# Appraising Software Product Quality Models Involving Users Perspective: (A Case Study of Authentication Models)

**Annie O. Egwali, Ph.D.*** **and Winifred R. Sule, M.Sc.**

Department of Computer Science, Faculty of Physical Sciences, University of Benin, PMB 1154, Benin City, Nigeria.

E-mail: annie.egwali@uniben.edu*

## ABSTRACT

The increase in authentication models to secure systems has led to the need to develop quality models for evaluating these authentication models. Past research in software products quality is focused on five different perspectives: product perspective, user perspective, value-based perspective, transcendental perspective, and manufacturing perspective. Generally, the qualities of these software products are required for three types of audience: manager, developer, and user. Nevertheless, most software quality models combine the different points of views and some researchers target more than one type of audience.

This research study is focus on establishing corresponding characteristics of user authentication models (UAMs) and software product quality models. The aim is to propose a framework for measuring the quality of UAMs from users' perspective. The proposed framework is applied in a survey that comparatively evaluates fingerprint biometrics, one-time password, token, username and password, and graphical password models' efficiency from a usability perspective.

Results showed that 21 usability metrics and 24 design metrics are the benchmarks for measuring the usability competence of user authentication models. From the occurrence of the sub-characteristics set for FURPS, ISO 9126-1, Boehm, ISO 8402, ISO 25010 and ISO 9126-11 a total of 25 of the UAMs characteristics and sub-characteristics relating to the SPQMs set were taking into consideration. The WEBUSE quality rating technique realizes the quality level of the six UAMs in terms of 11 characteristic quality factors. The overall quality average merit point ranking shows that graphical password scored 0.81, fingerprint biometrics (0.74), token (0.66), one-time password (0.61), and the username and password model (0.60). In assessing the effectiveness of the evaluation framework designed, the combined quality level results of the WEBUSE analysis and respondents' direct assessment of the selected UAMs rating shows the same similarities. The quality rating for graphical password was 0.83, fingerprint biometrics (0.81), token (0.67), one-time password (0.55) and the username and password model (0.41).

(Keywords: authentication, quality, software product, user, biometrics, software quality, WEBUSE)

## INTRODUCTION

Authentication is the most prevalent approach to securing systems and reducing the impact of sensitive data compromise. Authentication in computer security is the process of attempting to verify the digital identity of the sender of a communication. The protective nature of authenticating technologies is significantly leading many organizations to spend tremendous amounts of money in developing, incorporating and managing new and innovative models. Organizations financing novel authenticating models are considering advancing their horizon to realize the benefits of their investments as there is a constant battle between securing a system and the innovative moves of attackers. However, this would not be possible without an appropriate tool or technique for measuring the quality of these existing authenticating models.

Generally, the quality of a software product is required for the following three different classes of people: managers, developers, and users. Furthermore, the determinants of the quality of a software product are needed for different purposes and thus can be appraised from five different perspectives (Garvin, 1984): product perspective, user perspective, value-based perspective, transcendental perspective, and manufacturing perspective. Although the perceived software product quality can be significantly different from the actual quality, a lot depends on the perception of users who are the key players in the software development and implementation arena. Users generally are divided into different categories on the basis of the tasks required of them in any system. Users may act as system designers, developers, and so on, and they are always at the end of the system chain (Wilson, 2000). The requirements, specifications, design, implementation, and deployment of software products always center on the needs of the users. Therefore it is a prerequisite that software product design should easily be perceived and translated into user demands that still fall within product specifications that are valid from the developer's perspective.

To embrace users' perspective in a software product quality, the software design must begin with users' requirements and end with users' perceptions of a quality solution to satisfy their want. However, for software design, this is a complex issue, because how users perceive a software product before and after use differs. Therefore the drive towards enhanced software product quality must incorporate the need of users. To do this, software developers must address their product quality from users perceived quality perspectives. Past researches submit that consumer perceptions of product quality are generally formed on the basis of an array of extrinsic cues because, most times, consumers cannot use the intrinsic characteristics to judge software product quality easily.

Presently, many authentication models exist. Finding a method which enables users to swiftly and easily evaluate and compare the quality of different authenticating models is a major challenge for users who are the key players for authenticating models usage, and who must play a major role in the search for a measure to evaluate model qualities. There is a dearth of literature in determining important software quality characteristics and sub-characteristics from users' perspective in the domain of assessing the quality of authentication models. Some of the existing software quality models address users view from related or different outlook. Some could not explain how to measure the proposed software quality dimensions. It is always a challenge to justify the characteristics that should be used for a particular software domain as is the case for user authentication models. To address the gap, between what is available and the choices to be made, a user centric and collective authenticating models evaluation technique is essential. Although a high request does not guarantee the quality level of an authentication model as users vary in their particular preferences, but continuous evaluation of the quality of authentication models from the perspective of users in a region of study will assist in the deployment choices by security software developers and agents in an organization.

