Texila International Journal of Management
ISSN: 2520-310X
DOI: 10.21522/TIJMG.2015.06.02.Art004

Multi-Factor Biometrics for Enhanced User Authentication in an E-Health System, Ghana

Article by Lazarus Kwao[1], Richard Millham[2], David Oppong[3], Wisdom Xornam Ativi[4]
[1]Ghana Baptist University College, Kumasi
[2]Durban University of Technology, South Africa
[3]Jain University, Bangalore, India
[4]University of Electronic Science and Technology of China
E-mail: l.kwao@gbuc.edu.gh[1]

Abstract

For most existing computer systems, once the user's identity is verified at login, the system resources are available to that user until he/she exits the system. In high-risk environments such as healthcare or where the cost of unauthorized use of a computer is high, a dynamic check of the user's identity is extremely important. This study evaluated the feasibility of multifactor authentication with biometrics, incorporating both traditional and the time dynamics-based techniques of keystrokes (behavioural) and fingerprint swipes (user's physical characteristics), for adoption into an eHealth system (DHIMS 2). The results indicate that individual authentication by Keystroke and Fingerprint dynamics yields acceptable results. However, when combined with the traditional methods of authentication, extremely high security is obtained than could be obtained by each paradigm acting independently. Hence, it is concluded that combining Keystroke and fingerprint dynamics with traditional authentication procedures into an eHealth system (DHIMS 2) will yield a system with improved account security and integrity of health information.

***Keywords**: DHIMS 2, Keystroke Dynamics, Fingerprint Dynamics, Biometrics, Multifactor Authentication, Ghana Health Service.*

Abbreviations

District Health Information Management Systems 2	DHIMS2
Multi-Factor Authentication	MFA
Ghana Health Service	GHS

Introduction

A major barrier to the successful implementation of e-Health systems, can be found in the growing problem of user authentication as picked up by both the research community and Information Systems (IS) security practitioners in recent times (Iakovidis, 1998; Prabhakar, Pankanti, & Jain, 2003; Miller & Sim, 2004; FERREIRAabd, Ricardo, Antunes, & Chadwick, 2007; Bath, 2008; Rindfleisch, 1997; Ben-Assuli, 2015; Dinev, Albano, Xu, D'Atri, & & Hart, 2016; Ozair, Jamshed, Sharma, & Aggarwal, 2015; Stamatian, Baba, & Timofe, 2013). A major user authentication challenge agreed by the authors, identified password issues as the most likely human error risk factor to impact an ehealth system adoption. The gravity of this problem is heightened because passwords are the primary user authentication method for several information systems (Coley, Kenderdine, Piper, & Martin, 2015; Bonneau, Herley, Van Oorschot, & Stajano, 2015; AuthenticationWorld.com, 2015).

Practical problem setting

Several Sub-Saharan Africa have adopted and deployed a completely web-based and standalone national E-Health System, hereafter referred to as District Health Information Management System (DHIMS) (Karuri, Waiganjo, Daniel, & Manya, 2014; Gathogo, 2014; Poppe, 2012). DHIMS is used as a national health information system for data management and analysis purposes, for health program monitoring and evaluation, as facility registries and service availability mapping, for logistics management and for mobile tracking of pregnant mothers in rural communities (DHIS 2 Documentation, 2016;

Dehnavieh, et al., 2019; Manya, Øverland, Titlestad, Mumo, & Nzioka, 2012).

DHIMS have helped improve the policy and regulatory environment, the uncoordinated nature of health information reporting and improving the quality of health information management. This has mostly been in response to request from donor agents such as UNDP, WHO, Norad, Research Council of Norway, PEPFAR, USAID, The Global Fund, the Korean International Cooperation Agency (KOICA), and Samsung Corporation continue and the University of Oslo to support the digitization of health information (Poppe, 2012; DHIS2 Documentation Team, 2012; Dehnavieh, et al., 2019).

After DHIMS was implemented in 2007, it did not see any essential maintenance and upgrading to meet the changing demands of the service and stakeholders. This lack of pace with developments in the sector has forced stakeholders such as the area-specific health programmes (e.g., malaria control or HIV/AIDS) to develop parallel reporting systems to enable them to meet data demands of their sponsors. The situation resulted in a fragmented Health Information System (HIS) and made the data management process prone to many errors with the knock-on effect of many local-level managers distrusting their data, hence rarely using it in decision-making or predicting trends in healthcare delivery (Adaletey, Poppe, & Braa, 2013). In turn data collation and aggregation at central level was made even more difficult. This resulted in heavy reliance on international estimates.

Ghana Health Service (GHS) and its partners in 2010 upgraded DHIMS to DHIMS2 by adopting DHIS 2 as a platform. Their decision identified a number of issues to review (Dehnavieh, et al., 2019; DHIS2 Documentation Team, 2012) including, duplication of efforts due to multiple e-Health systems being implemented around the country, difficulty in gauging progress in the health sector, difficulty in determining intra-district reporting rates, limited analysis capabilities and often conflicting statistics of the Excel-based databases and lack of ownership of the existing HIS. GHS ensured an in-house capacity building and modification of the DHIS2 platform to adapt it as DHIMS2, trained by the technical assistants from the University of Oslo through the Health Information Systems Programme (HISP). DHIMS 2 is "an integrated, web-based, country-owned and managed, national health information system that integrates quality data used at all levels to improve health service delivery" (Manya, Øverland, Titlestad, Mumo, & Nzioka, 2012; Awoonor-Williams, et al., 2013; Nyonator, Ofosu, & & Osei, 2013).

GHS controls who accesses GHS data and what they can see and do. Once you set up a user, only trusted Data Center operational staff access GHS data. DHIMS2 offer multiple permission levels that let us limit the access privileges of each user. Districts data travels between your computer and GHS server it is encrypted by a technology called Secure Sockets Layer (SSL) using 128-bit encryption. This is the same technology used by banks and offers the highest level of encryption currently supported by commercial Web browsers. DHIMS2 uses advanced, industry-recognized safeguards and procedures, such as password-protected login, with encryption technology and firewall-protected servers as its main user authentication method (Nyonator, Ofosu, & & Osei, 2013). Each DHIMS2 user has an online account created with a unique password.

A simple password is a primary choice when it comes to password selection, such as date of birth, nickname, initials, and regular dictionary words (Pinkas & Sander, 2002; Wang & Wang, 2015). Nevertheless, the ability for passwords to provide confident and secure authentication has been wearing, due to reasons such as the wrongful use of password such as easily guessed and comprised by a hacker and increased intrusion attacks (Anwar, et al., 2015; Coley, Kenderdine, Piper, & Martin, 2015). To aggravate the situation, users always tend to use the same or similar password for multiple systems (Wash, Rader, Berman, & Wellmer, 2016; Li, Wang, & Sun, 2016). These bad usage habits contribute to the deterioration of knowledge-based authentication.

