African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

AN INVESTIGATION INTO SYSTEM COMPONENTS THAT SUPPORTS BIOMETRIC FRAME IN GHANA

Dakudjie, J. K.[1], Braye, A.[2] and Otchere, A.A.[3]

[1&3] Department of Information Communication and Technology, Faculty of Applied Science Takoradi Technical University, P.O.Box 256, Takoradi, Western Region, Ghana.
[2] Faculty of Computing and Information Systems, Ghana Technology University College (GTUC), Takoradi Campus, Takoradi, Western Region, Ghana.

[1]johndakudjie@yahoo.com

Abstract
The purpose of this paper was an investigation into System Components that Supports Biometric systems. The study specifically sought to investigate the following components; the architectural models, systems, and components that support biometric system and the limitation of the architectural components. A quantitative research design was adopted. The respondents were selected with the Purposive and Convenience sampling methods and out of the 100 questionnaires used 76 were received and used in the descriptive analysis. The study found out that the architecture made the system effective, ensured data security, and provided accurate data. Based on the findings of the analysis the following recommendations were made: to avoid noise in sensed data, data controllers should ensure that the sensor is properly maintained and the introduction of temporal variations of the system minimize since it causes the system from successfully matching for genuine user or be incorrectly matched with the imposters, resulting in decrease in the performance of the system.

Keywords: *Architectural model, protocols, OSI Reference model, ATM, DNA*

INTRODUCTION

Due to the increasing security vulnerability of identifying persons, the biometric systems components, a security system (s) which comprises of hardware and software architectural designs is use as a secured authentication method. The biometric systems are the most secured authentication method in our time and probably for the next generations. Components of biometric systems are not a new invention. Components of biometric systems are the most secured methods of identifying a person. The biometric systems uses various forms or methods to identify a person by using Fingerprint, Face, Voice (Eriksson et al., 1997), Palm (Zhang et al., 2003), Iris or Fingerprint, combined with face recognition, Palm print (Zhang et al., 2003), Iris , Multimodal biometric and also the use of DNA (Deoxyribonucleic Acid) (Jäckle and Tautz, 1989).

Components of biometric systems are a general term for measurement of humans, to identify them or authenticate that they are who they claim to be. A biometrics data captured in isolation is relatively meaningless. It is only when the biometrics data is processed, or aligned with other data, stored in a database or transmitted for other purpose(s) that it becomes of practical use.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

Biometric systems involved the use of a system, typically a system based upon computers and related components. Consequently, when considering practical aspects of the use of biometric technology, such considerations cannot divorce from the systems that support such practice, their composition, their connectivity and their relative security.

Indeed, many of the questions that arise while discussing biometric technology may be mostly its security. It follows that we should take a holistic view of its security advantages over the traditional security systems such as PIN, badges etc. and ensures that we understand these broader systems architectural components, its implications, dependencies and inter-connectivity. This is particularly the case when considering large-scale systems security of a national or even international dimension. Before architectural component of biometric may be used within a system, its data must be captured. There exist a variety of components with which to facilitate such a capture, often with variations of design and operation of the system even with respect to a given architectural components of biometric systems. In addition, architectural components of biometric information, especially with respect to that of behavioral biometric systems, may be captured via a combination of system components; such as fingerprint, Iris, Palm print, voice, etc. Jain, Ross & Pankanti (2006).

Bolle, Connell, Pankanti, Ratha, & Senior, (2013) argued that the front-end architectural component of biometric systems has the task of capturing the biometric data from a single or multiple sources and transforming it into a form from which either a reference template may be produced and stored in medium, or a match against a reference template may be undertaken. The relative quality of the biometric data captured will be influenced by its component(s), a factor to take into account if multiple architectural components of a different design, or originating from its own source, are employed within a single application. Similarly, if biometrics data is shared between applications, an understanding of the capturing components (capturing devices) used in each application will be important. These components may be specific devices such as fingerprint readers, or scanners, vein pattern detectors, special imaging devices, Iris devices, face devices and so on. The paper investigates the architectural models, systems, protocols, other components that support biometrics system and limitation of the architecture (Bolle, et al., 2013).

