Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Alese, B. K., Omojowo, A. A., Adesuyi, A. T., Thompson, A. F., Adewale O. S., & Osuolale F. O. (2015). An Enhanced Graphical Password Technique Using Fake Pointers. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015,* 79-89. Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p079-089Alese1551.pdf

An Enhanced Graphical Password Technique Using Fake Pointers

B. K. Alese, A. A. Omojowo, A. T. Adesuyi, A F. Thompson, O. S. Adewale, and F. O. Osuolale

bkalese@futa.edu.n.g manwalon2012@gmail.com
atadesuyi@futa.edu.ng afthompson@futa.edu.ng
adewale@futa.edu.ng aofestus@futa.edu.ng

Abstract

Security is the degree of resistance to, or protection from harm. It applies to any vulnerable and valuable asset, such as person, community, nation, or organization. Thus, the determination of a user being allowed access to a resource(s) is done cautiously. Alphanumeric password has been used for authentication, however, it is inherently limited. Graphical password is a possible alternative. Consequently, this paper designs a new graphical password technique based on images, rather than alphanumeric strings. Although, graphical password technique is more secure than textual password. It is also vulnerable to attacks. The most common problem therefore with Graphical Password is the Shoulder Surfing problem, also called "PEEPING ATTACK". In this paper, we proposed a user authentication technique called "FAKEPOINTER"- a user authentication technique that conceals users' authentication secret regardless of a shoulder surfer success by video camera(s). In the software designed, a graphical password fake indicator (pointer) is incorporated to enhance users' login (password) against attack. The system is designed to run on windows platform with .Net support with Microsoft Structured Query Language Server as the back end, C# as front end. The system performs better when compared to existing system.

Keywords: Security, Graphical password, Textual password, Authentication

Introduction

Security system plays an important role in the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. In order that the computer systems and the information associated to them should also be protected. Computer security systems should take into consideration the human factors such as ease of a use and accessibility, in this context. Current secure systems exhibit various limitations due to ignorance of the pertinent impact of human factors in security. An ideal security system considers items such as security, reliability, usability, and gives attention to human factors. Passwords are simply secrets that are provided by the user upon request by a recipient. They are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists. Passwords are the most common

Editor: Eli Cohen

means of authentication which do not require any special hardware. Typically, passwords are strings of letters and digits (alphanumeric). Thus, passwords have the shortcomings of being hard to remember. Weak passwords are vulnerable to dictionary attacks and brute force attacks whereas Strong passwords are harder to remember (Dhamija & Perrig, 2000).

Overcoming the problems associated with password based authentication systems, researchers have proposed graphical passwords technique and developed the alternative authentication mechanisms. Due to the security vulnerabilities of networks and the ease of security threat to shared data, several security measures have been employed, even with the advance security measures, they are still potentially vulnerable to shoulder-surfing attack. This work is motivated by the need to overcome aforementioned attack using Fake Pointers. Majority of Nigeria banks web authentication still uses textual based login technique. These are vulnerable to diverse attacks such as peeping attacks, eavesdropping. However, very few banks enhances their web authentication logon with the use of Hybrid authentication system (alphanumeric password) thereby attacks are minimized. Better still, it is very vulnerable to peeping attacks, therefore, there is a need for an improved security to enhance users' verification and minimize shoulder surfing attacks during login. Fake Pointer Scheme is be employed using disposable password, indicators and pointers. The scheme is designed on a .Net platform using C# programming language and Microsoft Structured Query Language Server as the back end.