Another major issue with textual password authentication is its susceptibility to credential theft (Shen, Yu, Xu, Yang, & Guan, 2016; Missaoui, Bachouch, Abdelkader, & Trabelsi, 2018). So, if a hacker gains access to a person's account via a data breach, all the other accounts for that person can become vulnerable due to the stolen credentials. That problem is multiplied typically because hackers are not only accessing one person's account but hundreds or thousands at a time.

DHIMS 2 deals with a far more complex constellation of roles and sensitive data: doctors, patients, pharmacists, insurance companies, medical administration, etc. Thus, health data must be protected and unauthorized access prevented. (Dasgupta, Roy, & Nag, 2017; Dinker, Sharma, Mansi, & Singh, 2018; Frank, Biedert, Ma, Martinovic, & Song, 2013).

Challenges from the current system are issues relating to in-depth health information security; where the system (1) cannot check user identity in the login phases; (2) is weak against the impersonation attack and privileged-insider attacks; and (3) does not provide dynamic authentication to explore the possibility to establish the identity of the intruder or adversary for forensic evidence (surveillance).

Related literature

Having several passwords for different purposes can overload the human memory capabilities as the level of passwords complexity increases (Carnegie Mellon Computer Emergency Response Team, 2004). In a study conducted by NIST (1992), over 50% of incidents that occur within government and private organizations have been connected to human errors. Research by Wood and Banks (1993) agrees that human error is one of the main factors causing up to 52% of corporate information damage due to information security lapses. Previously, the information technology industry focused too much attention on managing or eliminating the risk of malicious intruders invading private company databases. However, in recent times, research has proven that human error makes up as much as 65% of incidents causing economic loss for a company and that only 3.0% or less are security breaches caused by external threats such as computer hackers (Boujettif & Wang, (2010), Kreicberge (2010) and Brady (2011). Although external malicious intruders can be costly to organizations, these intentional acts causing security breaches are among the lowest risk of information security incidents (Li, Wang, & Sun, 2016). The organizational effort to address the human factor risks of authentication is minimal, although it is the highest form of information security incidents (Wood & Banks Jr, 1993; Carstens, McCauley-Bell, Malone, & DeMara, 2004).

To fill the gap, the need for a second layer of authentication in information systems is significant as confirmed by (Abdullah, Abdullah, Ithnin, & Mammi, 2008; Zheng, Liu, Yin, & Liu, 2009; Alsultan & Warwick, 2013), (Zaeem, Manoharan, Yang, & Barber, 2017). Multi-Factor Authentication (MFA) with biometrics is amongst the most promising alternative in user authentication research as opposed to single sign-on upon entry or just a strong authentication in a single activity (Abomhara, Gerdes, & Køien, 2015; Gebrie & Abie, 2017), (Erlich & Zviran, 2009; Rajamäki & Pirinen, 2017). MFA with biometrics makes the user confident, that the data is safe and secured because it combines two or more biometric methods, thus, enables stronger authentication by reducing the risks of compromised passwords. It works by combining something you know (such as a username/password combination) with something you have (such as a text message code on your mobile phone) or something the user is, (like a fingerprint, optics, voice or signature). By combining two or more distinct protocols, you decrease the likelihood of someone using stolen credentials to attack your systems by 52 percent, according to the 2015 Annual Report to Congress on the Federal Information Security Management Act (Harris, 2016).

Many researchers have conducted several studies in developed countries to understand the adoption of MFA with Biometrics. However, a limited number of studies were conducted in developing counties, and their findings are insufficient to provide meaningful insight into predicting and explaining what factors influence end-users and their organizations to adopt MFA with Biometrics as an enhanced authentication technique. MFA with Biometrics is nascent in health systems in developing counties.

Research objective

This paper develops an enhanced authentication technique that meets authentication constraints of DHIMS 2 using Multi-Factor Authentication with Biometrics: A Study of the District Health Information Management Systems 2, Ghana.

Research design

A Research Design guides the researcher in planning and carrying out the study in a way that is most likely to achieve the intended goal (Black, 1999). Design Science Research (DSR) was deemed appropriate for this study. DSR focuses on the development and performance of (designed) artefacts with the explicit intention of improving the functional performance of the artifact (March & Smith, 1995; Kuechler & Vaishnavi, 2012). Its application is most notable in the Engineering and Computer Science disciplines, though it is not restricted to these and can be found in many disciplines and fields (Hevner & Chatterjee, 2010). In DSR, as opposed to explanatory science research, academic research objectives are more pragmatic.

Research in these disciplines be a quest for understanding and improving human performance (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). Through DSR, a prototype model was adopted in designing the proposed system because it permitted more flexibility for consideration of the system functionalities. Further, this model made it easy to discover mistakes associated with the system functionalities and features at the early stages of the system design. Therefore, the development of the proposed authentication technique to supplement passwords authentication in the web-based system was done along with the structures of prototyping techniques through a series of experimental designs.

Biometric techniques used in the proposed authentication system

Fingerprint Dynamics Authentication Technique (Physical)

Just like traditional fingerprint systems make use of a biological feature (fingerprint pattern) unique for every person, the relatively novel technology of fingerprint dynamics makes use of the timing characteristics of individuals' finger movements to achieve the same goal. The technique exploits the fact that every individual swipes his/her finger on a fingerprint scanner in a specific way, with precise and noticeable timing characteristics. The study aims to research this technique for inclusion in multifactor authentication for the DHIMS 2 health information system.

Experiment design

An experiment was conducted to evaluate the feasibility of incorporating fingerprint dynamics in traditional fingerprint authentication systems. It involved the following activities:

A. Data collection
B. Feature extraction
C. Algorithm Selection and Training
D. Performance evaluation

The following figure illustrates the workflow.

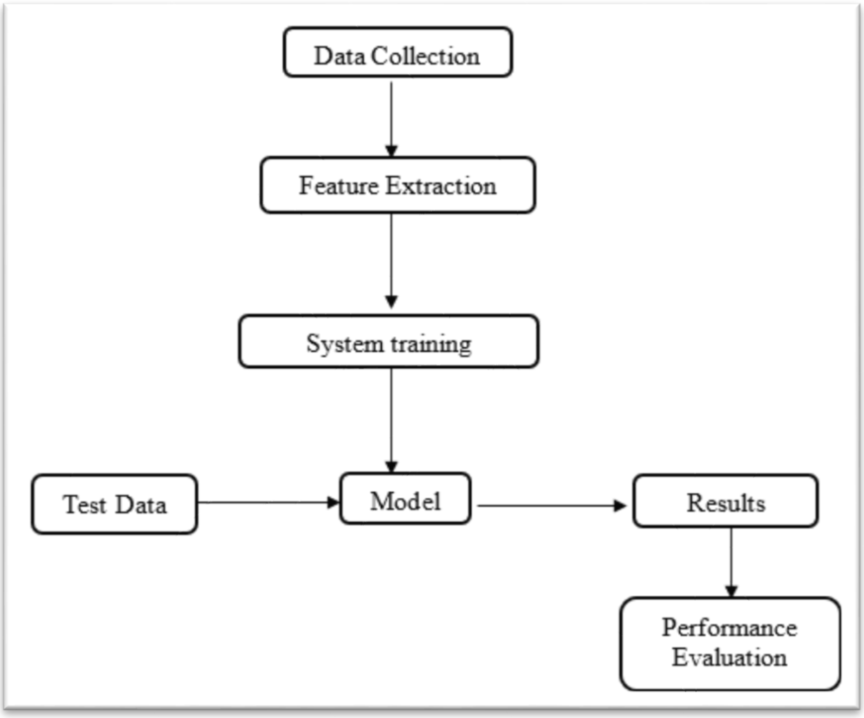


Figure 1. Workflow for development of fingerprint dynamics authentication system

A. Data collection

Fingerprint dynamics data were collected from a pool of 26 volunteers.

