I.
http://www.casestudiesjournal.com/
Impact Factor: 4.428

Investigating the Influence of Human Factors on Choice of Images for Graphical Password

Author's Details:
[1*]Salihu Umar Suru, [2]Anas Muhammad Gulumbe [3]Dr. Abubakar Atiku Muslim, [4]Dr. Hassan Umar suru, [5]Dr. Danlami Gabi
[1]Dept. of Computer Science, Kebbi State University of Science & Technology, Aliero
surusalihu@yahoo.com
[2]Dept. of Computer Science, Kebbi State University of Science & Technology, Aliero
anasgulumbe89@yahoo.com
[3]Dept. of Computer Science, Kebbi State University of Science & Technology, Aliero
alatiku@yahoo.com
[4]Dept. of Computer Science, Kebbi State University of Science & Technology, Aliero
suruhassan@yahoo.com
[5]Dept. of Computer Science, Kebbi State University of Science & Technology, Aliero
gabsonley@gmail.com

Abstract:
The most important aspect of security in computing is user authentication which is the process of confirming the identity of users and granting such users access to their systems. Several graphical password schemes have been developed as alternatives to traditional alphanumeric passwords to overcome issues associated with user authentication problems present in traditional methods. Since the end users of each system are humans and humans are gullible in the understanding of security concepts, human factors represent the weakest part of a security system and the fundamental reason why many attacks on computers and systems are successful. This paper is designed to investigate the influence of human factors such as gender, age and familiarity on user choice of images for graphical passwords. In order to conduct acceptable and genuine investigation, we proposed and tested a hybrid authentication prototype using celebrities' images for face based graphical authentication systems. A questionnaire was designed and distributed to participants who partook in the prototype testing. Responses of the participants were collected and the data was analyzed via SPSS. Our evaluations suggested promising result to indicate that user choice of images for graphical password is affected by gender, age and the familiarity of system users to the images provided.
Keywords: *Authentication, Security, Usability, Password, Image, Celebrity*

1. Introduction

Human activity has changed and computing systems have very much affected the way people do things in the past years [1, 2]. Computers and the internet have come and have remained a vital part of our daily lives as many computers are connected to the internet every minute, and more computing devices are produced. Pervasive, embedded, mobile and cloud computing have brought about a generation of ubiquitous and online computing. With computers increasingly becoming "thin clients" and all forms of businesses and operations now moving online, there is an ever growing concern on system security, especially as online threats are becoming increasingly advanced and the need to share resources and data are ever increasing [3].
The most significant part of security in computing is user authentication, which aims to confirm the identity of users and granting such users access to their respective accounts. Authentication methods are based on four fundamental pieces of information: something the user is, something the user has, something the user

knows, and recently proposed, someone the user knows. If the user of the system can provide proof in some or all of this information, he/she is granted access to the system. A number of security software solutions have been developed to protect the user and communication between the user and the system. However, even using the very best of such software cannot guarantee 100% security because the end users are humans and humans are weak in the adoption of security protocols [4].

Much research has been conducted on system security. However, attention has been primarily focused on technical problems and solutions. Until recently, the role of human factors in system security has not been recognized. Research has shown that human factors represent the weakest part of a security system and system users are the weakest link in the security chain. As such, human factors are the fundamental reason why many attacks on computers and systems are successful. Research has also shown that attackers always try to take advantage of the weakest link and gain access to human activities on public forums and online social networking websites to mine personal attributes such as age, sex and other sensitive information such as to answer challenge questions (e.g. mother's maiden name) [4]. In graphical password systems, end-user behavior can affect their choice of images for password. As such, this presents a need to investigate the effects of human factors such as gender, age, familiarity and culture on a user's choice of images for graphical password. This paper is aimed at investigating the effects of gender, age and familiarity of users to images on the choice of image categories for graphical passwords. We proposed adopting pass faces technology in this study due to its usability advantages despite its drawbacks as with other authentication methods.

2. Literature review

For quite a while, Alpha-Numeric passwords have been dominantly used to authenticate users. Although password spaces have been designed both to capture a wide range of characters, as well as to accommodate lengthy passwords, users have become obsessed with using simple passwords often the names of relatives, items or places, utilizing only a small fraction of this space. This also makes it easy for such passwords to be easily guessed. Thus there has been a lot of effort to improve on this scheme, which included the development of mnemonic passwords, character substitution, passphrases [5], etc. None of these innovations was however able to entirely solve the problem of text passwords.

Text passwords were then followed by graphical authentication schemes. The first graphical authentication scheme was proposed by Blonder in 1996, and it used predefined tap regions within one image as password. The user was authenticated by clicking on the tap points in a definite order. Although it suffered from being predetermined, having a small password space as well as vulnerability to shoulder surfing, it formed the basis of some of the best graphical authentication systems [6]

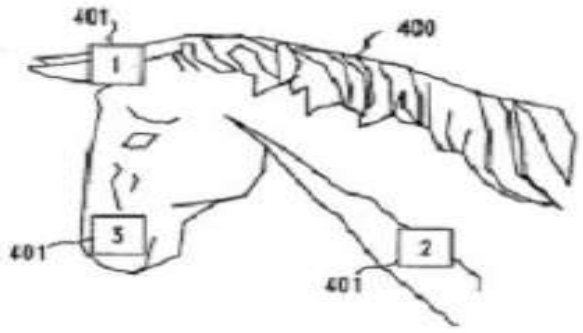

Figure 1. Blonder method

Another graphical password scheme based on the Hash Visualization technique was proposed by Dhamija and Perrig as an improvement to previous schemes. In this scheme, the user is required to select a number of images from a set of random images generated automatically by the system. A user is only required to identify the preselected images in order to be authenticated. However this method also suffered from weaknesses such as the fact that each user selected image needs to be stored by the server in a plain text and

the process of selecting a set of images from the image database can be tedious and time consuming. Users also encountered difficulty recognizing their chosen images and the scheme itself was vulnerable to social engineering, shoulder surfing as well as intersection attack [7]

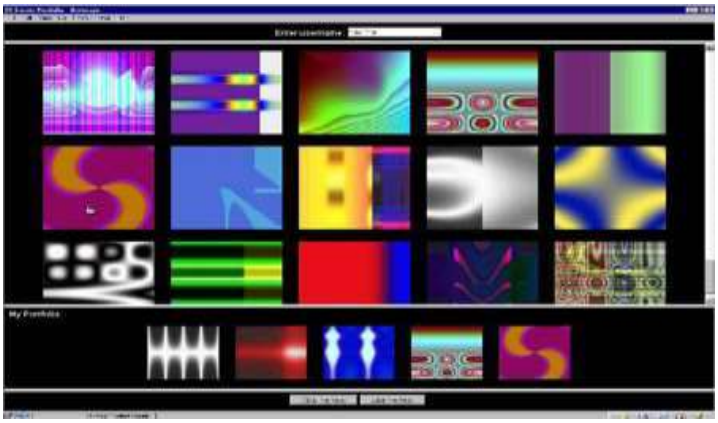

Figure: 2. A sample of Dhamija and Perrig scheme [8]

The Passfaces method was introduced by Real User Corporation [8]. This method allowed users to choose four images of human faces from the image database. The selected face images are stored as the user's password. During the authentication stage, the user is presented with a grid consisting of nine faces, including the previous face chosen by the user and eight decoy faces. The user is then required to recognize and click anywhere on his/her previously selected faces.

