PROJECT REPORT

TOPIC: USER AUTHENTICATION USING KEYSTROKE DYNAMICS

SUBMITTED BY:

ASHWIN SHARMA
&
VISHESH MISHRA

ABSTRACT

"**User Authentication Using Keystroke Dynamics**" is a method to get the user authentication to an application by recognizing the keystrokes. As mobiles become a ubiquitous, they are used more and more for operations that may involve sensitive data or huge amounts of money. The mobile is also increasingly being used as the tool of preference for browsing and using the Internet. Hence, new security measures must be developed to support increased functionality of these devices, to protect users in the case of any mishap. Authentication using keystroke dynamics for mobiles is an area that has received attention recently. We have studied some authentication techniques used earlier including relative and absolute distance measures, mean and standard deviation-based methods and feature fusion methods. We provide a method for authentication using fusion techniques for our own novel mean and standard deviation-based approaches, which gives low error rates.

TABLE OF CONTENTS

LIST OF FIGURES

1.Introduction:

Sophisticated Mobile Authentication techniques are becoming more ubiquitous and pervasive every day. When it comes to authentication, there are three general headings under which it can be classified. The first is secret knowledge authentication, where access grants depend on something known to intended users only. Passwords and PINS (Personal Identification Numbers) come under this heading. Secret knowledge authentication requires the user to protect the secret knowledge that he has. This often proves to be problematic and systems can be compromised because of carelessness of users. Moreover, many users choose not to use these methods even when available. The next is token authentication, which depends on an object possessed by the intended user. Since the token and the object, it unlocks generally go hand in hand, it is more likely to be stolen along with the object it authenticates. Lastly, there is biometric authentication, which uses a characteristic unique to every user to authenticate the intended ones. Fingerprints come under this category. Although it requires more effort to fake one's way past a biometric authenticator, the downside is that these methods are usually dependent on advanced hardware not found commonly. However, using keystroke dynamics as a biometric authenticator possesses an inherent advantage in that it does not require any specialized hardware on the device. Hardware with sensors that can measure keystroke time (and sometimes pressure) variations is fairly ubiquitous today.

2.Problem Statement:

These days there are various methods to break through password protection systems. Some of them are social engineering as well as other methods like brute force or man in the middle attack, etc. This project aims to solve this problem by using pattern recognition and neural networks to read a user's keystrokes and record them. Hence unless the hackers don't know the information in the log file (that is securely saved in device itself) they cannot hack the system, nor can they get or mimics the way in which the user types the password. Thus, providing a more secure system to store user's data.

Methods like authentication using password or lock patterns which is mostly used as security is now not reliable and secure due to rapidly increase in hacking of these passwords. In order to provide a second level of security, password authentication using keystroke dynamics can be applied. This verifies the user based on its typing patterns and does not allow intruders to access the system.

Neural networks have long been able to solve problems which are not solvable by traditional methods. The advantage of using neural network is that they are flexible throughout different types of datasets. Also, large number of datasets can be considered simultaneously. This data-driven approach is also relatively faster as compared to the statistical approaches. In other words, neural network can be trained specifically for a valid user. Existing statistical models for keystroke dynamics are difficult to be converted into comprehensible forms especially when the number of features increases. Neural networks on the other hand can support multiple features which in the end can still preserve the comprehensibility.

3.Literature Review:

Mobile Authentication using Keystroke Dynamics: Jan 2015. (International Conference on Communication, Information & Computing Technology). [5]

Authentication via Keystroke Dynamics is quite old. The earliest studies on this method were performed in the years 1985-1990 for desktop keyboards. D. Umphress and G Williams are among the first to write on the subject of using keystroke patterns to identify a user. Their work explains the concept and introduces the idea of latency (also called digraphs), the amount of time between two keystrokes. Much of the later work on the subject used the idea of latency and it is used even today in many Keystroke Dynamics Analyzers (KDAs). KDAs were also deployed for pre-touchscreen mobiles (the ones with 12 keys). With the mainstream adaptation of capacitive touch screens and consequently convenient touch keyboards on mobile phones in 2007, this method has been applied to touchscreen phones as well.

Neural network is a technique that mimics the biological neurons for information processing. Neural network is capable of providing an estimation of the parameters without precise knowledge of all contributing variables. A classical neural network structure consists of an input layer, output layer, and at least one hidden layer. Sample data is iteratively fed into the network to produce some outputs based on the current state of its initial predetermined weights. These outputs are compared to the true output, and an error value is computed. This value is then propagated backwards through the network so that the weights can be recalculated at each hidden layer to reduce the error value. The sequence is reiterated until the overall error value falls below a predefined threshold. Neural network is capable of producing better result than the statistical methods.

4.Objectives:

To provide the user with an application that uses Keystroke Dynamics to authenticate a user identity.

