

Keystroke Dynamics Authentication for a Web-Based Sales and Stock Solution

Oluwakemi C. Abikoye⁸ and Bilikis T. Sanni

Department of Computer Science, University of Ilorin, Ilorin, Nigeria

*Corresponding author: kemi_adeoye@yahoo.com

ABSTRACT

The importance of security in any financial sector cannot be over emphasized, a single factor authentication (username and password) is no longer sufficient. Therefore, a multifactor authentication is required to address security in financial systems. In this work, keystroke dynamics, a new behavioral biometric is proposed as an additional security measures. Keystroke dynamics is a very important tool for authentication with a high level of security which can be implemented to enhance other forms of authentication. This is achieved using static keystroke approach on passwords, statistical feature extraction method to analyze the keystroke time from hold-time and latency, and direct comparison with thresholds based on password length for users verification and authorization. This system is used in a web-based small and medium scale

⁸ Author's Address: Oluwakemi C. Abikoye⁸ and Bilikis T. Sanni, Department of Computer Science, University of Ilorin, Ilorin, Nigeria

Corresponding author: kemi_adeoye@yahoo.com

"Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than IJCIR must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee."

© International Journal of Computing and ICT Research 2008.

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.11, Issue 1, pp. 84 - 113, June 2017.

enterprises (SMEs) sales and stock solution and also it provides a stronger security measure than the conventional password authentication.

Keywords: Keystroke Dynamics, Password, Security, Multifactor Authentication, Biometric, Small and Medium Scale Enterprises (SMEs)

IJCIR Reference Format: Oluwakemi C. Abikoye and Bilikis T. Sanni. Keystroke Dynamics Authentication for a Web-Based Sales and Stock Solution, Vol. 11, Issue.1 pp 84 - 113. <http://ijcir.mak.ac.ug/volume11-issue1/article6.pdf>

1. INTRODUCTION

In this research work, an improved small and medium scale enterprise in terms of security is developed using keystroke dynamics biometrics to enhance the usual password authentication. Keystroke dynamics authentication is a multifactor authentication based on individual typing style that can be used with other forms of existing security biometrics that involves typing like the password used in this work. Keystroke dynamics is a very secure behavioral biometric, since each individual have different typing styles (Sawant, Nagargoje, Bora, Shelke, and orate, 2013). The purpose of this behavioral biometrics is to serve as a two-step security verification for user logins to facilitate higher level of security during verification and authentication so that only authorized users will have access to the information of the software.

Authentication is the process of identifying and verifying an individual for security purpose. User authentication is classified into three main categories (Modi, Upadhyay, and Thakor 2014; Abualgasim, and Osman 2011) which include; knowledge, object or token and biometrics based authentication. Knowledge based authentication is a type of authentication that is based on something one knows and is characterized by secrecy. e.g. Personal Identification Number(PIN) codes and passwords. PINS and passwords are individual user unique set of alphabets, numbers, or alphanumeric used for security during registration usually with a username.

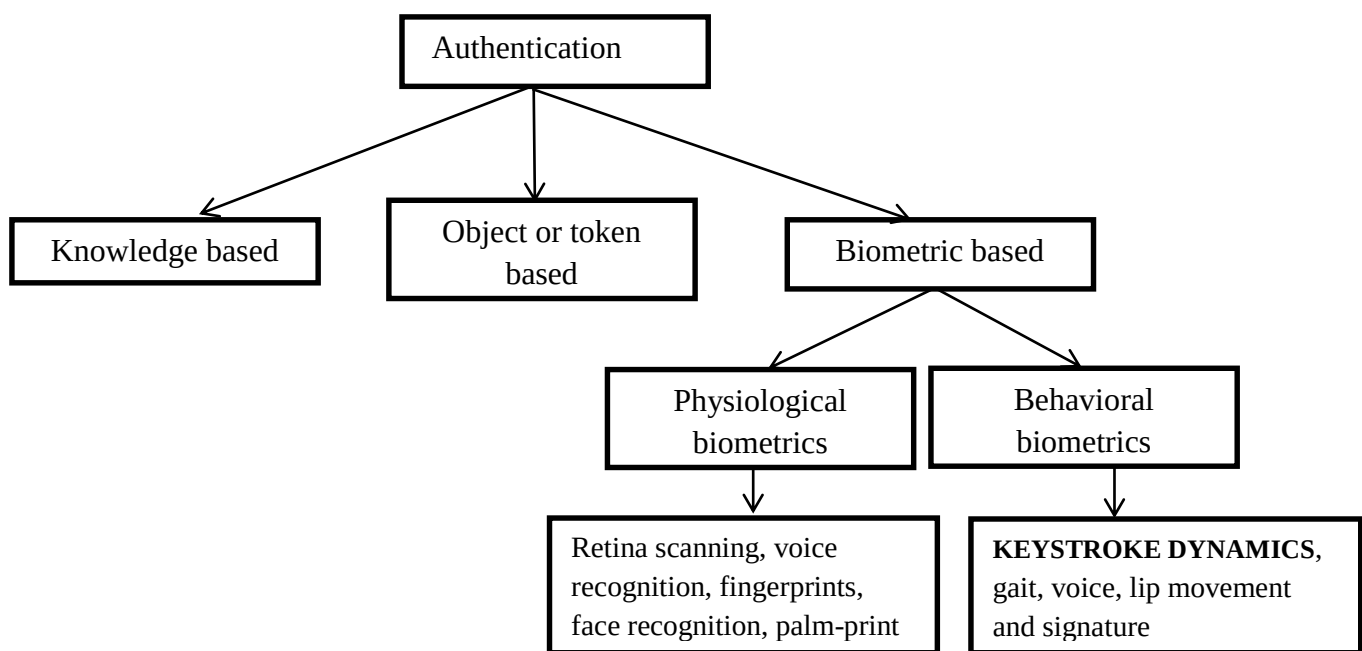


Figure 1: Classification of Authentication

Token based authentication is a method of authentication that is based on something one possess such as keycard or badge while Biometrics based authentication is a type of authentication that is based on individual physical or behavioral features.

Biometrics is derived from two Greek words bio meaning “life” and metric meaning “to measure. In computing, biometrics techniques are mainly used for user authentication for measuring and

analyzing individual's physiological or behavioral features like keystroke, gait, fingerprints, signature, lip movement, voice patterns, typing patterns, facial patterns, and palm-print for the identification and verification purpose.

1.1 Types of Biometrics

There are two main categories of biometric based authentication which includes:

- Physiological biometrics
- Behavioral biometrics

Physiological Biometrics

Physiological biometrics is a type of biometric that measures individual physical features of a certain part of the body. e.g. human eye (this involves iris and retina scanning), voice recognition, fingerprints, face recognition, palm-print etc. Physiological biometrics is normally considered more effective than behavioral biometrics because they are fairly consistent over time and are unique, but are very expensive and require different equipment.

Behavioral Biometrics

Behavioural biometrics is a type of biometrics based on what a person does, or how the person uses the body. e.g. **keystroke dynamics**, gait, and signature. Behavioural biometrics is considered weaker when compared to the physiological biometrics because they are less constant and can vary over time. Although Behavioural biometrics have unstable qualities, they are still successfully used because it is still difficult to imitate others behaviour such as typing rhythm. Keystroke dynamics is one of the cheapest biometric methods to implement since the only hardware required is the keyboard.

1.2 Keystroke Dynamics

Keystroke dynamics is one of the several innovative technologies used to automate the process of authenticating an individual based upon a unique and personal behaviour. Keystroke dynamics involve a technique of analyzing how a user types at a terminal by observing the keyboard in order to find the user based on his or her usual typing rhythm features (Sawant et al. 2013). Keystroke dynamics also involve inspecting timing features of individual's typing in order to identify patterns in their keystroke data. This may sometimes include the analysis of features such as the pressing time, releasing time and the latency of all authorized users extracted while typing their password during registration process.

Most of the papers used statistical methods and neural networks for keystroke based Authentication. Collection of data needs keyboard and software (Sawant et al. 2013). All Keystroke mechanism depends upon the key press and key release duration. The time duration between key press and key release convert into security parameters (Singh, and Arya, 2010)

1.3 Small Medium Enterprises

There have been related studies in the past and still on-going by different researchers, reviews have shown that integrated business software covers all relevant aspects of an enterprise (Davenport, 1998). The Small and Medium Scale Enterprises (SMEs) provide the cornerstones on which any country's economic growth and stability rest. Based on this, there is a need to take all available security measure on such systems. This work uses keystroke dynamics biometrics authentication as a plus to the usual login process. Research by experts has recommended and suggested principles that modern enterprise systems should be service-oriented, constructed in a modular form and communicates via Web services (Schmitt, 2007). This keystroke dynamics authentication SMEs research work is cost effective which helps to solve the problem further analyzed by Scott & Vessey (2002). Winkelmann and Klose (2008) stated that in small and medium companies in particular, the introduction of a new system or the migration of old to new platforms is accompanied by high costs in relation to turnover and naturally by associated risks because

integrating keystroke dynamics authentication to such system attracts no additional cost. It's almost free in terms of hardware because the most significant device used for data input is the keyboard which is part of the existing hardware of the system.