Aim and Objectives

The research seeks an investigation into System Components that Support Biometric Frame.

The specific objective of the research is to:

Identify the architectural models, identify the systems characteristics, components characteristics that support biometrics system and to determine the limitations of the models.

Justification of the Research

This research on Biometric Systems is timely because Biometrics Technology in Ghana is at an infant stage; and the output of this research will create more awareness of Biometrics usage in Institutions and organizations that face security challenges. The Biometric Technology will help sensitize awareness to improve data security in Ghana. Biometric security is a security mechanism used to authenticate and provide access to a facility or system based on the automatic and instant verification of an individual's physical characteristics.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

Expected Study Results and Possible Usage

The current research outputs would assist researchers on Biometric systems to further research to enhanced academic knowledge. Secondly, Biometric Systems would significantly be used as the leader of security tools for identification or authentication methods in Ghana.

Significance of the Study

The significance of the study is that findings from this work is expected to provide knowledge to academia and to research. The current research outputs would assist researchers on biometric systems to further research to enhanced academic knowledge. Secondly, it will help inform policy formulation, which involves developing strategies for dealing with policy issues that have been placed on an agenda.

Policy formulation takes both the effectiveness and the viability or acceptability of proposed actions into account. Effectiveness refers to valid, workable strategies that address the biometric systems situation, while acceptability refers to those strategies that are more likely to be put into action. It gives policy direction to the government.

REVIEW OF BIOMETRIC SYSTEMS

Biometric Systems in Ghana is a new Technological breakthrough in Computer security that is replacing existing Security networks like using Personal Identification Number (PIN), such as Password for identification and authentication purposes (Yinyeh and Gbolagade, 2013). Due to the increasing security vulnerability of identifying persons, the biometric systems components, a security system (s) which comprises of hardware and software architectural designs was used as a secured authentication method. The biometric systems are the most secured authentication method in our time and probably for the next generations. Components of biometric systems are not a new invention. The biometric systems use various forms or methods to identify a person by using Fingerprint, Face, Voice (Eriksson et al., 1997), Palm (Zhang et al., 2003), Iris, or Fingerprint combined with either face recognition, Palmprint (Zhang et al., 2003), Iris, Multimodal biometric and also the use of DNA (Deoxyribonucleic Acid) (Jäckle and Tautz 1989). Components of biometric systems are a general term for measurement of humans, to identify them or authenticate that they are who they claim to be. A biometrics data captured in isolation is relatively meaningless. This research seeks to find the challenges facing the Biometrics' Systems users and recommend some flexible way of dealing with the challenges. "This means that instead of the applicant submitting photographs with a passport application form that is already thumb-printed somewhere, it will now be required that the photograph and the fingerprints of the applicants are taken at the application centres when he presents the forms. This is also intended to eliminate middlemen," (Mumuni, 2010)

Components of Biometric Systems

Jain, Hong, & Pankanti, (2000) noted that the typical components of biometric systems are pattern recognition system. It acquires pattern using sensors; the acquired pattern that is input data is extracted using a feature extraction algorithm, and a decision is made based on the input pattern representations and the previously pattern representations stored in the biometric

ISSN: 2408-7920

African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

database or system Jain, et al., (2000). Components primary consists of two modules 1.Enrollment module and 2.Authentication module.

Enrollment module (training) both hardware and software module.

The function of enrollment module is also known as "training or "learning", is a pattern recognition system. It enrolls identities of person being enrolled with representations of their biometric engagements. The biometric signal and the person's name to be enrolled are fed to the enrollment module (software module) , a feature of finger print (minutiae) extraction algorithm is first applied to the representation signal, for example finger images or patterns or minutiae patterns are extracted and stored in the biometric database or system database.

The authentication module (both hardware and software module).

The authentication module authenticates the identity of a person who wishes or intends to access the system (Yaqub and McAuley 2011). The person to be authenticated supply his/her biometric features or characteristics to the system, the biometric sensor captures the input biometric features or characteristics or signal, features extracted from captured biometric signal or characteristics are matched against the

Person's representation stored in the biometric database or system database to verify the identity claim made by the person. An identification system determines the identity associated with the biometric features or characteristics for the claim made by the person.