The data collection system consisted of two modules:

- Hardware module
- Software module

Hardware module

The hardware module was a custom-built circuit using an LED under a constant light source. When a test subject swipes his finger over the LED, a voltage is generated which is used to modulate a sine wave. This is then amplified and fed into the audio port of a computer for further analysis. This configuration ensured a significant reduction in the cost of experimenting and assured volunteers that the data collection process was on an anonymous basis.

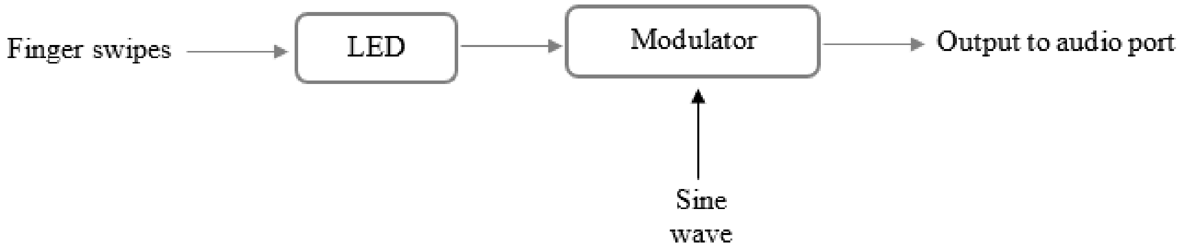


Figure 2. Description of the hardware module for data capturing

Software module

The software module was designed completely using MATLAB version R2019a. It was responsible for recording “audio” input from the hardware module and extracting the necessary features, which were then saved to a text file to be later fed to the training algorithms.

A set of experiments carried out by Bhardwaj, Londhe, & Kopparapu (2016), demonstrate that once users are familiar with fingerprint capture systems, most of them take less than nine seconds to scan their fingers in a sequence of five swipes. This works out to about 1.8 seconds per finger swipe. Hence, for a single sample, data capture from the hardware module was enabled for 18 seconds to accommodate the case that a test subject decided to swipe all ten fingers. This is in agreement with Kotani & Horii (2005) and Montalvão, Freire, Bezerra, & Garcia (2015) who have stated that system performance deteriorates dramatically when the capture sequence length falls below ten. Data sampling at the audio port was carried out at MATLAB’s default frequency of 8000 Hz. Four of such samples were taken for each test subject to improve the accuracy of the training procedure.

B. Feature extraction

Feature extraction is considered to have a substantial impact on system performance (Yu & Cho, 2003; Yu & Cho, 2004). From the data collected, two parameters are naturally evident: flight time – the duration between the release of a finger and the successive press of a finger; and dwell time – the amount of time between the press of a finger and release of the same finger. Given captured data as a vector $[P_1, R_1, P_2, R_2, \dots, P_n, R_n]$, where P_i and R_i represent the press and release times for the i-th finger, respectively, the extracted feature keeping in tune with Yilin Li et al., (2011) is given by

$$F = [\, R_1 - P_1, P_2 - R_1, P_2 - P_1, R_2 - R_1, R_2 - P_2, \dots, P_n - R_{n-1}, P_n - P_{n-1}, R_n - R_{n-1}, R_n - P_n \,]$$

which is a combination of flight and dwell times.

C. Algorithm selection and training

The Nearest Neighbor algorithm (using Scaled Manhattan Distance) and Support Vector Machine (SVM) algorithm, all provided in MATLAB’s Statistics and Machine Learning Toolbox were used. Killourhy & Maxion (2009) have proven that these produce excellent results for similar problems.

D. Performance evaluation

The performance curves below represent the outcome of the tests carried out on the derived models for each of the algorithms.

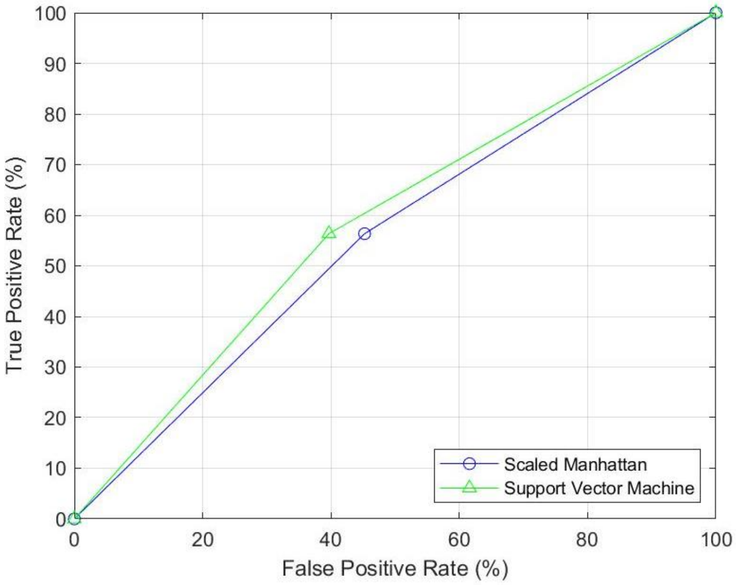


Figure 3. ROC curves for authentication using fingerprint dynamics

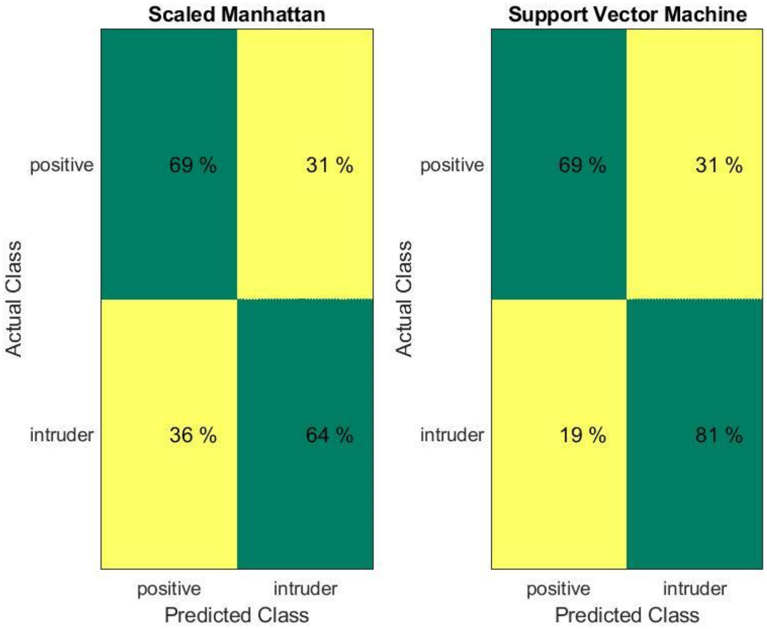


Figure 1. Confusion matrices for authentication using fingerprint dynamics

The following were observed:

