An Integrated Success Model for Adopting Biometric Authentication Technique for District Health Information Management System 2, Ghana

Lazarus Kwao
Ghana Baptist University College, Kumasi

Richard Millham
Durban University of Technology, South Africa

Enoch Opanin Gyamfi
University of Electronic Science and Technology of China

ABSTRACT
This paper evaluated users' perspective of adopting a biometric authentication technique by utilizing a proposed model derived from the technology acceptance model to determine how effective user accepts a proposed keystroke biometric authentication in an E-Health System. This paper combined the TAM of Davis et al with the success adoption model of DeLone and McLean where external variables for the TAM of Davis et al were derived from the four dimensions considered in the model of DM. The research design is a self-administered survey and the empirical part of the research is quantitative. The aim of the empirical part is to test the fit of the conceptual model with received data based on a questionnaire. This paper uses a cross-sectional approach that provides a "snapshot" of the secured system's usefulness and ease-of-use from the perspective of the end-users. Based on empirical findings, users with a higher degree of perceived usefulness, privacy concerns, and security concerns will demonstrate a more positive attitude towards adopting keystroke biometric authentication in an e-Health System. The proposed model and its elements prove that it can be a useful tool for decision makers in evaluating authentication techniques in e-health systems.

Keywords
DHIMS 2, Technology Acceptance, Delone and McLean, Keystroke Biometrics Authentication, Ghana e-Health Service

1. INTRODUCTION
In authentication field, the application of biometric technologies is increasingly apparent (1; 2). Practical evidence shows that augmented interest in these technologies is fueled by anticipating a decrease of technology costs, improved technical quality of the systems and socio-political pressures for better security-related controls (3). Nevertheless, an important issue stemming the deployment of biometrics or leading to their underutilization is user resistance to utilize such pervasive technology (4). Most users feel fearful, hesitant, or uncomfortable around these systems, especially because they perceive them as a means for potential infringements into their privacy (5). Such users' feelings and perceptions increase the risk of rejection and can lead to biometrics implementation failure. The need to inform biometric technologies implementation with various factors affecting biometrics acceptance is, therefore, of crucial importance (6).

2. PROBLEM STATEMENT
The Ghana government aims to provide equitable and adorable health care at the highest delectable standard for all its citizens. Several initiatives have been rolled out in line with Ghana's vision for a good, equitable, affordable and robust healthcare at the highest achievable standard in the health sector. One of these initiatives is E-Health where the Ministry of Health (MoH)'s vision is to develop an efficient, accessible, equitable, secure and end-user-friendly health care services enabled by ICT (7). The E-Health strategy identified, the District Health Information Management System 2 (DHIMS2) as the foremost priority in its endeavor to improve health service delivery (8; 9; 10). Ghana has since April 2012, used DHIMS2 nationwide with a full online deployment led by the Ghana Health Service. However, there is a plethora of authentication challenges.

Ghana Health Service (GHS) controls who accesses District Health Information Management System 2 (DHIMS2) data and what they can see and do. Once you set up a user, only trusted Data Center operational staff access GHS data. DHIMS2 offer multiple permission levels that let us limit the access privileges of each user. Districts data travels between a user's computer and GHS server, and it is encrypted by a technology called Secure Sockets Layer (SSL) using 128-bit encryption. This is the same technology used by banks and offers the highest level of encryption currently supported by commercial Web browsers. DHIMS2 uses advanced, industry-recognized safeguards and procedures, such as password-protected login, with encryption technology and firewall-protected servers as its primary user authentication method (11). However, in recent years the ability for passwords to provide confident and secure authentication has been wearing, due to reasons such as the wrongful use of a password that can be easily guessed and comprised by social engineering attack, and increase intrusion attacks (12; 13). According to Pinkas & Sander, (14), Wang & Wang, (15), a simple password is a primary choice when it comes to password selection, such as date of birth, nickname, initials, and regular dictionary words. Users always tend to use the same or similar password for multiple systems (16; 17). So, if a hacker gains access to a person's account via a data breach, all the other accounts of that person can become vulnerable due to the stolen credentials. That problem is multiplied typically because hackers are not only accessing one person's account, but hundreds or thousands at a time (18; 19; 20). Use of strong passwords (mixed case, min length, characters and symbols) that is changed frequently causes people to forget their password or write them down, defeating their purpose. Cost-effectiveness and simple implementation have been the forefront reasons for the continued dominance of password authentication.

This paper uses an integrated success model to investigate the security dimensions for adopting keystroke biometrics for

enhanced authentication in E-health systems (DHIMS2). The study thus examines how users conceptualized the keystroke biometric authentication and if it will be accepted and further used.

3. LITERATURE REVIEW

To date, only a few authors have discussed biometric systems from an end-user acceptance perspective (21). Yet, the perception and behavioral response of end users is an important consideration when designing systems that employ digital identities (22) as issues of privacy, security and online identity management are frequently a source of concern to end-users (23). A study aiming to identify relevant non-technical issues such as the perceptions of future end-users' fears and anticipations is likely to be a prerequisite for the development of a strategy to support the acceptance of such a pervasive innovation. Biometrics have often been associated in the popular press at least - and in the public consciousness Ng-Kruelle et al. (24) argue - with the encroachment of state control through technologies. This study will therefore address the following research question: What are the key determinants of end-user acceptance (or reject) of disruptive IT like biometric systems in healthcare environments? What appropriate model influences the adoption of the proposed authentication technique in E-Health Systems?