According to Berry and Stoney (2001) Scotland Yard Police adopted a fingerprinting system in 1901. Fingerprinting technology, now used all over the world, and is the best known example of biometric architecture. Security is the most essential that must be sought, not only with information and communication technology, but as well as in areas, such as terrorism actions, voter registrations, national identification cards, passport processing, ghost names in the national payroll processing systems, information thefts or any activities that posed a security treats. (Jain and Pankanti, 2001)

Ahonen, Hadid and Pietikainen, (2006) said human face is one of the oldest and most basic examples of characteristics that are used for recognition. In some part of the world for that matter tribal marks in the face are the basic examples of a characteristics used for recognition. Since the beginning of civilization, human faces were used to identify individuals.

The limitations of components of biometric systems

Some of the limitations of the components of biometric systems are as follows:

- Noise in sensed data: Noise in sensed data may result from improperly maintained sensor or due to temporal variations being introduced in the biometric data over time. Noisy biometric data may not be successfully matched for genuine user or may be incorrectly matched with the impostors, resulting in decrease in the performance of the system.
- Interoperability issues: Most biometric systems have their basic module designed under the assumption that the biometric data to be compared are obtained using the same sensor and, hence, are constrained in their ability to match or compare biometric data originating from different sensors.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

RESEARCH METHODOLOGY

The methodology examines how the research was structured and conducted. It begins by underlining the research design relevant to the study and giving basis for the choice of that particular research method. It further probes into how data is gathered and analyzed. This serves as a preparation for the data analysis and the conclusions that are drawn in subsequent sections.

Target Population

Data was collected and collated from a population of institutions and organizations who are involved in the use of architectural components that support biometric systems in Ghana; such institutions and organizations are the Ministry of Finance and Economic Planning, the Ministry of Foreign Affairs (Passport office), the Ministry of Interior (Kotoka International Airport), and the Electoral Commission (EC) of Ghana.

Sampling Size

In this research, sample of 100 users of architectural components that support biometric systems in Ghana were selected from four Institutions and Organizations. These users were selected with the Purposive and Convenience sampling methods (non-probability sampling methods that select sample members based on the researcher's judgment of it being typical of what they wants, time and other constraints). However out of the 100 questionnaires that were administered seventy-six (76) were received and used for the analysis.

Data Collection Instruments

Data collection instruments are those tools used by the researcher to collect the necessary information for the analysis of the phenomenon studied and discovering the facts. In this research, the main data collection tool is the questionnaire; a questionnaire is one of the most practical and easiest tools for collecting data out of the population (Neuman, 2007). It should be noted that the questionnaire selected in this research has been of structured closed type in most cases in which the researchers have promoted the respondent to answer one of the five questions prepared based on Likert Scale by designing some special and purposeful questions (including five dimensions in SERVQUAL model) and restricting the options.

One major phase of the survey process is the execution of the survey instrument. The structured questionnaires will be purposively distributed to users of architectural components that support biometric systems in Ghana. For the purpose of this study, only users of the biometric systems for more than a year were given questionnaires to fill from four selected institutions and organisations such as Ministry of Finance and Economic Planning, Ministry of Foreign Affairs (Passport office), Ministry of Interior (Kotoka International Airport), Electoral Commission (EC) of Ghana. When questionnaires are filled, they will then be returned and picked up by the researchers.

Reliability & Validity of the Questionnaire

Reliability or Permanence of a measuring instrument means that similar results will be achieved if a measuring instrument, manufactured for variable measuring, is use in different places or at

ISSN: 2408-7920

African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

different times under similar conditions. In other words, permanent or reliable tools are those tools that can repeatedly be used for measuring similar results. The validity of behavioral research is of utmost importance and is a complicated and challenging subject. Measuring and evaluating specialists consider some specifications for measuring tools, such as the validity of questionnaire. The validity of a measuring tool means that it can measure the relevant specification and not any other variable. Content validity was use for measuring the validity of the questionnaires of this research. For this purpose, the content of the questionnaire has been prepared by referring to scientific texts, theories and the model relevant to the subject and the questions of the research. In view of this, a reliability test was conducted and a Cronbach Alpha value of 0.870 was obtained. This indicated that the items on the questionnaires were good in measuring the objectives of the study.