## Overview of Authentication Models

Authentication in computer security is the most prevalent approach to securing systems and is the process of attempting to verify the digital identity of the sender of a communication. In this context, the sender being authenticated is a user operating a computer. In every connected or standalone system it is the first line of defense against attacks. Presently, many authentication models exist. They are categorized under knowledge-based, token-based, and biometric-based authentication. It can also be classified based on where the user is located (location-based authentication), which can be used to determine if a user is attempting to authenticate from an approved location. This is typically used as a secondary check to identify suspicious login activities. Approved locations may be specific such as a user's office, or more general, such as identifying the city or country of origin. They can also be based on single factor models, two-factor models or multifactor models.

Knowledge-based systems (i.e., something the user knows) includes textual passwords, pass phrases or personal identification numbers (PIN), and graphical passwords. Of all the existing knowledge-based systems, the text-based password involving the use of passwords, personal identification numbers (PINs) and user identification (User IDs) is still the most pervasive used to secure systems. During enrolment, under a password system, a user accessing an agency's electronic application or a system is requested to enter a 'shared secret' such as a password or PIN number along with their User Identity

Graphical passwords are classified into pure recall/reproduce, a drawing-based system; cued recall/repeat, a sequence of actions based systems; and recognition based systems. In pure recall based graphical password models, during enrolment, users choose images or icons or symbols from a large collection or create a graphic password. Then during authentication, users need to reproduce their password without being given any hints or cues (Jermyn, et al. 1999). In cued recall, users have to recall a password, but the system offers a framework of hints, context, and cues, that help the users reproduce their password or help them make the reproduction more accurate (Tao and Adams, 2008; Wiedenbeck, et al. 2005).

In recognition-based systems, during enrolment, a user chooses images or icons or symbols from a large collection; to be authenticated, the users need to recognize and identify the images during the enrollment stage. The decision is binary: either the image is known (recognized) or not known (Weinshall and Kirkpatrick, 2004; Takada and Koike, 2003). Token-based authentication models (i.e. something the user have) includes the use of token devices like smart cards and Automated Teller Machine cards. When a user attempts to login to the secure area, the system first searches for the token device, if the system recognizes the device, the user will be asked for their textual password.

Biometrics system (i.e., something the user is) refers to the automatic identification of a person based on his or her physiological or behavioral characteristics. Generally to authenticate, a user enters an account, username, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user. There are two major categories of biometric technologies according to what they measure: behavioral characteristics and physiological characteristics. In behavioral characteristics, several traits are learned or acquired relating to a person’s behavior (Yang and Fang, 2009) and speech recognition. Physiological characteristics are related to the shape of the body. They include: fingerprint and face thermography.

## Corpus of Authentication Models Usability and Design Characteristics

Several researchers and software technologists have submitted a number of characteristics to evaluate the competencies of existing authentication models based on their usability and design characteristics**.** Cornel de Jong (2008) created an overview of eight characteristics metrics namely, scalability, cost, acceptability, portability, additional hardware, additional software, complexity and login time. Suo, et al. (2005), proposed four measuring metrics, which include usability, memorability, reliability, storage and communication in form of challenge response. Monrose and Reiter (2005) postulated key regeneration (i.e., changeability) and usability.

## Usability Characteristics

According to the International Organization for Standardization (ISO, 2009), the world's largest developer and publisher of International Standards, the usability of an authentication model include several factors and there are only three different ISO methods that describe usability and its features in details: the ISO 9241, ISO 9126 and ISO 13407. According to ISO 9241-11, usability is defined as: *“Extent to which a product can be used by users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”* (ISO, 2009). There are seventeen different parts in this ISO under four categories. Under ‘’Software category’’, parts 10 to 17 deal with software characteristics (ISO, 2009) and part eleven specifically defines the usability from three main components which are: *Effectiveness, Efficiency* and *Satisfaction.* Thus ISO 9241-11 recommends a usability process oriented approach by which the usable interactive system is achieved through a human centered design process. Usability can thus be further broken down into the following eight sub features: *learnability, context of use, ease of use, error management, ease creation, ease execute, and flexibility.*

ISO 9126 addresses software quality from the product point of view. It divides software quality into six general categories which are: functionalities, reliability, usability, effectiveness, maintainability and portability (ISO, 2009). Part three of ISO 9126 defines the usability as: *"A set of characteristics that bear on the effort needed for use and on the individual assessment of such use, by a stated or implied set of users".* The major characteristics consist of *understandability, learnability, operability* and *attractiveness* (ISO, 2009). The ISO 13407 standard focused on human centered design in order to create interactive system development for making systems more usable (ISO, 2009). The application of human factor enhances effectiveness, efficiency and human working condition. In order to achieve this aim, ISO 13407 emphasizes on learnability of user and quality to the system, which provides more productivity for the system for it will be easier to understand and use, thus reducing training and support cost. Thus in the ISO 13407, while usability, effectiveness, efficiency and satisfaction are similar to the definitions given under the ISO 9241-11, it further characterizes: *ease to use and not complicated, ease to create the password, learnability and error correction and design and view mode is acceptable.*

## **Design Characteristics**

In analyzing design and implementation issues of authentication model capabilities, Behzad, et al. (2008), advanced the idea of interface changeability. Onibere and Egwali (2011) posit credentials reusability and decoupling and that authenticating software interface should be randomized to enhance security. *Jain et al, (1999) proposed nine design metrics, which are* performance, acceptability, circumvention resistance, cost-effectiveness, universality, uniqueness, permanence, collectability and distinctiveness. Ratha, et al. (2001), and Onibere and Egwali (2011), suggested conveyable image as a design requirement.