The procedure is repeated in several rounds. The user is authenticated if he/she correctly identifies his/her previously chosen faces [9]. The technique is based on the assumption that people can recall human faces easier than other pictures [10]. When Passfaces was used to investigate the vulnerability of human faces to descriptions [11] and how authentication could be done using such descriptions, the likelihood of users choosing decoys instead of original images was discovered, when the description of the original image was given.

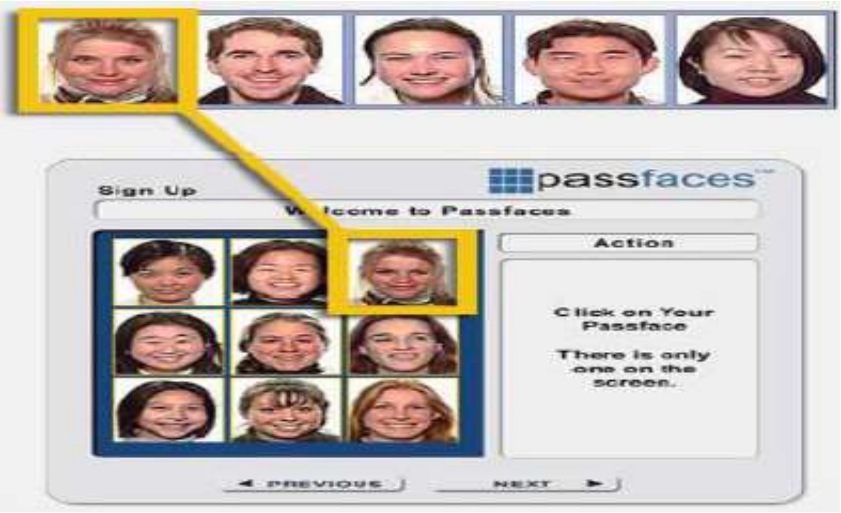

Figure 3. A Sample of Passface scheme [8]

Three schemes were proposed and implemented by Sobrado and Briget in 2002 to overcome the problem of shoulder surfing attacks. Shoulder surfing is the ability of someone to observe a user's password entry on the system by simply looking over their shoulders [12]. In their schemes, at each authentication, a user is presented with many icons on a computer screen in which he is expected to locate his password images among many decoy images. In the first implementation, a user had to locate any three of his chosen password images and click inside the triangle formed by those images in order to authenticate. In the second

method, the user needed to position one of his chosen images in a movable frame, and then move the frame to align with any other two of his chosen images to authenticate. In the third scheme, the user had to locate any four of his chosen images and then click on the point of intersection of the invisible lines joining the images placed at the opposite vertices of the quadrilateral formed by the four images. Although the system may have good security, it may suffer usability flaws [12, 13].

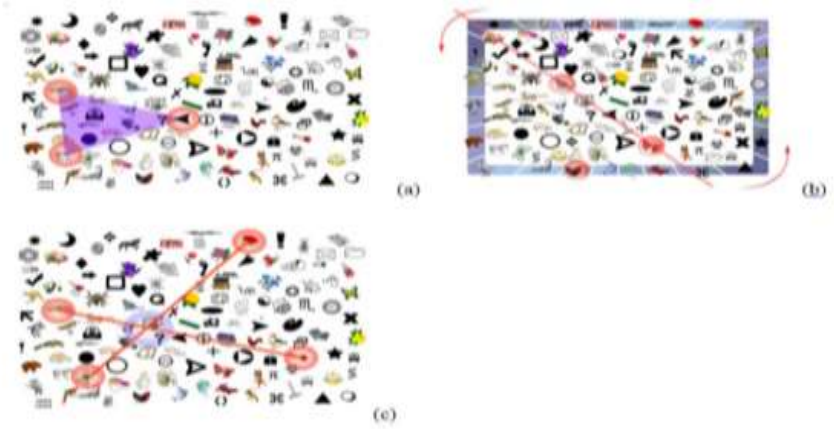

Fig. 4: Sobrado and Birget schemes [15]: a – Triangle, b – Movable frame, c – Intersection. [12]

Another method was proposed by Hong et al as an improvement to the existing schemes in which the user assigns his own codes to each of his preselected pass images. In this scheme, a user is required to assign his/her own code and also need to memorize his/her assigned code. The need to memorise the code, however, meant that it suffered the same usability flaws as the system it sought to improve upon [12].

Fig. 5 : Shoulder surfing resistant scheme by Hong et al. [12]

Picture Password Scheme was also proposed in 2003. This method was designed for handheld devices like Personal Digital Assistants (PDAs). A user is required to select a theme identifying the thumbnail photos to be used and then registers a sequence of thumbnail images used for his password during enrollment. After the PDA is switched on, the user will be asked to supply the current enrolled image sequence for verification to logon to the device. The user may change his password by selecting a new sequence or theme after successful authentication. However, the addition of shift key will make the memorability of the created password become more complex
and difficult [13].

Fig. 6: Picture Password Scheme, 2003 [13]

The story scheme was also proposed in 2004 by organizing the available picture into nine categories as follows: animals, cars, women, food, children, men, objects, nature and sport. According to this scheme, the users have to select their passwords from the mixed pictures of nine categories in order to make a story easily to remember. According to the researchers, this method can be used without users having to define a story for themselves. Research also showed that the story method was more difficult to remember than the Passface scheme [13].

Fig. 7: Story Scheme, 2004 [13].