Data Analysis

In this research, quantitative methodology was use to analyze data using descriptive-inferential statistics and Statistical Package Social Scientists (SPSS) computer software. In using descriptive statistics, the data was analyzed using statistical indexes such as frequency, percentage, average and standard deviation.

RESULTS AND DISCUSSION

The analysis and discussions of the study is based on the study's objectives. It consists of the demographic characteristics of the respondents; the architectural models, systems, other components that support biometrics system and limitations of the architecture.

Architectural Models, Systems, Protocols, Other Components that Support Biometrics System and Limitations of the Architecture

The objective of the study was to investigate the architectural models, systems, protocols and other components that support biometrics system and the limitations associated with them. It should be noted that the respondents were asked to rate the characteristics of the architecture models on a Likert scale of 5 (where 5 = Strongly Significant, 4 = Significant, 3 = Neutral, 2 = Insignificant and 1 = Strongly Insignificant).

Architectural Models of the Biometric System

The study looked at the characteristics of the architecture models of the biometric systems being used in the country and the results of the analyses are presented in Table 1.

Descriptive analysis on the architecture models that support the biometric systems was also conducted and the result is presented in Table 1.

ISSN: 2408-7920

African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

Table 1: Architectural Models' Characteristics

Characteristics	Mean Rate	Std. Deviation	N
Exterior models	4.25	0.502	76
Interior models	4.18	0.623	76
Landscaping design models	3.58	0.849	76
Urban models	3.55	0.776	76
Engineering and construction models	4.15	0.644	76

5 =Strongly Significant; 4 =Significant; 3 =Neutral; 2 =Disagree; 1 =Strongly Disagree
Source: *Field Work, 2017*

Table 1 indicated that the most notably significant characteristics of the architecture models were external, internal looks and engineering and construction models with mean scores of 4.25; 4.18 and 4.15 respectively of the biometric systems.

Architectural Systems of the Biometric System
In assessing the biometric systems, the study also looked at the characteristics of the architectural systems and the findings from the corresponding analyses are presented in Table 2.

Table 2: Architectural Systems' Characteristics

Characteristics	Mean Rate	Std. Deviation	N
Hardware architecture	4.20	0.584	76
Software architecture	4.15	0.732	76
Enterprise Architecture	3.70	0.635	76
Collaborative systems architectures	3.40	0.815	76
Manufacturing systems architectures	3.35	0.855	76
Strategic systems architecture	3.27	0.741	76

5 =Strongly Significant; 4=Significant; 3 =Neutral; 2 =Disagree1 =Strongly Disagree
Source: *Field Work, 2017*

Six characteristics were observed as playing vital roles in Architectural Systems' Characteristics these included hardware design, software design, enterprise architecture, collaborative systems architectures, manufacturing systems architectures and strategic systems architecture. Hardware design, software design, enterprise architecture had mean scores of 4.20; 4.15 and 3.70 respectively. Hardware and software systems that allow their users to collaborate with each other respectively, it can be seen that the respondents indicated that they considered these

ISSN: 2408-7920

African Journal of Applied Research
Vol. 4, No. 2 (2018), pp. 171-179
http://www.ajaronline.com
http://doi.org/10.26437/ajar.04.02.2018.15

characteristics as significant. This suggests that in assessing the biometric systems in Ghana the users mostly consider the hardware, software, enterprise and collaborative systems of the architecture systems.

Limitations of the Biometric System

The study also sought to find out the limitations that are associated with the biometric systems currently being use in the country.

