et al. (2012) implemented a predetermined series of five-digit contact gestures and found that each recipient's touch gestures are unique (based on biometric qualities such as hand dimension and finger size). They evaluated their procedure and found that it was over 90% accurate, with high usable input from participants. Singh, Y, et al., (2012) combined the ECG data with facial and phalanges biometrics for authorization using revival-based rating combination. The equal error rate of the multifactor process was 0.22 percent, relative to 10.80 percent, 4.52 percent, and 2.12 percent for the ECG date, facial, and phalanges biometrics, respectively.

5. Proposed System

In this system the user must kick off the process of getting himself registered and acquainted with the mechanism. In order to get registered, the user has to enter his necessary credentials like username etc. after which the user will be shown a pattern which is to be drawn on the screen. The numbers at the nodes will guide user to draw the shown pattern. The user will keep on drawing same and other different patterns several times in order to let the system's mechanism recognize and extract the unique touch dynamics and features which user is having while drawing pattern. In the mean while the user would also be prompted to draw pattern in position like sitting, standing and walking. The sensors will extract and record uniquely recognizable data and features and save that with link to the user. This will be the information which device will learn along with the Behavioral changes. Figure 3 shows the proposed system with user registration and authentication.

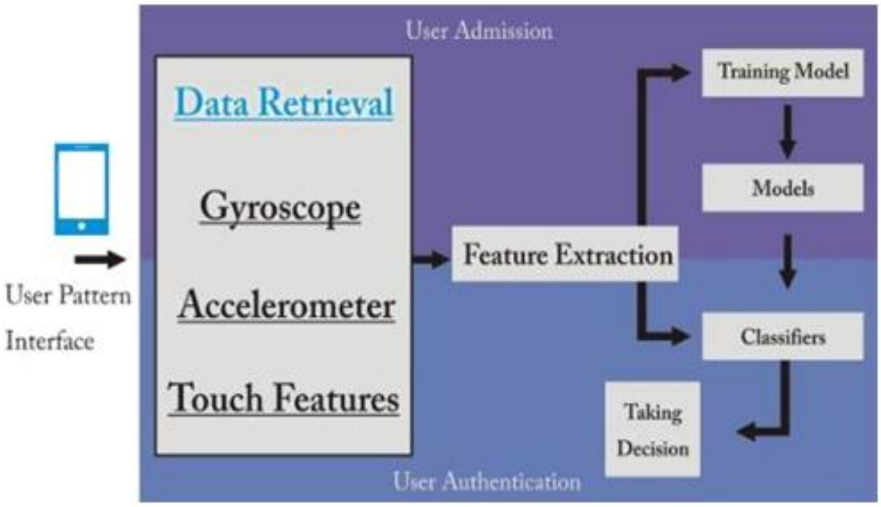


Figure 3: Overview of the proposed system with user registration & authentication

After letting the system know the unique touch dynamics and features of the user, the system will prompt user to put hand in the shape of the oval in the middle of the screen. This action allows the user to perform mathematical operation. After this action the system will show user a number and arithmetic sign of either addition or subtraction randomly. The user will be advised to do the suggested arithmetic operation of the given number with a number of user's choice so as to choose the Registration Number or R-Number. For example, the suggested S-Number with arithmetic operator is shown as +3. The user wants the Registration number to be 5. So, the result would be 8, which user later will use in the final combination of the pattern and this process number is named as the Pattern number or P-number. Figure 4 shows the snapshot of the pattern.

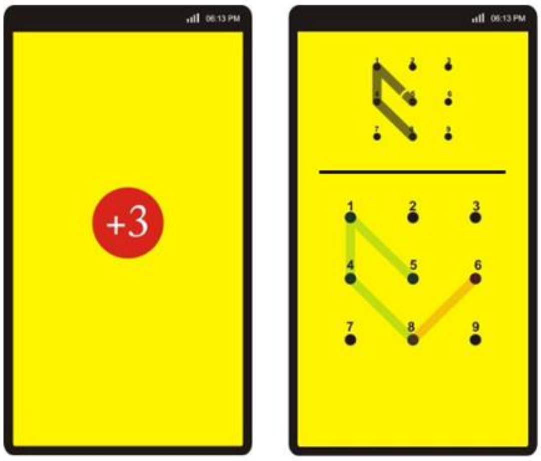


Figure 4: Pattern sample (top portion) Pattern made by user along with red line of the processed digit (bottom portion).

Due to the use of hand input on the screen, the R-number will never be shown to the adversary or any recording device nearby which records the process of registration. This method of concealing the R-number can be easily performed anywhere without the need of any special device or equipment. The P-number can result in negative, so the user has to just take the number into consideration if such case occurs, not the sign. This means the user always can subtract greater number from the lesser number which will always be an ease on the part of any user. Figure 5 shows authentication process.

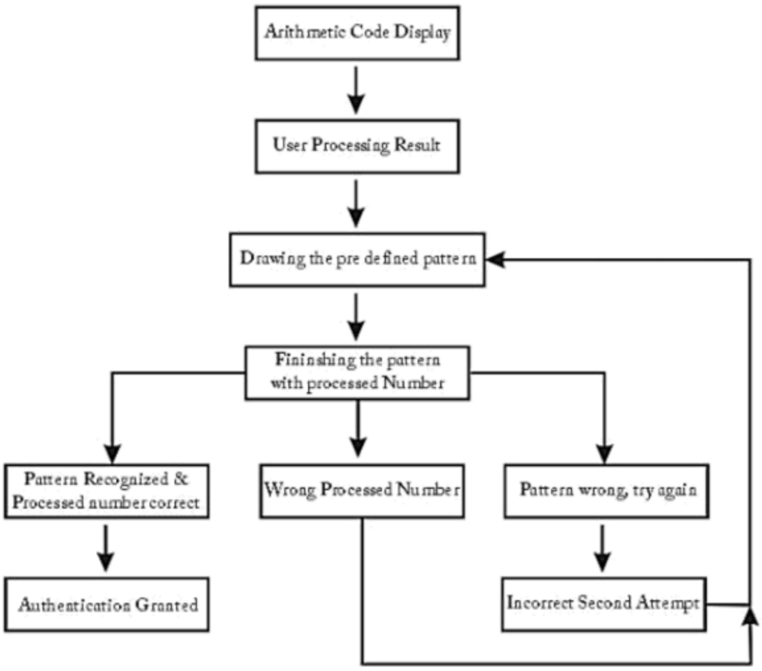


Figure 5: Diagram of login and registration process

For extraction of features while drawing pattern, the system uses the sensors which are present by default in the mobile phone. Most modern mobile phones have a range of sensors such as accelerometers, gyroscopes, and magnetometers. These sensors can be used to measure the movement and orientation of the phone in real-time. Table 1 shows touch proceedings which the corresponding sensors will be extracting while user draws the pattern.