2. RELATED WORK

Keystroke dynamics authentication, a behavioral biometrics has drawn a lot of research interest and a number of techniques in different aspects were proposed. Several methods and modules have been suggested with special emphasis on data collection, feature extraction, storage database and matching process. Most of the papers used statistical methods and neural networks for keystroke based Authentication, collection of data needs keyboard and simple software (Sawant et al. 2013).

Avasthi and Sanwal (2016) carried out a comprehensive study on Keystroke Dynamics based on identification, verification, methods and performance measures & metrics. Modi, Upadhyay, and Thakor (2014) compared existing systems based on some features such as the authentication provided, classification method, outlier handling, keystroke hardening scalable, False Acceptance Rate (FAR), False Rejection Rate(FRR) ration, limit ID and password text.

Giot, El-Abed, and Rosenberger (2014) used two (2) main families of keystroke dynamic methods in making use of statistical methods; (1) The static families, where the user is asked to type several times the same string in order to build its model, and (2) The dynamic families which allows the authentication of individuals independently of what they are typing on the keyboard.

In Sawant et al. (2013) proposed two algorithms to implement the keystroke efficiently. The Gaussian Probability Density Function and Direction Similarity Measures were proposed. The fusion of the two algorithms was done by different methods which from among them the AND rule showed the best result. The resulted mean, standard deviation and weight formula used to calculate the weight in the first step and the login time keystroke data was compared with the registered mean $\pm$ standard deviation which resulted into match count in the second step. Monte Carlo approach was used for Data Collection; the time duration between key press and key release was converted into security parameters while the Parallel Decision Tree (DT) was used for the identification of a genuine user.

Shukla and Solanki (2013) focused on the problem of human emotion recognition in the case of naturalistic. Users' behavioral or physiological patterns were mapped to emotional categories collected. Six basic emotional classes were worked on, confidence, sadness, nervousness, happiness, tiredness, hesitation. The study aimed to develop a web application that recognizes human emotional states using four modules; Data Collection Process which consists of gathering and labeling users' keystroke and mouse data. The feature extraction and attribute selection which reduces the number of attribute to facilitate the classification process were performed. Data Labeling and the data provided by the human were labeled while questioning the best accuracy of the trained system. Classification: fuzzy logic was used as a solution to recognize user's emotional state.

Bajaj and Kaur (2013) applied statistical method to measure the mean time and average time and developed an application using java. Some studies based on selection process on normality statistics applied. Abernethy and Rai (2012) captured time values associated with keystroke events, keystroke duration and digraph latency metrics were calculated from the raw data files and Artificial Neural Networks were used for classification, and results were calculated as the false acceptance rate (FAR) and the false rejection rate (FRR). Karnan and Krishnaraj (2012) implemented statistical method on various keystroke dynamics feature extracted: (i) Duration (Amount of a time a key is pressed), (ii) Latency (Differences of time between two key events), (iii) Mean, standard deviation (Mean and standard deviation value of each type of PIN), (iv) Press–Release (Latency between pressing and releasing the key), (v) Digraph

Al-Jarrah (2012) used a password typing rhythm to detect the actual and unauthenticated user. The study introduced two phases; training phase and testing phase. The calculation of key down/up time of every key and latency time between keys were done. The comparison in testing phase check the value in binary for analysis, the binary score is 1 if it is within a close distance threshold from the median stored else 0. The use of benchmark data in the study of the detection performance of authentication systems is a scientific approach. A novel technique was proposed for free text keystroke dynamics in Singh & Arya (2011), keys were classified into two halves (left-right) and

four lie (total eight groups). They used timing vector to calculate the flight time. Timing vector technique used to define the difference between fraud and actual users. The best results were obtained and very supporting.

In Giot et al. (2009) a comparative study was conducted, considering the operational constraints of collaborative systems. The main scheme used includes:(i) the enrollment (which consists of registering the user in the system) embeds the data capture, eventually some data filtering, the feature extraction, and the learning step; and (ii) the verification process realizes the data capture, the feature extraction and the comparison with the biometric model. Depending on the studies, this scheme may be slightly modified. Some algorithms can also adapt the model of the user by adding the template created during the last successful authentication.

3. METHODOLOGY

Nigeria is still a developing country especially when it comes to technology, and majority of the enterprise in Nigeria especially the small and medium scale enterprise still operate on the manual method of inventory. The staff record, stock record and daily sales are still being recorded manually especially in the small enterprises because of the fear of expansion. In this research, after series of direct interview, it was deduced that two things causes the fear, inadequate knowledge about computing technology and assumed the new technology is too expensive. This project, design with the aid of computer system, an inexpensive solution that doesn't require expert knowledge to effectively handles operations of the SMEs in Nigeria from the information gathered by visiting some stores (small and medium enterprises) and designing a web-based application using PHP, JavaScript and HTML at the front-end, MYSQL at the back-end for the database and also apply keystroke dynamics biometrics on the password using PHP, JavaScript (Query) and HTML at the front-end, MYSQL at the back-end for the database, to be able to give the organization (SMEs) a more secure system than using password alone. The cost of adding keystroke dynamics to any system is almost free since the only hardware required is the keyboard which is already part of the Computer system. This keystroke dynamics authentication security based system is designed to eradicate the problems associated with the old system of unauthorized users accessing the data of an organization to perform any form of fraudulent actions.

In this new system, though if the unauthorized users lay hands on password (that is guessed, lost or stolen), the imposter would not be able to gain access to the system. This is so because during the registration process of new system users, as the password is being typed, keystroke time is also been calculated for every users. Even if unauthorized user knows the password, he/she would not have access to the new system because of the individual keystroke time access control. To access the new system, the inputted username, password and keystroke time must be the same in the database

3.1 Basic Modules Used

There are four main basic modules used in keystroke dynamics from the papers reviewed Modi, Upadhyay, and Thakor (2014); Sawant, Nagargoje, Bora, Shelve, and Borate (2013); Bajaj, and Kaur (2013); Abernethy, and Rai (2012), which includes:

- Data Collection
- Feature Extraction
- Storage Database
- Matching Process

3.1.1 Collection of Data

This is the enrollment phase where by the authorized staff (both the admin staff and the sales representative) register to create an account in the sales and stock web application. During registration, each user registers with their specific password and username which will be saved in the database against that specific user and while processing the password, the keystroke dynamics program will also be performing its operation by using Static Approach where the same username and password are maintained for each authorized users in order to build its model. In Static approach, the system checks the user only at the authentication time. It provides additional security than the username/password. It also provides more robust user verification than simple passwords. In this approach, the analysis is performed on the password while typing during registration for all the individuals using the application. The minimum password length used is 4 while the maximum is 30. The static analysis is done at login time in conjunction with the password authentication

methods. The username and password used during registration are saved against each user for verification during login. Collection of data is done using keyboard and software.

3.1.2 Feature Extraction

The keystroke data is based on the password using the system time. The key press (the time in which the key is held down), key release (the time in which the key is released), the latency (the time between two consecutive keys) and the password length (the total keys of the password) of each users (staff) which are produced while typing each characters of user password for the registration. The passwords are further analyzed using the statistical method to find the keystroke time which will be stored in the database for future verification for each registered users.

Latency is the distance between two successive keys.

$$L = K_2P - K_1R$$

Where L = Latency, K_1R = the time Key 1 is Released, and K_2P = the time Key 2 is Pressed.

Duration is the amount of time a key is pressed or the hold-time for each key of individual password. The difference between the time a key is released and pressed.

$$D = K_1R - K_1P$$

Where D = Duration, K_1R = the time Key 1 is Released, and K_1P = the time Key 1 is Pressed.

Digraph is the duration or hold-time of a key plus latency between successive keys.

$$DI = D_{K1} + L_{K1,2}$$

Where DI = Digraph, D = Duration, K_1 = Key 1, L = Latency, and $K_{1,2}$ = Between Key 1 and Key 2.

Keystroke Time is the amount of time of typing the whole password used considering the key press time, key release time, latency and password length.