1. Both algorithms exhibit the same average true acceptance rate; the Support Vector Machine algorithm, however, has higher individual true acceptance rates.
2. The average true acceptance rate stays above 65% for both algorithms.
3. SVM produces the lowest false acceptance rate (19%).
4. False acceptance rates stay below 40% for both algorithms.

Keystroke Authentication Technique (Behavioral)

Keystroke dynamics or typing dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard (Obaidat & Sadoun, 1997; Karnan, Akila, & Krishnaraj, 2011; Alsultan & Warwick, 2013). Keystroke dynamics is a behavioural biometric; this means that the biometric factor is ‘something you do’. Conceptually closest correspondence among biometric identification systems is signature recognition. In both signature recognition and keystroke dynamics, the person is identified by their writing dynamics which are assumed to be unique to a large degree among different people. Several names identify the technique: keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms (Obaidat & Sadoun, 1997; Karnan, Akila, & Krishnaraj, 2011).

Experiment design

The initial stage of the data collection involved collecting user typing data samples using a structured text (i.e. username and password). The writing samples that were used in this part of the data collection were a collection of 5 instances of every participant user credentials. A large amount of typing data needed to be recorded in order to create good reference profiles. However, this required users to be typing for a significant amount of time. We hoped to make the experience more bearable by having interesting/humorous writing samples. The typing samples totalled at least 8 characters forming the password and at least 4 characters forming the username. The data logged were: key that was pressed, time the key was depressed, and time the key was released. The time recorded was the amount of time passed since the start of the application and the unit of measurement was in milliseconds. The data structures used to store this data was a multidimensional 2-dimensional array table. The key-code of every character was determined by the embedded JavaScript as when the participants invoke the keys that form their user credentials by appending the keystroke timings of each character typed.

Once a user finished typing the 5 instances, all the data that was logged is processed and first inserted into a MySQL database and then an acknowledgement is made to notify that a successful writing sample had just been captured but before the data is stored it goes through series of process. If an error occurs anywhere in the process, the error message will prompt the user to follow the expected rules set about the user credentials in order to proceed. Because of the limitation of time, this project only collected data from Latin characters such as A-Z and the “space”, and “@”. The difference between uppercase and lowercase is assumed to be handled by the multi mixtures in each key. All other unsupported characters (e.g. Backspace key and delete key) would be removed from the raw data to avoid recording keystroke timings of most outliers. The 26 volunteers submitted a complete 5 instances of their typing samples which are the data that will be used to feed and evaluate the proposed system.

The following steps were carried out in the experiment to evaluate the feasibility of user authentication by keystroke dynamics:

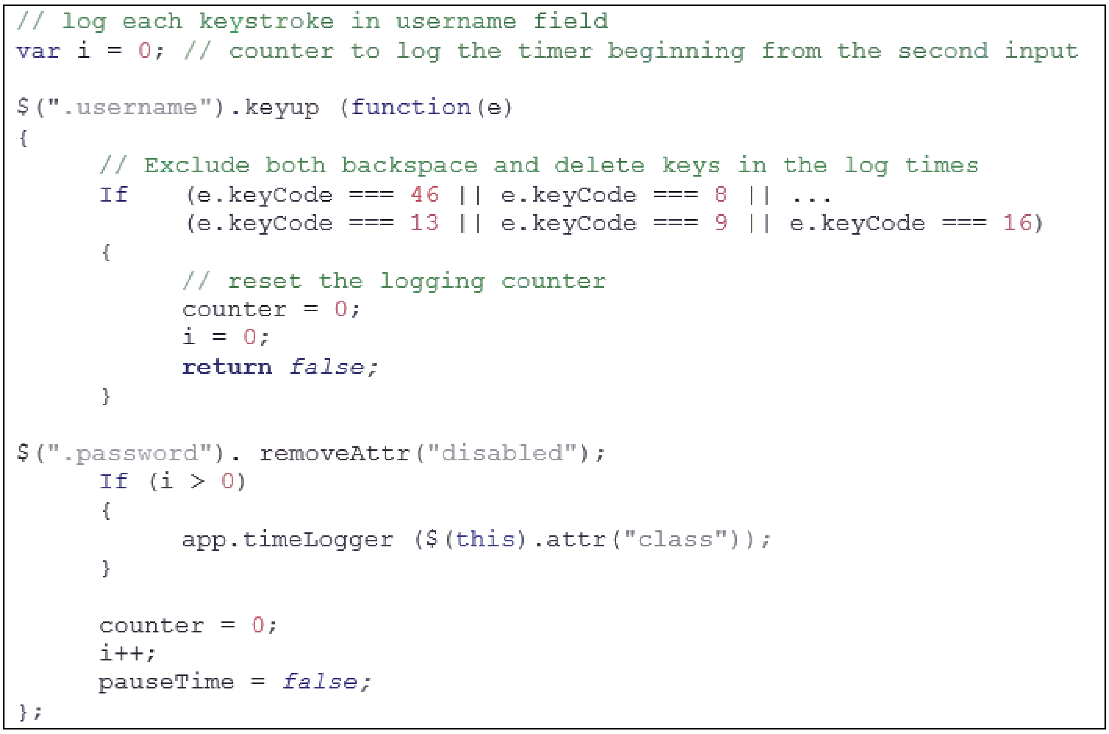
A. Data Acquisition
B. Feature Extraction
C. Algorithm Selection and Training
D. Performance Evaluation

Each of these is explained further;

A. Data acquisition

Collection of data through the proposed algorithm can also be categorized into two main procedures the Data Preprocessing Stage and the Data Feature Extraction Stage.