## **Software Product Quality**

Software Product Quality is a subjective concept with different meaning because it has been viewed from different perspectives (Sebastianelli and Tamimi, 2002). Software product quality is not viewed only from a product perspective but also from the production processes and organization, which makes it a yardstick for comparison with similar products available in the market. Specifically, definitions proffered on software product quality from users' perspective embraces quality perceived upon the basis of the user's decision on the overall excellence or superiority of the software product. According to McGraw-Hill (2002) software product quality is the collection of features and characteristics of a software product that contribute to its ability to meet given requirements.

Over the years many software quality models have been proposed. However, each model has a uniqueness that makes it different from the others because of their target purposes. Consequently different researchers and standard bodies have diverse classification of software quality models which are focused on the different software quality views: manager, developer, and user. As posited by Anas (2011), the manager is interested in the overall quality characteristics with a certain level of quality within specific time, limited resources, and limited cost. The developers are mainly required to develop software products within certain level of quality as users' needs and are interested on the internal quality characteristics. The users are mainly interested in the software usage without knowing its internal aspects. Therefore, they considered the reliability and the ability of the software to perform the required functions easily and efficiently in different environments. According to ISO 9126, the main consideration of the users is the software usability, performance, and its effects without knowing what's inside it, how it is work, or how it was developed.

The quality of a software product is also needed for different purposes and thus can be appraised from five different perspectives (Garvin, 1984): product perspective, user perspective, value-based perspective, transcendental perspective and manufacturing perspective. As posited by Boehm, et al. (1976), successful software development requires that all the success-critical stakeholders come to concession, taken into cognizance the context in which it exists. Software product users are not concern with all of software characteristics required to identify the quality of a software product, therefore the focus should be on quality characteristics of software products as needed by users in the market. Most software quality models combine the different points of views and some researchers discusses on the different purposes they are meant for.

This research study focuses on models that address users' needs and perspective. Specifically, classifications of quality models in the user domain are based on: Internal and External Characteristics (e.g., McCall Quality Model, ISO/IEC 9126-1), Internal, External and Quality in Use Characteristics (e.g., ISO 9241-11), Project, Product and Process Metrics (ISO 8402), Definition (e.g., FURPS and ISO/IEC 25010), Assessment (e.g., ISO Standard 14598, Maintainability index and EMISQ) and Prediction

Models (i.e., McCall Quality Model), Decompositional (McCall, et al., 1977 and Boehm, et al., 1976) and Process Quality, Internal Quality, External Quality and Quality In Use (ISO 9126-1).

## RELATED WORKS

Over the years, very few numbers of works have been submitted to evaluate the capabilities of existing authentication models. Cornel de Jong (2008) evaluated the strength of online authentication methods and created an overview of eight characteristics metrics of the authentication methods using values (1 – 5) to point out the individual strengths and weaknesses. Boehm, et al. (1976) first identified and classified a set of characteristics which are important for software. Then they considered a FORTRAN based software and developed candidate metrics for assessing the degree to which the software has the identified and defined characteristics. Boehm, et al. (1976) then went on to investigate the correlation between characteristics and associated metrics with the software quality and also quantifiability, which was done by developing an algorithm. In order to determine if there are overlaps, dependencies, shortcomings etc., the author evaluated each candidate metric with respect to the above mentioned criteria and with respect to its interactions with other metrics.

Chang et al (2008) proposed the directions to evaluate software quality by the use of fuzzy theory and AHP. These authors also based their model upon ISO/IEC 9126 quality model. Onibere and Egwali (2011) carried out a study that focuses on the efficiency of single factor against multifactor authentication models and derived thirty derived characteristic metrics set for authentication models. However the focus was on the efficiency of single factor against multifactor authentication models as it relates to countering identity attacks. Sharma et al. (2008) derived a quality model which was based in ISO/IEC 9126. Their model was from the perspective of Component Based Software Development. The author included track ability, complexity, reusability, and flexibility as new sub dimensions in their model. Chang, et al. (2008) proposed the directions to evaluate software quality by the use of fuzzy theory and AHP. These authors also based their model upon ISO/IEC 9126 quality model. Instead of taking a conventional way of weighing the values either by survey or interviews, the authors used fuzzy theory to get relative weights of characteristics and sub characteristics. Alvaro, et al. (2005) investigated a Software Component Certification framework with the aim of acquiring quality in software components.

## MATERIALS AND METHODS

The intention of the study is four-fold: first, to establish the corresponding characteristics of UAMs and SPQMs that can be used as a framework to measure the quality of UAMs from users' perspective. Secondly, to propose a framework that correspond the characteristics of UAMs and SPQMs from users' perspective. Thirdly, to apply the proposed framework in a survey that comparatively evaluates fingerprint biometrics, one-time password, token, username and password and graphical password models from a usability perspective and fourthly, to establish the quality rating of the selected UAMs in satisfying the needs of users from a users' perspective.

