ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Authentication System for Online Banking Application by Using Keystroke Dynamic on Android Phones

Dnyaneshwari S. Dhundad, Prof. D. N. Rewadkar

Post Graduate Student, Dept. of Computer Engineering, RMD Sinhgad College of Engineering, Pune, India

Head of Department, Dept. of Information Technology, Government Polytechnic Awasari, Pune, India

ABSTRACT: Now a day's use of mobile is rapidly increasing. Mobiles are used for various applications such as mailing, chatting, online shopping and online banking. This leads to data leaking or stealing. In such scenario security becomes critical aspect when it comes to online solutions that have millions of secure transactions occurring in the network. Once the user credentials are passed to unintentional user the security of that particular entity becomes vulnerable and harmful events could occur in various magnitudes. What is required is an efficient, reliable, secure and hardware independent solution to authenticate online users. This system provides hardware independent online authentication solution based on methodology called keystroke dynamics. We are applying keystroke dynamics on image because graphical passwords are easy to remember. Image in the password will be divided in to 4×4 block; user has to click any 4 blocks on the image in sequence. The rhythm of image clicks (i.e. timing information) of user is calculated and biometric templates are stored in order to authenticate the user. Comparing with other existing method this is more secure and efficient manner to authenticate the users of online systems.

KEYWORDS: keystroke dynamics; user authentication; behavioral biometric; dwell time; flight time; mobile security

I. INTRODUCTION

Currently, people use mobile devices as a part of their lives. From mobile phones to computer tablets, people communicate to each other through these devices. Most of them are operated by touching a display because the touch screen interface is easy to use and user-friendly to operate. Mobile devices are used not only to make or receive a call, take photos, and play video games, but also to give the special assistance in the business, such as providing internet access, directing access to e-mail and cooperating data, transferring money, and managing bank account. Consequently the authentication of users on mobile becomes an important issue. According to [1], the authentication on mobile devices can be classified in three fundamental approaches. The first approach is using a PIN (Personal Identification Number) or a password is technique called a secrete-knowledge based technique. It offers a standard level of protection and provide cheap and quick authentication.

Unfortunately, it is not enough to the safeguard mobile device and data access through them because passwords have never been completely protected by the owners because there are various unavoidable problems such as sharing passwords with other people or any other systems. Moreover, the result of a survey from [2] has shown that most users agree that using PIN is very inconvenient and they do not have confidence in the protection of the PIN facility provides. The second approach is the SIM (Subscriber Identification Module) or token-based technique. By using this approach when users do not wish to use the mobile, the mobile's SIM must be removed. However, removing SIM is not convenient that is why not recommended. The last approach is biometric technique in which unique characteristic of a person is observed that provides an improvement on the current authentication.

A. *Different Biometric Techniques*

Biometric approaches are of two types:
1. Physiological Biometric
2. Behavioral Biometric

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

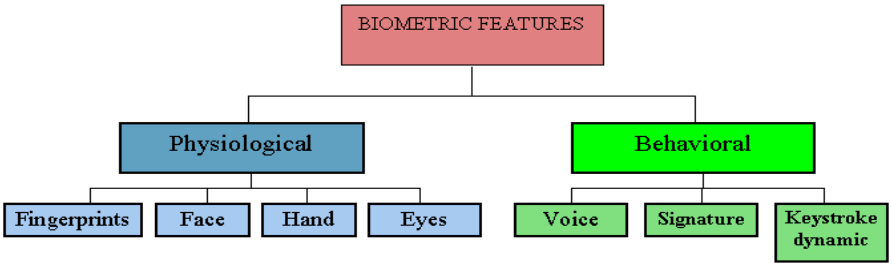

Fig.1. Types of Biometric

Physiological biometric is based on physical characteristics, such as face recognition, fingerprint, DNA, hand and iris scanning.
Behavioral biometric is based on the way people do things, such as keystroke dynamics, mouse movement, and speech recognition.
While using any kind of mobile phones, people can't avoid interaction with keystroke dynamics. On the other hand each person may have different styles to press the key because the typing style is based on users Experience and individual skill which is difficult to copy. With all these new technological advancements the next major issue that has arisen is the concern for the information security and integrity of online users. In parallel to the increase in the number of users accessing the internet, the ratio of cyber-attacks has also been increasing. For example in systems like online Banking Systems where security is of the highest concern evidence suggests that many banking systems are attacked by intruders and hackers, this happens because the online systems use password verification to authenticate users [3]. In such systems as thousands of transactions are performed by users in a fraction of a second. So having a proper authenticating mechanism is integral.