Password Length is total keys of the password.

$$KT = \frac{DI_{K1} + DI_{K2} + \dots + DI_{Kn}}{PL}$$

Where KT = KeystrokeTime, DI = Digraph, K_1 = Key 1, K_2 = Key 2, and K_n = Key n, and PL = Password Length

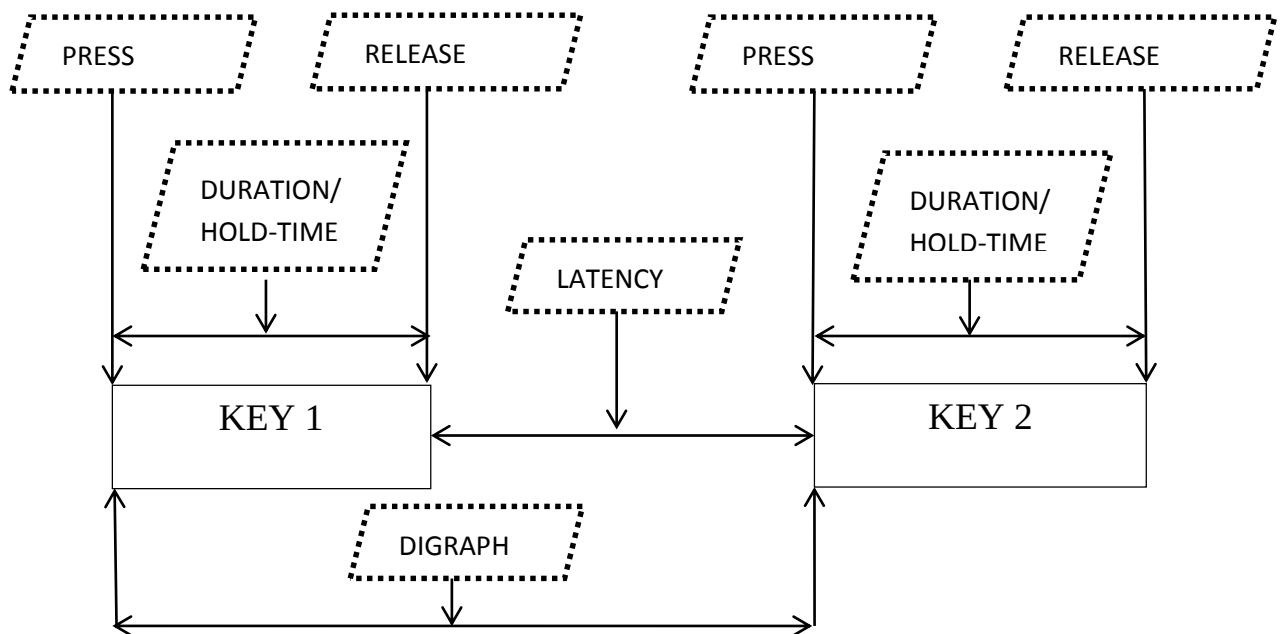


Figure 2: Feature Extraction

3.1.3 Storage Database

The database stores all information of the new system in a systematic way, which makes the update, retrieval and maintenance of the new system easy. After featured extraction and the statistical calculations on the feature, the keystroke time is stored on the database which will be retrieved for login verifications. The database houses all the business information; inventories of staff, stock and daily sales (name of goods, quantity of goods sold, price of each item sold (unit

price) and the cost of goods sold which is its unit price multiplied its quantity, against each sales representative).

3.1.4 Matching Process

In the matching process, genuine users are identified by direct comparison. During the login process, the system compares the user name and password to the pre-registered data on the database; if it doesn't correspond it pops-up incorrect username or password with a back check box to restart the process, otherwise as the user is typing his password to login, the keystroke also counter check. The keystroke time of the present login is compared with the existing keystroke time stored in the database. This system uses threshold considering the password length. The default threshold is ± 10 for the keystroke time (in microseconds) for password length that ranges from 4:10 characters, for password length that ranges from 11:20 characters, threshold ± 15 is set for the keystroke time (in microseconds) and for password length that ranges from 21:30 characters, threshold ± 20 is set for the keystroke time (in microseconds). These thresholds are used during the verification between the present keystroke time and saved keystroke time for authentication. If the present keystroke time falls between the given range, the user is able to login otherwise pops up accessed denied which directs the user back to the login page to enter the password again and follow the same process.

3.2 Proposed Algorithm

3.2.1 Algorithm for Creating New User

Step1: User opens the create account page to fill

Step 2: Input username, password, retype password, and full name

- `input name="username" type="text" id="username" size="30"`
- `input name="pass1" type="password" id="pass1" size="30"`
- `input name="pass2" type="password" id="pass2" size="30" and`
- `input name="name" type="text" id="fullname" size="30"`

Step 3: Select branch and role from branch and role table respectively in the database

Step 4: Submit

Step 5: The System Confirm password and the retyped password to be the same

```
if (password == retyped password)
{Create Keystroke Dynamics for Password}
Else {"Your Password do not match, Please try again!!!"}
```

Step 6: The system Extract keystroke feature from the password to create keystroke time

- The key press (the time in which the key is held down) is extracted
- The key release (the time in which the key is released) is extracted
- The latency (the time between two consecutive keys) is extracted and
- The password length (the total keys of the password) is extracted
- The keystroke time is calculated using statistical method.

Step 7: Create and Save Authorized user username, password and Keystroke time in database against individual username.

Step 8: display account creation page

3.2.2 Algorithm for Feature Extraction

Begin;

Input password; //Character by character

int Size = *strglen*(password);

if $i = 0$; //extract key press & key release

do { **float** *timepress*[size], *timerelease*[size];

timepress[i] = *timestamp*(*evt.keypress*); *timereleases*[i]

= *imestamp*(*evt.keyrelease*);

$i++$; }

while ($i < size$);

// Calculate duration, latency & digraph.

for ($j = 0; j < size; j++$;)

{ **float** *duration*[size], *latency*[size], *digraoh*[size];

duration[j] = *timerelease*[j] – *timepress*[j];

```

        latency[j] = timerelease[j + 1] - timepress[j];
    digraph[j] = duration[j] - latency[j]; }
//Calculate keystroke as the mean value of the digraph
        for (i = 0, i < digraph.length; i ++;)
            {    keystroke = keystroke + digraph[i];
    KeystrokeTime = keystroke/digraph.length; }
Else
{    “go back to registration page”    }
End

```

3.2.3 Algorithm for User Authentication and Keystroke Verification

User opens the login page.

Begin;

// Test for password and username match

```

        if ((user.pass == password)&&(username = username))
    {
//Set threshold
    int threshold = 10;    //default threshold for password length is 10
        int length = strlen(user.pass);
        if length ≥ 11 && length ≤ 20;
    {    int threshold = 15;    }
        if length ≥ 21 && length ≤ 30;
    {    int threshold = 20;    }
// Test for keystroke
        if ((user.keystroke + threshold ≥ keystroke)&&(user.keystroke - threshold
            ≤ keystroke))
    {    “Login successful”    }
else
{    “Access denied due to keystroke conflict”    }

```

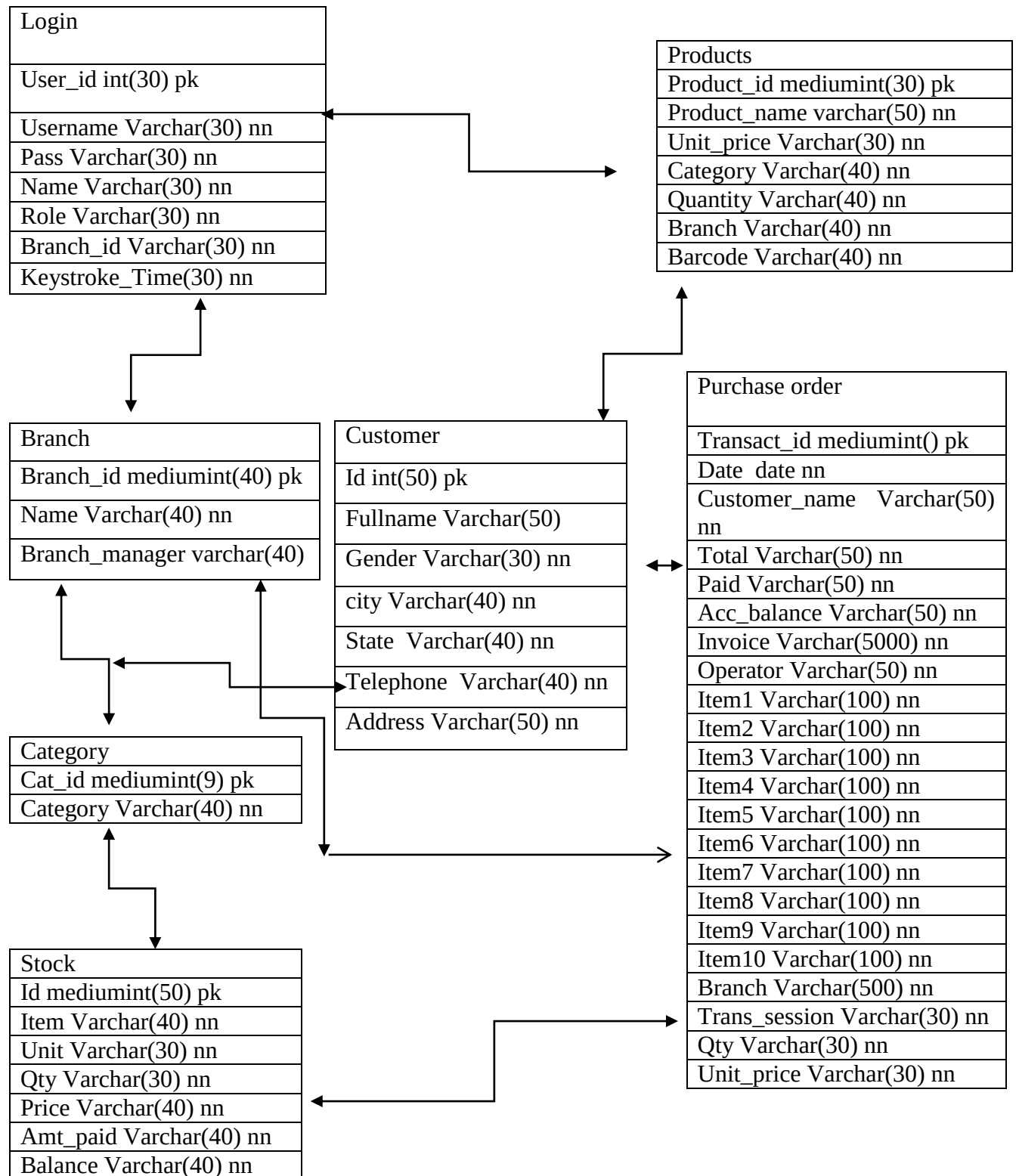
```
else  
{      “Password or username incorrect”      }  
End
```