Related Works

Information security entails protecting the confidentiality, integrity and availability of information (Kwangjo, 2009). A major focus of information security is preventing authorized and unauthorized individuals from accessing, creating, or modifying information inappropriately. There are many graphical password schemes that have been proposed and implemented. Jansen (2004) worked on graphical password scheme, the work proposed an authentication schemes based on graphical password for mobile devices. In general, these schemes consist two major phases: registration phase and authentication phase. In registration phase, the users are required to create their password object by choosing set of images in thumbnail size. Whereas, in the authentication stage, the users must input the password object correctly as it is in registration phase. However, each chosen image is represented by a numerical value, and the sequence of the chosen images generate numerical password as well. Sreelatha et al (2011) Proposed scheme using two authentication techniques that is based on text and colors for personal digital assistant (PDAs): pair based technique and hybrid textual technique. These two techniques employ grid for session passwords generation, the password authentication scheme is secure since the password is used once for one login process. Gao et al (2010) proposed their graphical password Scheme CDS to be Resistant to shoulder-surfing by using N × N grid image. Divyans (2009) work emphasize on secure password entry scheme in ATM network with resistant to peeping attacks. The research describe a model that entails ATM card users to request for a transaction pin number from their card issuer. Upon receiving the pin called "FAUX" (a fake pin number) which is encrypted with the card holder's password, the user decrypt it with an install application on it mobile phone. The decryption uses symmetric method and the "FAUX" is only valid for a single login. Sonkar et. al. (2012) developed graphical password system that uses color image gallery for authentication. The system allows user to register textual information and most importantly select at least a colored image and at most N numbers of images at random. During authentication the user must also select colored images in the order at which it was selected during registration time. Mohammad et. al (2012) designed a graphical password based on shape. Their research aimed at system access control that enables only authorized users to use only resources enlisted for them. Their proposed system has two phase: registration and authentication. The registration phase allow users to select password from series of standard shapes which are used to create an object. Minimum of five shapes are required to create password object. The phase focuses on shape abbreviation, order of drawing shapes and size of the drawing shapes. On the other hand, the authentication phase deals with user logging in with their username and password to access their intend resources. Chiasson et. al. (2007) proposed a graphical password authentication using Cued Click Points. The work offers cued-recall and prompt visual cues that immediately alert authentic users if they have mistakenly clicked a wrong point at their last click-point. The research focuses on hotspot-based attacks. The password phase uses a discretization method to determine a click-point's tolerance square and corresponding grid. 400 grids were used with image size of 451x331 pixel and tolerance squares of 19x19 pixels with a required username that uniquely maps each tolerance square to a next-image. The model allows user to click a point on an image which is then lead to the next image in the 5 stages. This then lead to a path as a sequence of click-points that is used against authentication phase.

Shoulder Surfing Attack

Peeping attack in the real world is one of threats to a user authentication. It is a well-known attack method that is called "shoulder surfing attack". The attack occurs when an attacker steals a target user's secret by looking into her/his authentication action. The major cause of the attack is a loose user interface because it forces users to print or type a secret directly and it enables attackers to identify a secret visually. Even worse, in recent days, the threat has been magnified by emerging a new attack method. An attacker starts using a video camera or camera phones to capture an authentication action, user's screen or keyboard as they logged in. And extracts a target user's secret from the video record later (Takada, 2008; Chiasson, 2007). Attackers have recently come up with different vision-enhanced devices to perpetrate this attacks. These devices ranges from binoculars for long range distance, affordable miniature closed-circuit television cameras to observed data entry. According to research, this attack is belief to be effective in public places (Divyans, 2009).

Fake Pointers

Fake Pointer is a user authentication scheme that does not reveal users authentication secret even if an attacker capture's target authentication action by a video camera. Fake Pointers has two features to alleviate a shoulder surfer's threat**:** First, feature is a double-layered user interface for a secret input. This user interface makes it hard for attackers to identify a secret visually. The Second, feature is that the fake pointer makes use of two secrets. One secret is a fixed secret; this is a same with traditional authentication. The other secret is a disposal one-time secret named "answer indicator". This is also a necessary feature in order to guarantee its security against another potential threat that could result from a video capturing. In the fake-Pointer, as far as a user changes an answer indicator prior each authentication trial, a secret input operation is randomized even if a user keeps using a fixed secret, and it seems the input is a random number. This makes it hard for attackers to extract a secret by statistical analysis even if they have multiple video records about the same user. These features ensure a more secure authentication against a peeping attack with a video camera.