The solution developed through this system will authenticate online users in a more efficient and precise manner as it analyses the way a user types the keys of a keyboard and measures the time taken for the press and release of keys and creates a biometric template for each individual user, this is known as keystroke dynamics. This is possible as some characteristics of keystrokes for each user are unique as a handwriting or signature. Therefore rather than only using the traditional password for authentication through this proposed solution the authentication process is done in two ways.

1 Authentication of user by Username and Password;
2. Authentication by keystroke dynamics (patterns of rhythm and timing created when person clicks on different block of image).

In this system we are using keystroke dynamics and On_Touch up and On_Touch down values as a feature to authenticate users to increase the accuracy of behavioral biometrics.

II. RELATED WORK

We present the related research in a systematic manner which enriches our work. We start by a collection of researches have been presented in the literature using Keystroke Dynamics for Human authentication. It can be utilized for various user authentication processes. Karnan [4] have proposed that the feature subset selection in Keystroke Dynamics for identity verification and it reports the results of experimenting Ant Colony Optimization technique on keystroke latency, digraph and duration for feature subset selection. Here, the Ant Colony Optimization was used to reduce the redundant feature values and minimize the search space. Optimum feature subsets were obtained using keystroke duration values when compared with the other two feature values. Here mean and Standard Deviation was used to extract the features from the Keystroke latency, digraph and duration.

S. Benson Edwin Raj and A. Thomson Santhosh [5] have proposed a biometric identification problem by focusing on extracting the behavioral features related to the user and using the features for computer security. Standardized mouse dynamics biometrics involves a signature that was based on selected mouse movement characteristics under different screen resolution and mouse pointer speed settings. Several experiments were conducted under different settings to form the mouse dynamics signature of the user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Danish lamilet al. [6] have proposed a biometric access control measure, computer access via keystroke pattern recognition and discusses its direct connection to prevent electronic characteristics theft. They found that keystroke dynamics as being one of the most costs efficient and easy to implement biometrics for online and enterprise based systems. The accent was put both on strategies and mathematical models used for implementing the keystroke pattern algorithms. They explained that the keystroke recognition's efficiency in a potential business environment and came up with a schema suggestion for all the phases of a process based on keystroke dynamics.

It was concluded that the keystroke dynamics was a user friendly biometric authentication technique and already there are Keystroke Dynamics Based Human Authentication Systems using Genetic Algorithm available for online applications; web based emailing and other online services. It minimizes the impact on the user's privacy and was very simple to integrate. The keystroke pattern recognition technique could be used effectively as a safeguard to unauthorized access to computer resources and sensitive data.

D. Raghu et al. [7] have proposed an association of ideas of neural network that was trained with the timing vectors of the keystroke dynamics and then used to discriminate between the owner and fake user. They offered an application of neural nets to user identity authentication on computer access security system.

Ahmad A. and issa traore [14] presented a new approach for free text analysis of keystroke that combines monograph and digraph analysis and uses a neural network to predict missing diagraphs based on the relation between the monitored keystroke.

Retinal scanning [8] analysing the use of Retinal scanning, it is observed that it is not feasible for online Banking. For example when you access in a public place it is not secure and also most use home PCs or laptops for online banking system because of that it is difficult to maintain high cost of hardware individually.

Vasco servers (Tokens) [9] Vasco server is more suitable for online banking System. But it is much expensive which is very costly. [9] As a solution for this we propose Keystroke Dynamics. The flowing are the existing products developed by using keystroke dynamics.

