PERFORMANCE EVALUATION OF FINGERPRINT AGAINST AUTO-PIN AND PASSWORD IN CLOUD COMPUTING

BY

Dr. Emmanuel Ogala
Mathematics, Statistics & Computer Science
(Computer Science Option)
Faculty of Natural Sciences,
Kogi State University, Anyigba

Alih Ohimogbo Sylvester
Department of Computer Science
(Information Technology)
Faculty of Sciences,
National Open University of Nigeria (NOUN)

Abstract

The world has grown so fast in science and technologies. The area of computer science and its application is never left out. As the world advances, knowledge is expanded into a different field of discipline. As this goes on and on, data is collected and mined or processed. The security of these files/data and the authorization of whom to view them is never undermined. This is because security threats are the most trending challenge in the world today. The security of any system must be taken so seriously because negative intentions towards the successful landing of any facility are on the minds of malicious users. In all, cloud computing with the implementation of some sorts of security measures tends to address these issues to some extends. Despite the measures taken, there are still weaknesses therein, but this research brings into light the extent biometrics security model can work side-by-side with a personal identification number (PIN) and password (self-created) to boost up the security of a given facility/system. Note, in cloud computing as applicable to this research work, the relationship established between the access control models and it is also ideal to note "some factors that impact the accuracy of biometrics systems includes noisy input and non-universality. Also, a biometrics system that integrates the "combined security gateway model" can overcome some of the limitations experienced in biometrics fingerprint". This propels better performance as stated in the body of the work.

Keyword: Ogala, Sylvester, Fingerprint, Auto-Pin, Password, Ohimogbo, cloud computing, performance Evaluation.

1. Introduction:

Many frameworks have been put into place and thus form models for identification of a person trying to have access into a facility or a system. Many scholars in the field of science and technology, most especially in the field of information communication technology (ICT) and cyber security did a pretty job in forming and algorithm that could actually checkmate the authenticity of claim of ownership of an identity tag. In line with the primary objectives of this whole research work, though there are different models of soft and primary biometrics identifies like iris check, facial equivalence, height detection and many more, but this work tries to feature out fingerprint biometrics system alongside personal identification number (PIN) and personal password (PP) given that these details can be extracted with 100% accuracy each time they are needed for verification of identity. In view of achieving a more secure system, a framework "Bayesian" was employed out of other frameworks due to its accuracy in identification algorithm. From experiment and

findings, soft biometrics traits could enhance the biometric system performance if there is balance of complement between it and primary biometric traits. This system can be wired or integrated into cloud environment as the case may be.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, 2009).

With the proliferation of large-scale computer networks (e.g., Internet, Intranet and extranet), the increasing number of applications making use of such networks (e.g., e-commerce, e-learning, e-Computing), and the growing concern for identifying theft problems, the design of appropriate personal authentication systems is becoming more and more important. Such systems should have the ability to authenticate persons accurately, rapidly, reliably, without invading privacy rights, cost effectiveness and in a user-friendly manner

A computer's operating system, applications and data are typically installed and stored in the 'traditional' computing environment. In a cloud computing environment, individuals and businesses work with applications and data stored and/or maintained on shared machines in a web-based environment rather than physically located in the home of a user or a corporate environment. Lew Tucker, Vice President and Chief Technology Officer of Cloud Computing at Sun Microsystems, explained that cloud computing is 'the movement of application services onto the Internet and the increased use of the Internet to access a wide variety of services traditionally originating from within a company's data centre' Creeger (2009). For example, web-based applications such as Google's Gmail™ can be accessed in real time from an Internet-connected machine anywhere in the world.

Use of cloud services creates a growing interdependence among both public and private sector entities and the individuals served by these entities. This thesis provides a snapshot of risk areas specific to cloud services and those that apply more generally in an online environment which clients of cloud service providers should be aware of. Akinyokun e atl (2010)

2. Performance Evaluation of Fingerprint Against Auto-PIN and Password

These are three distinct security systems with Auto-PIN and paswword having some sort of similarities in their algorithm. Notwithstanding, the three are known security systems.