3.2.4 Sales and Stock Processes

This step is after the login, the user click on the process he wants to perform operation on, follow the steps and submit after wards. The follow lists are the pages on the index page for performing the named operations;

- View Transaction
- Add Product
- Daily Report
- Transaction list
- Change password
- Create User Account
- Stock Category
- View stock
- Branch
- Logout

3.3 Relational Database Model for the System



Login Table

The user id, username, password, users' privilege, branch and the keystroke time are stored on the login table.

		user_id	username	pass	name	role	branch_id	Keystroke_time
☐	 Edit  Copy  Delete	19	balo	1234	azzeez	1	Lagos	197
☐	 Edit  Copy  Delete	20	sanni	tope	Sanni Bilikis	1	Lagos	140
☐	 Edit  Copy  Delete	21	bolaji	awijare	Bolaji	1	Akure	143
☐	 Edit  Copy  Delete	22	kemi	oluwakemi	Dr Mrs Abikoye	1	Lagos	192
☐	 Edit  Copy  Delete	23	yinka	sanni	Yinka Sanni	1	Ibadan	162
☐	 Edit  Copy  Delete	24	sanni	bisi	Bisi Sanni	1	Ado-Ekiti	265
☐	 Edit  Copy  Delete	26	dalegan	funmi	Funmi Dalegan	1	Lagos	159
☐	 Edit  Copy  Delete	27	salawu	oyin	Salawu Oyinda	1	Ado-Ekiti	293
☐	 Edit  Copy  Delete	28	aleem	malik	Aleem Malik	1	Akure	178
☐	 Edit  Copy  Delete	29	bilikis	temitope	Bilikis Temitope	1	Ado-Ekiti	181
☐	 Edit  Copy  Delete	30	nallah	bilikis	Naallah Bilikis	1	Ibadan	178
☐	 Edit  Copy  Delete	31	wasiu	amsat	Amsat Wasiu	1	Akure	215
☐	 Edit  Copy  Delete	32	mobolaji	bolaji	Sanni Mobolaji	1	Ado-Ekiti	198
☐	 Edit  Copy  Delete	33	sanni	bilikis	Sanni Bilikis Temitope	1	Lagos	187
☐	 Edit  Copy  Delete	34	deborah	olufemi	Olufemi Deborah	1	Ibadan	238
☐	 Edit  Copy  Delete	36	akala	abimbola	Akala Abimbola	1	Lagos	330
☐	 Edit  Copy  Delete	37	olaniyi	jubril	Olaniyi Jubril	1	Ado-Ekiti	237

4 RESULTS AND DISCUSSION

Create Account

This page is used for the creation of new user account by users with admin level privilege.

In this module, the keystroke feature is extracted from the password typed in by the authorized user when creating account to statistically calculate the Keystroke Time which will be saved in the database against each user.

Home | Add Product | Daily Report | Log out

Create Account

Username A value is required.

Password A value is required.

Retype Password A value is required.

Fullname A value is required.

Branch

Admin ☒

Figure 3: The create account page

- Branch: the branch selected will be profiled to the new user.
- Admin (if it is an admin user)

Creation of Keystroke Dynamics Authentication

This page shows the initial keystroke data of an individual user created which will be stored in the database after creating the account.



Figure 4: The keystroke created

Home | [Add Product](#) | [Daily Report](#) | [Log out](#)

Create Account

Username	sanni	A value is required.
Password		A value is required.
Retype Password		A value is required.
Fullname	Sanni Bilikis Temitope	x A value is required.
Branch	Lagos	
Admin	☒	
	Submit Reset	

Figure 5(a): Account creation for user 1

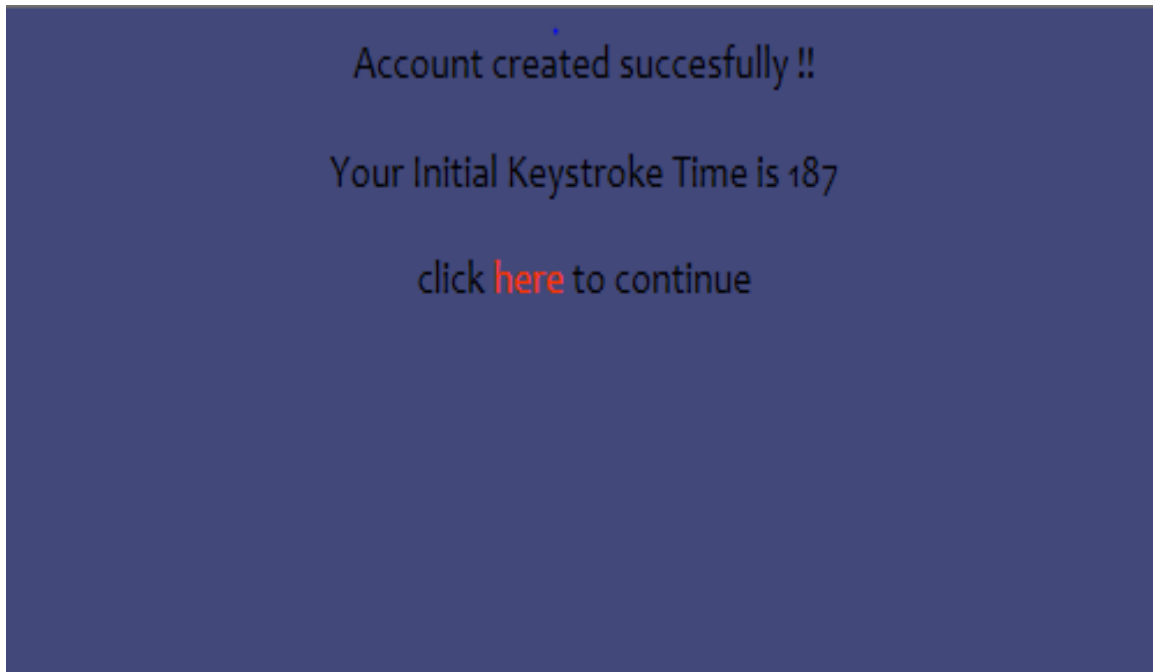


Figure 5(b): Keystroke dynamics authentication created for user 1

A dark blue rectangular box with a grid pattern. At the top right, there are links: "Home | [Add Product](#) | [Daily Report](#) | [Log out](#)". On the left, there is a vertical menu with "Create Account" highlighted. The form fields are: "Username" with value "deborah" and error "A value is required."; "Password" with masked characters "••••••" and error "A value is required."; "Retype Password" with masked characters "••••••" and error "A value is required."; "Fullname" with value "Olufemi Deborah" and error "A value is required."; "Branch" with a dropdown menu showing "Ibadan"; "Admin" with a checked checkbox; and "Submit" and "Reset" buttons at the bottom.