Cvmetrics [10] which uses a variety of hyper accurate methods for identifying and validating users on a continuous basis across applications.

KeyTrac - TM3 Software [11] KeyTrac works with any text the user enters (not only passwords or always-the-same-text methods)

BehavioSec-BehaviometricsAB [12] solutions is about keystroke, mouse & environment dynamics for both client-less web based and windows continuous authentication to aid fraud prevention. "Table I" presents a summary of existing solutions and drawbacks.

TABLE I. EXISTING SOLUTIONS AND DRAWBACKS

Product	Drawbacks
Retinal Scanning	Devices required (Camera) and are very intrusive. It has the stigma of consumer's thinking it is potentially harmful to the eye. Comparisons of template records can take upwards of 10 seconds, depending on the size of the database. Very expensive
Vasco Server(Tokens)	Very expensive and is difficult to understand.
BehavioSec	Not well-suited for detecting and preventing fraud. Problems with password-based identity verification.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

III. PROPOSED SYSTEM

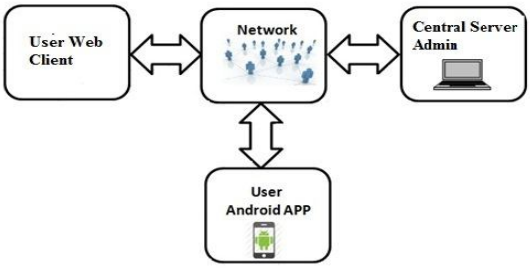

Fig.2. Block Diagram of system

Above fig. 2 shows the overview of the system which contains three main parts
A. *User Web Client*
B. *Central Server Admin and*
C. *User Android App*
The above three parts are communicating to each other via network.
1. Through the user web client user will do the registration for online banking application with the central server of the bank. This registration will be on the basis of Username and password.
2. At central server side there is a database where the all user details are stored which will required at the time of authentication. The administrator at the server side is responsible for uploading the images, user registration; approve/reject the user and user administration.
3. User android application is the part which will be used on mobile phone. User can use E-banking application on their mobile phones where they will first login by user-id and password then they will register their keystroke rhythm if they are login first time to the system .Then one images is shown to user, user has to click on any 4 blocks on that image, this image click rhythm is matched with the stored rhythm in the database, if it is matched then user will be successfully login to the banking menu otherwise it will reject the user.
This system provides two level of security to online banking application

1. In the first level we are going to authenticate the user by Username and Password.
2. In the second level we are authenticating the user by matching entered keystroke template with stored keystroke template.

In the first level of authentication that is username and password we are using AES (Advanced Encryption System) Algorithm for encryption/decryption.
In the second level of authentication we are using image instead of text to set the password. In this level the user is shown with an image which is divided in 4×4 block, user has to click on any 4 blocks on that shown image.

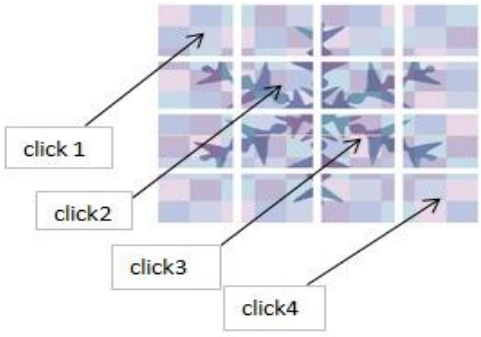

Fig.3. Image with 4×4 block and 4 clicks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

When user will go on clicking on that image then by making the use of press and release timings we create the keystroke template for each user. These stored templates are match with the current template at the time of authentication.

A. *Working of KDA Algorithm*

The KDA (keystroke Dynamic authentication) algorithm is used in second level. A touch event includes the On_Touch down and On_Touch up values from which we are producing four features DU, DD, UD, UU defined as follows.
Step 1: Calculate DD, DU, UD, UU time

- Down-Up (DU) time: DU time is the interval between the same click being pressed and being released.
- Down-Down (DD) time: DD time is the interval between the click being pressed and the next click being pressed.
- Up-Down (UD) time: UD time is the interval between the click being released and the next click being pressed.
- Up-Up (UU) time: UU time is the interval between the click being released and the next click being released.