In the Data Preprocessing Stage, unwanted keystroke timings are removed from the main list keystroke timings that are used in the next stage Data Feature Extraction Stage. With the Data Preprocessing Stage, the proposed algorithm is designed to remove outliers in the form of unwanted keystrokes timings recorded during data acquisition from users. It further describes the actual parameter used to extract the final keystrokes timings that are used as the main benchmark for user authentication. These outliers removed at the Data Preprocessing Stage, are keystroke timings of special keys which are the backspace, delete, enter, shift and tab keys. First, in excluding some unnecessary key characters typed, the individual key codes of these three key characters were included in the code for the exclusion of their keystroke timings. The below code snippet indicates the portion of the algorithm that removed unwanted keyed characters in a submitted text.



```
// log each keystroke in username field
var i = 0; // counter to log the timer beginning from the second input

$(".username").keyup (function(e)
{
      // Exclude both backspace and delete keys in the log times
      If    (e.keyCode === 46 || e.keyCode === 8 || ...
            (e.keyCode === 13 || e.keyCode === 9 || e.keyCode === 16)
      {
            // reset the logging counter
            counter = 0;
            i = 0;
            return false;
      }

$(".password"). removeAttr("disabled");
      If (i > 0)
      {
            app.timeLogger ($(this).attr("class"));
      }

      counter = 0;
      i++;
      pauseTime = false;
};
```

Figure 2. Code Snippet for removing backspace, delete, enter, shift and tab keys

Figure 5, demonstrates how the system restricts and removes keystroke timings of special keys (backspace, delete, enter, shift and tab keys), which are termed as outliers. The script illustrates in Figure 5, shows how special character (backspace, delete, enter, shift and tab keys) on the keyboard are excluded from forming the actual extracted keystroke timings from the users of the system. The key code corresponding to each key character is as follows, Tab = 9, Enter = 13, Delete = 46, Backspace = 8 and Shift = 16. These outliers are removed because they are not part of the actual character sets that a user intended to include in his/her user credentials (passwords and username) but used them as a result of getting the actual character set typed in case there is an error. Users hit the ‘delete’ and the ‘backspace’ keys to remove or delete mistakenly type characters. The user also presses the tab key to move the computer’s focus from one control onto the other. For instance, after the user has finished typing the username, he/she may press the tab key to move the insertion cursor from the username textarea onto the password textarea. Therefore, the script is responsible for removing and restricting the log times of these keys from forming part of main extracted keystroke timings that can be used as a benchmark for verifying users to the system.

B. Feature extraction

The next stage to Data Preprocessing is the Data Features Extraction Stage. In order to use the keystroke dynamics to verify users, this study is based on some features, which were captured from keystroke events invoked through key-pressed and key-down cases. These features which are ‘***keystroke latency****’* (flight time), ‘***keystroke duration’*** (Source or dwell time) and ‘***locate time****’* (Terminus) can be acquired from processing the embedded JavaScript and PHP script. In description, ***keystroke duration*** also known as the ***dwell time*** is the time taken in “Pressing down” a same keystroke while ***keystroke latency*** also known as the ***flight time*** is the period taken in “Releasing up” the same keystroke Also, ***locate time****’* also known as the ***Terminus*** is referred as the period between “Releasing time” of the previous key and “Pressing time” of next key. All these features were put together to determine the time every character way keyed to the system by a user and used to draw the typing pattern of every participant enrolled in the system. All these features are captured in milliseconds and calculated upon, to form the bounds of the pressed keys.

The same procedure used in extracting training features from fingerprint dynamics data, as explained above, was applied here also, based on flight and dwell times, this time defined for key presses of a computer keyboard.

Thus,

$$F = R_1 - P_1, P_2 - R_1, P_2 - P_1, R_2 - R_1, R_2 - P_2, \dots, P_n - R_{n-1}, P_n - P_{n-1}, R_n - R_{n-1}, R_n - P_n$$

where P_i and R_i represent the press and release times, respectively, of the *i-th* key for a single password, typed.

C. Algorithm selection and training

The researcher determined that the experiment being carried out qualified as a supervised learning problem. Accordingly, the following algorithms were selected in consultation with the MATLAB eBook series on machine learning and previous work carried out by (Killourhy & Maxion, 2009):

a. Support Vector Machine (SVM)

b. Decision tree

c. Nearest Neighbor Classification (using Scaled-Manhattan distance)

D. Performance evaluation

Each algorithm-based model was tested to verify the usefulness of the keystroke authentication technique. Performance (Receiver Operating Characteristics – ROC) curves as well as confusion matrices were generated, and are shown below.