Figure 6 (a): Account creation for user 2

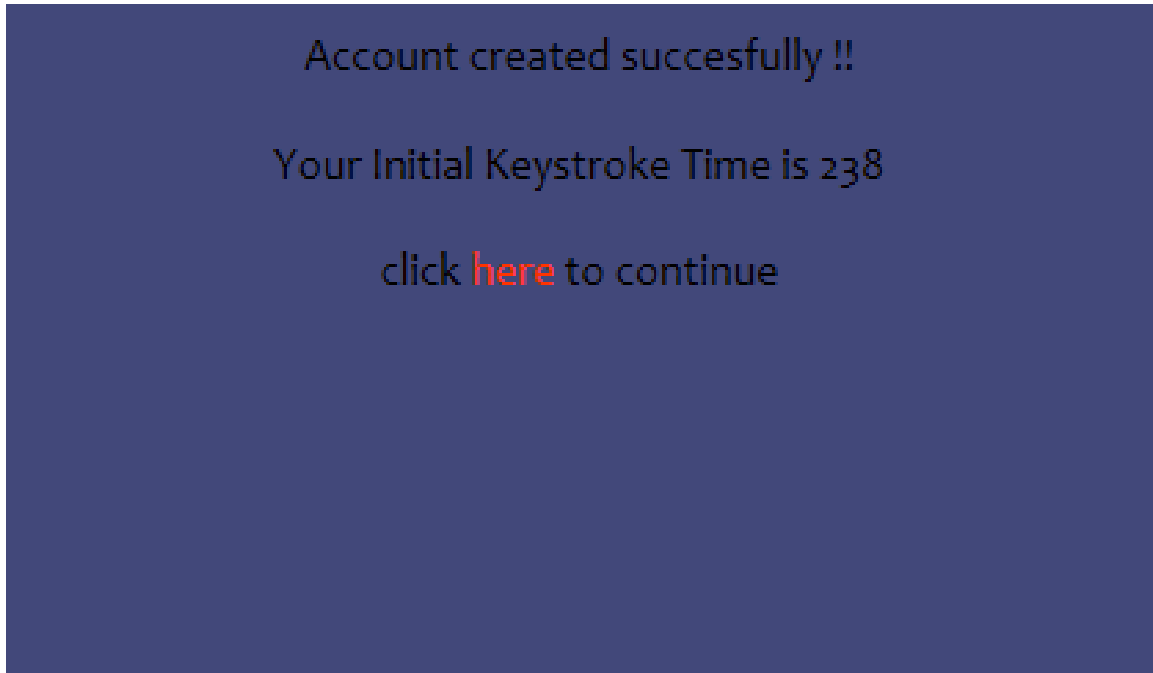


Figure 6 (b): Keystroke dynamics authentication created for user 2

Login Page

The login page is where users are accessed by identifying and authenticating the user through the username and password presented by the user. All other pages of the application will refer the user to the login page for authentication.



Figure 7: The application login page

- Username: enter username used for registration
- Password: is a secret word or alphanumeric used to gain admission into the system which can only be created by an authorized user.

Error Page for Wrong Login Details

This page shows the error, to inform the user that the username or password doesn't correspond with the initially stored in the database. The system only proceeds to keystroke verification only if the username and password corresponds.

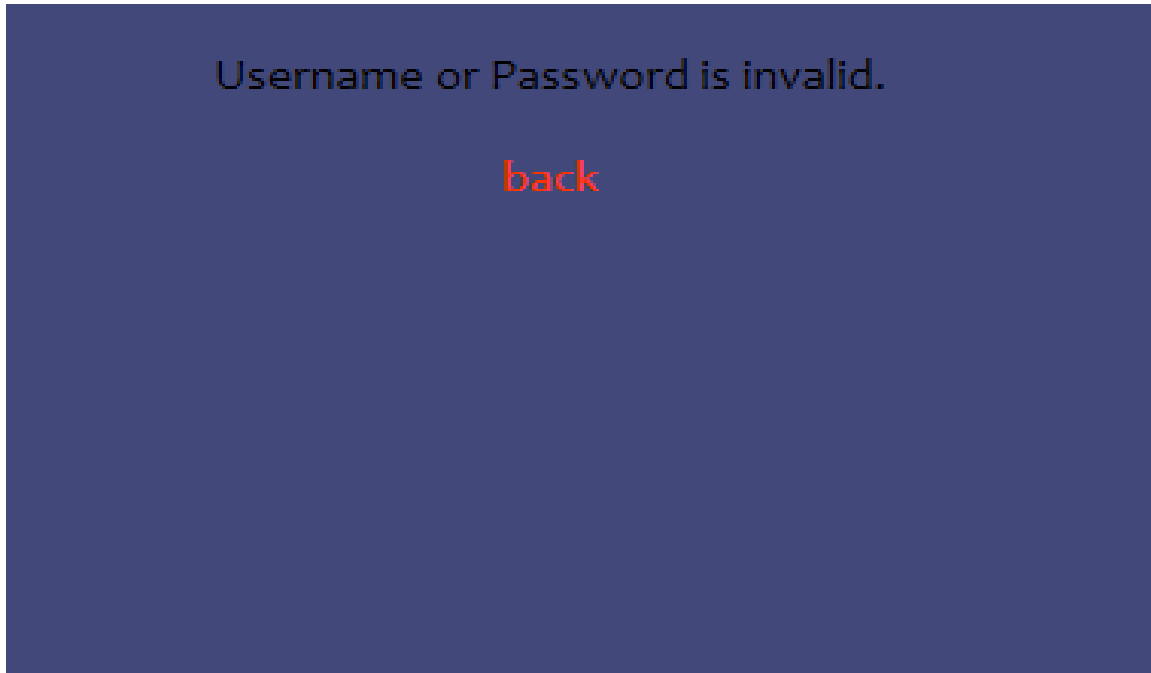


Figure 8: Error page for wrong username or password

- Back: it directs the user back to the login page

Error Page for Keystroke Dynamics

This page shows the error, to inform the user about the reason for being unable to login. It will get the information detail stored in the database against the present one from the login page. If a malicious transaction is suspected, even if the password is correct, the unauthorized user won't be able to login because of the keystroke data saved against each user in the database. The present keystroke data of an individual user might be more or less than initial keystroke data stored in the database. The page takes you back to re-login.