The selected UAMs characteristics and sub-characteristics are applied in a survey design that used instrument of questionnaires. The questionnaire was developed and administered to solicit information from respondents. It was randomly distributed to current students, lecturer and staffers of some organizations in Nigeria who actively engaged in the use of the computer system. The participants were assured of confidentiality the information provided that will be used exclusively for research purpose. The questionnaires were randomly distributed to current students, lecturer and staffers of some organizations in Nigeria who actively engaged in the use of the computer system. Respondents were requested to tick the right response and add additional comments where necessary, which best describe their assertions.

The research instrument was administered between September and November 2016 and were distributed to 250 individuals, however a sample size of 209 (84%) complete responses were used for data analysis. The research instrument was divided into three sections: (1) participants bio-data, (2) the most frequently used authentication model (3) the preferred authentication model. The first section, determine the profile of participants comprise participant's organization, designation, area of expertise, gender, age, qualifications and program of studies. The second section examines the frequently, usage pattern of respondents, the period and circumstance of usage, if the model used needs additional software or hardware and the systems' requirement. Also included are several questions to ascertain the different usability characteristics observed during usage. The second section includes seven-point Likert scales, ranging from ''Strongly Disagree" (1) to ''Strongly Agree" (5). Different levels of disagreement or agreement were established using 33 items adopted and adapted from previous related literatures (Chang et al., 2008). The third section determines the preferred authentication model and several questions to determine the in-built interface characteristics and usability characteristic observed that affected users' assessments of quality rating decisions.

Respondents profile was analyzed using percentages. To establishing the corresponding characteristics of UAMs and SPQMs that can be used as a framework to measure the quality of UAMs from users' perspective, a review of existing literature were used to establish what actually constitute the complete usability and design characteristic of UAMs, the corpus of SPQMs characteristic that should act as a benchmark for measurement from users perspective and to propose a framework that correspond the characteristics of UAMs and SPQMs from users' perspective. Since the case study is on authentication models, the focus is on the UAMs characteristic set. Some characteristics were eliminated from SPQMs and UAMs because they were not related, others were concealed as is the case with 'Machine Independence', 'Software Independence' and 'Transferability' because they are all embedded inside 'Portability' as defined in UAMs. Yet others were expanded as is the case of 'Simplicity' in SPQMs which is best defined and subdivided into 'Easy to create' and 'Ease of Execution' in UAMs to enable their measurement.

The quality characteristics and sub-characteristics in the proposed framework were applied in a survey conducted on fingerprint biometrics, one-time password, token, username and password and graphical password models to test the designed evaluation framework and analyze the quality of the selected UAMs. A usability quality analysis technique called WEBUSE (Chiew and Salim, 2003) was used to analyze the quality of the selected UAMs. The method was basically designed to evaluate the usability of websites by means of questionnaire (Chiew and Salim, 2003). However, literature research shows that it has been utilized for the evaluation of communication protocols systems, e- learning applications and web portals (Thiam and Siti, 2003). WEBUSE makes use of a five Likert scale items format ranging from ''Strongly Disagree" (1) to ''Strongly Agree" (5). In this rating techniques, questions are first categorizes based on the quality factors they address; a category indicates a characteristic. Then merit values are assigned to participants responses in the following format: 'Strongly Agree= 1.00', 'Agree = 0.75', 'Neutral = 0.50', 'Disagree = 0.25' and 'Strongly Disagree = 0.00'.

Steps for WEBUSE usability evaluation are as follows:

(i). Respondents answers the usability evaluation questionnaire on software products

(ii). Respondents responses are evaluated

(iii). Merit based on the answers of the respondents for each question are generated, and then accumulated for each category of usability

(iv). Points usability category is the mean value of each sub-characteristic

(v). Point usability of the software product is the mean value of each characteristic

(vi). Level usability point is determined based on usability

The total merit value for each characteristic denoted as x is represented as Equation (1):

$$x = \sum_{i=1} \frac{(\text{Merit point of each question of a Characteristic})}{(\text{Total number of questions for the Characteristic})} \quad (1)$$

Finally, to calculate the overall quality of the software product, the mean average of the characteristics is calculated as follows (see Equation 2):

$$Y = \sum_{i=1}^{n} \frac{x_i}{n} (2)$$

Where, Y is the mean average of the overall quality of the software product, *x* is the average merit point of a characteristic, and n is the total number of items in the questionnaire. The values of the merit points of the characteristics range between 0 and 1, which are divided into five categories to indicate five different levels of quality (bad, poor, moderate, good and excellent) as shown in Table 1. The quality merit points establish the quality levels of the software product. In this research, the technique enables the evaluation of the UAMs usage. The quality levels of characteristics of the case study UAMs were determined based on the above quality points and quality levels of the WEBUSE method.

**Table 1:** Quality Points and Levels.

| Characteristic Average Merit Point | Quality Level |
|---|---|
| 0 ≤x < 0.2 | Bad |
| 0.2 ≤x < 0.4 | Poor |
| 0.4 ≤x < 0.6 | Moderate |
| 0.6 ≤x < 0.8 | Good |
| 0.8 ≤x < 1.0 | Excellent |

Section one of the survey questionnaire captured the bio-data of respondents. Out of the 209 respondents, 97 (46%) were males and 112 (54%) were females. A summary of respondents' bio-data is presented in Table 2.