Table 1: Touch events and their descriptions for feature extraction

Touch Proceedings	Description
amTP	Amount of Touch Proceedings of each section
avgTG	Touch Gravity average of each section
sdTG	Standard Deviation of Touch Gravity of each section
maxTG	Maximum Touch Gravity of each section
minTG	Minimum Touch Gravity of each section
avgTD	Average of Touch Dimension of each section
sdTD	Standard Deviation of Touch Dimension of each section
maxTD	Maximum Touch Dimension of each section
minTD	Minimum Touch Dimension of each section
avgSS	Average of Slide Speed of each section
stdSS	Standard Deviation of Slide Speed of each section
maxSS	Maximum Slide Speed of each section Minimum Slide Speed of each section
minSS	Slide Speed of each section from point A to point B

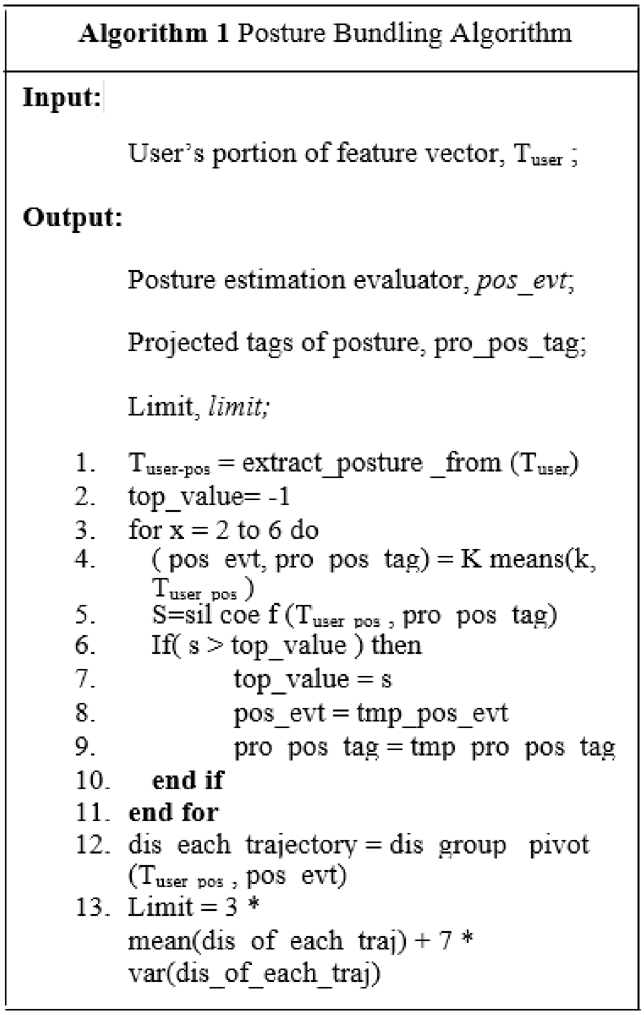
5.1 Algorithm

In order to grant user authentication using one of the aspects of the proposed system, Behavioral authentication pattern should be able to recognize the user's drawn pattern in a certain behavior or posture. For attaining this goal, the algorithm of Posture clustering or Posture bundling is used Rousseeuw, P. J, et al., (1987). This method has few steps in which the first one is that we use silhouette coefficient to get the value of the number of postures (K) along with K-means algorithm to get the posture predictor and projected tags of postures. Then we will be able to compute the threshold which will tell us that whether the posture of a feature trajectory belongs to an authorized user. Each user can normally have not that much of postures so similar postures can be bundles or clustered as a unit posture. Along with this method the threshold method is used which makes sure that the legal user's postures can be rightly recognized. The K bundles are renowned as the K posture of legal user. The detachments between all the trajectories are computed respectively.

Then their average and variance are calculated. This process is given by the Algorithm 1. Algorithm 2 on the other hand shows the pseudo code of SVM based classifier which takes the number of input vectors and output vectors into account along with the features and arrays, gives us the decision function outputs.

5.2 Pre-Processing

Before forwarding the original information to the classifier, it must be processed, sized, and normalized.



Algorithm 1 Posture Bundling Algorithm

```
Input:
        User's portion of feature vector, $T_{user}$ ;
Output:
        Posture estimation evaluator, pos_evt;
        Projected tags of posture, pro_pos_tag;
        Limit, limit;
$T_{user-pos}$ = extract_posture _from ($T_{user}$)
top_value= -1
for x = 2 to 6 do
    ( pos evt, pro pos tag) = K means(k, $T_{user\ pos}$ )
    S=sil coe f ($T_{user\ pos}$ , pro pos tag)
    If( s > top_value ) then
            top_value = s
            pos_evt = tmp_pos_evt
            pro pos tag = tmp pro pos tag
    end if
end for
dis each trajectory = dis group pivot ($T_{user\ pos}$ , pos evt)
Limit = 3 * mean(dis of each traj) + 7 * var(dis_of_each_traj)
```

The data is clearer during pre-processing. To obtain the necessary functionality, the pre-processing code is run on the entire raw data. The parts in the pre-processing procedure:

i. While deleting redundant timestamps from a certain account, the whole data will be displayed and ordered based on specific User IDs (UUID) and action timestamps.

ii. If the occurrence count is less than 2 attempts, use other instances under a particular threshold.

iii. If position data, such as latitude and longitude, is available, remove it. The raw data's variants and estimates are used to derive the functions.

iv. Locate contact activity records depending on the Button clicked and Action Type which is the pattern making touch features. The user is prone to making errors when entering the data. If a user makes the same error repeatedly, it is the user's typing habit. When estimating the right contact cases for a person, their perspective or behavior is taken into account.

v. For each button clicked and activity type case, create features from the raw information variables. The X and Y coordinate functions are derived from the distance formula through sensors of the smartphone. The derivatives are used to create the timestamps for the letters, and is shown in Table 2. Each letter has its own touch pressure and scale that correlates to a distinct attribute. The raw data was pre-processed, yielding 155 features for 25 consumers.