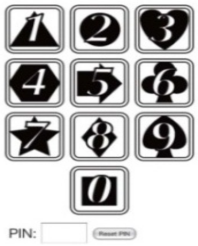


Figure 1: A typical FakePointer interface with randomly sorted pictures behind the numbers (Takada, 2008)**.**

Our Approach

The design system comprises of three phases. The Administrator, Registration Phase, Authentication Phase.

Administrator

The administrator is authorized to: Effect changes to theme icons; Change password characters and lengths; Changes password indicators and mapping.

Registration Phase

At this phase, the window based application allows user to do the following:

- New user input user details: email address and name in order to create user session.
- The user then clicks Register button to indicate the completion of registration and redirect to login page.
- The new user login with email address.
- Mapped icons for pointer appear after user selection.
- The control box is the fake pointer pointing towards theme icons. It ranges from 1-9
- Verification control box is to verify user authentication.
- Advanced control box link un-register user to registration page

i. **Session and Password configuration page**

- For a user to authenticate into his / her account there must be an active session.
- At this page, active session and password configuration of a user is done.

a. **Session phase**

It consists of password session ID and User ID. User ID appears automatically when user enter password session id manually.

b. **Password Configuration**

- Desired Password length P_L is selected that is the number of digits which varies from three to six characters is selected during session creation
- Total life span of the password is computed.

For example, a four character password has a total life span of twenty-four times using permutation.

- Password digit ranges from one to nine in which a user can select randomly. Thus, therefore,

Let E represent User Id, and P denotes Password length range such that P = [3:6] where $3 \geq P \leq 6$

$$\text{Let } P_L = \prod_{y=1}^{p} y \qquad 1$$

where $y \in R$

Let dp denote digit pointer and U represent set of selected digit pointer such that;

$\mathrm{dp} = [1:9]$

$\mathrm{U} = \{U_1, U_2, \dots, U_x\}$ and $\mathrm{X} \leq \mathrm{P}$

There exist 3 classes of images set indicator $\mathrm{T} = \{\mathrm{t}_1, \mathrm{t}_2, \mathrm{t}_3\}$ such that

$t_i = \{\mathrm{M}_1, \mathrm{M}_2, \mathrm{M}_3, \ldots, \mathrm{M}_9\}$ where $t_i \in \mathrm{T}$ and $M_i \in t_i$ are any instance of indicator and images respectively.

ii. **Indicator Selection Page**

- The theme drop down box allows user to select different indicators. (Indicators are graphical images from theme icons).
- The submit control box activates selected indicators by the user.

iii. **Mapping Page**

- The Map control box mapped the generated themes icons with the selected password character digits

Let γ represent user mapping function and *M* a selected set of Mapped digit pointer to selected set of indicator V. Therefore, *V* can be written as:

$$\mathrm{V} = \{V_1, V_2, \ldots, V_x\}$$

and

$$M_k = \overset{x}{\underset{k=i,j}{\gamma}} (U_i, V_j)_k \qquad 2$$

$$such\ that\ \ i \neq j \ \wedge \ i = j\ where\ \ i, j \in x$$

Therefore, $M_{(E,view)}$ for mapped set of digit pointer to indicator view set for a user ID E can be written as

$$M_{(E,view)} = \{(U_i \Rightarrow V_j)_1, (U_i \Rightarrow V_j)_2, (U_i \Rightarrow V_j)_3, \ldots, (U_i \Rightarrow V_j)_x\}$$

where $u_i \in \mathrm{U}$, $v_j \in \mathrm{V}$ and $\Rightarrow$ is the mapping symbol.