A usable graphical password scheme known as Jetafida scheme was proposed in 2008. The aim of this method was to implement all the usability features in a single algorithm. During registration, the user is required to select three pictures as his/her password and then sort them according to the way he/she wants to see them in the login phase. The user password images are mixed with seventeen color pictures in login phase. According to the article, all the usability features in the scheme were implemented successfully. The research article did not, however, investigate any of the security issues of the system [14].

Fig. 8: Jetafida Scheme, 2008 [14].

In an earlier study to investigate the risk of shoulder surfing [15] associated with a variety of authentication schemes, however, it was discovered that there was no difference in terms of vulnerability between difficult text based passwords and common graphical authentication schemes. It was also seen that users found it equally difficult to remember multiple graphical passwords [16]. Although some studies have shown graphical passwords to be more user friendly, their usability may in fact be closer to text passwords when looking at retention with respect to multiple passwords.

Researchers in [15] studied the use of Passpoints for user authentication. Although similar to Blonder's authentication scheme, in that the user needed to select a group of points from an image, it allowed users to select points from any part of the image. The results were a great success for graphical authentication systems, yet they also suggested that graphical authentication systems were more difficult to learn and graphical passwords more difficult to remember. Feedback from user evaluation of this graphical authentication systems was, however, not conclusive.

There have been a lot of concerns with regards to graphical authentication systems, most especially with regards to password space and shoulder surfing attack. Further test conducted on Passpoints in [17] with both field and lab tests, had field tests showing less success rates and some security concerns such as the use of common password patterns.

Fig. 9: A sample of Passpoints Sytem

As an improvement to Passpoints, Cued Click Points (abbreviated CCP) was proposed in [18]. Though similar to Passpoints, it allowed the user to select each point from a different image. This saw a great improvement in both security and usability as the user only needed to remember a point on each image. This

system, however, also came to face the same problems as Passpoints. One of these was the fact that it had the same pattern and hotspots as the Passpoints scheme.

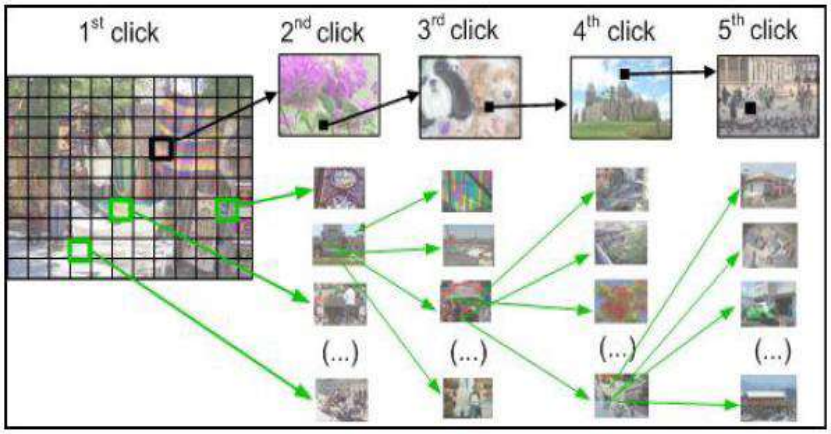

Fig. 10: A sample of CCP Scheme

A further security improvement was made on the development of Cued Click Points system by the development of a technique known as Persuasive Cued Click Points [19]. The new system maintained the features of the CCP, with improvements only at the create login phase. The system encouraged random click points and discouraged hotspots, thereby greatly improving security of the system.

With all these improvements, however, usability still remained the bottleneck in system design, although in a statistically insignificant manner. Apart from security and usability, one important consideration in the design of modern systems is consistency, which is being violated in the move from text to graphical authentication systems as most people are used to text based authentication systems.

Rather than a total replacement of text based passwords, it is suggested that a combination of graphical and text based passwords will be more desirable. Several security advantages of such a combination over traditional text passwords such as better password strength (or space), better protection from password guesses, protection from phishing and man in the middle attacks were given to support this idea [20]. This system shall consider varieties of face based images, with the aim being to find a solution to the problems inherent in the earlier schemes and maintaining better security and usability while supporting concurrency.

3. New Prototype Design

In this research, the pass faces technology was adopted in the system design due to its usability advantages. The hybrid prototype is categorized into Sport model, Non-Sport model and Mixed model (a combination of sport and non-sport models) and each model consists of faces of celebrities from three major sport or non-sport categories. Faces of Football stars, Basketball stars and Wrestling stars were implemented in the sport model while non-sport model used face images of movie stars, music stars and famous non sport celebrities. The researchers deviated from implementing the idea of using the faces of unknown people in this study in order to improve the usability of the new system because users prefer to create their passwords with images that are familiar to them. The prototype of a system known as sports faces which is similar to our system has been developed earlier by researchers. However, sports faces is more concerned about the security of the system. The sports faces model was designed using the faces of all sports celebrities and the national flags of all countries that had participated in football and cricket in a particular FIFA world cup competition [21].

In the Sports faces scheme, a user has to select twelve images from a particular category (i.e. football or cricket): one country's flag, three players belonging to that particular country and the process is repeated thrice during registration [21]. Sports faces offers security advantages such as resistance to shoulder surfing attack, exhaustive search and guessing attacks as multiple levels of challenges are involved during the registration phase. This study considered a slightly different approach due to the belief that some users may not be familiar with cricket or football or do not have interest in such sports categories coupled with a

perception of the long period of time taken to create a password. This meant that the system suffered serious usability flaws.

.

.

Fig 11: Last screen of user registration phase in sports faces [21].

The new system combined the traditional text based and graphical passwords technologies with maximum flexibility as the researchers believed that a user may have an interest in either sports or non-sports or a combination of both. As such, users have an opportunity to select images from sport category, non-sport category or mixed category in a single authentication window. Regions (i.e. Africa, Europe and Asia) where each selected sport or non-sport types (i.e. football, basketball, music, movies etc.) belong to, have been provided in the prototype to improve user convenience and password security as shown in figure 12.