5.3 Feature Assortment

Feature Assortment, also known as variable or characteristic preference, is the process of selecting the

Table 2: Showing the last half of the data of the single user

		Touch	Touch	X-	Y-	X	Y	Action
Lat	Long	Pressure	Size	coordinate	coordinate	precision	precision	Timestamp
0	0	0.176589		105	1105	1	1	1615208011
0	0	0.176589		105	1105	1	1	1615208011
0	0	0.176589		125	1145	1	1	1615208011
0	0	0.176589		133	1098	1	1	1615208011
0	0	0.176589		197	645	1	1	1615208011
0	0	0.176589		344	654	1	1	1615208011
0	0	0.176589		525	755	1	1	1615208011
0	0	0.176589		224	811	1	1	1615208011
0	0	0.176589		88	1011	1	1	1615208011
0	0	0.176589		378	672	1	1	1615208011
0	0	0.176589		649	914	1	1	1615208011
0	0	0.176589		411	1149	1	1	1615208011
0	0	0.176589		289	788	1	1	1615208011
0	0	0.176589		344	951	1	1	1615208011
0	0	0.176589		186	917	1	1	1615208011
0	0	0.176589		78	816	1	1	1615208011
0	0	0.176589		307	873	1	1	1615208011
0	0	0.176589		68	1037	1	1	1615208011

most effective or important features for use in the classification algorithm. The data is minimized by overlooking unnecessary attributes, which reduces the model's runtime. It also improves performance indicators by focusing the classifier on the most important features. Feature selection can aid performance and minimize classification mistakes. It chooses a subset of the selected features to use in the classification model. There are three categories of feature selection algorithms, filtering procedure, wrapping procedure and embedding procedure.

5.4 Classification

The method of estimating a learning algorithm to map data points to output systems is called as classification. The mapping pattern defined as the model predicting the class for the dataset. Data points may be classified under one or greater classes whether they are re-valued or discreet. Multi-label classification strategies have several criteria that have to be configured as per the issue. The Python science kit library provides classification algorithms that can be adapted to the specific problem. The classification tools are developed in a classification class.

The authentication enactment of Behavioral authentication might rest on which classifier is performed and which blend of features is applied to the classifier. In this deference, we should be able to check which classifier and feature groups are operative in relations of user discernment. For the study that needed further experiments, we installed the system on a Samsung Galaxy S8 running Android OS. We used a Python-based machine learning library, to contrivance the six classifiers.

The classifier resilience impacts the time required to start deciding. This interpretation forms the different modules. For example, if only a few acts are needed to have an accurate classification, an attacker can be detected quicker and will do less harm. But for updating the device's security settings, it is possible to disable standard password protection in this situation. If the phone requires to track, say, an hour of use before classifying it, our suggested system might clearly support traditional security features and act as an identity verification system, triggering GPS, sending SMS, or locking the smartphone.

5.5 The Dataset

The dataset which we applied in our tests is defined as it contains values for all the attributes that reflect a user's behavior. As previous studies have shown and proved that touch features are different while user is performing it in different positions which make recognition of the legal user more accurate. The data is being exported as an Excel spreadsheet from a local database table. The database is Microsoft SQL, and the whole table can be exported as an Excel spreadsheet. Any person who contributed to the data analysis has an instance in the Excel file. To suit the classifier and forecast it using the test data, it is necessary to register the users and gather several specimens from them. Since certain users did not enter data during the whole data analysis, the number of cases for each user varies. Whenever the user clicks any button of the smartphone screen, a record in the database is made, and that person added in the database. If a user's number of samples is very small, it will be skipped in the preprocessing phase. Just 22 users are valid after pre-processing the dataset, which has 25 users who engaged in the data analysis. Clients for less than thirty occurrences are excluded from the study and are not used. There are 24 attributes in the raw data that can be used to classify a person. A total of 155 features are acquired during the feature extraction stage. While typing the password that appears on the phone, the occurrences are recorded. Daily, the user must launch the app and enter the code. The periods can be any duration, but the user must log in at least five times to input the password over the course of five days. The dataset across all clients is contained in an Excel file containing characteristics such as ID, Unique UserID (UUID), language, system model, SDK edition, make, pixel density, time zone, date time, country code, amount of CPU cores, country, location hemisphere, amplitude, button, touch force, touch density, action type, activity time stamp. To reflect all of the characteristics, the dataset was split into two pictures, as seen in the Tables 2 and 3.