Step 2: Calculate mean values of DD, DU, UD, UU of user.
Step 3: Calculate Standard Deviation of DD, DU, UD, UU of user.
Step 4: compare new mean values of user with stored mean values
If New_MeanValues – Stored_MeanValues < Deviation
Step 5: login successful.
Step 6: Otherwise login unsuccessful.

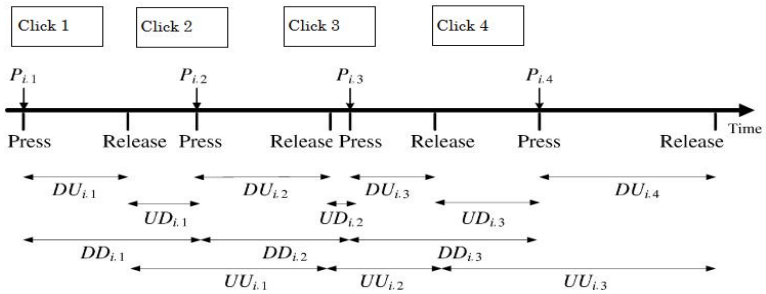

Fig.4. Keystroke Dynamics

Above fig. 4 shows the different keystroke values which we are going to calculate in our project. These four values we did not get directly, we have obtained the above four values by calculating the timing difference between On_Touch down and On_Touch up timing values of four clicks on the image.

B. *Mathematics Related to Proposed System*

The standard deviation of DD, DU, UD and UU is calculated by:

$$\sigma = \sqrt{\frac{\sum(x - \bar{x})^2}{N}}$$

Where

σ - the standard deviation

x - each value in the population

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

$\bar{x}$ - the mean of the values

N - the number of values (the population)

1. Calculate the mean:

$$\bar{x} = \frac{\sum x}{N}$$

$$= \frac{x_1 + x_2 + \ldots + x_N}{N}$$

2. Calculate $x - \bar{x}$ for each value in the sample

3. Calculate $\sum(x - \bar{x})^2$:

$$\sum(x - \bar{x})^2 = (x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \ldots + (x_N - \bar{x})^2$$

4. Calculate the standard deviation for sample of population:

$$s = \sqrt{\frac{\sum(x - \bar{x})^2}{N - 1}}$$

IV. EXPERIMENTAL PROCEDURE AND RESULTS

A. *Experimental Procedure*

In this system we are going to capture keystroke password entries 10 to 15 times and then we are calculating mean difference between these values and standard deviation.

We are calculating mean and standard deviation on DD, DU, UD, UU parameters. We stored the mean and standard deviation values of these parameters in database at server side. Every time when we perform the authentication then we subtract stored mean values from the new mean values and if the difference is less than the stored standard deviation then only user is able to login successfully otherwise login will be unsuccessful.

As well as we are repeating the above condition for all the four parameters due to which if one of the condition becomes fail, the authentication becomes fail. User will be successfully login only when condition for all the four parameters will becomes true. So, this system provides more security for online applications.

In addition to this we also measure values to assess the performance of keystroke dynamics are defined as following:

1. False Acceptance Rate (FAR) refers to the
Percentage of imposter was accepted by the system.
2. False Rejection Rate (FRR) refers to the percentage of authorized users was rejected from the system.
Moreover, these values are used to compare the performance of different biometric techniques.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

1. Registration Phase

"Table II" shows the registration values of one user, taken eight times on eight images at the first time of registration, in each attempt we get different values for the above four parameters, these values we store in database and then we calculate Mean and Standard Deviation of UU,UD,DU,DD separately on each parameter and stored it in to the database.