## Usability and Design Characteristics for Authentication Models

Twenty-one usability characteristics isolated from literature were defined from the end users' perspective. Each characteristic had one question designed from it and participants were required to answer each question in relation to selected UAMs. Similarly, twenty-four benchmarks for measuring the design propensity of user authentication models are defined from the end users' perspective with definition gotten from literature.

Each characteristic had one question designed from it and participants were required to answer each question in relation to selected UAMs. The following are the characteristics definitions:

## SPQMs Characteristic from Users Perspective

Determining the characteristics for usability evaluations of SPQMs from users' perspective from literature and ISO documentation was not an easy endeavor. Some SPQMs like McCall Quality Model (McCall et al, 1977) do not provide a means for measurement and lack important characteristics like the functionality of software product, it was omitted.

**Table 2:** Summary of Bio-Data of Respondents.

| Measure | | No. of Respondents | Percentage (%) |
|---|---|---|---|
| **Gender** | Male | 97 | 46 |
| | Female | 112 | 54 |
| **Age** | Less than 25 | 47 | 23 |
| | 26 – 40 | 71 | 34 |
| | 41 – 55 | 63 | 30 |
| | 56 and above | 28 | 13 |
| **Qualification** | Diploma | 53 | 25 |
| | First Degree | 66 | 31 |
| | Postgraduates | 43 | 21 |
| | Masters | 39 | 19 |
| | Ph.D. | 08 | 04 |
| **Fields of Study** | Engineering | 31 | 15 |
| | Computer Science | 66 | 32 |
| | Mathematics | 12 | 06 |
| | Medicine | 07 | 03 |
| | Business Admin. | 47 | 22 |
| | Public Admin. | 25 | 12 |
| | Accountancy | 21 | 10 |

ISO/IEC 14598 describes a process for evaluating software product quality which is consistent with ISO 9241-11 and ISO 9126-1, therefore ISO 9126-1was used instead. EMISQ defines a methodology for assessing the “internal” software product quality characteristics and although it clearly takes into account the knowledge of a user, it is based on the ISO standard 14598, consequently EMISQ was omitted.

Some of these SPQMs address users view from related or different outlook. Therefore one of the criteria for comparative usability evaluations is based on the SPQMs themselves. This research work evaluates the following six SPQMs from literature that specifically discusses software product quality from user perspective: FURPS, ISO 9126-1, Boehm, ISO 8402, ISO 25010 and ISO 9126-11. Even these six SPQMs that incorporate users’ perspective of assessing software product qualities varies based on their characteristics and sub-characteristics and usage for different software product. For instance, a comparison of ISO 25010 and ISO 9126-1 discloses the following:

(i) Some SPQMs with similar characteristics have different sub-characteristics. For example, *functionality* in ISO 25010 has appropriateness and accuracy as its sub-characteristics. But *functionality* in ISO 9126-1 has suitability, accuracy, interoperability and security.

(ii) A range of SPQMs could not define how to measure the proposed software quality characteristics and sub-characteristics. For example Boehm et al. (1976) proposed SPQMs based on the users’ needs but did not give any suggestions about measuring the software quality characteristics. This is also evident in ISO 9126-1*security* and *safety* characteristics.

(iii) Several characteristics are completely absent from some models. For instance *flexibility in use* is absent from ISO 9126-1.

(iv) Some SPQMs have similar characteristics, but the defined sub-characteristics are not comprehensive enough. For example, *reliability* in ISO 25010 has availability which was equated with maturity in ISO 25010. However, while maturity is related to fault tolerance, availability is more important than maturity and has a completely different meaning.

(v) Some SPQMs have different names for similar sub-characteristics with the same concept. For instance *ease of use* in ISO 25010 and *operability* in ISO 9126-1.

The level of occurrence of the sub-characteristics set for FURPS, ISO 9126-1, Boehm, ISO 8402, ISO 25010 and ISO 9126-11 were further derived.

## Proposed Framework that Corresponds the Characteristics of UAMs to SPQMs from Users’ Perspective

Only a total of 25 of the UAMs characteristics and sub-characteristics relating to the SPQMs set are taking into consideration. Characteristics were not meant for respondents in this research circumstance. For example, *testability* is common but omitted since it’s exclusively meant for the internal assessor in this circumstances and not for respondents. Non-Repudiation is a characteristic analyze by the internal assessor who in most cases is the system’s administrator. Some characteristics have similar names but different concept. For example reusability is evident in SPQMs and UAMs, but in each case they define different quality concept. Therefore, the 25 UAMs characteristics and sub-characteristics relating to the SPQMs set are finally reduced to 11 characteristics with 31 items.

## Reliability of Item Scores of the Proposed Framework

The Cronbach alpha (α) coefficient of the 31 items is 0.889, which satisfies the validated accepted threshold level value of 0.70. This means that there is good consistency between the questions.

## Application of WEBUSE Analysis Technique

To comparatively evaluate some selected UAMs (e.g., fingerprint biometrics, one-time password, token, username and password and graphical password) capability from a usability perspective, the WEBUSE rating technique is employed.