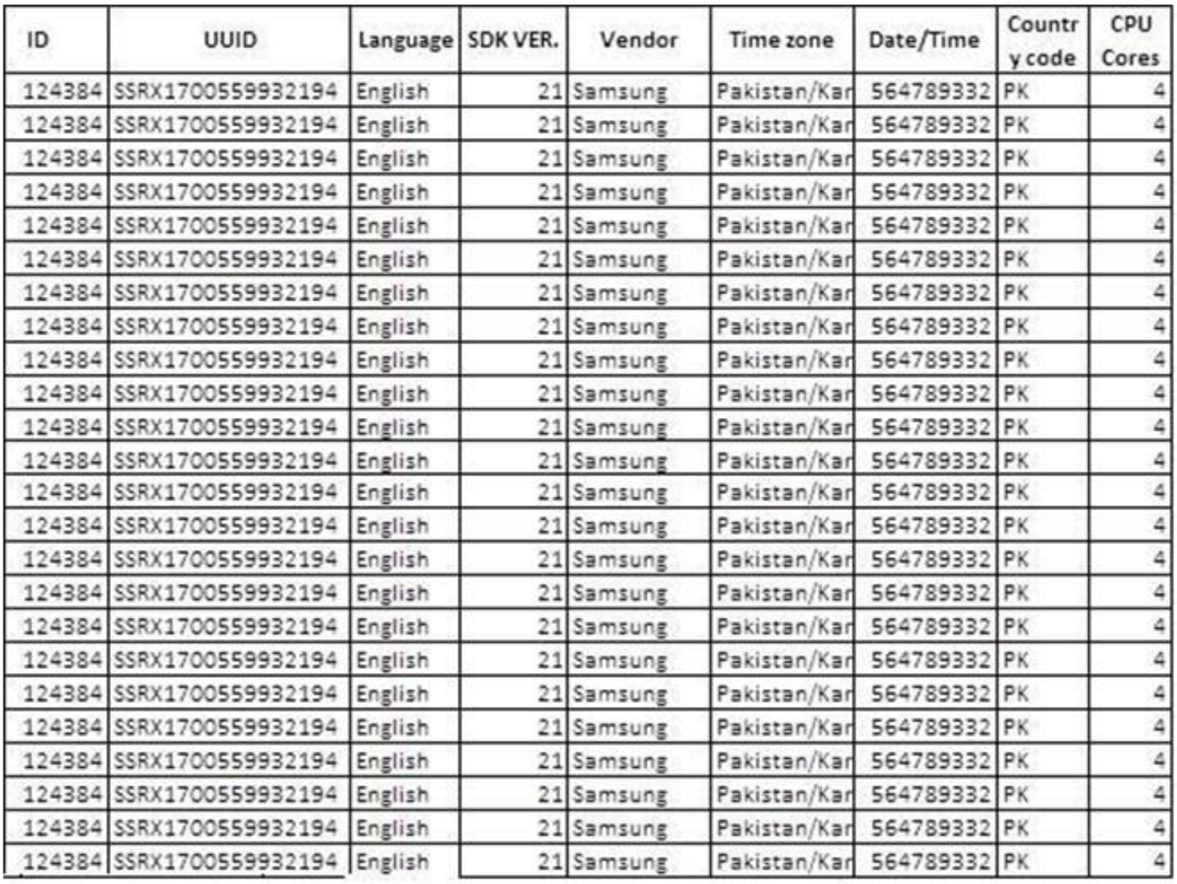
5.6 Feature Extraction and Classification

Classification is a machine learning technique for distinguishing and categorizing entities as they are identified. Classification is a form of supervised learning in which the training samples is named so that it can be correctly categorized, as per machine learning notation. Clustering, on the other side, is an unsupervised learning method in which the training set is unlabeled, and classification is done using a resemblance or difference scale. Classification is the method of identifying data points and determining which group of groups they apply to base on training samples. After selecting features, the system can provide better output metrics, lower generalization mistake, mitigate training time, mitigate over-fitting, and prevent the dimensionality burden. The algorithm conducts an extensive investigation throughout the room to locate a new function subset and ranks them using a scoring metric. The target is to lower the error rate and improve the classification system's accuracy. If the dataset is huge and has many functions, it is highly scalable. There are some types of feature selection techniques Krishnamoorthy, S, et al., (2018).

5.7 Extraction

To properly represent the data, it must first be converted into functions. The raw data includes the identifiers from which the functions must be created to show the input trends' distinct characteristics. It generates new capabilities to differentiate between clients and improve classification mechanism. The method for determining the features is determined by the dataset and specific issue. The classification model tests whether the produced framework fits a saved model that was produced once the client was

Table 3: Dataset for a single user displaying the first half of the information



ID	UUID	Language	SDK VER.	Vendor	Time zone	Date/Time	Country code	CPU Cores
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4
124384	SSRX1700559932194	English	21	Samsung	Pakistan/Kar	564789332	PK	4

recruited (training phase) into the method. The classification model then produces the final judgment based on the corresponding criterion. The people will be asked to reach the biometric technology if the ultimate verdict is yes. Alternatively, the user's authorization is refused. There are two kinds of biometric systems: identification and verification-based systems. In client authentication, a client's biometric is compared to other stored in the database to determine their identification. This is known as a 1-to-n match scheme, where n represents the number of clients in the database. For extraction of features while drawing pattern, the system uses the sensors which are present by default in the smartphone. Table 1 shows touch proceedings which the corresponding sensors will be extracting while user draws the pattern.

5.8 Posture Bundling

The features which are extracted and are of main significance are the ones which show the properties of time series like mean, variations, top and bottom numbers (n), assortment and span of time sequence (t). It also shows the features that show native properties of time sequence like initial position value (s_{init}), middle position value (s_{mid}), the relative location of maximum value ($s_{\max\_loc}$) and relative location of the minimum value ($s_{\min\_loc}$) along with usage of relative top location (i) and relative bottom location (j). Liu, Q, et al., (2016).

$$s_{init} = \frac{s_{t0} + s_{t1} + s_{t2}}{3}$$

$$s_{mid} = \frac{st_{\left[\frac{n}{2}-1\right]} + st_{\left[\frac{n}{2}\right]} + st_{\left[\frac{n}{2}+1\right]}}{3}$$

$$S_{end} = \frac{st_{[n-3]} + st_{[n-2]} + st_{[n-1]}}{3}$$

$$S_{\max\_loc} = \frac{i}{n}$$

$$S_{\min\_loc} = \frac{j}{n}$$

The features are extracted based on the postures as well as the touch dynamic features are also considered for a precise and unique extraction. The posture predictor and projected tags are the main features which will be able to calculate the threshold if the user's features match with the unique set already present.

6. Performance Assessment

These experiments and evaluation were done to get the accuracy of the system and different values and score of various classifiers in different postures like sitting, walking or lying. It was also checked that whenever the instance of false rejection or acceptance occurs then the tier of fourth factor stops that false assumption by the system.

6.1 Data Collection

To get the results, we performed experiments with 25 volunteers who participated without any charges. There were 17 male participants and 8 female participants who belonged to different fields and all of them were users of smartphones.