Let R represents shuffle function for V that is used for presenting authentication set of indicator for user login and β denote function for selected order of pointer by user, Thus shuffle set of indicator *S* is given as:

$$\mathrm{S} = \mathrm{R}(\mathrm{V}) \qquad 3$$

while order of selected set of pointer

$$\mathrm{R} = \beta(\mathrm{U}) \qquad 4$$

Therefore, let F denotes user's mapped set during authentication such that:

$$F_i = S_i \uplus R_i \qquad 5$$

User authentication validity identity E status $Auth_E$ can be written as

$$Auth_E \begin{cases} valid, & F_{(E,view)} = M_{(E,view)} \\ invalid, & F_{(E,view)} \neq M_{(E,view)} \end{cases}$$

- Save.

Registration Ends.

Sample Scenario

Figure 2 showcase the relationship between selected mapped indicators and selected digit pointer

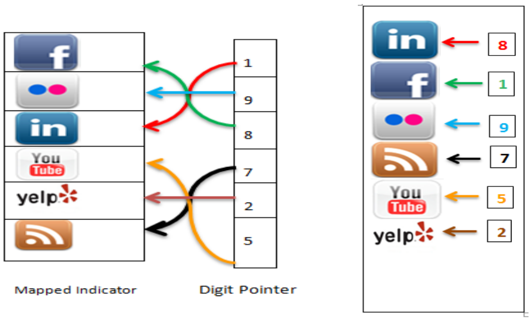


Figure 2: indicator and digit pointer mapping

This is one to one (1:1) mapping relationship in which sets of indicators are randomly selected, un-ordered and mapped with digit pointer within the range of 1-9. Selected digit pointers are used without repetition so as to enhance security against shoulder surfers while authenticating.

Verification Phase

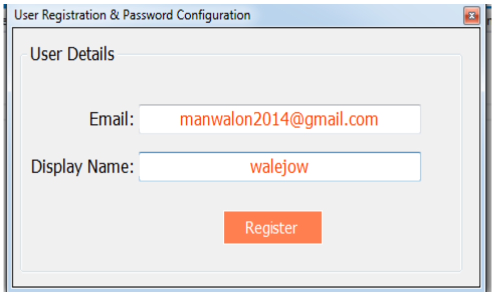
Fake Pointer Authentication Page

Authentication takes place immediately user registration is saved. At this phase, the following steps are followed:

- Existing user select registered email address.
- Application generates temporary password.
- The application encodes password using indicator (Indicators will be graphical images from theme icons).
- Application displays the encoding as FAKEPOINTER
- User clicks out the correct password in the number grid.
- Then verifies.

Implementation Phase

The implementation platform comprises of C#, Microsoft.NET and Microsoft Structured Query Language. The model is into three phases, registration, verification and administration phase. The window based Implementation is shown in figure 3a to 3h.


User Registration & Password Configuration

User Details

Email: manwalon2014@gmail.com

Display Name: walejow

Fig 3a :User registration

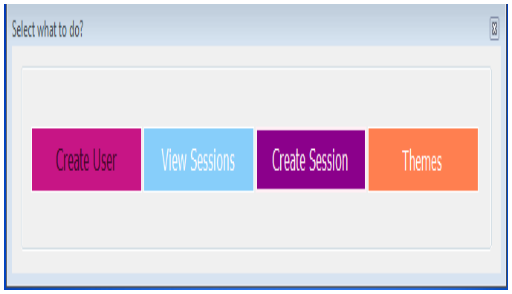
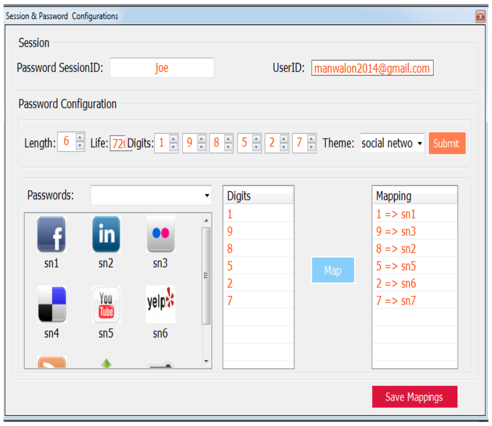

Select what to do?