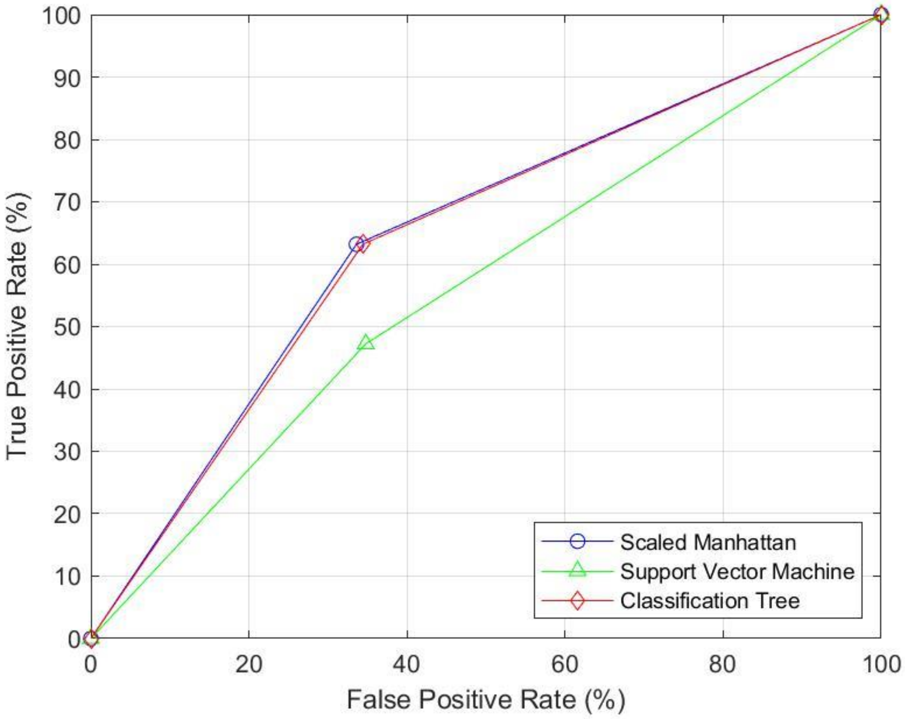


Figure 3. ROC curve for authentication using keystroke dynamics

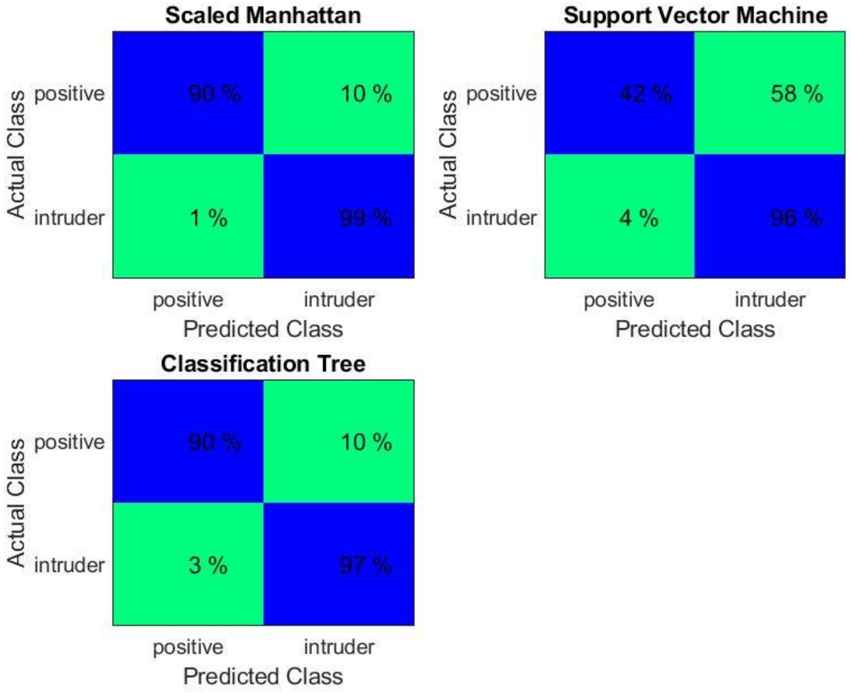


Figure 4. Confusion matrices for authentication using keystroke dynamics

The following were observed:

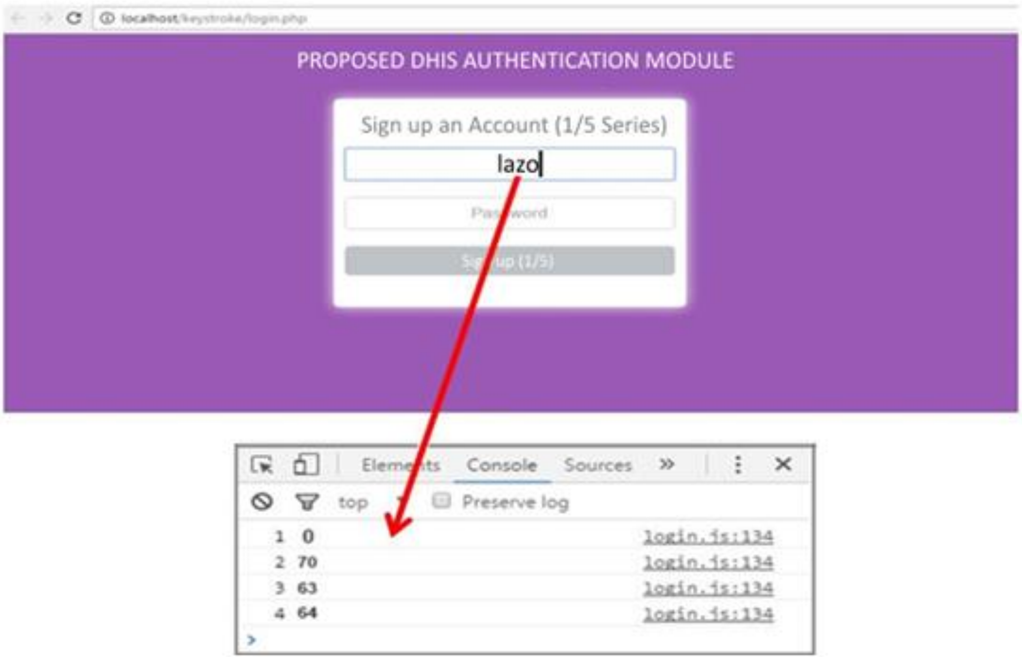
1. The Scaled-Manhattan classification algorithm produces the highest individual true acceptance rates and lowest individual false acceptance rates.
2. The classification tree algorithm produces a result that is close to the Scaled-Manhattan algorithm.
3. For these two algorithms (mentioned in 1 & 2 above), average true acceptance rates equal 90%, and false rejection rates ≥ 97%, an extremely good value.
4. The Support Vector Machine algorithm produces poorer results compared to the other two, with an average true acceptance rate of below 50%.

Multifactor Authentication Using Combined Fingerprint and Keystroke Dynamics

As a final step, it was necessary to evaluate the added advantages of the proposed dynamics-based authentication to a user authentication system using traditional fingerprint and username-password combinations.

The authentication scheme implemented is as follows:

1. The DHIMS2 portal includes a sign-in page, with fields for username and password.



PROPOSED DHIS AUTHENTICATION MODULE

Sign up an Account (1/5 Series)

lazo

```
1  0                                   login.js:134
2  70                                  login.js:134
3  63                                  login.js:134
4  64                                  login.js:134
```

Char	1/5	2/5	3/5	4/5	5/5
l	0	0	0	0	0
a	70	74	72	73	71
z	63	54	60	61	63
o	64	62	61	63	62

Figure 8. (a) Snipet of the first instance of Keystroke Timings for Username at Five- Series SignUp Process. (b) Recorded Keystroke Timings for Username at Five-Series Sign Up Processes. (username is 'lazo')

2. Validate the username and password

- The Username and Password are checked against those stored in the user's account (which were collected during registration) to determine a match between the entered username-password combination.

3. Collect keystroke dynamics data as the user types his username and password

- A background application, as described earlier, records the timestamps for key presses and releases. It is activated whenever a user begins to type his/her username and password.

4. Validate the user's identity using the collected keystroke dynamics data.

- The data collected in (3) is fed to the preferred classification algorithm, as described earlier – which has also been coded as a background application – to determine his/her ownership of the account. Sample timing data collected from the user during registration, and stored together with his/her account information is also given as input to the algorithm.

5. Require the user to execute his (unique) finger-swiping sequence.

- A fingerprint scanner is attached to the host computer.
- The fingerprint module developed is embedded into the DHIMS 2 portal.
- A background application captures timestamps for finger presses when the user begins to swipe his unique sequence.

6. Validate user's fingerprint pattern.

- The user's fingerprint pattern (image) is compared to the pattern captured during registration to determine ownership of the account.

7. Validate user's identity using fingerprint dynamics technique.

- The time-data collected in (5) is fed to the preferred classification algorithm, as also described earlier – which has also been coded as a background application – to determine his/her ownership of the account. Sample timing data collected from the user during registration, and stored together with his/her account information is also given as input to the algorithm.

8. The user is identified as the true owner of the account if at least 3 out of the four authentication techniques prove that he is.

- A condition statement, embedded in the portal, which uses results from the validation stages as inputs is executed, and the system allows the user entry only when at least three out of four of the authentication techniques identify him as the true owner of the account.