The proposed system was described to them along with the basic theme of work. All of them were provided by same model smartphone Samsung A50 with the proposed system installed and checked. They all were guided to make open patterns 25 times while sitting, walking, and lying. Mats and pillows were provided in the vicinity to perform the authentication while lying. We told the participants to use the smartphone and postures in a normal daily life way. A total of 3750 samples were acquired to perform experiments.

6.2 Top Performing Classifier

The result of the experiments while evaluating authentication through behavior depends upon the used classifier and the features which are used. The evaluation was done with the technique of one feature one time. Recursive feature elimination was applied to select the most suitable feature set for each classifier. This procedure was applied until the entire feature set became null. The procedure of selection of the feature set was done for six classifiers and three postures.

There are three postures along with the accuracy and F score. It can be seen from the table that the best performing classifier is GNB. It had the highest accuracy in the postures of sitting, walking, and lying**.** Figure 9 shows different postures feature set and their corresponding F-score.

6.3 Resultant Perentage (Rp) in Terms of EER

The proposed system contains two levels of percentages which combines and gives the resultant percentage. This resultant percentage can be derived by the concept of Percentage of a Percentage. To find this, first percentage P1 and the second percentage P2 both are divided by 100. These two results give us the derivatives which are then multiplied to give the Resultant Percentage Rp.

First Derivative (N1) = P1/100

Table 4: Touch events and their descriptions for feature extraction

Classifier	**Sitting**		**Walking**		**Lying**	
	Acc.	**F**	**Acc.**	**F**	**Acc.**	**F**
		Scor		**Scor**		**Scor**
		e		**e**		**e**
DT	**93.3**	**93.53**	**74.1**	**73.91**	**83.7**	**83.45**
	9		**2**		**6**	
SVM	**96.7**	**96.65**	**86.9**	**86.23**	**92.8**	**92.74**
	1		**4**		**8**	
KNN	**96.3**	**96.22**	**70.0**	**68.45**	**86.7**	**86.35**
	1		**1**		**9**	
GNB	**98.0**	**97.31**	**96.2**	**95.64**	**96.4**	**95.88**
	6		**2**		**2**	
RF	**96.8**	**96.45**	**91.7**	**90.77**	**95.5**	**94.09**
	5		**1**		**5**	
LR	**97.3**	**97.30**	**89.3**	**89.19**	**91.8**	**92.69**
	3		**4**		**8**	

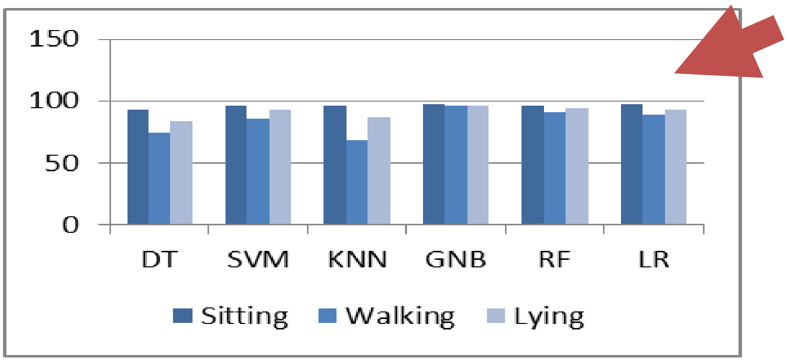


Figure 7: F-score of the three postures in different classifiers used

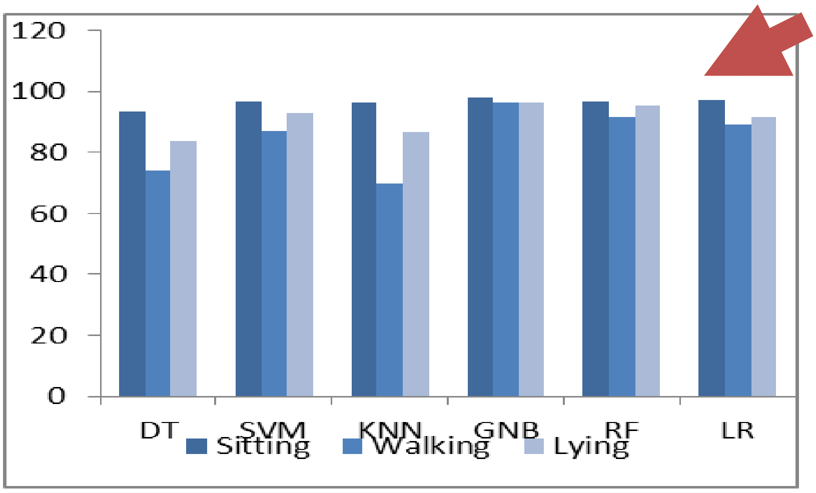


Figure 8: All of the classifiers accuracy in the three postures proposed in the system, i.e., Sitting, Walking, and Lying

Second Derivative (N2) = P2/100

Resultant Percentage (Rp) = N1 * N2

In this scenario the first percentage (P1) is EER and the second percentage (P2) is derived from the guessing chance of a number from the nine numbers of the grid while doing the arithmetic operation to get the processed result. As there are nine numbers so the guessing percentage would be found out using the following values.

P1= 3.5%

P2 = 1/9*100=11.11%

First Derivative (N1) = P1/100 = 3.5/100 = 0.035

Second Derivative (N2) = P2/100 = 11.11/100 = 0.11

Resultant Percentage (Rp) = N1 * N2

Resultant Percentage (Rp) = 0.035 * 0.11 = **0.0039%**

Table 5 shows comparison between the EER and Resultant Parentage between different technologies which clearly shows the marked difference between the EER scores and no change in the resultant percentage due to no other tier.