**Table 3:** Final Quality Merit and Quality Level of Five User Authentication Models.

| S/N | UAMs Characteristics | FB Value | | OTP Value | | T Value | | UP Value | | GP Value | | Quality Level of Quality Characteristics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | Performance | 0.71 | Good | 0.74 | Good | 0.75 | Good | 0.74 | Good | 0.72 | Good | **0.70 - Good** |
| 2. | Scalability | 0.81 | Excellent | 0.19 | Bad | 0.14 | Bad | 0.64 | Excellent | 0.82 | Excellent | **0.52 -Moderate** |
| 3. | Satisfaction | 0.66 | Good | 0.55 | Moderate | 0.57 | Moderate | 0.61 | Good | 0.82 | Excellent | **0.64- Good** |
| 4. | Reliability | 0.79 | Good | 0.67 | Good | 0.76 | Good | 0.72 | Good | 0.81 | Excellent | **0.75- Good** |
| 5. | Maintainability | 0.74 | Good | 0.15 | Bad | 0.55 | Moderate | 0.51 | Excellent | 0.86 | Excellent | **0.56 - Moderate** |
| 6. | Understandability | 0.71 | Good | 0.79 | Good | 0.77 | Good | 0.64 | Good | 0.85 | Excellent | **0.75- Good** |
| 7. | Portability | 0.76 | Good | 0.69 | Good | 0.67 | Good | 0.79 | Good | 0.77 | Good | **0.74- Good** |
| 8. | Efficiency | 0.75 | Good | 0.66 | Good | 0.64 | Good | 0.66 | Good | 0.78 | Good | **0.70- Good** |
| 9. | Harmless | 0.61 | Good | 0.69 | Good | 0.87 | Excellent | 0.45 | Moderate | 0.88 | Excellent | **0.62- Good** |
| 10. | Acceptability | 0.71 | Good | 0.77 | Good | 0.75 | Good | 0.44 | Excellent | 0.81 | Excellent | **0.70- Good** |
| 11. | Compliance | 0.85 | Excellent | 0.79 | Good | 0.77 | Good | 0.41 | Good | 0.79 | Good | **0.72- Good** |
| | **SUM** | **8.10** | | **6.69** | | **7.24** | | **6.61** | | **8.91** | | |
| | **AVERAGE** | **0.74** | **Good** | **0.61** | **Good** | **0.66** | **Good** | **0.60** | **Good** | **0.81** | **Excellent** | |

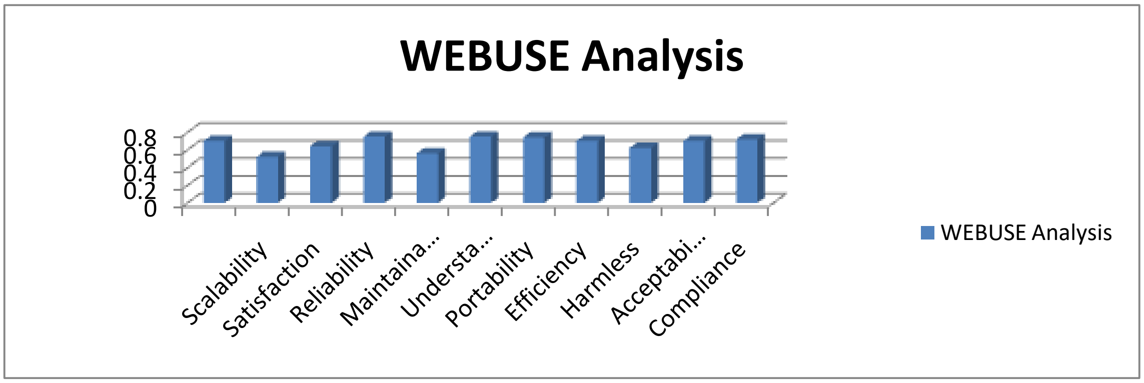

**Figure 1:** Quality Merit Points for each Characteristic.

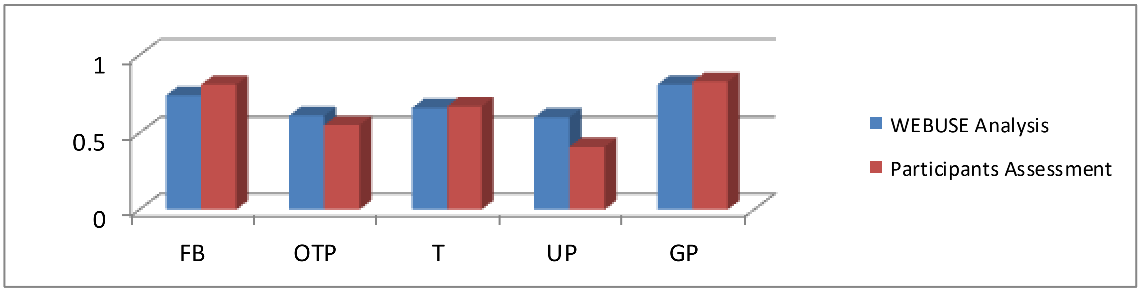

**Figure 2:** WEBUSE Analysis vs Participants Direct Question Assessment.

For the purpose of analysis, questions were classified according to characteristics in order to access the quality level of each UAMs according to the characteristics. It was therefore possible to realize the quality level of the five UAMs in terms of 11 characteristic quality factors.