TABLE II.REGISTRATION VALUES OF ONE USER

Sr.No	Stage	Attempt	Userid	Password	Image	No of points	UU	UD	DU	DD
1	Registration	1	Shahadeo	shahadeo	image 1	4	49	271	311	309
	Registration	2	Shahadeo	shahadeo	image 2	4	58	282	329	321
	Registration	3	Shahadeo	shahadeo	image 3	4	47	295	330	331
	Registration	4	Shahadeo	shahadeo	image 4	4	69	217	271	264
	Registration	5	Shahadeo	shahadeo	image 5	4	61	320	368	363
	Registration	6	Shahadeo	shahadeo	image 6	4	54	280	323	322
	Registration	7	Shahadeo	shahadeo	image 7	4	72	326	380	378
	Registration	8	Shahadeo	shahadeo	image 8	4	61	338	384	381
Standard D							8.8388	38.487	38.471	39.337
Mean							58.875	291.13	337	333.63

"Table III" shows the final mean and standard deviation values of every user who have registered for online banking application stored in the database.

TABLE III.REGISTRATION VALUES OF ALL USERS

User	UU	UD	DU	DD	UU_Dev	UD_Dev	DU_Dev	DD_Dev
Shahadeo	58.875	291.125	337	333.625	8.838835	38.48724	38.47077	39.33714
Sagar	95.125	166.25	238.875	238	17.65897	27.48896	29.21564	30.46778
Ashok	192.25	507.625	669.25	638.125	20.2749	40.45081	48.52613	55.30032
Abhishek	132.125	164.125	261.75	264.875	10.19016	7.529703	10.41633	9.920217
Rajesh	82.75	276.75	338.875	339	7.265378	48.50552	48.12614	46.2416

2. Testing Phase

In this phase we are testing the system by login one genuine user account by three fake user, test results are stored in "Table IV"

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

TABLE IV.LOGIN VALUES OF SHAHADEO BY DIFFERENT USER LOGIN ATTEMPT

User	Login Attempt By	UU	UD	DU	DD	UU_Dev	UD_Dev	DU_Dev	DD_Dev	Result
Shahadeo	Shahadeo	58	322	369	368	-0.875	30.875	32	34.375	Pass
Shahadeo	Abhishek	51	499	538	538	-7.875	207.875	201	204.375	Fail
Shahadeo	Akshay	111	376	458	456	52.125	84.875	121	122.375	Fail
Shahadeo	Sagar	122	400	492	489	63.125	108.875	155	155.375	Fail

"Table V" shows the success ratio of genuine user in which genuine user login in his own account then from four attempt he could login successfully three times and unsuccessful one time.

TABLE V.SUCCESS RATIO OF GENUINE USER

Login Attempt By	UU	UD	DU	DD	UU_Dev	UD_Dev	DU_Dev	DD_Dev	Result
Shahadeo	54	326	327	365	-4.875	34.875	-10	31.375	Pass
Shahadeo	59	333	361	305	0.125	41.875	24	-28.625	Pass
Shahadeo	46	338	367	398	-12.875	46.875	30	64.375	fail
Shahadeo	58	287	315	319	-0.875	-4.125	-22	-14.625	Pass

Pass	3
Fail	1

"Table VI" shows the success ratio of fake user in which one fake user login genuine user account then from four attempt he was unsuccessful in all the four attempt.

TABLE VI.SUCCESS RATIO OF FAKE USER

User	Login Attempt By	UU	UD	DU	DD	UU_Dev	UD_Dev	DU_Dev	DD_Dev	Result
Shahadeo	Akshay	51	499	538	538	-240.125	162	204.375	529.1612	Fail
Shahadeo	Akshay	111	376	458	456	-180.125	39	124.375	447.1612	Fail
Shahadeo	Akshay	122	400	492	489	-169.125	63	158.375	480.1612	Fail
Shahadeo	Akshay	46	338	367	398	-245.125	1	33.375	389.1612	fail

Pass	0
Fail	4

B. *Experimental Result*

The graphs and charts below shows the results of the experiments, in which we have calculated standard deviation of different users on DD,DU,UD,UU parameters in milliseconds and these values are stored in database.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