The scope of the system includes developing an application that can detect the user not only based on the password but also based on the typing biometrics by identifying the typing patterns. The scope includes the following implementations.

1. To develop data collector module which stores and accesses the data from DBMS.
2. To develop password check module which can check the password entered.
3. To develop key stroke recognition module which calculate time between keystrokes.
4. To develop pressure analyzer module that analyses the applied finger pressure.
5. To develop pattern matching module which checks the patterns which matches the existing patterns with the current one for authentication.
6. To develop decision module that grants permission.

5.Methodology:

Following are the steps that show the execution of the User Authentication program: -

1. On starting the android application user is shown the Instruction Layout with all the basic details on the usage of the application

2. Now the user is asked to enter the passcode of 6 digits that will be further used in training the data

3. This is done thirty times in order to get the keystroke style and the typing pattern of the user.

4. The Keystroke data from above 30 attempts is calculated.

5. User can now choose to view the Keystroke data that is being calculated on every attribute and will be feeding the data into the neural networks to train the data.

6. After all the successful attempts weight values will be calculated for every attribute and will be feeding the data into the neural networks to train the data

7. Data will be processed for the training and thus validation can be performed.

6. Use Case Diagram:

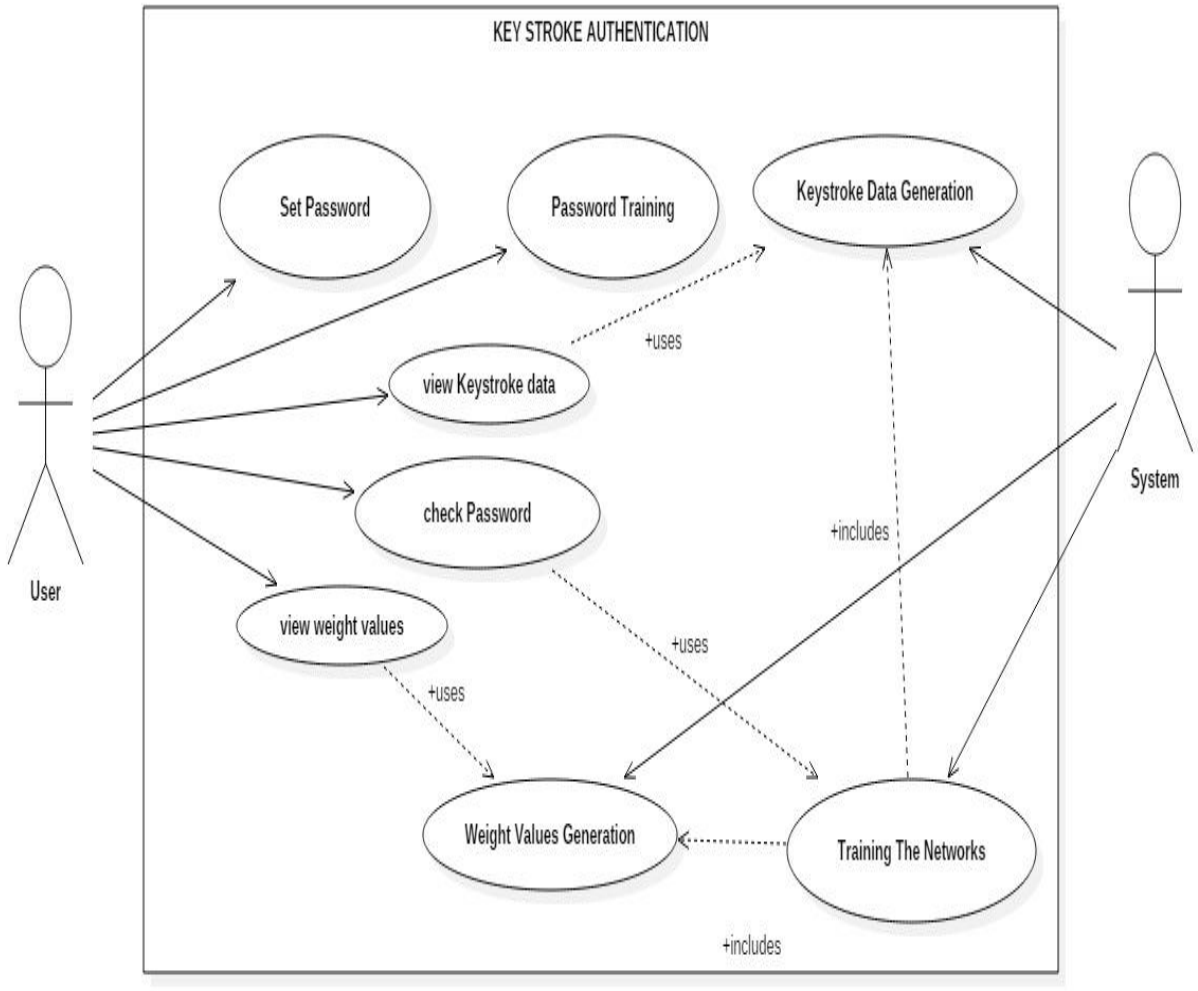


Figure 1: - Use Case Diagram

7. Activity Diagram:

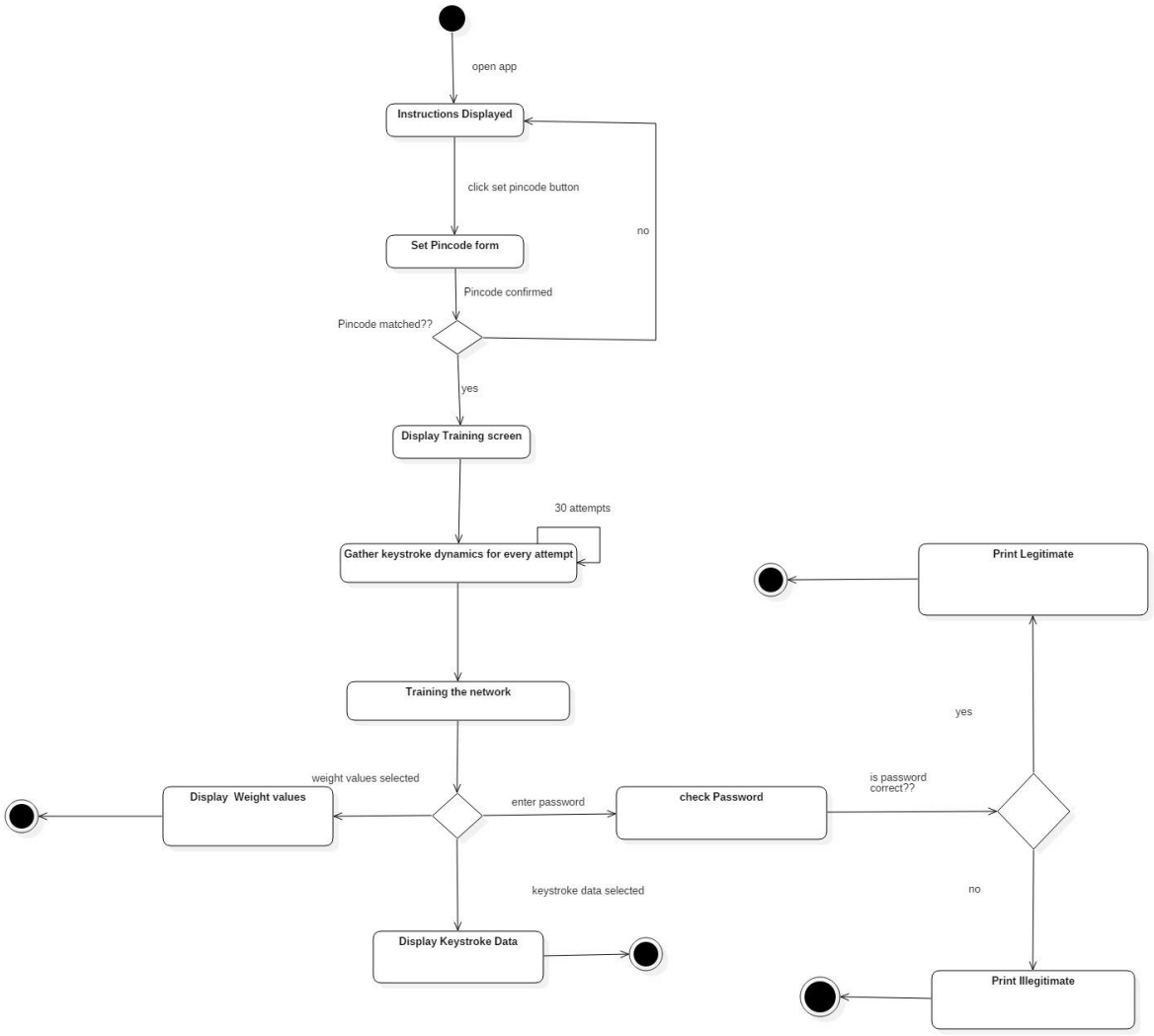


Figure 2: - Activity Diagram

8. Sequence Diagram:

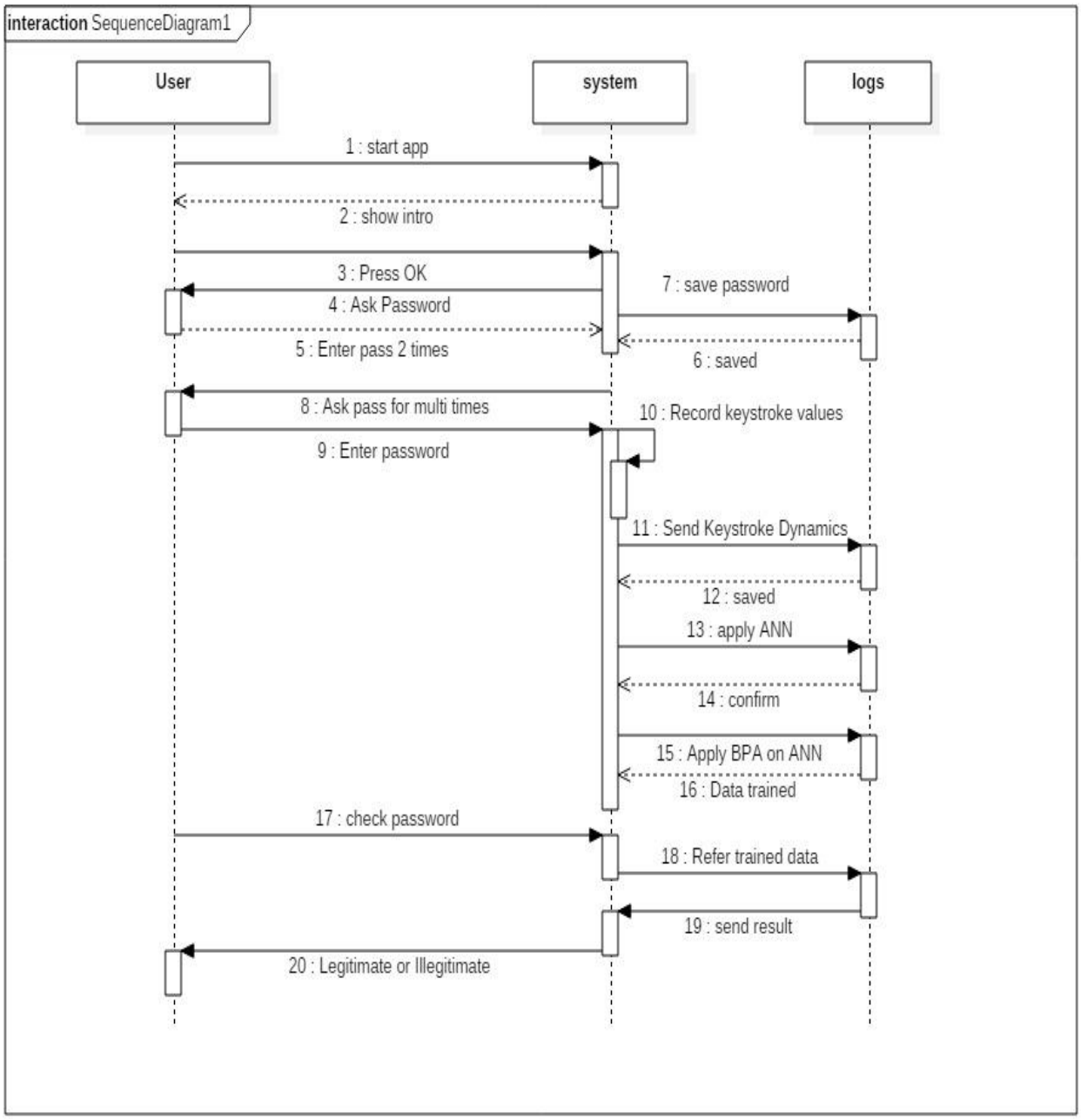


Figure 3: - Sequence Diagram

9. ER Diagram:

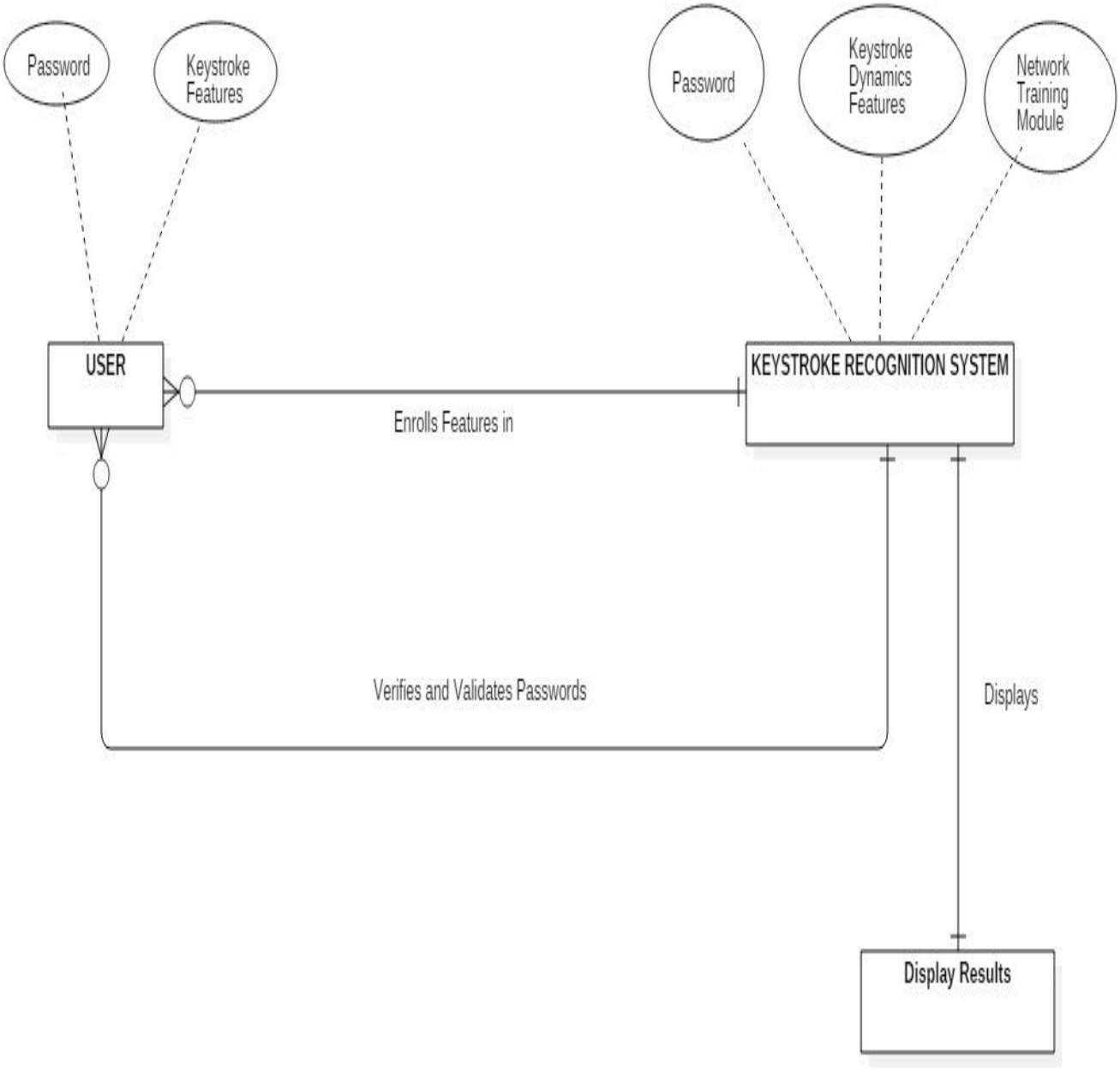


Figure 4 :- ER Diagram

10. Class Diagram:

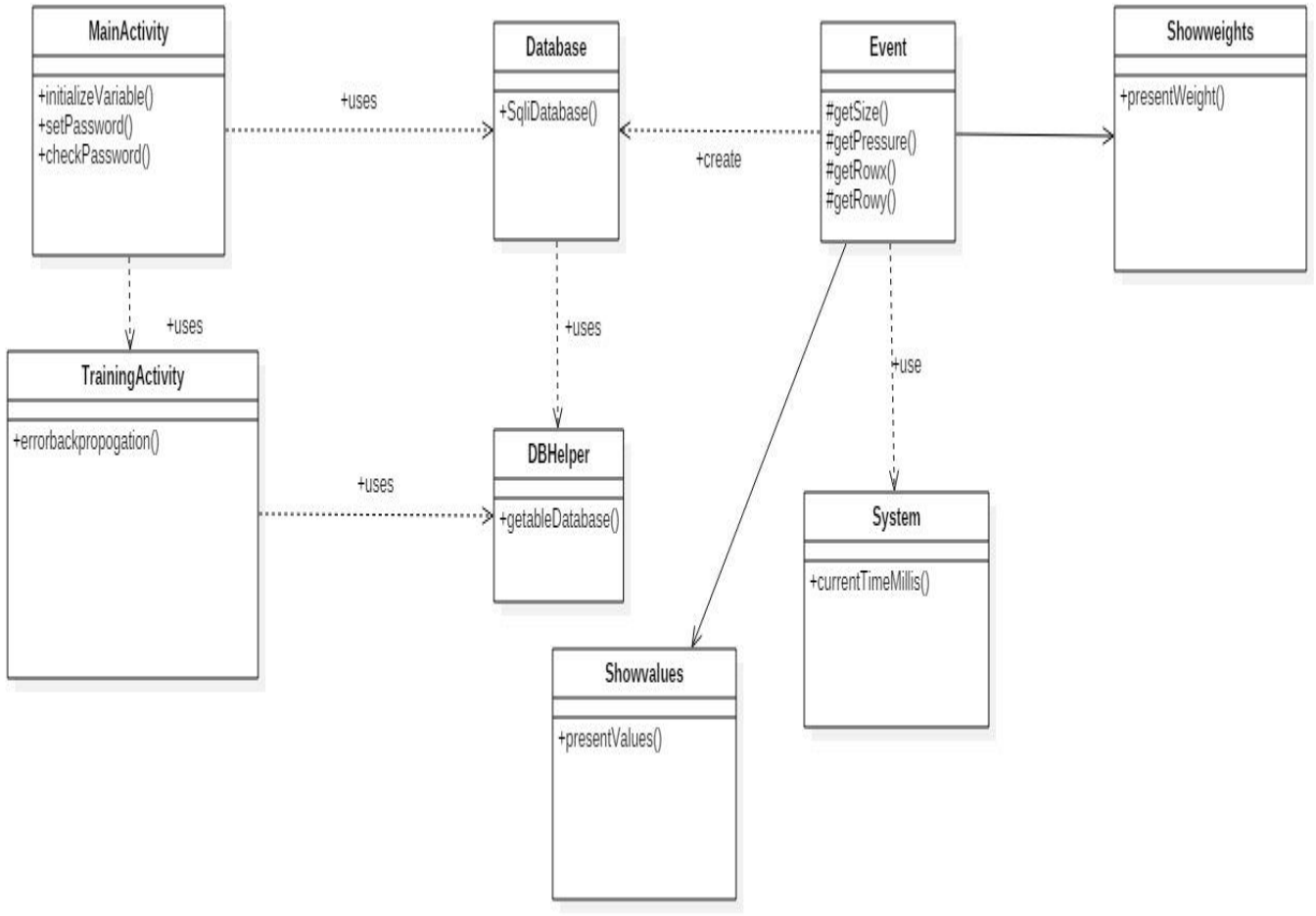


Figure 5: - Class Diagram

11. Object Diagram:

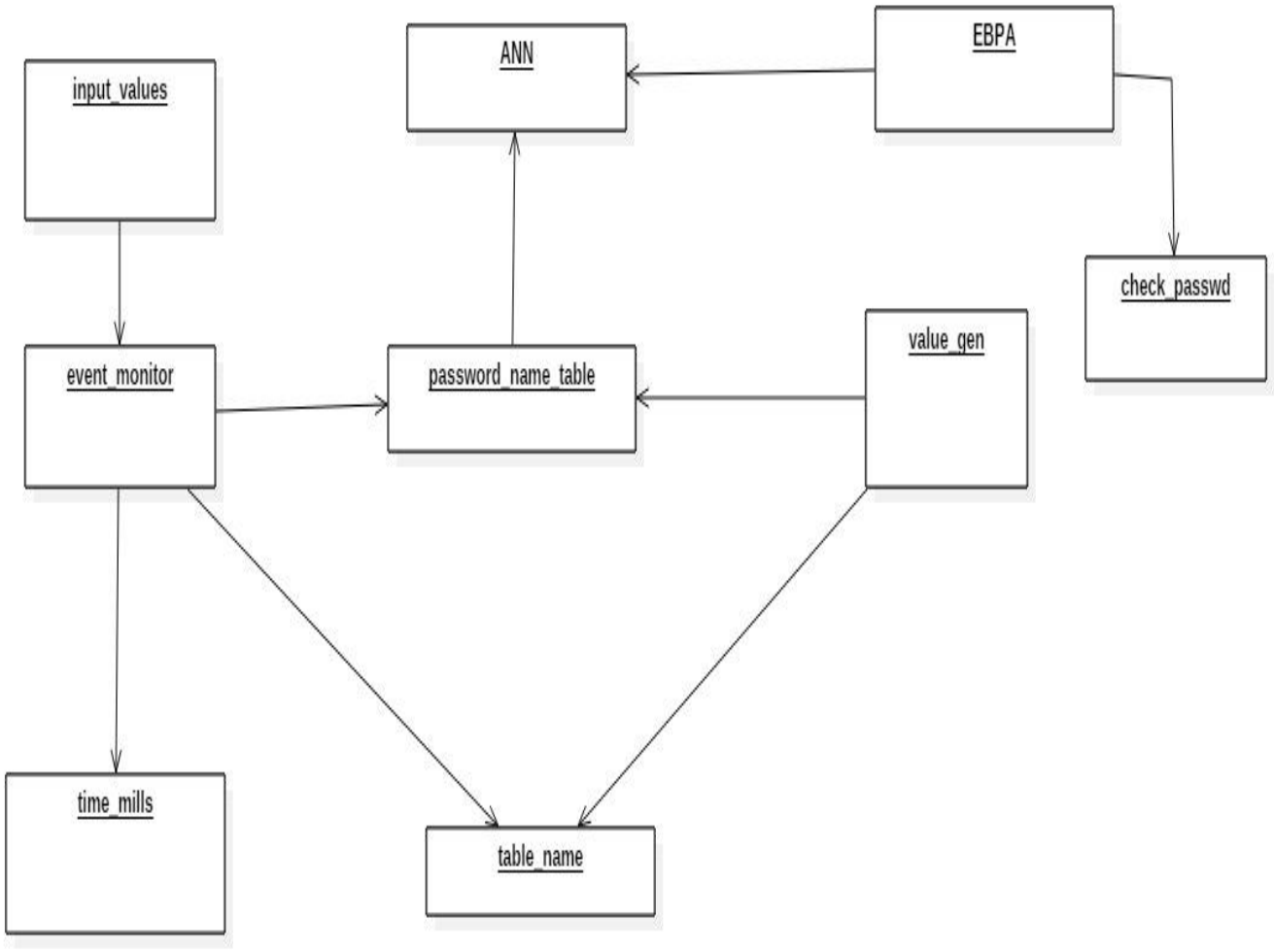
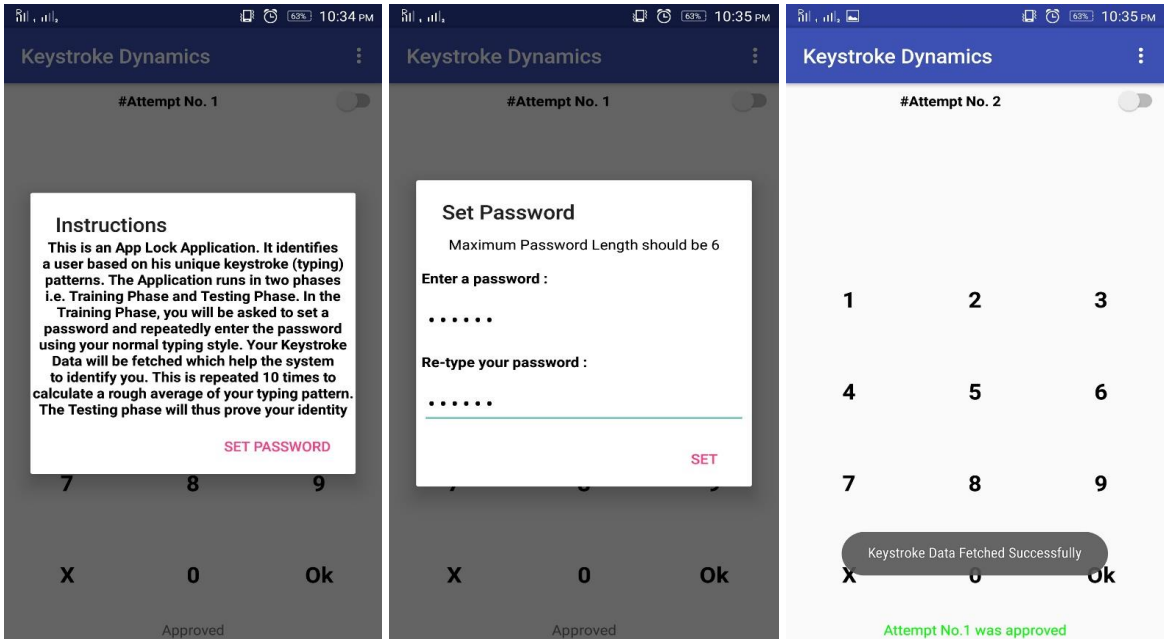
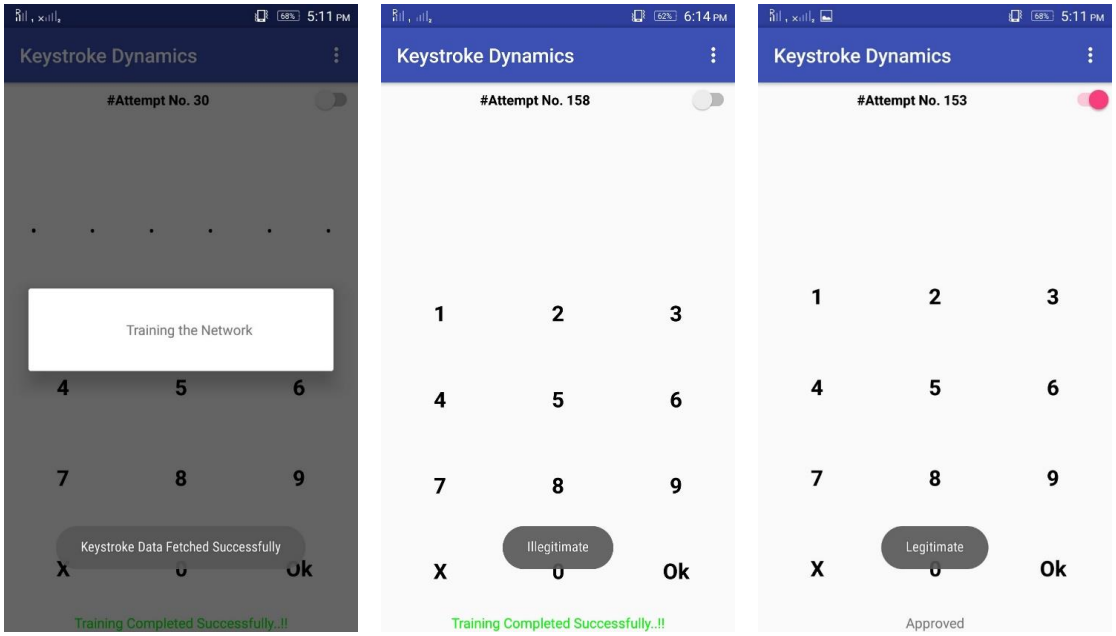