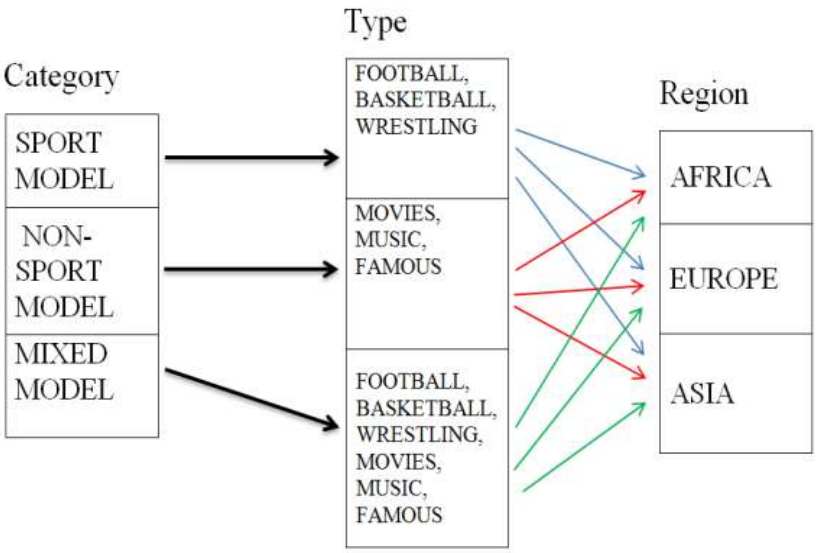

Fig 12: Processes of the model prototype

3.1 Registration Phase

After h/she has created ID and password, a user is allowed to select sport or non-sport types (i.e. football basketball, movies, music etc.) from the above mentioned categories, and then select the region (i.e. Africa, Europe, Asia etc.) where each selected sport or non-sport type belongs to, and finally the images of three or six celebrities from the selected region depending on the user choice are selected for registration.

Fig 13: Image based registration interface

3.2 Login Phase

In login phase, a user is only required to enter his/her created id and password and then select the correct images from the sequence of nine images displayed by the system including the decoy images. Although users are not required to remember the sequence of their chosen images, he/she must select the exact number of images he/she had selected during password creation for successful authentication.

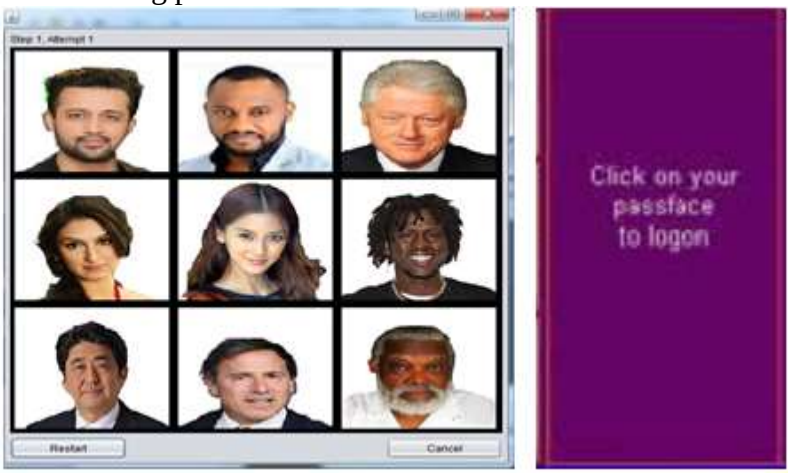

Fig 14: Image based login interface

4. Methodology

4.1 Participants

The experiment was conducted with a total of sixty (60) participants all of whom were Undergraduate and Postgraduate students of Kebbi State University of Science and Technology, Aliero, Nigeria who volunteered to take part in the experiment. This research was also conducted as a laboratory experiment in a within subject design, i.e. all participants received the same treatment by going through all of the experimental procedures the same way [22]. The following tables show the gender and age distribution of the participants.

	Male	Female
Football	14	3
Basketball	1	0
Wrestling	11	1
Total	**16**	**14**
Movies	4	9
Music	4	11
Famous	1	1
Total	**9**	**21**
Grand Total	**25**	**35**

Table 1: Gender Distribution Table

Table 1 shows the gender distribution of all the participants who volunteered to take part in the proposed prototype testing. The experiment was conducted with a total number of 25 (16 and 9 for sports and non sports respectively) male and 35 (14 and 21 for sports and non sports respectively) female participants who participated in the prototype testing.

<18	18-20	21-23	24-26	27-29	30-32	33-35	>35
14	19	8	4	5	6	2	1

Table 2: Age Distribution Table

Table 2 shows the age distributions of all the participants who partook in the prototype testing. Participants were distributed according to the range of their ages. For example, 14 participants were <18 years, 19 participants were in the category 18-20 years, 8 participants were in 21-23 years, 4 participants were in 24-26 years while 5, 6, 2 and 1 participants were in 27-29, 30-32, 33-35 and 33-35 years respectively.

4.2 Experimental Procedure

Data collection for the study was conducted in a controlled laboratory environment where participants worked with the experiment instructor in an isolated room to avoid any distractions. Participants were first given a questionnaire containing their demographic details including age, gender, level of proficiency with computers, etc. The participants were then given a brief introduction to graphical authentication system and the new prototype systems. After that introduction, participants received a short training session on how the new prototype system is used. Because the participants were very familiar with alphanumeric passwords, they received no training on this kind of authentication scheme [22].

Initial training and demonstration of the new prototype system was carried out using a laptop computer and projector to demonstrate and exemplify the use of the new prototype system to register a user and allow him to login to the system. Participants were organized in the form of a latin square and used the system for a period of three weeks. The system allows participants to supply a username, password and choose from a grid of images which will serve as their pass-image. The participants supplied a text password and the system demands that both the text password and the pass-images coupled with their username are supplied during login.

Three Hp laptop computers with high resolution were used throughout the experiment. Participants were assigned to use the graphical password prototype system to select the images of their choice for authentication. Participants were given privilege to use any model (i.e. sport, non-sport or mixed models) of their choice. Participants were required to partake in three trials, first trial, second trial after one week and finally third trial after two weeks. It is believed that the number of trials and the intervals between the three

trials will assist in password memorability assessment, as such; the researchers monitored the password memorability level of participants after each trial.

The use of the system prototype was subdivided into two phases namely registration phase and login phase. Registration phase involved multiple levels of challenges because a participant must select his password image from one of the three categories including category type before he/she proceeded to the region where a particular category type belonged for successful registration. In order to measure the performance of the proposed system, the researchers have captured the registration time, login time, login success rate and number of attempts at each trial.

During registration in the first trial, a participant is required to create his text based username and password before he proceeds to the graphical password section. In this section, a participant is required to manage multiple levels of challenges such as selecting category (i.e. sport, non-sport or mixed models), selecting category type (i.e. football, music or famous etc.), selecting region for each type of category he had selected (i.e. Africa, Europe, or Asia) and then select the images of celebrities that appeared in the selected region, depending on the number of images he had selected (i.e. 3 or 6 images.) to create his password. Having followed the above steps successfully, a dialog box showing "user registered successfully" is displayed.
At the second phase or login phase, a participant is only required to enter the username and password he had created during registration phase after which a window containing all images he had selected during password creation including decoy images is displayed. At this stage, the user is only required to select the correct images he had chosen during registration after which a dialog box is displayed with the words: "authentication successful". Questionnaires containing thirty nine questions were distributed to participants after each trial. Questions regarding user image selection behavior, usability features of the prototype, and the overall system performance were answered by the participants after each trial.