Table 5: Comparison between the EER and Resultant Parentage

Scheme	**EER**	**Resultant**	
		Exist	**%**
Proposed System	**3.50%**	**YES**	**0.0039%**
Shahzad et al. (2018)	**4.80%**	**No**	**4.80%**
Xu et al. (2014)	**10%**	**No**	**10%**
Sitova et al. (2015)	**7.16%**	**No**	**7.16%**
Alpar et al (2017)	**4.10%**	**No**	**4.10%**

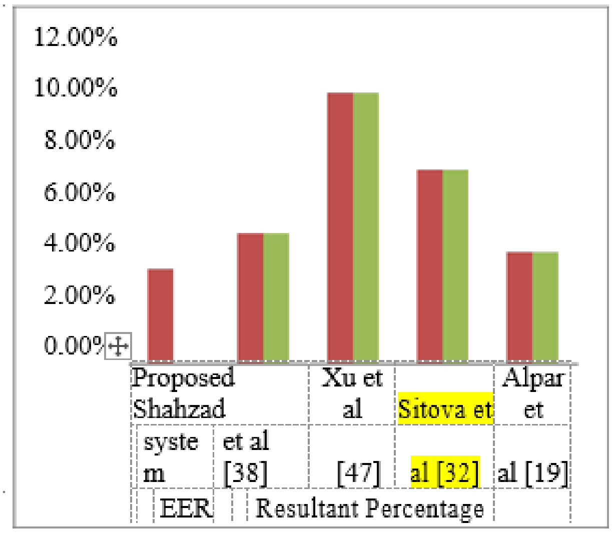


Figure 6: EER and Resultant Percentage of different systems with the proposed system with the only least Resultant Percentage

The graph shown in Figure 6 is from the very fact that values of the EER in a normal scenario are almost quite similar and there is not bigger difference amongst most of the systems. But when the resultant percentage criteria is applied then the EER decreases in the proposed system but others lack that change.

Table 6: This table compares and shows the availability of two technology's presence in different modern schemes along with the proposed one

Schemes	**Behavioral** Auth	**Something** you process	**Both**
Proposed system	Yes	Yes	Yes
Liu et al. (2016)	Yes	No	No
L. Lu et al. (2015)	Yes	No	No
Kayacık et al. (2014)	Yes	No	No
Shakir et al. (2009)	No	Yes	No

6.4 Evaluation

In Figure 6, it can be clearly seen that the resultant percentage is way less than other relevant methodologies. There is Shahzad et al. (2018) whose EER is 4.80 which in comparison to other systems is a good number but when another tier of defense is applied which others lack then there is a big difference significantly. Shahzad el al. (2018) mechanism was gesture based but along with other systems, they all lack the other layer, which can be acting as a part of the system but would add that extra edge and would be clearly shown in the numbers. The other schemes mentioned are based on touch and typing based respectively but have the same story. There were values of the schemes in sitting and walking postures, but we only considered lower one. Table 4 evidently specifies that modern system of authentication which use Behavioral authentication only are dependent on that particular scheme while the systems which used the factor, "Something you process" has not used it with Behavioral authentication.

7. Security Analysis

7.1 Against Shoulder Surfing

In this instance the 10 participants were given the task of being an attacker. While others were performing the authentication process, they attackers were allowed to peak from near or to record the session of the authentication. The attackers were fully guided on how to get maximum efficiency out of the authentication. These included postures, gait, arithmetic code, and processed result. Attackers were given the freedom of re-watching the video as many times as they want to get authentication. A total of 704 samples were used and free lunch was provided to the student who finds success in his attack. It was observed that none of the attacker was able to get authentication. The same experiment was performed without the usage of the 2nd tier of something you process. It was that time when there was success (3.7%) got by the attackers as shown in Table 7.

Another comparative experiment was done with simple pattern lock and the proposed system. The attackers were easily able to know the right pattern through peak and recording attack. The attacker success rate was 90 %.

7.2 Analysis of Usability

We assess our mechanism's usefulness in 2 aspects: by determining what other patterns are required to train the classifier to produce meaningful authentication precision, as well as using the basic System Usability Scale to collect user feedback on our possible framework. We also put effort to get the minimal sample collection time as shown in Table 8.

8. Discussion

8.1 Implications

While the thought process of most of the people would be that the pattern lock is getting outdated in this ever-growing era but there would be no two ways about it that it is one of the most used authentication processes till date. This system not only has used this well-known procedure but also has combined it with modern day machine learning mechanism. In addition, this has been backed up by the fourth factor.

Table 7: Three different entries showing success rate of shoulder surfing attack involving Pattern Entry

Scheme	Entry type	Shoulder Surfing
Proposed System	**With behavioral auth. And Something You Process**	**0.00%**
Pattern Entry 1	With Behavioral Authentication	3.5%
Pattern Entry 2	Without Behavioral Authentication	90%

This system has been made in such a way so that it can firstly identify the links between the patterns and their conciseness which are to be used in pattern recognition. Even till date the biometric sources of authentication like fingerprint is still backed up by pattern, pincode or password. Whenever in any mobile a user gets the authentication wrong using his fingerprint then the user is asked that he has exceeded the limit of invalid tries now the user has to enter the pattern or the password. This scenario makes the patterns and password very relevant and significant in today's modern ever evolving world.

Afterwards in the second stage the server generation of the number with arithmetic operation plays an important role to let user uses that only to comply the processing step. The pattern drawing system

Table 8: Sample collection timing comparison with proposed system and other system

System	Sample Collection time (s)
Proposed System	3.8
PIN	3.9
Password	8.01
Voice	5.35
Face	5.78
Gesture	8.11
Face + Voice	8.03
Gesture + Voice	10.11

grants user the opportunity to input the pattern as well as the final processed code. In this way the system not only makes this super easy for the user to just draw a pattern nonetheless protects this easy procedure. The system eases off the user by removing the burden of making and remembering difficult patterns and always trying to keep it away from close sitting people.