The final quality merit and quality level of the five user authentication models is shown in Table 3. The result for scalability showed excellent quality for fingerprint biometric models and graphical password models, but bad for one time password and token.

The result for satisfaction showed excellent quality for graphical password models, good for username and password and fingerprint biometric but moderate for the other models.

The quality merit points for each characteristic are shown in figure 1.The overall quality average merit point ranking shows that graphical password scored 0.81, fingerprint biometrics (0.74), token (0.66), one-time password (0.61), and the username and password model (0.60).

## Assessing the Effectiveness of the Evaluation Framework

To assess the effectiveness of the evaluation framework designed, the results of the WEBUSE analysis were then compared to the responses of respondents in answering one of the questions that required a direct assessment of the quality rating of the selected UAMs. Results of participants response is shown in Table 4.

**Table 4:** Participants Direct Quality Rating.

| UAMs Quality | Quality Rating | Quality Level |
|---|---|---|
| Fingerprint Biometrics | 0.81 | Excellent |
| One-Time Password | 0.55 | Good |
| Token | 0.67 | Good |
| Username And Password | 0.41 | Moderate |
| Graphical Password | 0.83 | Excellent |

The combined quality level results of the WEBUSE analysis and respondents' direct assessment of the selected UAMs rating shows the same similarities as shown in figure 2.The quality rating for graphical password was 0.83, fingerprint biometrics (0.81), token (0.67), one-time password (0.55) and the username and password model (0.41).

## CONCLUSION

An authentication model usability evaluation system provides a framework for measuring the quality of existing and incoming UAMs from users' perspective. The study further shows that WEBUSE method based on 23 isolated characteristics and sub-characteristics of usability classified into 11characteristic quality factors, can generate usability rating points and overall quality rating for existing authentication models. the WEBUSE analysis and respondents' direct assessment of the selected UAMs rating shows the same similar results which justifies the effectiveness of the evaluation framework designed.

The proposed evaluation framework focuses on only the users' perspective. In designing any authentication model using the approach presented in this work, it will be impossible to satisfy all characteristics requirements. Therefore, it is worthwhile to carry out a similar study on different group of users since research in software products quality is focused on five different perspectives: product perspective, user perspective, value-based perspective, transcendental perspective and manufacturing perspective. Identifying major characteristics and sub-characteristics for the quality of the authentication model been measured is vital.

## REFERENCES

1. Alvaro, A., A. Aleida, and S. Meira. 2005. "Quality Attributes for a Component Quality Model". *Proceedings of 10th WCOP/19th ECCOP*. Glasgow, Scotland.

2. Anas, B.A. 2011. "Software Quality Evaluation: User's View". *International Journal of Applied Mathematics and Informatics*. 3(5).

3. Behzad, M., O. Mauricio, and E. Abdulmotaleb. 2008. "Novel Shoulder-Surfing Resistant Haptic-based Graphical Password". Available at: http://lsc.univ-evry.fr/~eurohaptics/upload/cd/papers/f119.pdf.

4. Blonder, G.E. 1996. "Graphical Passwords". Lucent Technologies, Inc.: Murray Hill, NJ. Patent 5559961. Available at: http://www.usenix.org/events/upsec08/tech/full_papers/chiasson/chiasson_html/#Blonder

5. Boehm, B.W. 1984. "Software Engineering Economics". *IEEE Trans. Softw. Eng.* 1:4–21.

6. Boehm, B., J. Brown, and M. Lipow. 1976. "Quantitative Evaluation of Software Quality". *Proceedings of ICSE '76 2nd International Conference on Software Engineering*. 592-605.

7. Chang, C., C, Wu, and H. Lin. 2008. "Integrating Fuzzy Theory and Hierarchy Concepts to Evaluate Software Quality". *Proceedings of Software Quality Control*. 16(2):263-276.

8. Chiew, T. and S. Salim. 2003. "Web Use: Website Usability Evaluation Tool". *Malaysian Journal of Computer Science*. 16:47-57.

9. Cornel de, J. 2008. “Online Authentication Methods. Evaluate the Strength of Online Authentication Methods”. Available at: http://www.usenix.org/events/upsec08/tech/full_papers.html.

10. Elftmann, P. 2006. “Secure Alternatives to Password-based Authentication Mechanisms”. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.94.1803.

11. FURPS Model. 1999. “FURPS Model”. Available at: http://en.wikipedia.org/wiki/FURPS.

12. Garvin, D.A. 1984. “What Does Product Quality Really Mean”. *Sloan Manage. Rev*. 26(1):25–43.

13. Hajjat, M.M. and F. Hajjat. 2014.”The Effect of Product Quality on Business Performance in Some Arab Companies”. *Journal of Emerging Trends in Economics and Management Sciences (JETEMS)*. 5(5):498-508.

14. ISO. 1999. *ISO/IEC 14598-1: Information Technology - Software Product Evaluation - Part 1-General Overview*. International Organization for Standardization: Geneva, Switzerland.