4.3 Experimental Evaluation

The researchers only considered participant's image selection behavior in this study (i.e. their attitude towards selecting the images of celebrities for graphical password). The completed questionnaires were collected and responses of the participants towards their image selection behavior during the prototype testing were recorded and analyzed. Participants were categorized according to gender and age groups. Questions in the questionnaire included; which category of prototype a participant is familiar with, which category type a participant is familiar with, and which region of the celebrities will a participant select his images for password from, depending on the category of the celebrities chosen (Football, basketball, music, movies etc). All responses of both female and male participants regarding the these questions were gathered and analyzed using SPSS software.

5. Result Analysis

After analyzing the responses of the participants regarding the stated questions during prototype testing using descriptive statistics and chi-square statistical methods, the researchers found reliable results on image selection behavior of male and female participants. Results on the familiarity of participants with celebrities in terms of the participants' age groups and the regions of the celebrities were also taken into consideration in this study.

5.1 Effect of gender on user choice of images for graphical password

Tables 3(a) and 3(b) shows the type of sport/ non-sports provided in each category of the prototype and the numbers with percentages of male and female participants and their chosen images from either sports or non-sports types (i.e. No of participants per category type). From the results it can be seen that 14 (82.4%) out of the population of male participants and 3 (17.6%) out of the population of female participants agreed to create their passwords using images of football celebrities, 1 (100%) and 0 from the population of males and females respectively agreed to create their passwords using images of basketball celebrities, 11(91.7%) males and 1(8.3%) female agreed to use images of wrestling celebrities for their password. In non-sports prototype, only 4(30.8%) male and 9(69.2%) female participants agreed to use images of movie celebrities

for their passwords while 4(30.8%) males and 9(69.2%) females agreed to choose the images of music celebrities for their graphical passwords and finally, 1(50%) male and 1(50%) female agreed to use the images of famous people as their chosen passwords.

			Gender		Total
			Male	Female	
Sports	Football	Count	14	3	17
		% within Gender	87.5%	21.4%	56.7%
	Basketball	Count	1	0	1
		% within Gender	6.3%	0.0%	3.3%
	Wrestling	Count	1	11	12
		% within Gender	6.3%	78.6%	40.0%
Total		Count	16	14	30
		% within Gender	100.0%	100.0%	100.0%

Table 3 (a): category type per no. of participants by their gender

			Gender		Total
			Male	Female	
NonSport	Movies	Count	4	9	13
		% within Gender	44.4%	42.9%	43.3%
	Music	Count	4	11	15
		% within Gender	44.4%	52.4%	50.0%
	Famous	Count	1	1	2
		% within Gender	11.1%	4.8%	6.7%
Total		Count	9	21	30
		% within Gender	100.0%	100.0%	100.0%

Table 3 (b): category type per no. of participants by their gender

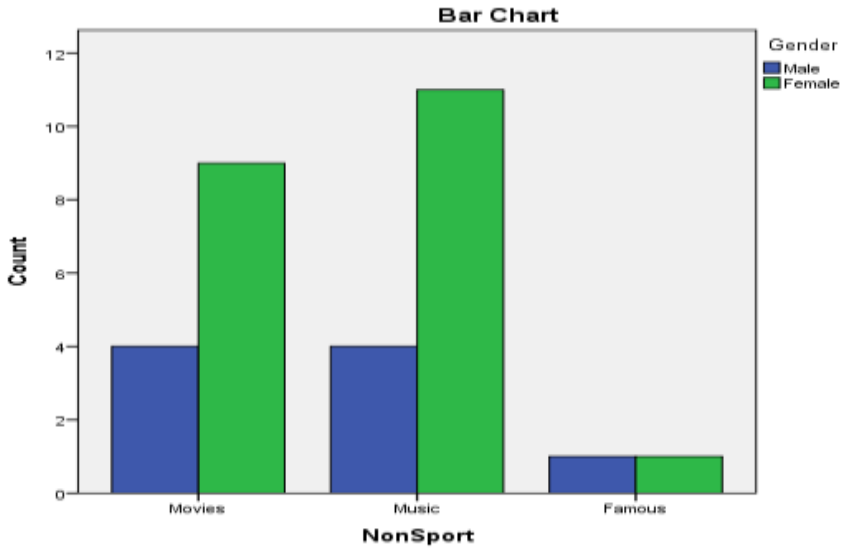

Fig 15: Category type per no. of participants Chart for Non sport model

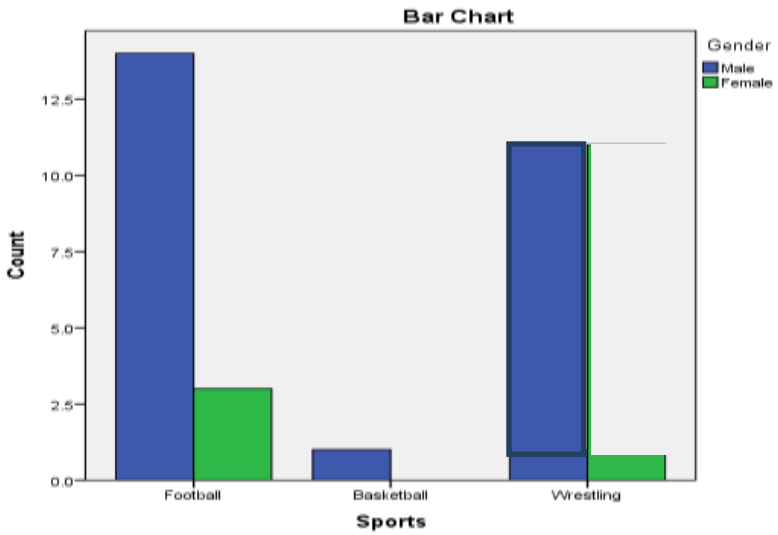

Fig 16: Category type per no. of participants Chart for sport model

5.2 Effect of age group on user choice of images for graphical password

		<18	18-20	21-23	24-26	27-29	30-32	33-35	>35
Sports	Football	3	8	4	1	0	0	1	0
	Basketball	1	0	0	0	0	0	0	0
	Wrestling	1	4	2	0	3	2	0	0
Non Sports	Movies	4	4	1	1	0	3	0	0
	Music	5	3	1	2	2	1	1	0
	Famous	0	0	0	0	0	0	1	1

Table 4: Category type per age group of participants

Table 4 shows the number of participants in each age group that participated in the prototype testing and category type from which participants under each age group have chosen their images for graphical password.