Fig 3b: User selection



Session & Password Configurations

Session

Password SessionID: joe

UserID: manwalon2014@gmail.com

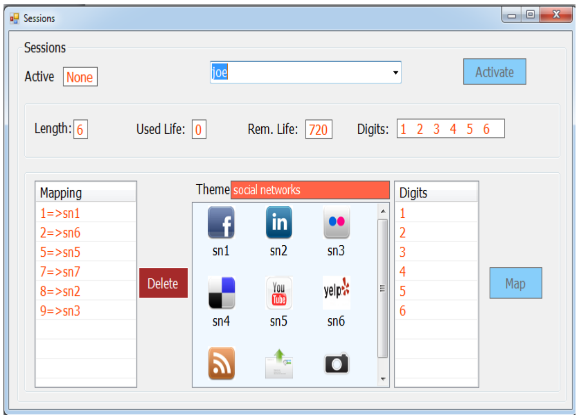
Password Configuration

Length: 6 Life: 72(Digits: 1 9 8 5 2 7 Theme: social netwo Submit

Passwords:

Digits	Mapping
1	1 => sn1
9	9 => sn3
8	8 => sn2
5	5 => sn5
2	2 => sn6
7	7 => sn7

Fig 4c : Mapped session



Sessions

Sessions

Active None

joe

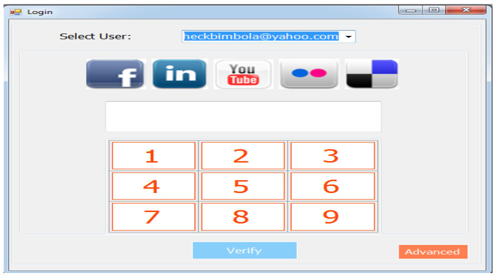
Activate

Length: 6 Used Life: 0 Rem. Life: 720 Digits: 1 2 3 4 5 6

Mapping	Digits
1=>sn1	1
2=>sn6	2
5=>sn5	3
7=>sn7	4
8=>sn2	5
9=>sn3	6

Theme social networks

Fig 3d : Mapped editing session

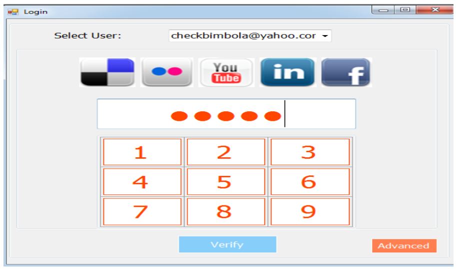


Login

Select User: heckbimbola@yahoo.com

1	2	3
4	5	6
7	8	9

Fig 3e: User verification login session



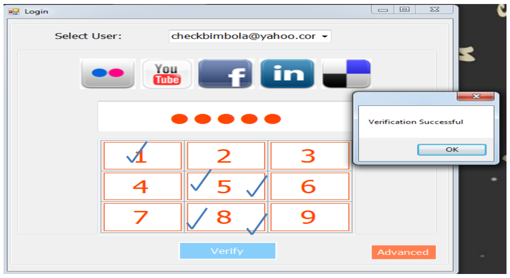
Login

Select User: checkbimbola@yahoo.cor

●●●●●

1	2	3
4	5	6
7	8	9

Fig 3f : User verification



Login

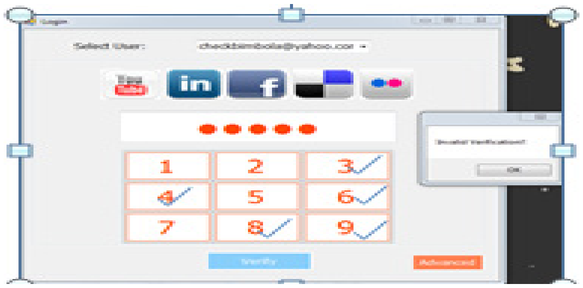
Select User: checkbimbola@yahoo.cor

●●●●●

✓1	2	3
4	✓5✓	6
7	✓8✓	9

Verification Successful

Fig 3g : User verification (sucessful)



Select User: checkbimbola@yahoo.cor

●●●●●

1	2	3✓
4✓	5	6✓
7	8✓	9✓

Fig 3h : User verification (unsuscessful)

Result

This work made use of 10 users. The users were registered with email address; pick password length of their choice; and were required to login. Their login success, denial and number of times password can be reused (lifespan) were captured. They were also required to login with their false login details in order to examine the false acceptance rate of the system. Details of the experiment is shown in Table 1.