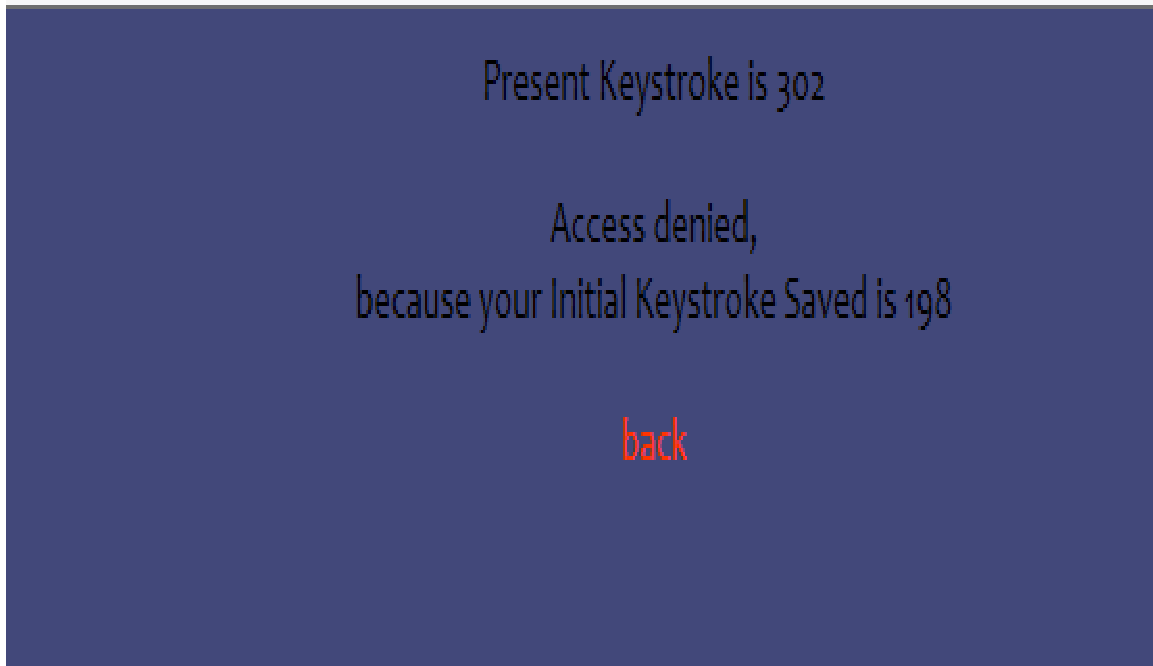


Figure 9: Error page for keystroke dynamics out of threshold

- Back: it directs the user back to the login page

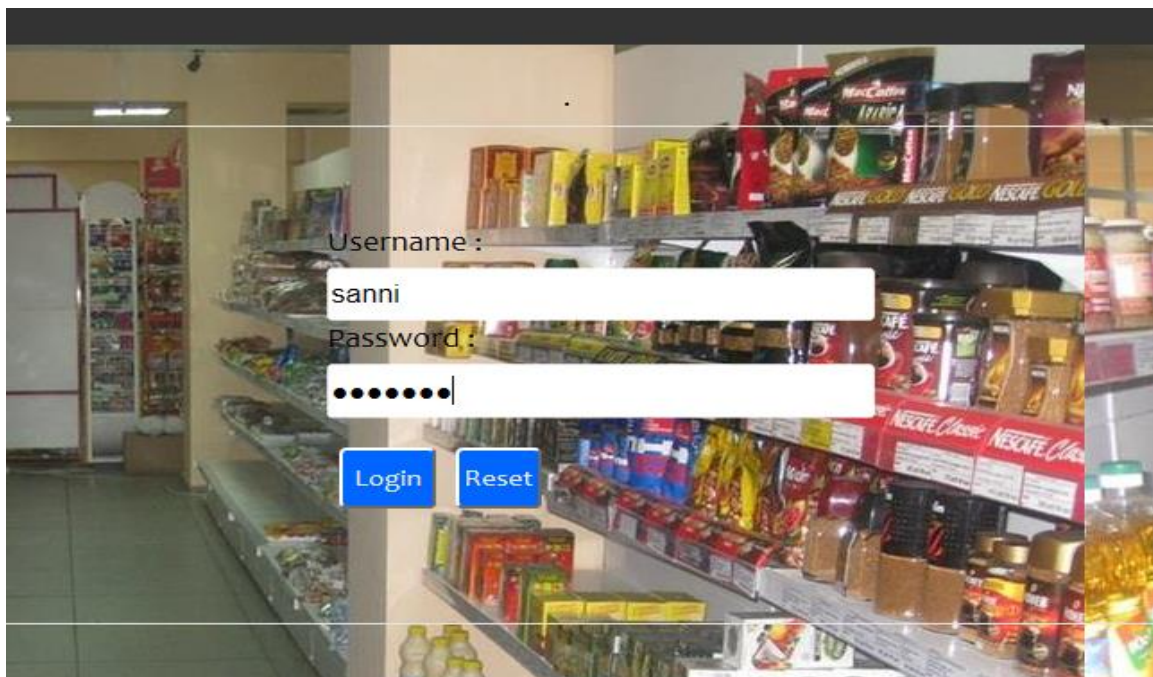


Figure 10(a): User 1 login page

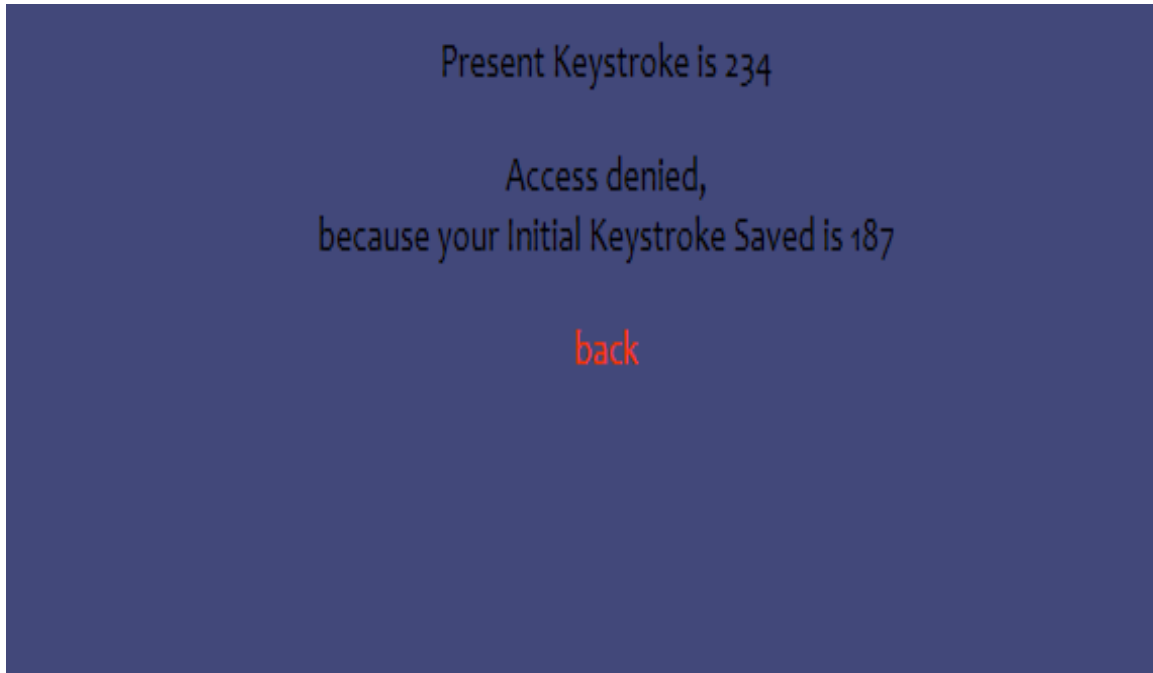


Figure 10(b): User 1 error page for keystroke dynamics authentication.



Figure 11 (a): User 2 login page

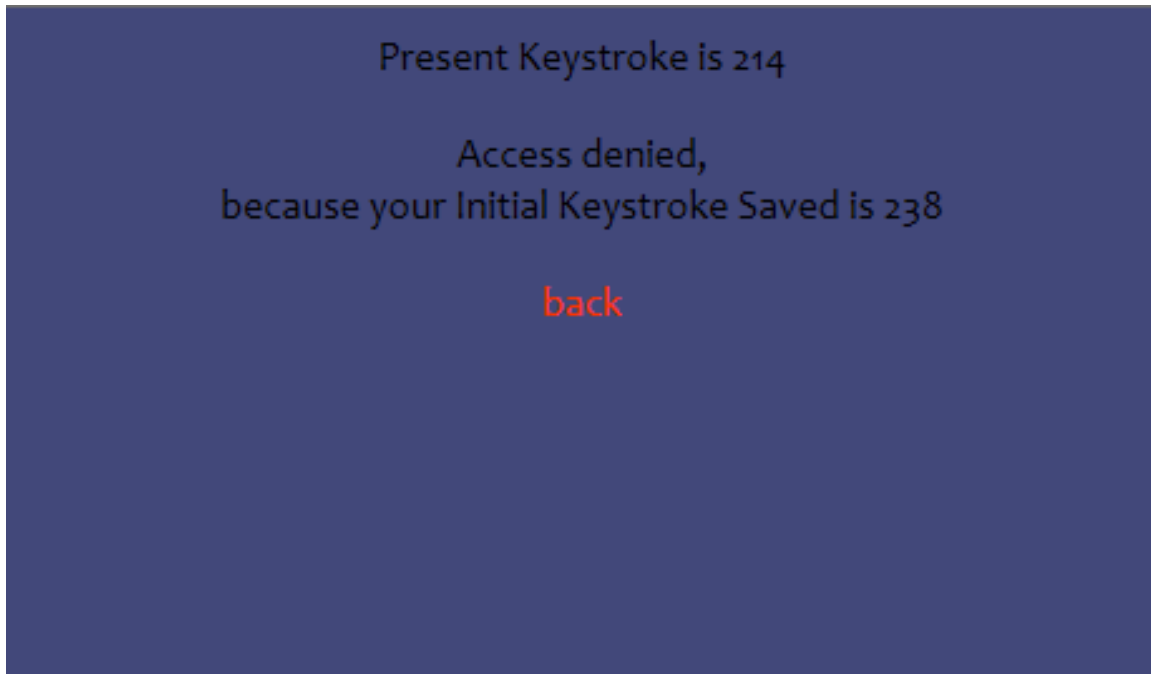


Figure 11(b): User 2 error page for keystroke dynamics authentication.

Home Page

This page is the initial page of the website, the point of entry to all the information stored within the application. It contains link to selection of all other available content. This page summarizes the aim of the work.



Figure 12: Home page

It contains the following options:

- Change password: this is where all the staff can change the secret word used, for a new user and when the user feels it is exposed.
- Create account: to create new account for staff.
- Manage users: this where the admin user can delete a staff id when resigned or fired
- Stock category: is the type of goods available for sales.
- View stock: this is where the staff can view the goods available in the stock.
- Transaction: is the day-to-day sale.
- Add product: is used to add product to the stock.
- Daily report: shows daily journal. An admin user can check for all staff transaction while the sales representative can see his transaction alone.
- Barcode Reader: shows transaction using a scanner or manual input of the product id.