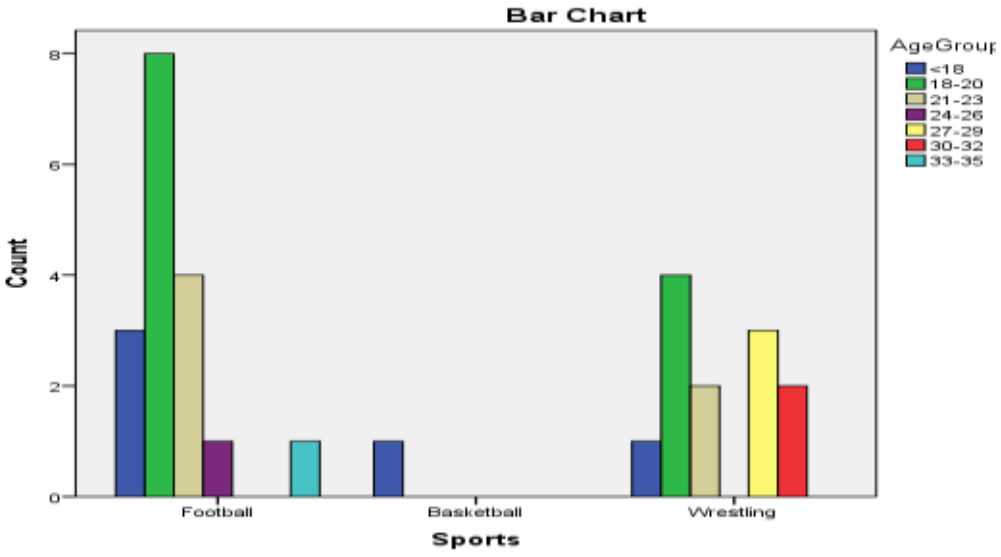

Fig 17: Age group per number of participant chart for Sport model

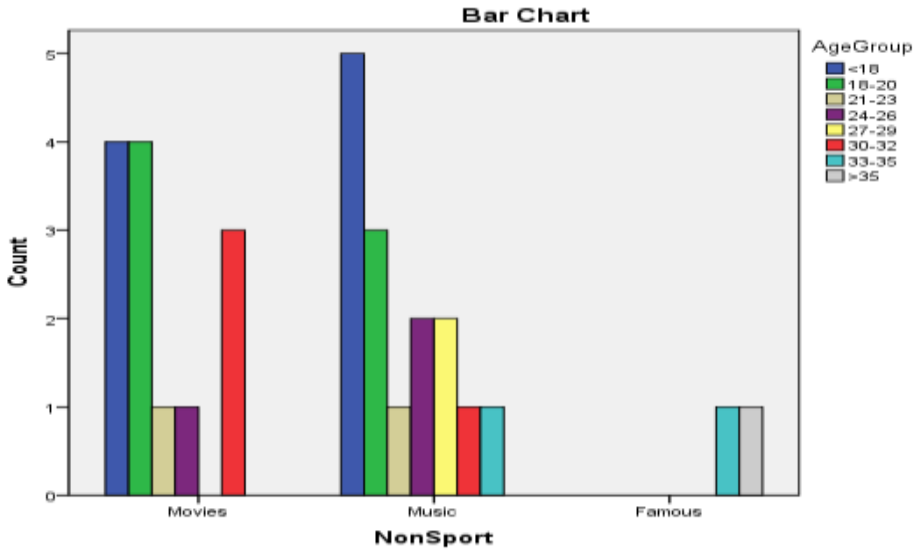

Fig 18: Age group per number of participant chart for Non sport model

Fig 17 and 18 shows the range of age groups per number of participants within each age group who have chosen their images for password from the various types of sports and non-sports category. Within the football category, the highest number of participants (8) with 47.1 % is in the 18-20 years group followed by the less than 18 year group with 3 participants (17.6%) and the 21-23 years group with 4 participants (23.5%). This shows that out of the 17 participants that chose football, 15 of them fall within the less than 18 and 24 year age group indicating that younger age groups were mostly interested in football. While not much can be said for basketball (having only 1 respondent), the number participants for wrestling show a more diversified age group distribution of age groups with 7 respondents within the less than 18 and the 21-23 year age group and 5 respondents in the group of 27-29 years (3 respondents) and the 30-32 years group (2 respondents).

In the non-sports model, higher numbers of participants from the movies category shows that younger age groups are more interested in using images of movie celebrities for their passwords with 4 participants each (30.8%) for the <18 and the 18-20 groups and 1 participant (7.7%) in the 21-23 age group, totaling 9 out of the 13 movie participants, though 3 participants (23.1%) are in the 30-32 age group. In the music category also, higher numbers from the younger age groups (5 participants (33.3%) in the <18, 3 (20%) in the 18-20) out of the 15 recorded respondents showed more interest than the other age groups. It is interesting to note that respondents have been recorded for all the age groups meaning that all the age groups have interests in music but more from the younger age groups. All the 2 participants that showed interest in famous personalities are from the 33-35 (50%) and beyond 35 years (50%).

5.3 Familiarity of users with images of celebrities from their respective region

			Region			Total
			Africa	Asia	Europe	
Sports	Football	Count	10	1	6	17
		% within Region	83.3%	50.0%	37.5%	56.7%
	Basketball	Count	1	0	0	1
		% within Region	8.3%	0.0%	0.0%	3.3%
	Wrestling	Count	1	1	10	12
		% within Region	8.3%	50.0%	62.5%	40.0%
Total		Count	12	2	16	30
		% within Region	100.0%	100.0%	100.0%	100.0%

Table 6: Region of each celebrity per no. of participants for Sport model

			Region			Total
			Africa	Asia	Europe	
NonSport	Movies	Count	5	6	2	13
		% within Region	55.6%	46.2%	25.0%	43.3%
	Music	Count	3	7	5	15
		% within Region	33.3%	53.8%	62.5%	50.0%
	Famous	Count	1	0	1	2
		% within Region	11.1%	0.0%	12.5%	6.7%
Total		Count	9	13	8	30
		% within Region	100.0%	100.0%	100.0%	100.0%