Machine learning based authentication is educating day by day but needs quite some input even after which there can be occasions where the scenario of False Acceptance or False rejection can occur. This problem which may look small, but it needs to be dealt with. The need of fourth factor of authentication is clearly awaited to seal and strengthen the security of the machine learning Behavioral authentication. It is to be anticipated that this system can eradicate the existing susceptibilities, which present parallel methods have. Many of the previous methodologies have admitted that there have been some insecure results which were obtained from their own experiments. This can be clearly observed that all of the systems are declaring that they are error resistant but not error free where our system provides that cushion for those instances. The contributions of the proposed system are as follows:

- There have been many systems proposed in the field of authentication but to the best of our knowledge, no one has ever proposed another tier of security when the instance of False Acceptance or False rejection has taken place in any of that system.
- As there is no system which claims to be having zero percent False Acceptance or Rejection rate so whenever that happens then there isn't any line of defense left afterwards. This much required layer is present in the proposed system.
- In this paper, we point out the abovementioned problems and propose a system which uses Behavioral authentication aided with machine learning and an additional tier of fourth factor of authentication namely "Something You Process".
- This system uses the open pattern lock system which would be visible to all as a sample which the user has to draw. There will be no need of making difficult patterns and remembering them every time.
- The system will be able to eradicate the threats of different attacks like shoulder surfing, guessing or smudge.
- The added layer of fourth factor will enable user to process the result of an arithmetic operation in his mind and then outputting it at the last of the pattern drawn. This will be the added wall of security whenever the scenario of False Acceptance or False rejection occurs.
- We give the probe of paramount classifiers for the proposed system which gives the better rates than other systems.

- Security assessment against different attacks were made including shoulder surfing attack with two different methods referred to as Peak attack and recording attack.
- The operation hiding technique through hand eradicates the shoulder surfing attacks while performing the method of "Something you Process".

8.2 Limitations and Future Work

No matter how much one can strive for perfection there would always be room for improvement and growth. The limitations which need improvement in future are that the experiments should be done even bigger scale with long term results and observations. The behavior features should be added with the added postures scenarios of using two hands and operating in different environment. There should also be a way that the user registration through features and classification should be done in as much less time as possible with minimum number of patterns. In this process the locking of phone can be problematic for which registration category should be introduced which either doesn't lock the phone or separate the data. Arithmetic processing by user can be little tiring for the mind which goes away with time and also can take few more seconds than other modes of authentication. This will be improved in the future study.

9. Conclusion

This system is recommended here Behavioral Authentication using something you Process, a unique addition to the pattern lock setup. We consider that this system with small additional step of fourth factor has given support to the vulnerabilities in the previous existing systems. The attack models which were applied on our system clearly showed the need for another layer of sanctuary in the post pattern security. The attack results clearly showed that usual pattern lock systems stand no chance in front of different attack models. Comparative study also enlightened the point that false acceptance or rejection occurs in machine learning based behavioral authentication. The system has strong approach stacking up three lines of defenses. Machine learning and Behavioral authentication in different postures along with the fourth factor of authentication can back up any smallest loopholes or errors in false acceptance or rejection.

References

A. Buriro, B. Crispo, and M. Conti. (2019). AnswerAuth: A bimodal Behavioral biometric based user authentication scheme for smartphones, *Journal of Information Security and Applications*, 89–103.

A. Bier, A. Kapczyński, and Z. Sroczyński. (2017). *Pattern lock evaluation framework for mobile devices: Human perception of the pattern strength measure*, in Proc. Int. Conf. Man–Mach. Interact, Cham, Switzerland: Springer.

Andriotis, G. Oikonomou, A. Mylonas, and T. Tryfonas. (2016). A study on usability and security features of the Android pattern lock screen, *Inf. Comput. Secur*., 53–72.

Cho, J. H. Huh, J. Cho, S. Oh, Y. Song, and H. Kim. (2017). *SysPal: System-guided pattern locks for Android,* in Proc. Symp. Secur. Privacy, 338–356.

Crouse, D., Han, H., Chandra, D., Barbello, B., Jain, A.K. (2015). *Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data*. IEEE.

G. Cola, M. Avvenuti, F. Musso and A. Vecchio. (2016). Gait-based authentication using a wrist worn device, *ACM MOBIQUITOUS*, 489-528.

H. Khan, U. Hengartner, and D. Vogel. (2018). *Evaluating attack and defense strategies for smartphone PIN shoulder surfing*, in Proc. CHI Conf. Hum. Factors Comput. Syst., 1–10.

H. Ketabdar, H. Moghadam, P. Naderi and B. Roshandel. (2012). Magnetic signatures in air for smartphone devices, *ACM Smartphone HCI*, 528-674.

H. Ketabdar, K. Y uksel,̈ A. Jahnbekam, A. Roshandel and M. Skripko. (2010). *Magisign: User identification/authentication: Based on 3D around device magnetic signatures*, Conference: UBICOMM, page 198-274.

H. Lee, S. Kim, and T. Kwon. (2017). *Here is your fingerprint!: Actual risk versus user perception of latent fingerprints and smudges remaining on smartphones*, in Process. 33rd Annual Computer Security, 512–527.

He Fang, Xianbin Wang, and Stefano Tomasin. (2019). Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks, *IEEE Wireless Communications*, 26(5), 55-61.

Hong, M. Wei, S. You, Y. Feng, and Z. Guo. (2015). *Waving authentication: your smartphone authenticate you on motion gesture,* In Proc. of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, 321-456.

J. Aviv, J. T. Davin, F. Wolf, and R. Kuber. (2017). *Towards baselines for shoulder surfing on mobile authentication*,'' in Proc. Annu. Comput. Secur. Appl. Conf. (ACSAC), 486–498.

J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. (2010). *Smudge attacks on smartphone touch screens*, in Proc. USENIX Conf. OffensiveTechnol. (WOOT), 1–7.

J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. Makela and S.M. Ailisto. (2005). *Identifying users of portable devices from gait pattern with accelerometers*, IEEE ICASSP, 88-211.

Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. (1999). *The design and analysis of graphical passwords*, in Proc. 8th USENIX Secur. Symp., 1–15.

José Torres, Sergio de los Santos. (2019). Efthimios Alepis, Constantinos Patsakis *Behavioral Biometric Authentication in Android Unlock Patterns through Machine Learning*, in Proc. ICISSP, 146-154.

Kayacık, M. Just, L. Baillie, D. Aspinall, and N. Micallef. (2014). *Data driven authentication: On the effectiveness of user behavior modeling with smartphone device sensors*, In Smartphone Security Technologies, 22-128.