Table 1: List of experimented users and their outcome

Users	Password Length	Password Lifespan	Successful	Unsuccessful	False Acceptance	False Rejection	Times logged in	Days logged in interval
X_1	5	120	YES	NO	NO	NO	2	7
X_2	6	720	YES	NO	NO	NO	2	7
X_3	4	24	YES	NO	NO	NO	2	7
X_4	4	24	YES	NO	NO	NO	1	0
X_5	5	120	YES	NO	NO	NO	1	0
X_6	6	720	YES	NO	NO	NO	2	7
X_7	3	6	YES	NO	NO	NO	1	0
X_8	6	720	NO	YES	NO	NO	3	0
X_9	5	120	YES	NO	NO	NO	1	0
X_{10}	5	120	YES	NO	NO	NO	2	7

Password Complexity

In the quest for enhancing weakness in password and strengthening security to a system, a level of complexity in terms of combinations of digits, alphabets, images and symbols may be reached. This may be slightly difficult for password owner to remember. This work focuses complexity in password based on degree of remembrance for owners in relation to the length of the password. Combinations of simple and easily recognizable Images were used in order to reduce password recall complexity. Ten registered users with each having difference password length were placed on 7 days to be inquired if they are still able to remember their password. It was discovered that all but one was not able to recall his password.

Table 2: Degree of password recall complexity based on password length

PASSWORD LENGHT	RECALL (LEVEL OF REMEMBRANCE)
THREE	VERY EASY
FOUR	VERY EASY
FIVE	EASY
SIX	SLIGHTLY EASY

Comparative Analysis

Our approah was compared with existing model (Takada model) based on four metrics. Firstly is the level of success that shoulder surfers can attain after shoulder surfing a user while login in. Secondly is the number of times a user can repeatedly use a password (hightest password lifespan). Next is the Password length which measure the strength of the password. The indicators are th image icon used, and lastly is the Pointers which are numeric digit mapped to indicators. Table 3 shows details of the comparism.

Table 3: Comparative analysis of the proposed model versus Takada model

METRICS	TAKADA MODEL	PROPOSED MODEL	SONKAR ET. AL
Shoulder Surfing success	Low	Very Low	Low
Highest Password Lifespan	24 Times	720 Times	Permanent
Highest Password Length	4	6	nth numbers
Indicators (images)	Few	Many	Many
Pointers (digits)	Not used	Used	Not used
Password Combinations	Images only	Images and numeric pointers	Text and Images

Conclusion

In this work, the proposed enhanced graphical password scheme using fake pointer has been established to have reduce the level of shoulder surfing attacks on password. The model has high password lifespan which lessen the burden on users the need to register for another password. Also the long password length which enhances the password strength. Password recall complexity level was also considered and addressed to an appreciable state. We are keen at improving our proposed model to having zero tolerance for shoulder surfing attacks. This we tend to achieve in our next research by having several shoulder surfer standing behind an authenticating user. This will enable us to measure success rate of shoulder surfers against various password length. More so, to increase the password length and lifespan and to still reduce password recall complexity level.

References

Chiasson, S., Oorschot, P. C., & Biddle, R. (2007). *Graphical password authentication using cued click points*. School of Computer Science, Carleton University, Ottawa, Canada; Human-Oriented Technology Lab, Carleton University, Ottawa, Canada

Dhamija, R., & Perrig, A. (2000). Déjà vu: A user study using images for authentication, In *Proceedings of 9th USENIX Security Symposium*, 2000

Divyans, M. (2009). Secure password entry scheme in ATM network which is resistant to peeping attacks. *International Journal of Engineering and Technology, 1*(2).