Table 7: Region of each celebrity per no. of participants for Non sport model

Table 6 and table 7 shows the number of participants who had chosen the images of celebrities from a particular region based on the type of prototype used during testing. More than half, 58.8% of participants that selected password images from the football celebrities selected mostly from Africa (10) and 35.3% from Europe (6), and 83.3% of those that chose from images of wrestling celebrities displayed more interest in European wrestling stars (10 participants). From this table also, 46.2% of participants showed interest in movie celebrities from all the regions with images of Asian movie actors used mostly (6) followed by African movie stars (5) having 38.5% and lastly European movie stars (2) having 15.4%. Similarly, 46.7% of participants were found to be interested mostly in Asian music celebrities (7) and 33.3% for those of European region (5) and least recorded is that of the African music celebrities with 3 respondents (20.0%). The two (2) respondents that selected images of famous personalities chose those from Africa and European region.

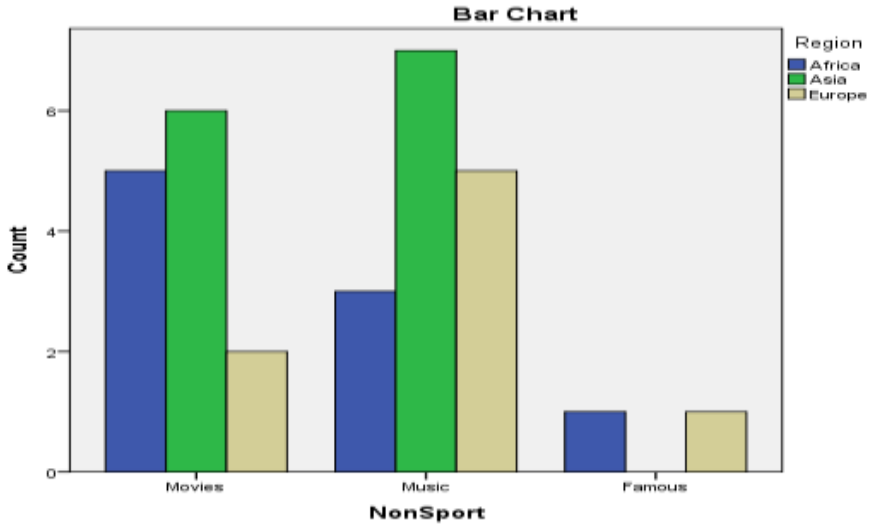

Fig 19: Number of participants per region chart for None sports model

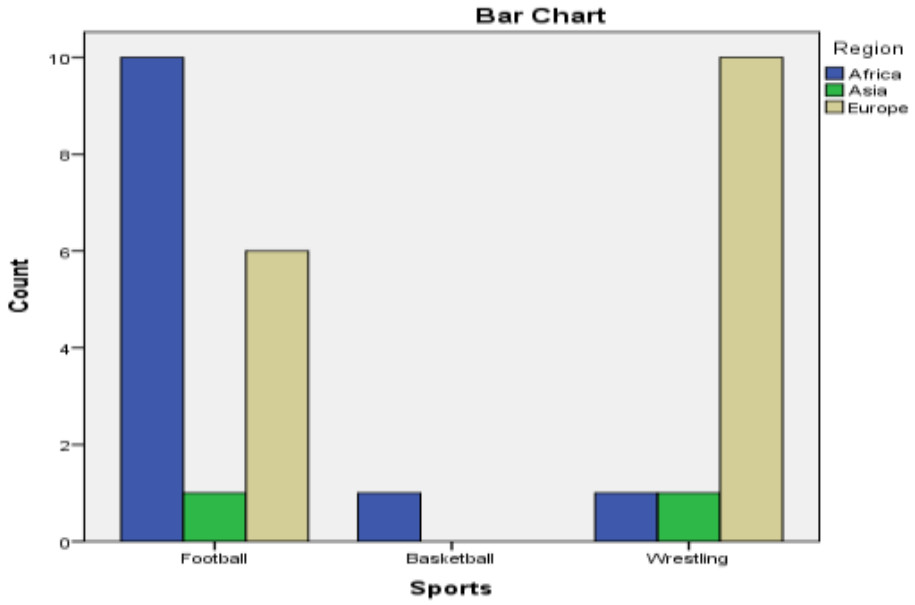

Fig 12: Number of participants per region chart for Sports model

The charts in figure 11 and 12 shows that respondents in this study are more familiar with sports celebrities from Africa and Europe with total number of 12 respondents and 10 respondents respectively and only 5 respondents are familiar with non-sports celebrities such as movies and music celebrities of African region. We have found that non-sports celebrities such as music and movies celebrities in Europe have the highest number of 14 participants who are familiar with their images during non-sports prototype testing. The researchers also found out that 10 participants are also familiar with non-sports celebrities of Asian region with only 5 participants who are also familiar with sport celebrities of the Asian region.

6. Results Discussion

At the end of prototype testing, questionnaires containing responses of participants were collected and analyzed and we have found and categorized our result as follows:

i. The effects of gender on user choice of image for graphical password

This study confirmed that most of the female participants were interested in images of movies and music celebrities for their graphical password because they are likely to be more familiar with and be able to remember faces of the movies and music celebrities or they are likely more interested and indulge in movies and music than other category types such as sporting activities. Similarly, our study also confirmed that male participants were interested in using images from football players and wrestlers for their graphical passwords and this shows that they are likely to recall images of football players and wrestling stars or they are likely more interested in such images than the images from other category types.

ii. The effects of age on user choice of images for graphical password

This research has confirmed that participants within the age range of 18-20 have chosen their images from those of football, music and movies stars and this implies that they are most likely more interested in such category types or they are most likely more familiar with images from football, music and movies. Participants with less than 18years tended to use images of movies and wrestling stars to create their graphical passwords. As such, they are most likely interested or most likely more familiar with images of movies and wrestling stars. The study has also confirmed that participants within the ages of 21-23 and 24-26 have chosen their images from movies, music, football and basketball and this shows that they are most likely more interested in such images or that they are more familiar with such images. The study also confirms that the participants with age range of 27-29, 30-32, and 33-35 have chosen the images of music, movies, wrestling and football and with the above response; we can conclude that participants within the

above age group are most likely more familiar with their chosen images or that they are more interested in the images from the categories they had chosen.

iii. **The effects of familiarity on user choice of images based on regions:**

This research has found out that participants have chosen images from different regions and has noticed that their chosen images are based on the familiarity of the participants with players from such regions. Users who chose wrestling were found to be mainly interested in those from Europe and those who were interested in football were primarily interested in African and European footballers. In the movies category, Africa and Asia were shown to be the regions majority of the users were familiar with. For music celebrities, Asian musicians were mostly chosen by the users even though higher instances were recorded for both African and Asian music celebrities.