From our analysis in 5.3, you would see all the algorithm based on how the system works. To carry out our evaluation proper, we have to work based on some metrics, which would serve as the quantities with which the measure is/are carried out. In light of this, we would look at

a. Response Time (Speed)

b. Durability

c. Strenght

i. Response Time:

This experiment was carried out at testing time of the sofware before final packaging. Technically, CPU time used calculation is done by the programmer and system analyst before any system goes into market. What is expected of users is to see how it works based on diffent workload per given time. More to this, if the CPU time keep prompting each time a variable or instruction is given to the system, that mean it has defile user friendliness as proposed of the system.

For more clarity, we designed three set of analysis.

1 Code module Analysis

2. Non-Code Based Analysis

3. Flowchart Analysis

- **Code Module Analysis**

In this, we developed three set of modules. One for fingerprint, one for auto-PIN and one for password (user-defined)

Module-1 Fingerprint

Option Explicit

Private Declare Function GetTickCount Lib "kernel32" () As Long

Private Sub Command1_Click()

Case 0c (Line 10-190 executed)

End Sub

Private Function YourFunction() As Long

Dim lngTime As Long

Dim lngIndex As Long

'record start

lngTime = GetTickCount

'do your thing

For lngIndex = 1 To 10000

Caption = CStr(lngIndex)

Next lngIndex

lngTime = GetTickCount - lngTime

10 *Print "execution took " & CStr(lngTime); " ms"*

End Function

Module-2 Auto-PIN

Option Explicit

Private Declare Function GetTickCount Lib "kernel32" () As Long

Private Sub Command1_Click()

Case 1 (Line 1-35 executed)

End Sub

Private Function YourFunction() As Long

Dim lngTime As Long

Dim lngIndex As Long

'record start

lngTime = GetTickCount

'do your thing

For lngIndex = 1 To 10000

Caption = CStr(lngIndex)

Next lngIndex

lngTime = GetTickCount - lngTime

20 *Print "execution took " & CStr(lngTime); " ms"*

End Function

Module-3 Password

Option Explicit

Private Declare Function GetTickCount Lib "kernel32" () As Long

Private Sub Command1_Click()

Case 2 (using case-1(Line 1-35 executed))

End Sub

Private Function YourFunction() As Long

Dim lngTime As Long

Dim lngIndex As Long

'record start

lngTime = GetTickCount

'do your thing

For lngIndex = 1 To 10000

Caption = CStr(lngIndex)

Next lngIndex

lngTime = GetTickCount - lngTime

30 *Print "execution took " & CStr(lngTime); " ms"*

End Function

3 Non-Code Based Analyis (Explanation of Module 1, 2 and 3)

MODULE 1:Fingerprint	MODULE 2:Auto-PIN	MODULE 3:Password
Fingerprint is not in a loosed data family, which could probably need high ecryption and decryption algorithm. When a finger is captured, it is passed into a timer that is already set up as a function. The time it takes the system to get the minuate, compare it and find a match or not for verification and bring output to the user is printed out in an alert box on line 10. **(System Dependent)**	Unlike Fingerprint,this is a heavy instruction one of the differences between this and user-defined password is that it is automatically generated. The auto-PIN is given to a user, entered into PIN provision, the saved one is decrypted and compared with the new entry on confirmation, the FA (Fail to Accept) could take place or may be successfule, after that, the PIN is re-encrypted and stored back in the	Like the auto-PIN, the password is formulated at the point of user registration, this password is used to login into the system at any given time. The password is entered into password login provision; the saved one (password) is decrypted and compared with the new entry on confirmation, the FA (Fail to Accept) could take place or may be successfule, after that, the PIN is re-encrypted and stored back in the

	before the CPU time used will be printed out on 20 on page 200.	before the CPU time used will be printed out on 30 on page 201.

3. Flowchart Analysis

This part shows the pictorial representation of the code module and non-code module based analysis of the evaluation of the three security systems discussed. Figure1 and 2 shows the two basic flowchart that are concerned with this.