Results

Table 1 illustrates the outcome of the possible combinations of successfully validated users.

Table 1. Successful authentication combinations statuses

Logon	Keystroke	Fingerprint Pattern	Fingerprint Dynamics	Result
Pass	Pass	Pass	Fail	Pass
Pass	Pass	Fail	Pass	Pass
Pass	Fail	Pass	Pass	Pass
Fail	Pass	Pass	Pass	Pass
Pass	Pass	Pass	Pass	Pass

The total possible combinations of all four variables is 70. Out of this, 5 yield positive results, giving a probability of 5/70 = 0.0714.

The following table presents a summary of performance metrics for both traditional and dynamics-based authentication techniques.

Table 2. Summary of performance metrics for traditional and dynamics-based authentication

Paradigm	Technique	True Acceptance Rate	False Acceptance rate
Traditional	Username-Password	> 90 %	< 10 %
	Fingerprint	> 90 %	< 10%
Dynamics-based	Keystroke	90 %	< 5 %
	Fingerprint	≈ 70 %	< 20 %

Deductions from Tables 1 and 2, Table 3 is obtained.

Table 3. Calculation of weighted probabilities

Variable	True Acceptance Rate (TAR)	Probability (P_{TAR})	Weighted Probability (TAR * P_{TAR})	False Acceptance Rate (FAR)	Probability (P_{FAR})	Weighted Probability (FAR * P_{FAR})
Logon Status	> 90 %	0.929	> 84 %	< 10 %	0.0714	< 1 %
Fingerprint Pattern Status	> 90 %	0.929	≈ 84 %	< 10%	0.0714	< 1 %
Keystroke Pattern Status	90 %	0.929	≈ 84 %	< 5 %	0.0714	< 0.5 %
Fingerprint Dynamics	≈ 70 %	0.929	65 %	< 20 %	0.0714	< 1.5 %

Substituting Table 3 into Table 1,

Table 4. True acceptance rates for combined authentication

Logon Status (Weighted Probability)	Keystroke Status (Weighted Probability)	Finger Pattern Status (Weighted Probability)	Fingerprint Dynamics Status (Weighted Probability)	Result
0.84	0.84	0.84	-	≈ 0.6
0.84	0.84	-	0.65	≈ 0.5
0.84	-	0.84	0.65	≈ 0.5
-	0.84	0.84	0.65	≈ 0.5
0.84	0.84	0.84	0.65	≈ 0.4

From Table 4, it is evident that combining traditional authentication techniques with dynamics-based authentication produces added security, reducing intruder attacks by 10% to 50%.

Conclusion

This study evaluated the feasibility of multifactor authentication with biometrics, incorporating both traditional and the time dynamics-based techniques of keystrokes (behavioural) and fingerprint swipes (user’s physical characteristics), for adoption into an eHealth system (DHIMS 2). Greater attention was given to the analysis of the dynamics-based techniques since the traditional techniques are relatively well established. The results indicate that individual authentication by Keystroke and Fingerprint dynamics yields acceptable results. However, when combined with the traditional methods of authentication, extremely high security is obtained than could be obtained by each paradigm acting independently. Hence, it is concluded that combining Keystroke and fingerprint dynamics with traditional authentication techniques into an eHealth system (DHIMS 2) will yield a system with improved account security and integrity of health information. MFA with biometrics is not an alternative security solution for the initial login; rather it provides an added security measure alongside the initial login.

References

[1]. Abdullah, M. D., Abdullah, A. H., Ithnin, N., & Mammi, H. K. (2008). Towards identifying usability and security features of graphical password in knowledge-based authentication technique. In Modeling & Simulation (pp. 396-403). Asia: AICMS 08.

[2]. Abomhara, M., Gerdes, M., & Køien, G. M. (2015). A stride-based threat model for telehealth systems. Norsk informasjonssikkerhetskonferanse (NISK), 8(1), 82-96.

[3]. Adaletey, D. L., Poppe, O., & Braa, J. (2013). Cloud computing for development—Improving the health information system in Ghana. In 2013 IST-Africa Conference & Exhibition (pp. 1-9). IEEE.

[4]. Alsultan, A., & Warwick, K. (2013). Keystroke dynamics authentication: a survey of free-text methods. International Journal of Computer Science Issues (IJCSI), 10(4), 1.

[5]. Anwar, S., Zain, J. M., Zolkipli, M. F., Inayat, Z., Jabir, A. N., & Odili, J. B. (2015). Response option for attacks detected by intrusion detection system. In Software Engineering and Computer Systems (ICSECS), 2015 4th International Conference, (pp. 195-200).

[6]. AuthenticationWorld.com. (2015, 02 02). Password Authentication. Retrieved from Password Authentication: http://authenticationworld.com/Password-Authentication/index.html

[7]. Awoonor-Williams, J. K., Bawah, A. A., Nyonator, F. K., Asuru, R., Oduro, A., Ofosu, A., & Phillips, J. F. (2013). The Ghana essential health interventions program: a plausibility trial of the impact of health systems strengthening on maternal & child survival. BMC health services research, 13(2), S3.

[8]. Bath, P. A. (2008). Health informatics: current issues and challenges. Journal of Information Science, 34, 501-518.

[9]. Ben-Assuli, O. (2015). Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments. Health Policy, 119(3), 287-297.

[10]. Bhardwaj, I., Londhe, N. D., & Kopparapu, S. K. (2016). A novel behavioural biometric technique for robust user authentication. IETE Technical Review.

[11]. Black, T. R. (1999). Doing quantitative research in the social sciences: An integrated approach to research design, measurement and statistics. Sage.

[12]. Bonneau, J., Herley, C., Van Oorschot, P., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. Commun. ACM, 58, 78–87.

[13]. Boujettif, M., & Wang, Y. (2010). Constructivist approach to information security awareness in the Middle East. In 2010 International Conference on Broadband, Wireless Computing, Communication and Applications (pp. 192-199). IEEE.

[14]. Brady, J. W. (2011). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. In System Sciences (HICSS), 2011 44th Hawaii International Conference (pp. 1-10). IEEE.

[15]. Carstens, D. S., McCauley-Bell, P. R., Malone, L. C., & DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security.

[16]. Coley, S. C., Kenderdine, J. E., Piper, L., & Martin, R. A. (2015). Use of Password System for Primary Authentication. In CWE Version 2.9 (p. 601).

[17]. Dasgupta, D., Roy, A., & Nag, A. (2017). Advances in User Authentication. Springer International Publishing.

[18]. Dehnavieh, R., Haghdoost, A., Khosravi, A., Hoseinabadi, F., Rahimi, H., Poursheikhali, A., & Radmerikhi, S. (2019). A literature review and meta-synthesis of its strengths and operational challenges based on the experiences of 11 countries. Health Information Management Journal, 48(2), 62-75.