7. Conclusion and future area of research

Previous research on system security has been primarily focused on technical problems and solutions. Until recently, the role of human factors in system security has not been recognized. Research has shown that human factors represent the weakest part of a security system and system users are the weakest link in the system security chain, hence, human factors are considered the fundamental reason why many attacks on computers and systems are successful [4]. In this paper, a hybrid authentication scheme was developed and a comprehensive study was conducted to ascertain the effects of human factors such as gender of the participants, age group of the participants and familiarity of the participants with their choice of images for graphical passwords based on regions. Our study showed that user's gender plays a role on their choice of images for passwords as it has been observed that selection of password images has placed a significant weight on the category of the images chosen by different genders. Age groups have also been observed to affect the choice of certain image categories where users belonging to a certain age group prefer images from a certain category as opposed to other groups. Similarly, the regions of the celebrities also have an impact on the familiarity and the memorability of the users who choose images of celebrities from them. The study can be extended to investigate the effect of other human factors such as skill, culture etc. and more category type and region can be added for future research. Participants used for conducting this study were all University students with common cultural background, but another exciting result can be achieved by using participants with different cultural background.

References

i. W. Aspray, "Computers, information and everyday life" *IEEE Annals of the History of Computing* 35(4) (pp. 96-99), 2013

ii. K. Sakamura, "Human interface with computers in everyday life" *The Ninth TRON Project Symposium* (pp. 2-3) IEEE Computer Society, January, 1992

iii. P. Dourish and D. Redmiles "Approach to Usable Security Based on Event Monitoring and Visualization" In *Proceedings of the 2002 workshop on New security paradigms,* (pp. 75-81) ACM Press, 2002.

iv. K. Weber, A. E. Schutz, T. Fertig and N. H. Muller "Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users". In *International Conference on Human-Computer Interaction,* (pp. 660-668), Springer, Cham, 2020.

v. C. Kuo, S. Romanosky and L. F. Cranor "Human Selection of Mnemonic Phrase-based Passwords". In Proceedings of the Second Symposium on Usable Privacy and Security, (pp. 67-78), 2006.

vi. G. E. Blonder "Graphical Passwords" United States Patent 5559961 1996.

vii. M. Z. Jali "A Study of Graphical Alternatives for User Authentication" A thesis submitted to the University of Plymouth. (2011).

viii. T. Khodadadia, M. Alizadeb, S. Gholizadeb, M. Zamani and M. Darvishi "Security Analysis Method of Recognition-based Graphical Password*" Jurnal Teknologi*, 72(5), (pp. 57–62) 2015

ix. S. Sharma and J.S. Sodhi "Implementing Choice Based Graphical Password Authentication in Social Networking Site" *World Applied Sciences Journal* 32 (10): 2140-2145, 2014

x. Real User Corporation, "How the Passface™ System Works," vol. 2005, 2005

xi. P. Dunphy, J. Nicholson and P. Olivier "Securing Passfaces for Description" In *Proceedings of the 4th Symposium on Usable Privacy and Security* (PP. 24-38) 2008.

xii. H. U. Suru, A. A. Muslim, S. U. Suru and H. U. Suru "A Review of Graphical, Hybrid and Multifactor Authentication Systems" In *International Journal of Scientific & Engineering Research* 10(1), January, 2019.

xiii. F. Towhidi and M. Masrom "A Survey on Recognition-Based Graphical User Authentication Algorithms" In *International Journal of Computer Science and Information Security*, 6(2), 2009.

xiv. A. M. Eljetlawi and N. Ithnin " Graphical Password: Prototype Usability Survey" *International Conference on Advanced Computer Theory and Engineering* 2008

xv. S. Wiedenbeck, J. Waters, J. C. Birget, and A. Brodskiy "PassPoints: Design and longitudinal evaluation of a Graphical Password System" *Symposium On Usable Privacy and Security*, 2005

xvi. K. M. Everitt, T. Bragin, J. Fogarty and T. kohno "A Comprehensive study of Frequency, Interference and training of multiple graphical passwords" In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 889-898, 2009.

xvii. S. Chiasson, R. Biddle and P. C van Oorschot "A Second Look at the Usability of Click Based Graphical Passwords". In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, (pp. 1-12), PittsBurgh, 2007.

xviii. S. Chiasson, R. Biddle and P. C van Oorschot "Graphical Password Authentication Using Cued Click Points" In *European Symposium on Research in Computer Security*, (pp. 359-374) Springer, Berlin, Heidelberg, 2007.

xix. S, Chiasson, A. Forget and R. Biddle "Influencing Users Towards Better Passwords: Persuasive Cued Click-Points" In *People and Computers XXII Culture, Creativity, Interaction*, (pp. 121-130), 2008.

xx. P. C. Van Oorschot, T. Wan "TwoStep: An Authentication Method Combining Text and Graphical Passwords" In *International Conference on E-technologies*, pp. 233- 239) Springer, Berlin, Heidelberg, 2009

xxi. S. Kalsoom, S. Ziauddin and M. Tahir "SportsFaces: A Graphical Password System based on Images of Sports Celebrities" In *11th International Conference on Innovative Internet Community Systems (I2CS 2011)* Berlin, Germany June, 2011.

xxii. F. Tari, A. A. Ozok and S. H. Holden "A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords**"** *Symposium on Usable Privacy and Security (SOUPS)* July, Pittsburgh, PA, USA 2006.

Author Profile

Salihu Umar Suru received his B.Sc. degree in Computer Science from Usmanu Danfodiyo University Sokoto (UDUS) in 2005 and M.Sc. degree in Business Information Systems from University of East London (UEL) in 2011. He is currently working on his PhD thesis from University of Bakht Alrudah in Sudan and his area of research is Usability and Security of Hybrid Authentication Systems. He was the Director of Information and Communication Technology Directorate (ICT Directorate) of Kebbi State University of Science and Technology, Nigeria from 2014 to early 2018 and also a lecturer in the Department of Computer Science from 2007 to date and held the post of Examinations officer in the Department of Computer Science of Kebbi State University of Science and Technology from 2012 to 2016.