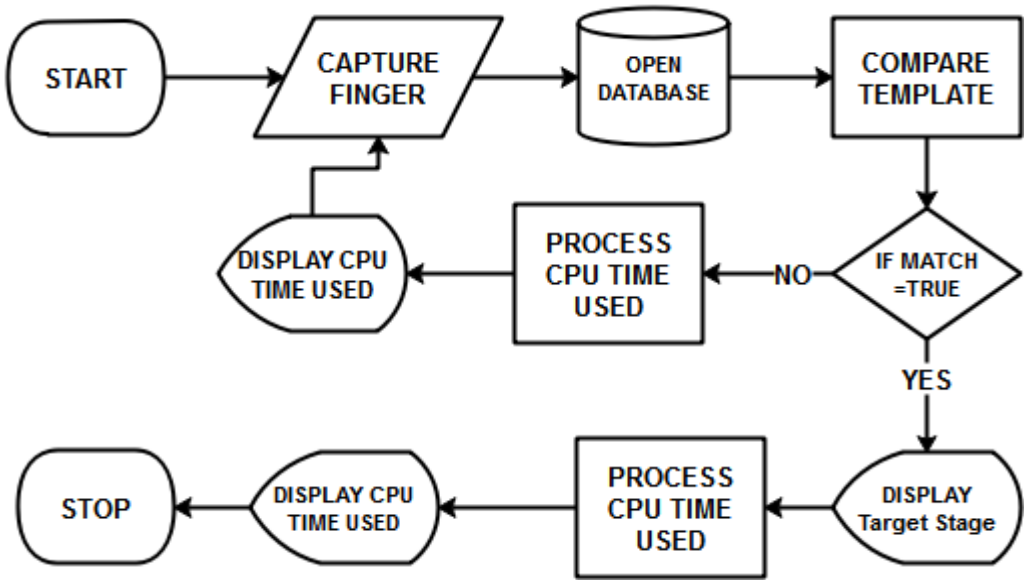


Fig1: Fingerprint login process CPU time capturing flowchart

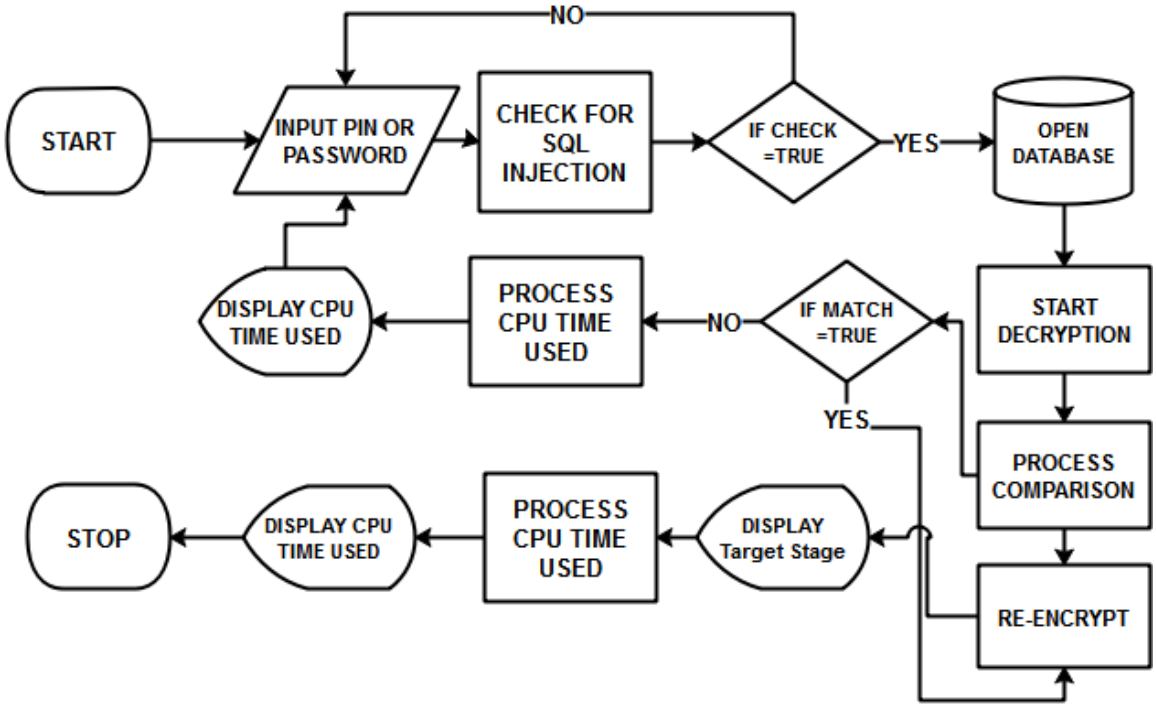
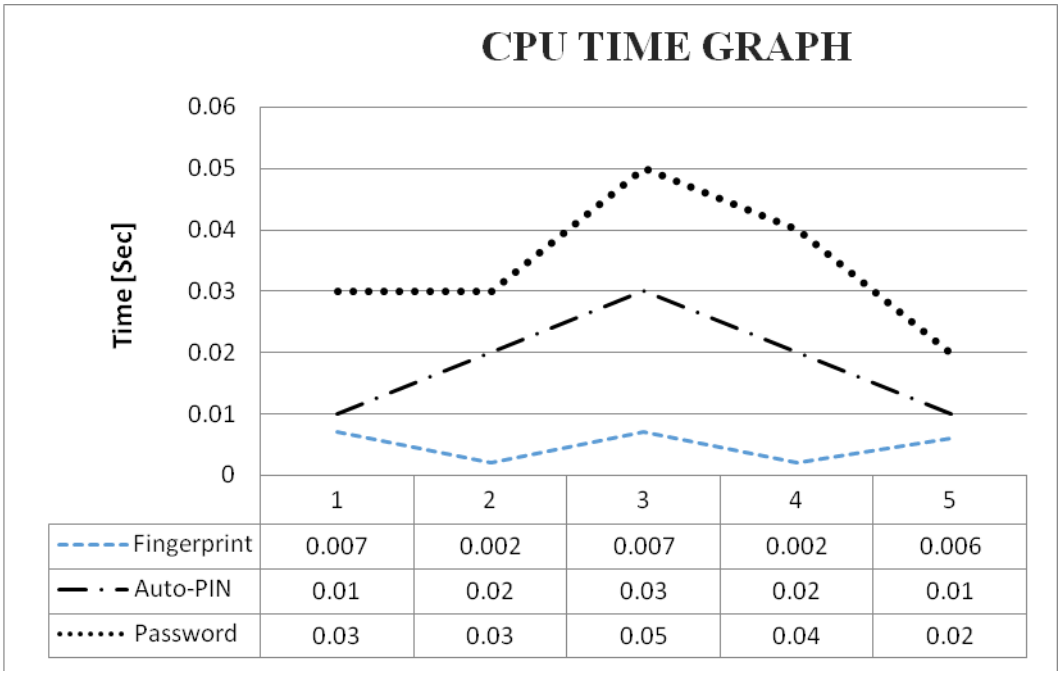


Fig 2: Auto-PIN and Password login process CPU time capturing flowchart



	1	2	3	4	5
Fingerprint	0.007	0.002	0.007	0.002	0.006
Auto-PIN	0.01	0.02	0.03	0.02	0.01
Password	0.03	0.03	0.05	0.04	0.02

Fig 3: fingerprint Auto-PIN and Password login process CPU time capturing flowchart

4. Durability

Durability has to do with longevity. The only condition that could make a fingerprint not to be effective is a medical case know as lyphotnephic, which allow or make ones finger ridges above the apidermic layer to be hidden. Else finger print of a being will remain active until man die and even after death, the fingerprint will still be active until he decays. Now let us look at the

case of auto-PIN and password together. This two can easy be forgotten and even what is used, some times called third-party recovery mail could be forgotten that you will permanently be denied of access into any digital system. In this case, the law of longevity does not hold. Because of the forgetfullness of man, they tend to write down their password or PIN on a paper where they can easy reach out to, but physical damage can occur and the paper would be destroyed, this making the issue of durability are rare case in the usage of PIN and passord security system.