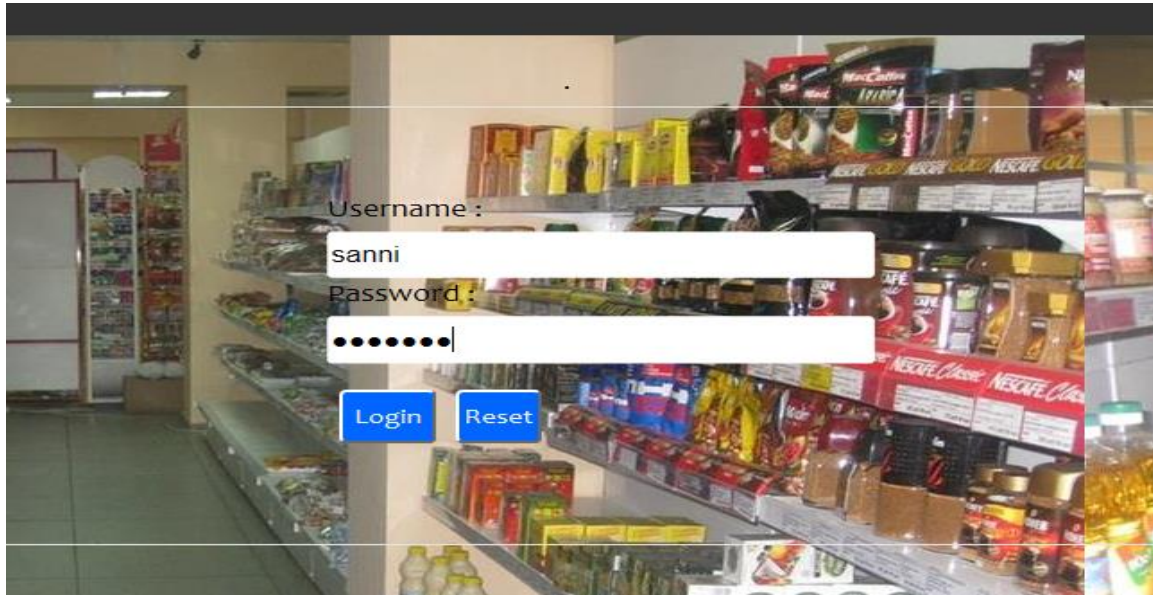


Figure 13(a): User 1 login page with correct username, password and keystroke

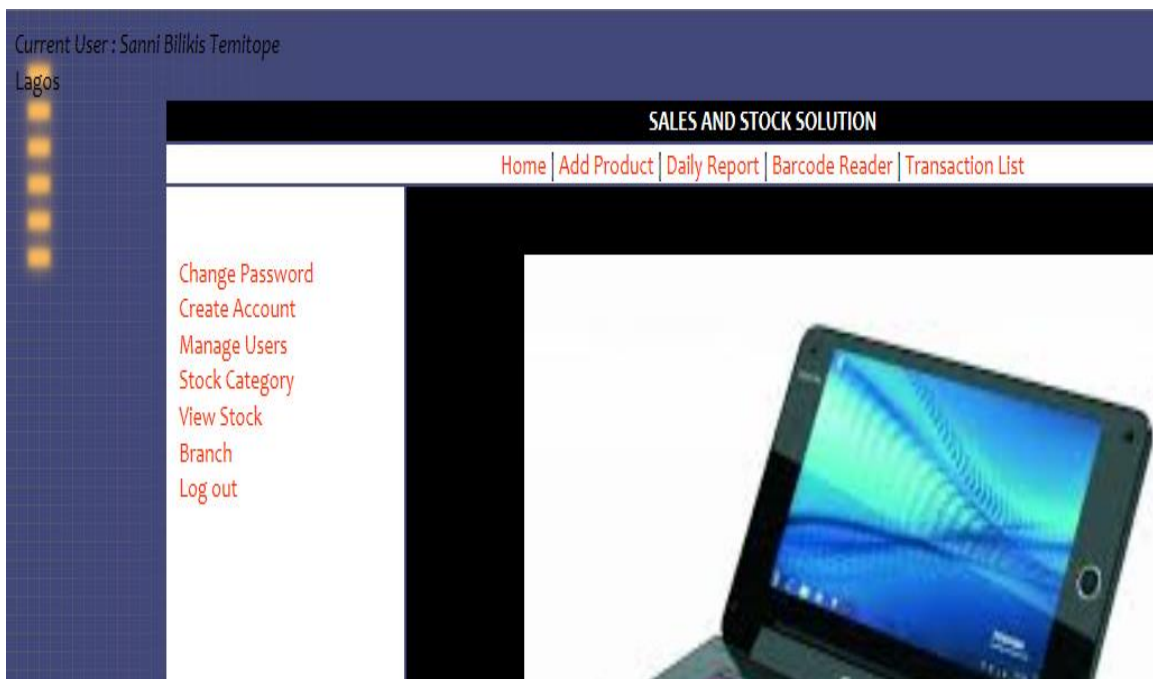


Figure 13(b): User 1 Home page after Keystroke Dynamics Authentication

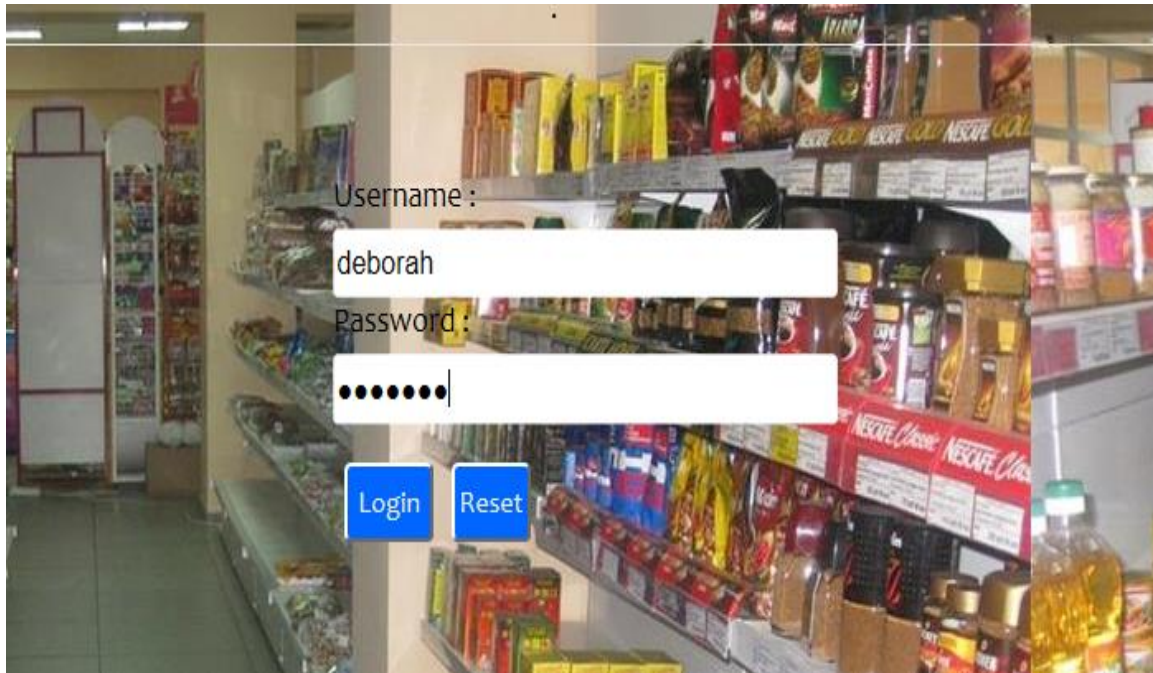


Figure 14(a): User 2 login page with correct username, password and keystroke



Figure 14(b): User 2 Home page after Keystroke Dynamics Authentication

Change Password

This page allows user to change the password to protect their accounts from fraudulent transactions. The keystroke data will be extracted from the new password which will be saved against the user in the database. It is advisable for a user to change their password every three months to protect their accounts and saves the company from losses.

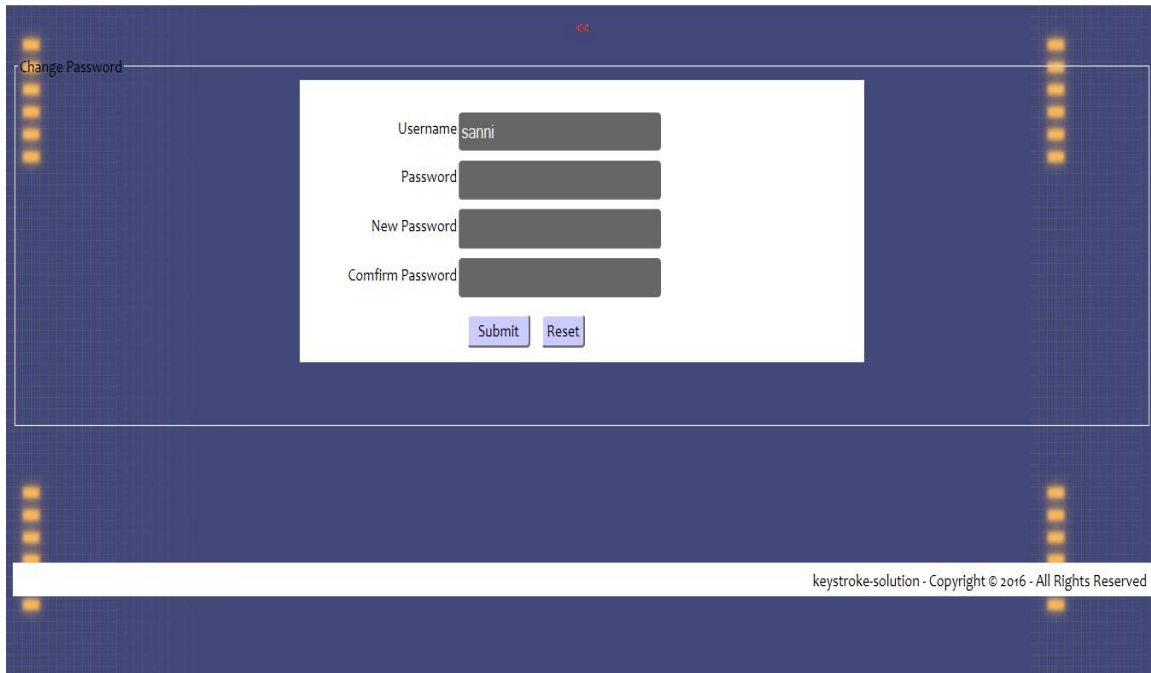
The image shows a web application interface for changing a password. The background is a dark blue grid with four vertical columns of five yellow dots each, one in each corner. In the top center, there is a red double-left arrow icon. The main content is a white rectangular form. Inside the form, there are four input fields: 'Username' with the text 'sanni', 'Password', 'New Password', and 'Confirm Password'. Below these fields are two buttons: 'Submit' and 'Reset'. The text 'Change Password' is visible in the top left corner of the form area. At the bottom right of the page, there is a copyright notice: 'keystroke-solution - Copyright © 2016 - All Rights Reserved'.