Figure 6: - Object Diagram

12. User Interface Design:





13. Objectives Achieved:

1. Performing calculation of key stroke dynamics on passcode
   a. Calculated Dwell time - how long we press a key.
   b. Calculated Flight time - how long we take to type successive keys
   c. Calculated Di-graph - Time elapsed between releasing the key and pressing the next key
   d. Calculated Tri-graph - latency between three keys.
   e. Calculated Finger size - Amount of space occupied by finger touch.
   f. Calculated Button pressure - Finger pressure applied while typing
   g. Calculated Coordinate values- Location of Button pressed.

2. Application Graphical User Interface created.

3. Database connectivity established with android app.

4. User password authentication created
   a. Artificial Neural Network implemented
   b. Error Back Propagation Algorithm applied on ANN
   c. Training of data on ANN to verify user password
   d. Ultimately determining the legitimacy of the user

14. Pert Chart:

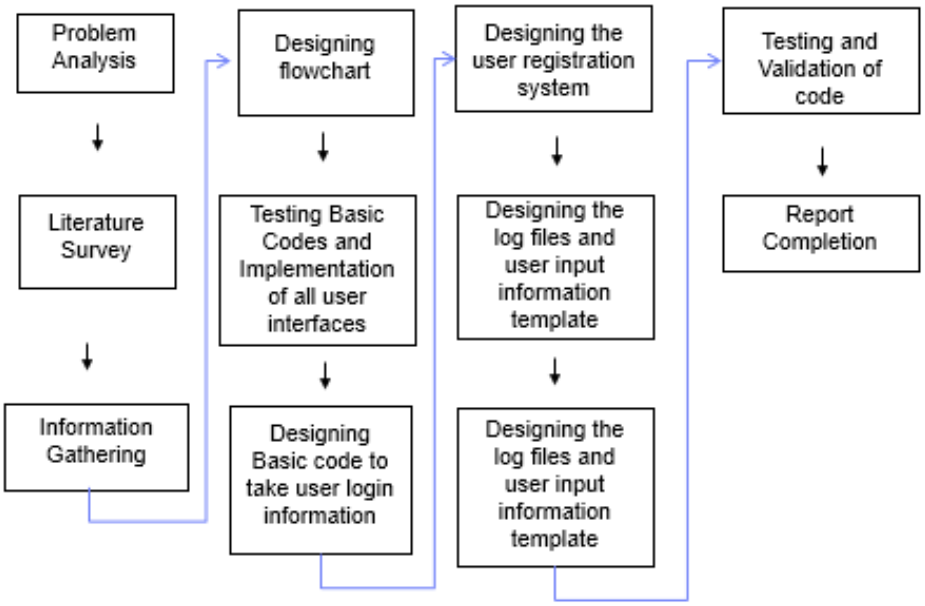


Figure 7: - Pert Chart

15. System Requirements:

Operating System	Android 5.0
IDE/Workbench	Android Studio
Emulator	Nexus 5x API 24
RAM	512 MB or above
Hard disk	512 MB or more

16. References:

[1] http://www.biometric-solutions.com/keystroke-dynamics.html

[2] http://www.cs.columbia.edu/4180/hw/keystroke.pdf

[3] https://link.springer.com/chapter/10.1007/978-3-642-35864-7_39

[4] http://ieeexplore.ieee.org/document/6496441/?reload=true

[5] Mobile Authentication using Keystroke Dynamics: Jan 2015. (International Conference on Communication, Information & Computing Technology