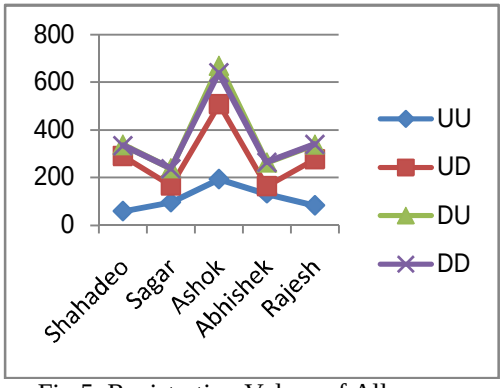

Fig.5. Registration Values of All users

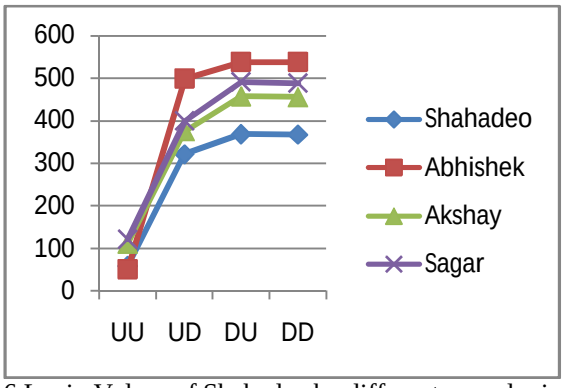

Fig.6.Login Values of Shahadeo by different users login Attempt

Fig.5 shows registration values of all users in milliseconds who have registered for online banking application and Fig.6 login values of Shahadeo by different users login attempt, in this graph Shahadeo is genuine user and other are fake user, we can clearly see that the deviation values of all the fake user are above the genuine user deviation due to which they fails in login attempt.

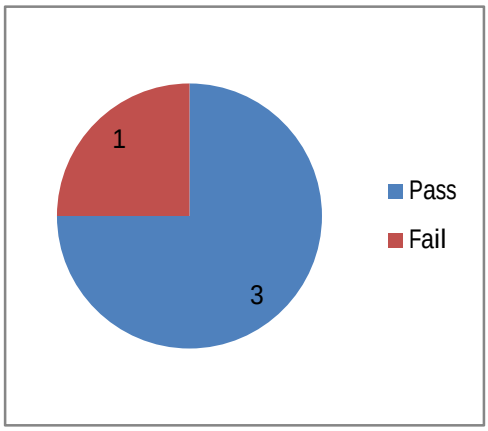

Fig.7.Success Ratio of Genuine user

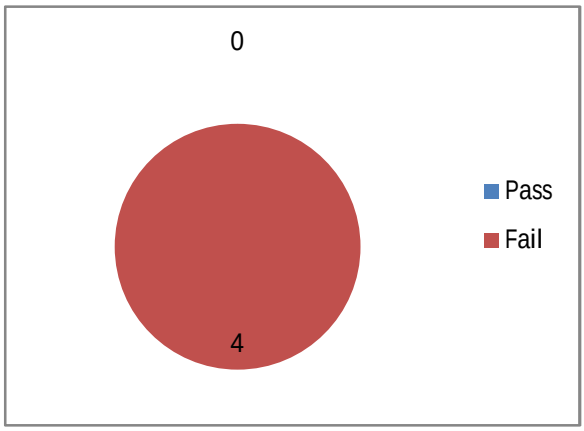

Fig.8.Success Ratio of Fake user

Then the accuracy of system is checked by doing login of genuine user by fake user. In the above Fig.7 and Fig. 8 the system is checked against one genuine user and three fake users. It is found that success ratio of genuine user that is FRR (False Rejection Rate) is 25% and success ratio of fake user that is FAR (False Acceptance Rate) is 0%. As the number of user login attempt will increase in test data set the FRR and FAR result will change accordingly.

V. CONCLUSION AND FUTURE WORK

Most of the online banking systems use just a password to authenticate users. But some other banks introduce additional hardware token to authenticate users. But it is inefficient since these hardware devices are expensive and they can be easily misplaced. It is also a burden to online banking user since they have to maintain it physically. In our solution we use keystroke patterns of the online banking user and create a biometric template for future authentication. It is more secure, cost effective, efficient and easy to use and graphical password is easy to remember than textual password.