Table 3: Limitations of Biometrics Systems' Characteristics

Characteristics	Mean	Std. Deviation	N
Noise in sensed data	4.28	0.526	76
Inter-class similarities	4.05	0.681	76
Non-universality	3.73	0.820	76
Interoperability issues	3.51	0.645	76
Spoof attacks	3.49	0.913	76
Intra-class variations	3.44	0.930	76

5 =Strongly Significant; 4=Significant; 3 =Neutral; 2 =Disagree1 =Strongly Disagree
Source: *Field Work, 2017*

It can be observed that in assessing the limitations of the biometric system, the noise in sensed data, inter-class similarities, interoperability issues, spoof attacks, intra-class variations and non-universality were the characteristics that were considered significantly with mean scores of 4.28, 4.05,3.73, 3.51, 3.49 and 3.44 respectively.

CONCLUSION

This study was conducted with the main purpose of investigating the components that supports biometrics system in Ghana.

The study found out that the architecture made the system effective; ensured data security; provided accurate data; provided easy and speedy data collection; used both hardware and software; and reduced government's expenditure as the other components of the value chain of the biometric system contributed to the successful data execution through the sensor; matching algorithms and result display. Based on the findings of the analysis the following recommendations were made:

- To avoid noise in sensed data, data controllers should ensure that the sensor is properly maintained
- The introduction of temporal variations of the system minimize since it causes the system from successfully matching for genuine user or be incorrectly matched with the imposters, resulting in decrease in the performance of the system.

REFERENCES

Ahonen, T., Hadid, A., & Pietikainen, M. (2006). Face description with local binary patterns:

Application to face recognition. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, (12), 2037-2041.

Berry, J., & Stoney, D. A. (2001). The history and development of fingerprinting. *Advances in fingerprint Technology*, *2*, 13-52.

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). *Guide to biometrics*. Springer Science & Business Media.

Eriksson, A., and Wretling, P. (1997).How flexible is the human voice? A case study of mimicry.In Proc. of European Conference on Speech Technology, Rhodes, Greece, pp. 1043–1046.

Giesing, I. (2003).Chapter 5: Biometrics. University of Pretoria etd. Unpublished.http://repository.up.ac.za/bitstream/handle/2263/29139/05 chapter5.pdf?sequence=6 [Retrieved 06/04/2017].

Hong, L., and Jain, A. K. (1998).Integrating faces and fingerprints for personal identification: IEEE Trans. *Pattern Anal. Mach. Intell*. 20(12): 1295-1307.

Jackle, H., and Tautz, D. (1998). *U.S. Patent No. 5,766,847*. Washington, DC: U.S. Patent and Trademark Office.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, *43*(2), 90-98.

Jain, A and Pankanti, S. (2001). Biometric systems: Anatomy of performance. IEICE Trans. Fundamentals: Special Issue on Biometrics. E00-A(1): 1-11.

Jain, A. K., Ross, A., and Pankanti, S. (2006). Biometric: A Tool for Information Security, IEEE Trans. *Information Forensics and Security*. 1(2): 125-144.

Jain, K., Ross, A., and Prabhakar, S. (2004). An introduction to biometric recognition, IEEE Trans. Circuits Syst. Video Technology. *Special Issue Image and Video-Based Biomet*. 14(1): 4-20.

Mumuni, M. (2010) Ghana's biometric passport ready. ghanabusinessnews.com [Retrieved 01/03/2017].

Neuman, W. L. (2007). Basics of Social Research: Quantitative and Qualitative Approaches (2nd ed.). Boston: Allyn and Bacon.

Yaqub, R., & McAuley, A. (2011). *U.S. Patent No. 8,060,139*. Washington, DC: U.S. Patent and Trademark Office.

Yinyeh, M. O., and Gbolagade, K. A. (2013). Overview of biometric electronic voting system in Ghana. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(7).

Zhang, D. and Shu, W. (1999).Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching, Pattern Recognition. 32(4): 691-702.

Zhang, D., Wai-Kin Kong, Y. J. and Wong, M. (2003).Online palm print identification. *IEEE* Transactions on Pattern Analysis and Machine Intelligence.25, Issue 9, pp. 1041 – 1050

ISSN: 2408-7920