Figure 15: Change password page

Error Page for Change Password

This page occurs if the new password and the confirm password doesn't match.

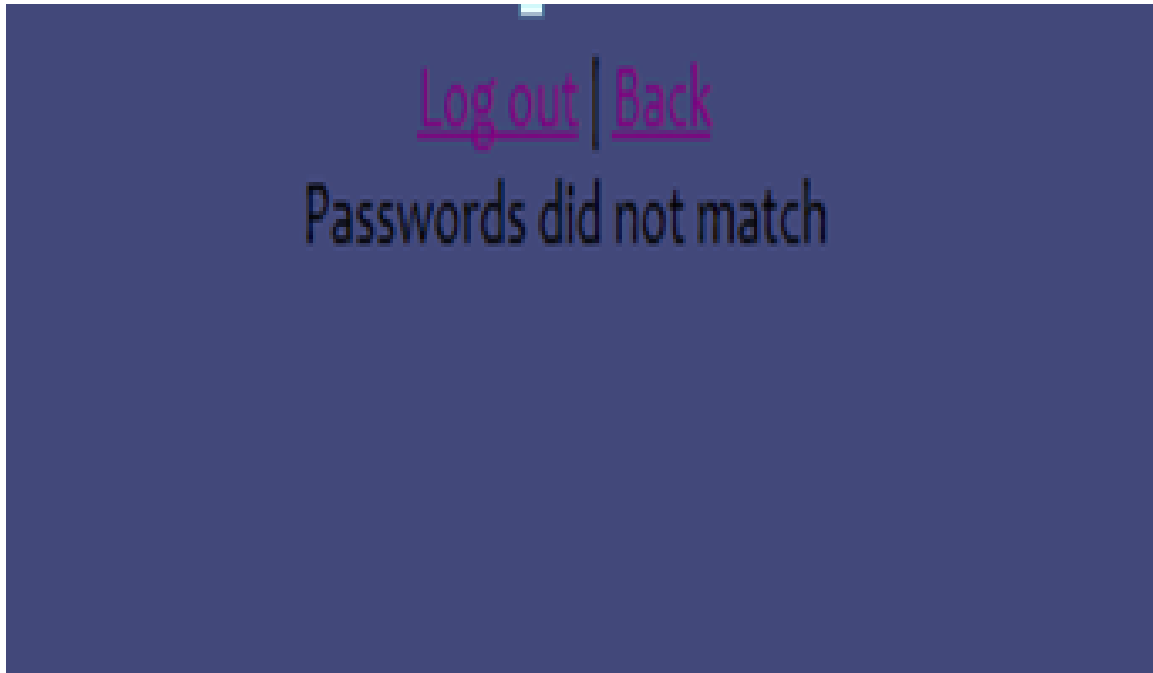


Figure 16: Error page for mis-match password

- Logout: exit the application.
- Back: it directs the user back to the change password page

5 CONCLUSION

In this work, a behavioral biometrics, keystroke dynamics authentication solution is proposed on the usual password authentication used for authorization. The inventory of different steps in business enterprises where taken with emphasis on stocking, transaction and staffing processing to develop an e-commerce system that a multifactor authentication is implemented on with the aim of enhancing the security system. The researchers implemented a behavioral biometric method, keystroke dynamics authentication static method on the usual passwords authentication for login to produce a multifactor authentication system that helps tackle the variety of security frauds involved in user login process, whether in house or from the outside by using the typing style of the authorized users which has been proven unique with the password. The researchers suggested a more secured method for Authentication, as well as a business solution for SMEs. This work can also detect whether a user is authorized or fraudulent which makes it secure. Experimental results show that the performance and effectiveness of this system demonstrate the usefulness of implementing it. The system is also scalable for handling large volumes of transactions. This new system meets user needs, easy to understand and can be used by both educated (professionals) and uneducated (local traders) users. This system has qualities such as reduction in the cost of adding new features to the existing system since the keyboard is the only hardware required and also built in maintenance view with low execution and response time.

REFERENCES

- ABERNETHY, M., AND RAI, S. 2012. Applying Feature Selection to Reduce Variability in Keystroke Dynamics Data for Authentication Systems. In proceedings of the 13th Australian Information Warfare and Security Conference, Perth, Western Australia, December, 2012, 17-23.
- ABUALGASIM, S.D., AND OSMAN, I. 2011. An Application of the Keystroke Dynamics Biometric for Securing PINs and Passwords. *World of Computer Science and Information Technology Journal (WCSIT)* ISSN: 2221-0741, 1(9), 398-404.
- AL-JARRAH, M.M. 2012. An Anomaly Detector for Keystroke Dynamics Based on Medians Vector Proximity. *Journal of Emerging Trends in Computing and Information Sciences*, 3(6), 988-993.
- VASTHI, S., AND SANWAL, T. 2016. Biometric Authentication Techniques: A Study on Keystroke Dynamics. *International Journal of Scientific Engineering and Applied Science (IJSEAS)* ISSN: 2395-3470, 2(1), 215-221.
- BAJAJ, S., AND KAUR, S. 2013. Typing Speed Analysis of Human for Password Protection (Based On Keystrokes Dynamics). *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN: 2278-3075, 3(2), 88-91.
- DAVENPORT, T. 1998. Putting the Enterprise into the Enterprise System. *Harvard Business Review*, 76(4), 121-131.
- EPP, C. 2010. Identifying Emotional States through Keystroke Dynamics. A thesis submitted to the college of Graduate Studies and Research in partial fulfillment of the Requirements for the Degree of Master of Science in the Department of Computer Science, University of Saskatchewan Saskatoon, Canada.
- FERREIRA, J., SANTOS, H., AND PATRAO, B. 2011. Intrusion Detection through Keystroke Dynamics. In proceedings of the 10th European Conference on Information Warfare and Security, Tallinn, Estonia, July 2011, 81-90.

GIOT, R., EL-ABED, M., AND ROSENBERGER, C. 2014. Keystroke Dynamics Authentication. Biometrics, In Tech, Chapitre 8. 2011. 978-953-307-618-8. <10.5772/170647>. <hal-00990373> 157-182.

GIOT, R., EL-ABED, M., AND ROSENBERGER, C. 2009. Keystroke Dynamics Authentication for Collaborative System. The IEEE International Symposium on collaboration Technologies and Systems (CTS), Baltimore, United States, May 2009, IEEE Computer Society, 172-179. <10.1109/CTS2009.5067478> .<hal-00432764>

KARNAN, M., AND KRISHNARAJ, N. 2012. A Model to Secure Mobile Devices Using Keystroke Dynamics through Soft Computing Techniques. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, 2(3).

MASOCHA, R., CHILIYA, N., AND ZINDIYE, S. 2011. E-banking adoption by customers in the rural milieus of South Africa: A case of Alice, Eastern Cape, South Africa. African Journal of Business Management, 5(5), 1857-1863.

MODI, J., UPADHYAY, H.G., AND THAKOR, M. 2014. Password less Authentication Using Keystroke Dynamics: A Survey. International Journal of Innovative Research in computer and Communication Engineering, 2(11), 7060-7064.

MONROSE, F., AND RUBIN, A.D. 1999. Keystroke Dynamics as a Biometric for Authentication. Future Generation Computer Systems, 16(2000), 351-359.

SAWANT, M.M., NAGARGOJE, Y., BORA, D., SHELKE, S., AND BORATE, V. 2013. Keystroke Dynamics: Review Paper. International Journal of Advanced Research in Computer and Communication Engineering, 2(10), 4018- 4020.

SCOTT, J. E., AND VESSEY, I. 2002. Managing Risks in Enterprise Systems Implementations. Communication of the ACM, 45(4), 74-81.

SHUKLA, P., AND SOLANKI, R. 2013. Web Based Keystroke Dynamics Application for Identifying Emotional State. International Journal of Advanced Research in Computer Communication Engineering, 2(11), 4489-4493.

SINGH, S., AND ARYA, K.V. 2011. Key Classification: A New Approach in Free Text Keystroke Authentication System. In proceedings of the 3rd Pacific- Asia Conference on Circuits and Communication Systems (PACCS), Wuhan, China, July, 2011, 1-5.

VANDOMMELE, T. 2010. Biometric authentication today. Seminar on Network Security.

Retrieved from: <http://www.cse.hut.fi/en/publications/B/11/papers/vandommele.pdf>