L. Fridman, A. Stolerman, S. Acharya et al. (2015). Multi-modal decision fusion for continuous authentication, *Computers and Electrical Engineering*, 142–156.

L. Lu and Y. Liu. (2015). Safeguard: User re authentication on smartphones via Behavioral biometrics, *IEEE Transactions on Computational Social Systems*, 778-889.

Liu, Q., Wang, M., Zhao, P., Yan, C., & Ding, Z. (2016). *A Behavioral authentication method for mobile gesture against resilient user posture*. 3rd International Conference on Systems and Informatics (ICSAI).

M. Harbach, E. Von Zezschwitz, A. Fichtner, A. Luca, and M. Smith. (2014). *It's a hard lock life: A field study of smart-phone (un) locking behavior and risk perception*, In10th Symposium on Usable Privacy and Security, 834-967.

M. Jakobsson, E. Shi, P. Golle, and R. Chow. (2009). *Implicit authentication for smartphone devices*, In 4th Usenix Conference on Hot Topics in Security. Usenix Association, 141-253.

M. Shahzad, A. Liu and A. Samuel. (2013). *Secure unlocking of smartphone touch screen devices by simple gestures: you can see it but you cannot do it*, In 19th Annual International Conference on Smartphone Computing & Networking. ACM, 2241-2297.

M. Zhou, Q. Wang, J. Yang, Q. Li, F. Xiao, Z. Wang, and X. Chen. (2018). *PatternListener: Cracking Android pattern lock using acoustic signals*, In Proc. ACM SIGSAC Conf. Comput. Commun. Secur. 224-445.

M.O. Derawi, C. Nickel, P. Bours and C. Busch. (2010). *Unobtrusive user-authentication on smartphones using biometric gait recognition,* IEEE Intelligent Information Hiding and Multimedia Signal Processing, 573-694.

Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. (2013). *Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication*, IEEE Transactions on Information Forensics and Security.

N. Sae-Bae, N. Memon and K. Isbister. (2012). *Investigating multi-touch gestures as a novel biometric modality*, IEEE BTAS, 2245-2412.

O. Alpar. (2017). Frequency spectrograms for biometric keystroke authentication using neural network based classifier, *Knowledge-Based Syst.*,163–171.

Oakley, J. H. Huh, J. Cho, G. Cho, R. Islam, and H. Kim. (2018). *The personal identification chord: A four button authentication system for smart-watches*, in Proc. Asia Conf. Comput. Commun. Secur., 75–87.

P. J. Rousseeuw. (1987). Silhouettes: a graphical aid to the interpretation and validation of cluster analysis, *Journal of computational and applied mathematics*, 53–65.

R. V. Yampolskiy and V. Govindaraju. (2008). Behavioral biometrics: a survey and classification. International *Journal of Biometrics*, 81–113.

S. Cha, S. Kwag, H. Kim, and J. H. Huh. (2017). *Boosting the guessing attack performance on Android lock patterns with smudge attacks*, in Proc. Asia Conf. Comput. Commun. Secur. (ASIACCS), 313–326.

S. Egelman, S. Jain, R. Portnoff, K. Liao, S. Consolvo and David Wagner. (2014). *Are you ready to lock?* ACM SIGSAC Conference on Computer & Communications Security, ACM, 1047-1169.

S. Krishnamoorthy, S. Saad and L. Rueda. (2018). *Identification of User Behavioral Biometrics for Authentication using Keystroke Dynamics and Machine Learning*. ETD. 189-278.

S. Narayanaswamy, J. Hu and R. Kashi. (1999). User interface for a pcs smart phone, *IEEE Multimedia Computing and Systems*, 834-972.

S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz. (2013). *Quantifying the security of graphical passwords: The case of Android unlock patterns*, in Proc. Conf. Comput. Commun. Secur. (CCS), 161–172

Shakir Ullah Shah, Fazl-e-Hadi, Abid Ali Minhas. (2009). *New Factor of Authentication: Something You Process*, International Conference on Future Computer and Communication.

Tao and C. Adams. (2008). Pass-Go: A proposal to improve the usability of graphical passwords, *Int. J. Netw. Secur*., 273–292.

Van Bruggen. (2014). *Studying the impact of security awareness efforts on user behavior*, Ph.D. dissertation, Graduate Program Comput. Sci. Eng., Univ. Notre Dame, Notre Dame, IN, USA.

X. Wang, T. Yu, M. Zeng, and P. Tague. (2017). *X Rec: Behavior-Based User Recognition Across Mobile Devices*, Proceedings of the ACMon Interactive, Mobile, Wearable and Ubiquitous Technologies, 1–26.

Xu, Y. Zhou and M.R. Lyu. (2014). *Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones*, ACM SOUPS, 244-379.

Y. Sheng, V. V. Phoha, and S. M. Rovnyak. (2005). A parallel decision tree-based method for user authentication based on keystroke patterns, *IEEE Transactions on Systems, Man, and Cybernetics, Cybernetics*, 826–833.

Y. Singh, S. Singh and P. Gupta. (2012). Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system, *Pattern Recognition Letters*, 258-369.

Y. Song, G. Cho, S. Oh, H. Kim, and J. H. Huh. (2015). *On the effectiveness of pattern lock strength meters: Measuring the strength of real-world pattern locks*, in Proc. Conf. Hum. Factors Comput. Syst. (CHI), New York, NY, USA, 2343–2352.

Y. Yangt, G. Clarkt and J. Lindqvistt. (2016). *Free-form gesture authentication in the wild*. 34th Annual ACM Conference on Human Factors in Computing Systems, ACM, 456-567.

Ye, Z. Tang and D. Fang. (2018). A video-based attack for Android pattern lock, *ACM Trans. Privacy Secure*, 15-104.

Ye, Z. Tang, D. Fang, X. Chen, K. I. Kim, B. Taylor, and Z. Wang. (2017). *Cracking Android pattern lock in five attempts*, in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 1–15.

Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti and K. Balagani. (2015). *Hmog: A new biometric modality for continuous authentication of smartphone users*. arXivpreprint arXiv:1501.01199.