Note, Fingerprint is not the only biometrics system on the shelf. So to you might want to ask a question like - what if user finger is shopped off, what become of him and the system that he uses? To this question I would say - there are many digital systems that are built now that uses skin tecture, odor, temprature, iris scanning, hair system, toes etc for access authentication. That is the major reason advance tech professional and higher companies incorporate 10-finger biometric system, facial recognition system and other types like Iris-reflex action cycle for security checkmate. From findings and practical experiecnce, biometrics (fingerprint) are (is) more durable compared to the later two.

4.1 Strength

This is another good matrix. The natural features in fingerprint makes it more diffult to hack into. Every intruder need access to the object (owner of the finger) to extract content of what his hand touches with moist to be able to form a fake finger to hack into his system. But in the case of auto-PIN and password (user-generated), some guesses by professional and even code kiddies could compromise them. Notwithstanding, user-defined password is more stronger to hack compared to auto-PIN. This is because, common PIN ranges from 1-4 digits and 1-6, but user-defined password could range from 1-40 characters in length with special character combinations, which makes it more stronger in terms of strength compared to auo-PIN. To this very end, we have not been able to break the minuitae but the auto-PIN and passwords have been compromised in a way during our raw test run.

4.2 Description of Experiment

Regarding the percentages allocated to the security system listed in table 5.2 below, we created a practical environment whereby the software was proctected by password. Series of trials and guess-work led to access grant because most at times, password are user-defined and it's related to things that surround them (the users). Redefining our module to use Auto-PIN (Personal Identification Number), there was a bridge after series of trial by unauthorised users (as defined by us). This was as a result of people having the idea of MD5 encryption system and how such code is generated. Combining 4 bits, 8 bits, 16 bits or 32 bits rand function could give any intruder access into the system. Just as predicted, after few trials, the system was hacked. More to this, for the sake of confirmation of the system security. The System was finally given biometrics module as the security measure. On this account, all trials to break into the system was proved futile because the system store minuate or template, which is further processed into binary coded decimal. This kind of code cannot be guesed easily except the object is made available to recapture the main biometrics part (finger) that was used to store the minuate. Conclusively, we say that the strength of biometrics security system is 95% i.e it's better than most of the other security systems in terms of speed and durability and strength as stated earlier.

Table 4.1 Performance Level of confidence (%) of Fingerprint, Auto-PIN, and Password

Matrix Security Systems	Durability	Speed	Strenght
Fingerprint	95%	95%	95%
Auto-PIN	40%	50%	35%
Password	40%	60%	50%
These are percentage evaluation of the listed security systems.			

From our analysis, if you look at table 4.2, you will see that Biometrics (Fingerprint) tend to be 95% stronger in terms of durability, speed and strenght (Matrics).

4.3 Similarities

FINGERPRINT	AUTO-PIN	PASSWORD
Password system	Password system	Password system
Needs database to operate	Needs database to operate	Needs database to operate
Works offline	Works offline	Works offline
Works online	Works online	Works online
Portable	Portable	Portable
Verifiable	Verifiable	Verifiable
Editable	Editable	Editable
Can be hacked	Can be hacked	Can be hacked
Session oriented	Session oriented	Session oriented

4.4 Difference

FINGERPRINT	AUTO-PIN	PASSWORD
Light Algorithm	Medium Algorithm	Heavy Algorithm
Not memorable	Memorable	Partially memorable
Not Easily hacked	Easily hacked	Partially hard to hack
MinData are used for functions	Text files are used	Alphanumeric characters are used
Unique all over the world	Not Unique	Partially Unique
Has many features to consider	Fewer features to consider like the bitrate and data type	Medium features to consider like the bitrate and data type, encryption type and combination protocol
Fingers are used	Few characters from four to eight digits are used	Up to 40 characters are used