15. Jain, A., R. Bolle, and S. Pankanti. 1999. “Introduction to Biometrics”. In: Jain, A.K., et al. (eds.). *Biometrics: Personal Identification in Networked Society*. Boston/Dortrecht/London. 1-41.

16. Jermyn, I., A. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin. 1999. “The Design and Analysis of Graphical Passwords”. *Proc. 8th Usenix Security Symp*. Washington, DC.1–14.

17. McCall, J.A., P.K. Richards, and G.F. Walters. 1977. *Factors in Software Quality, Vols I, II, III*. US Rome Air Development Center Reports NTIS AD/A-049 014, 015, 055, 1977.

18. McGraw-Hill, Inc. 2002. “Product Quality”. *McGraw-Hill Concise Encyclopedia of Engineering*. McGraw-Hill Companies, Inc.: New York, NY.

19. Monrose, F. and M. Reiter. 2005. “Graphical Passwords”. In: *Security and Usability: Designing Secure Systems That People Can Use*. L. Cranor and S. Garfinkel (eds). O’Reilly Media: Sebastopol, CA .157–174.

20. Onibere, E.A. and A.O. Egwali. 2011. “Enhancing Authentication Models Characteristic Metrics via Probability Modelling”. *Journal of the Nigerian Association of Mathematical Physics*. Indexed in AJOL.18, 395 – 400.

21. Ratha, N., J. Connell, and R. Bolle. 2001. “Enhancing Security and Privacy in Biometrics-Based Authentication Systems”. *IBM Systems Journal*. 40(3): 614– 634.

22. Scheuermann, D.M., S. Schwiderski-Grosche, and B. Struif. 2002. “Usability of Bometrics in Relation to Electronic Signature”. EU-Study 502533/8, Darmstadt, Germany. http://www.sit.fraunhofer.de/english/SICA/sica_projects/project_pdfs/eubiosig.pdf.

23. Sebastianelli, R. and N. Tamimi. 2002. "How Product Quality Dimensions Relate to Defining Quality". *The International Journal of Quality and Reliability Management*. 19(4):442-453.

24. Sharma, A., K. Rajesh, and P. Grover. 2008. “Estimation of Quality for Software Components: An Empirical Approach”. *Proceedings of ACM, SIGSOFT Software Engineering Notes*. 33(6):1-10. New York, NY.

25. Suo, X., Y. Zhu, and G.S. Owen. 2005. “Graphical Passwords: A survey”. 21st Annual Computer Security Applications Conference (ACSAC'05). 463-472.

26. Takada, T. and H. Koike. 2003. "Awase-E: Image-Based Authentication for Mobile Phones using User’s Favorite Images", *Human-Computer Interaction with Mobile Devices and Services*. 2795:347 – 351. Springer-Verlag GmbH.

27. Tao, H. and C. Adams. 2008. “Pass-Go: A Proposal to Improve the Usability of Graphical Passwords”. *International Journal of Network Security*. 7(2):273–292.

28. Thiam, K.C. and S.S. Siti. 2003. “WEBUSE: Website Usability Evaluation Tool”. *Malaysian Journal of Computer Science*. 16(1):47-57.

29. Weinshall, D. and S. Kirkpatrick. 2004. “Passwords You’ll Never Forget, but Can’t Recall”. *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. ACM: Vienna, Austria. 1399-1402.

30. Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. 2005. “PassPoints: Design and Longitudinal Evaluation of a Graphical Password System”. *International Journal of Human-Computer Studies*. 63:102-127.

31. Wilson, T.D. 2000. “Recent Trends in User Studies: Action Research and Qualitative Methods”. *Information Research*. 5(3):1 -20.

32. Yang, W. and F. Fang. 2009. “Application of a Dynamic Identity Authentication Model Based on an Improved Keystroke Rhythm”. *Int'l J. of Communications, Network and System Sciences*. 2 (8):714-719. Available at: http://www.scirp.org/journal/ijcns.

## ABOUT THE AUTHORS

**Annie Egwali** is an Associate Professor in the Department of Computer Science, at the Faculty of Physical Sciences, University of Benin. Benin City. Nigeria. She holds a Ph.D. degree in Software Engineering from the University of Benin. She is a member of the Nigeria Computer Society (NCS), Institute of Electrical and Electronics Engineers (IEEE), International Network for Women Engineers and Scientists (INWES), Third World Organizations of Women Scientists (TWOWS), National Association for the Advancement of Knowledge (NAFAK), and Nigerian Association of Educationists for National Development (NAEND). Her areas of interest include information technology, software engineering, E-commerce, fuzzy systems, software, and network security. To date, she has supervised several undergraduate and postgraduate students.

**Winifred Sule,** holds an M.Sc. in the Department of Computer Science, at the Faculty of Physical Sciences, University of Benin. Benin City, Nigeria. Her research interests are in the areas of information technology, software engineering, e-commerce, and software security.

## SUGGESTED CITATION

Egwali, A.O. and W.R. Sule. 2018. “Appraising Software Product Quality Models Involving Users Perspective: (A Case Study of Authentication Models)”. *Pacific Journal of Science and Technology*. 19(2):74-85.

Pacific Journal of Science and Technology