[19]. DHIS 2 Documentation. (2016, June). DHIS 2 User Manual. Retrieved from DHIS 2 User Manual: https://docs.dhis2.org/2.22/en/user/html/dhis2_user_manual_en_full.html#d5e157

[20]. DHIS2 Documentation Team. (2012). Rolling Out A Nationwide Web-Based District Health Information System, DHIMS2- The Ghana Experience. Retrieved from dhis2.org/doc/snapshot/en/implementer/dhis2.

[21]. Dinev, T., Albano, V., Xu, H., D'Atri, A., & & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In Advances in healthcare informatics and analytics (pp. 19-50). Springer, Cham.

[22]. Dinker, A. G., Sharma, V., Mansi, & Singh, N. (2018). Multilevel authentication scheme for security critical networks. Journal of Information and Optimization Sciences, 39(1), 357-367.

[23]. Erlich, Z., & Zviran, M. (2009). Authentication methods for computer systems security. In Encyclopedia of Information Science and Technology, Second Edition. IGI Global, 288-293.

[24]. FERREIRAabd, A., Ricardo, C. C., Antunes, L., & Chadwick, D. (2007). Access Control: how can it improve patients' healthcare? Medical and care compunetics, 4(4), 65.

[25]. Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur, 8, 136–148.

[26]. Gathogo, J. K. (2014). A model for post-implementation evaluation of health information systems: The case of the DHIS 2 in Kenya (Doctoral dissertation). Nairobi: University of Nairobi.

[27]. Gebrie, M. T., & Abie, H. (2017). Risk-based adaptive authentication for internet of things in smart home eHealth. In Proceedings of the 11th European Conference on Software Architecture (pp. 102-108). Companion Proceedings ACM.

[28]. Harris, J. (2016). Multi-Factor Authentication Gains Traction in Healthcare. SIGNiX.

[29]. Hevner, A., & Chatterjee, S. (2010). Design research in information systems: theory and practice. Springer Science & Business Media.

[30]. Iakovidis, I. (1998). Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe1. International journal of medical informatics, 52(1-3), 105-115.

[31]. Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. Applied Soft Computing, 11(2), 1565-1573.

[32]. Karuri, J., Waiganjo, P., Daniel, O. R., & Manya, A. (2014). DHIS2: The tool to improve health data demand and use in Kenya. Journal of Health Informatics in Developing Countries, 8(1).

[33]. Killourhy, K. S., & Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. In 2009 IEEE/IFIP International Conference on Dependable Systems & Networks (pp. 125-134). IEEE.

[34]. Kotani, K., & Horii, K. (2005). Evaluation on a keystroke authentication system by keying force incorporated with temporal characteristics of keystroke dynamics. Behaviour & Information Technology, 24(4), 289-302.

[35]. Kreicberge, L. (2010). Internal threat to information security countermeasures and human factor with SME. Business Aministration and Social Sciences, Lulea University of Technology, 1-66.

[36]. Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: multiple perspectives. Journal of the Association for Information systems, 13(6), 395.

[37]. Li, Y., Wang, H., & Sun, K. (2016). A study of personal information in human-chosen passwords and its security implications. In INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications (pp. 1-9). IEEE.

[38]. Manya, A. B., Øverland, L. H., Titlestad, O. H., Mumo, J., & Nzioka, C. (2012). National roll out of District Health Information Software (DHIS 2) in Kenya, 2011–Central server and Cloud based infrastructure. In IST-Africa 2012 Conference Proceedings (Vol. 5). IIMC International Information Management Corporation.

[39]. March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision support systems, 15(4), 251-266.

[40]. Miller, R. H., & Sim, I. (2004). Physicians' use of electronic medical records: barriers and solutions. Health affairs, 23(2), 116-126.

[41]. Missaoui, C., Bachouch, S., Abdelkader, I., & Trabelsi, S. (2018). Who Is Reusing Stolen Passwords? An Empirical Study on Stolen Passwords and Countermeasures. In International Symposium on Cyberspace Safety and Security (pp. 3-17). Springer, Cham.

[42]. Montalvão, J., Freire, E. O., Bezerra Jr, M. A., & Garcia, R. (. (2015). Contributions to empirical analysis of keystroke dynamics in passwords. Pattern Recognition Letters, 52, 80-86.

[43]. Nyonator, F., Ofosu, A., & & Osei, D. (2013). District Health Information Management System DHIMS II: The Data Challenge for Ghana Health Service. Retrieved from NetHope Solutions Center Case Studies: https://solutionscenter.nethope.org/assets/collaterals/dhims2_crs_presentation.ppt

[44]. Obaidat, M. S., & Sadoun, B. (1997). Verification of computer users using keystroke dynamics. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 27(2), 261-269.

[45]. Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal. (2015). Ethical issues in electronic health records: a general overview. Perspectives in clinical research, 6(2), 73.

[46]. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

[47]. Pinkas, B., & Sander, T. (2002). Securing passwords against dictionary attacks. In Proceedings of the 9th ACM conference on Computer and communications security (pp. 161-170). ACM.

[48]. Poppe, O. (2012). Health Information Systems in West Africa: Implementing DHIS2 in Ghana (Master's thesis). Accra, Ghana: UNIVERSITY OF OSLO.

[49]. Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. IEEE security & privacy,, (2), 33-42.

[50]. Rajamäki, J., & Pirinen, R. (2017). Towards the cyber security paradigm of ehealth: Resilience and design aspects. In AIP Conference Proceedings (Vol. 1836, No. 1) (p. 020029). AIP Publishing.

[51]. Rindfleisch, T. C. (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 92-100.

[52]. Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. Computers & Security, 61, 130-141.

[53]. Stamatian, F., Baba, C. O., & Timofe, M. P. (2013). Barriers in the implementation of health information systems: a scoping review. Transylvanian Review of Administrative Sciences, 9(SI), 156-173.

[54]. Wang, D., & Wang, P. (2015). Offline dictionary attack on password authentication schemes using smart cards. In Information Security; Springer, (pp. 221–237). Berlin, Germany.

[55]. Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In Symposium on Usable Privacy and Security (SOUPS), (pp. 175-188).

[56]. Wood, C. C., & Banks Jr, W. W. (1993). Human error: an overlooked but significant information security problem. Computers & Security, 12(1), 51-60.

[57]. Yu, E., & Cho, S. (2003). Novelty detection approach for keystroke dynamics identity verification. In International conference on intelligent data engineering and automated learning (pp. 1016-1023). Berlin, Heidelberg: Springer.

[58]. Yu, E., & Cho, S. (2004). Keystroke dynamics identity verification—its problems and practical solutions. Computers & Security, 23(5), 428-440.

[59]. Zaeem, R. N., Manoharan, M., Yang, Y., & Barber, K. S. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. Computers & Security, 65, 50-63.

[60]. Zheng, Z., Liu, X., Yin, L., & Liu, Z. (2009). A stroke-based textual password authentication scheme. In Education Technology and Computer Science, (pp. 90-95).