5. Conclution

Cloud computing has been envisioned as the next-generation architecture of Information Technology (IT) enterprise. In contrast to traditional solutions where IT services are under physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. This unique attribute, however, many new security challenges which have not been well understood but formed an important aspect of quality of service delivery (Qos). This thesis contributes to the improvement of cloud computing security. The work is motivated by two problems: first, the observed easy access to cloud computing resources and complexity of attacks to vital cloud computing data system NIC requires that dynamic security mechanism evolves to stay capable of preventing illegitimate access. Second; lack of good methodology for performance test and evaluation of biometric security algorithms for securing records in cloud computing environment. The aim of this thesis was to evaluate the performance of an integrated security system (ISS) for computing for securing exams records in cloud computing environment. In this thesis, we design and implemented an ISS consisting of three security mechanisms of biometric finger print, auto-PIN and password into one stream of access control and used for securing examination records in KSU. Conclusively, the system we built has been able to overcome guessing abilities of hackers who guesses people password or pin. We are certain about this because the new system needs the presence of the user of the software before a login access can be granted. This is based on the placement of his/her finger on the fingerprint biometrics scanner for capturing and verification purpose for user's authenticity confirmation. The study adopted the conceptual quantitative design. The object oriented and design methodology was adopted. In the analysis and design, PHP, HTML5, CSS, Visual Studio Java Script, and web 2.0 technologies were used to implement the model of ISS for cloud computing environment. Note; PHP, HTML5, CSS were used in conjunction with visual Studio front end engine design tools and MySQL + Access 7.0 were used for the backend engine and Java Script was used for object arrangement and also validation of user input for security check. Finally, the performance of the proposed framework was evaluated by comparing with two other existing security systems and the results showed that the proposed approach allows overcoming the two main weaknesses of the existing systems.

References

Akinyokun .O.C and Gaberil.B (2010) proposed a mathematical modelling method for fingerprint ridge segmentation and normalization using matrix laboratory (mathlab) as frontend engine and fvc2004 fingerprint database DB3 set. Proceeding of the international conference on software engineering and intelligent systems, Vol. 1 2010.

Akhil, O. A. Hari, G. Kirtika and G. Sakshi, (2012) " Secure Authentication with Encryption Technique for Mobile on Cloud Computing," International Journal of Scientific Research Engineering & Technology (IJSRET), Volume 1 Issue 5 pp 028-033

Andre A. Moenssens (1971). Fingerprint techniques [by] Andre A. Moenssens. Chilton Book Co. Philadelphia,, [1st ed.] edition.

Atoda, N., T. Suruga, and T. Tachibanaki, 1988, Statistical inference of functional forms for income distribution. The Economic Studies Quarterly 39, 14–40.

Banerjee A. and D. Kundu, "Inference Based on Type-II Hybrid Censored Data From a Weibull Distribution", *IEEE Trans. Reliab*., Vol. 57. No. 2, pp. 369-378, Ju. 2008.

Bazen A. M., G. T. B. Verwaaijen, S. H. Gerez, L. P. J. Veelenturf, and B. J. van der Zwaag. A correlation-based fingerprint verification system. In 11th Annual Workshop on Circuits Systems and Signal Processing (ProRISC), Veldhoven, the Netherlands, pages 205 213, Netherlands, November 2000. Technology Foundation STW.

Chen, F.; Zhou, J. & Yang, C. (2009). Reconstructing Orientation Field From Fingerprint Minutiae to Improve Minutiae-Matching Accuracy, IEEE Transactions On Image Processing, Vol. 18, No. 7, pp. 1665-1670, JULY 2009

Chen, K. and Liu, L. (2005). Privacy preserving data classification with rotation perturbation. In Proceedings of Fifth International Conference of Data Mining, 589–592. IEEE.

Chib, S. and S. Ramamurthy, (2010), Tailored randomized block MCMC methods with applications to DSGE models. Journal of Econometrics 155, 19–38.

Chotikapanich, D. and W.E. Griffiths, (2000), Posterior distributions for the Gini coefficient using grouped data. Australian and New Zealand Journal of Statistics 42, 383–392. 2003.

GiTae Park and Soowon Kim (2013). Hand Biometric Recognition Based on Fused Hand Geometry and Vascular Patterns. www.mdpi.com/journal/sensors

Gudavalli, M., Raju, S. & Kumar, K., (2012). A Template Protection Scheme for Multimodal Biometric System with Fingerprint, Palprint, Iris and Retinal Traits. *ACM,* pp. 102-106.