In future we can add more layers of authentication to provide more security to critical application like online banking. We can also make multimodal biometric authentication system by combining physical and behavioral biometrics of the user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

REFERENCES

1. S. Nanavati, M. Thieme, and R. Nanavati, Biometrics identity verification in a networked world, John Wiley & Sons, 2002
2.N.L. Clarke and S.M. Furnell, "Authentication of users on mobile telephones – A survey of attitudes and practices", Computers & Security, October 2005, Vol.24, pp. 519-527.
3. Picard, R. W. 2007. Affective Computing. MIT Press
4. Marcus Karnan, M. Akila and A Kalamani, "Feature Subset Selection in Keystroke Dynamics Using Ant Colony Optimization," Journal of Engineering and Technology Research, Vol. l,No. 5, pp. 072-080, Aug2009.
5. S.Benson Edwin Raj and A Thomson santhosh, "A Behavioral Biometric Approach Based on Standardized Resolution in Mouse Dynamics," IJCSNS International Journal of Computer Science and Network Security, Vol. 9, No. 4, pp. 370-377, Apr 2009.
6.Danish Jamil and Muhammad Numan Ali Khan, "Keystroke Pattern Recognition Preventing Online Fraud," International Journal of Engineering Science and Technology (IJEST), Vol. 3, No. 3, pp. 1953-1958, Mar2011.
7.D. Raghu, C. H. Raja Jacob and Y. V. K. D. Bhavani, "Neural Network Based Authentication and Verification for Web Based Key Stroke Dynamics," International Journal of Computer Science and Information Technologies, Vol. 2, No. 6, pp. 2765-2772, 2011
8.A.Zalman, "Biometrics: Retinal Scanning", About.com,[Online]. A vai lable: http://terrorism. about.comlod/controversialtechnologies/g/RetinaIScans.htm. [Accessed: 8th Feb 2012].
9.O. Mangelschots, L. Meys, Vasco digipass, Orbit One International, 2008
10.Intensity analytics, "cvmetrics", 2012, [Online], Available http://www.intensityanalytics.com/products.aspx?tab=2[Accessed: 2nd Feb 2012].
11.TM3 Software,"KeyTracHow it works",[Online], Available: http://www.keytrac.de/how-it-works.html.
[Accessed: 27th Jan 2012].
12.BehaviometricsABMulti layered security through behavioral biometrics", BehavioSec, [Online], Available:http://www.behaviosec.coml. [Accessed: 8th Feb 2012
13.Jeanjaitrong, N.; Bhattarakosol, P., "Feasibility study on authentication based keystroke dynamic over touch-screen devices," Communications and Information Technologies (ISCIT), 2013 13th International Symposium on, vol., no., pp.238, 242, 4-6 Sept. 2013
14.Ahmed A. Ahmad and Issa Traore, "Biometric Recognition Based on Free-Text Keystroke Dynamics," Cybernetics, IEEE Transactions on, vol.44, no.4, pp.458, 472, April 2014.

BIOGRAPHY

Dnyaneshwari S. Dhundad a PG student in the Computer Engineering Department, RMD Sinhgad School of Engineering, Savitribai Phule Pune University. She received B.E. in Computer Technology from Computer Technology department of Yeshwantrao Chavan College of engineering and from R.T.M.University of Nagpur, Nagpur. Her research interest area is mobile security.

Prof. Deepak. N. Rewadkar received M.E Computer Technology from S.R.T.M University, Nanded in 2000. Currently he is working as a Head of Dept. Information Technology in Govt. Polytechnic Awasari, Pune. Prior to Govt. Polytechnic he is working as a Head of Dept. Computer Engineering in RMD Sinhgad School of Engineering, Pune. He was a Member of Board of study committee of S. R. T. Marathwada University, Nanded for Computer Science and Engineering. He has 21 years of teaching experience.