Gao, H., Ren, Z., Chang, X., Liu, X., & Aickelin, U. (2010, October). A new graphical password scheme resistant to shoulder-surfing. In *Cyberworlds (CW), 2010 International Conference on* (pp. 194-199). IEEE.

Jansen, W. (2004). *Information security – cryptography. "Authenticating mobile device users through image selection," in data security.*

Kwangjo, K. (2009). Computer Science Department, KAIST. Verified at http://caislab.kaist.ac.kr/kkj

Mohammad A. A., Adnan A. H., Hayam K. A., & Abdelfatah A. T. (2012). Graphical password based on standard shapes. *Science Series Data Report, 4*(2). Department of Computer Information Systems, Faculty of Science and Information Technology, Al Zaytoonah, University of Jordan.

Sonkar, S. K., Paikrao, R. L., & Awadesh, K. (2012). Graphical password authentication scheme based on color image gallery. *International Journal of Engineering and Innovative Technology (IJEIT), 2*(4), October.

Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M. S., & Kumar, V. M. (2011). Authentication schemes for session passwords using color and images. *International Journal of Network Security & Its Applications, 3*(3).

Takada, T. (2008). Fake pointer: An authentication scheme for improving security against peeping attacks using video cameras. *UBICOMM 2008*, pp.395-400. 2008. National Institute of Advanced Industrial Science and Technology. Tokyo, JAPAN.

Biographies

Alese Boniface Kayode is presently an Associate Professor with the Computer Science Department of the Federal University of Technology Akure, Ondo State, Nigeria. He holds a Ph.D. degree in Computer Science from The Federal University of Technology Akure, Ondo State, Nigeria in 2004. He has several awards of excellence. His areas of research include, Computer and Network Security, Quantum Computing and Digital Signal Processing. He is the current holder of the First Bank Professorial Chair in Computer Science of the Federal University of Technology, Akure, Nigeria.

Adewumi Adewale Omojowo is a Computer Graphics Designer. He had his Postgraduate diploma in the department of Computer Science of the Federal University of Technology Akure, Ondo State, Nigeria. His areas of research are Computer Grahpics and Network Security.

Adesuyi Akinwale Tosin presently a Software Engineer with the Computer Resource Center of the Federal University of Technology Akure, Ondo State, Nigeria. He holds a Masters degree in Computer Science from The Federal University of Technology Akure, Ondo State, Nigeria in 2014. His areas of research include; E-learning, Ontology, Computer and Network Security, and Machine learning.

Dr (Mrs) A.F **Thompson** is working as a Senior Lecturer in the Department of Computer science, Federal University of Technology, Akure. She finished her PhD in the year 2014. She has attended numerous international conferences and workshops where she presented papers that had appeared in reputable journals. Her areas of research interest spans Biometrics, Network Security and Image Processing Algorithms.

Prof. Adewale Olumide Sunday is presently the Head of Computer Science Department of the Federal University of Technology Akure, Ondo State, Nigeria. He holds a Ph.D. degree in Computer Science from The Federal University of Technology Akure, Ondo State, Nigeria in 2002. His areas of research include; E-learning, Ontology, Computer and Network Security, Computer Networks and Telecommunications, High Performance Computing and Cloud Computing.

Osuolale, A. Festus received the B.Tech. (with honours) and M.Tech degrees in Computer Science from the Federal University of Technology, Akure, Nigeria in 2002 and 2011 respectively. A former banker who has worked in the Information Technology unit of the United Bank for Africa Plc, Nigeria for several years before joining the teaching profession with the Federal University of Technology, Akure, Nigeria few years ago. He has since been involved in research and teaching of undergraduate courses in his home university with specializations in cloud computing, computer and internet security, networking and information risk and security, and biometrics. He is currently pursuing his PhD in the area of cloud computing with specifics in security risk assessment model in cloud computing. He is currently an Assistant Lecturer with some publications to his credit. He is happily married with children.