Although isolated impacts of technical, social, and risk factors on intention to accept technology have been well documented within existing technology acceptance models, a more comprehensive understanding regarding the various factors explaining technology acceptance, is needed. This isolated approach limits the ample view of different factors that organizations trying to succeed with technology implementation have to carefully address in order for the target users to accept the technology under investigation. To address this gap, we explored how an interplay of previously identified factors from existing IT/IS acceptance models and theories adds to the richness of explaining biometric technology acceptance among end-users of an E-Health system.

Our contribution to the technology acceptance literature is. Firstly, our results highlight the relative importance of diverse drivers and individual, technical, social, and risk determinants in explaining the intention to accept biometric technologies. To date, rather limited attention has been paid to technology-specific antecedents that may provide significantly stronger guidance for the successful design and implementation of specific types of systems. Therefore, in addition to classical antecedents to technology acceptance, we incorporate particular factors linked with the specificities of biometric systems. Developing a theory that is more focused and context specific – here, technology specific – is considered an important frontier for advances in IS research (25; 26). Such comprehensive and focused model appears to be more explanatory compared to a general model that attempts to address many classes of technologies (26) and should also provide designers with levers to augment adoption.

Secondly, we identify that through integration of different technology acceptance models, and some other theories we are able to provide a better picture of technology acceptance antecedents and their relationships. As such, privacy concerns are an important consideration in successful biometric implementation and uptake amongst citizens (5). Although the issue of privacy has emerged as a major inhibitor of biometrics (5), however, the research on this issue is quite rare to date, especially from the viewpoint of customers. A model that integrates knowledge from technology adoption and privacy research and which encompasses both privacy and trust as components central to effective acceptance (5) is clearly lacking, a gap that this paper seeks to address. In doing so, we answer the call from Venkatesh et al. (27) to integrate the technology adoption stream with another dominant research stream, which in turn will move us toward a more cumulative and expansive nomological network (26).

In the next section we develop the conceptual research model and then outline the sources of data and our data analysis procedure. This is followed by a description of the role of the different factors explaining the intention to accept biometrics. We then discuss the theoretical contributions and managerial implications of our findings. The paper concludes with avenues for future research.

4. MODEL DEVELOPMENT

4.1 The Biometric Identification Systems

Keystroke Biometric analysis also called typing rhythms, is described as a novel behavioural biometric approach (28; 29). This technique observes the typing patterns of an individual on a terminal by capturing the keystroke timings. The advantages associated with keystroke analysis consist of interruption from regular computer activities because the user would be inputting keystrokes when given a password to the system. Keystroke analysis makes use an existing device, thus the computer keyboard, therefore adopting this technology incur a reduced cost as compared to other biometric techniques that deploy expensive devices (30; 31). The major advantages for deploying keystroke dynamics in systems are that keystroke dynamics is not invasive, because the input device required is the keyboard of the computer, keystroke dynamics is inexpensive to deploy and install, and finally, keystroke patterns of an individual cannot be easily replicated or stolen by an imposter.

There is an abundance of research regarding technology acceptance from a variety of viewpoints such as new software, mobile commerce, electronic commerce, ubiquitous computing and others. Despite an extensive search, only few articles were found that extended the Technology Acceptance Model (TAM) into the realm of the intention to use keystroke biometric authentication techniques (James et al. 2006). The website of the International Biometrics Group (IBG) lists a plethora of such articles that examine the security implications of biometrics, in the society, public policy, and national security systems but a very few on the end-user acceptability of keystroke biometrics (source). This means that there is a coinciding lack of keystroke biometric-specific constructs and health-associated validated research instruments. As a result, the only recourse available is to identify very closely related constructs and measures within the realm of health sectors and adapt them as necessary being ever vigilant to ensure that the instruments do, in fact, measure the underlying construct. As with all research, this will be an iterative and lengthy process as measurement instruments are continually fine-tuned, keystroke biometric-specific research becomes more robust, and more parsimonious models are developed.

4.2 Theoretical Frameworks of Technology Acceptance

Technology acceptance model are mostly adapted by most systems users to evaluate the performance of the systems they use. The technology acceptance model provides a quick, reliable tool for measuring the adoption and usability (32). It allows a system user to evaluate a wide variety of products and services, including hardware, software, mobile devices, websites and applications that are technologically based. Technology acceptance model has become an industry standard, with references in over 4381 articles and publications (33). The noted benefits of using the technology acceptance model is that is a very easy scale to administer to participants, it can be used on small sample sizes with reliable results, and it is valid as it can effectively differentiate between usable, unusable acceptable or unacceptable systems. Therefore, this study as evaluated in users' perspective is performed by utilizing a proposed model derived from the technology acceptance model to determine how effective user will adopt the proposed keystroke biometric authentication in the DHIMS 2.

Technology Acceptance Model (TAM)

Building upon the Theory of Reasoned Action (TRA) and Theory of Planned Behaviour (TPB) models, the Technology Acceptance Model, depicted in Figure 1, was developed (34). While TRA and TPB are generic and therefore support cross-disciplinary application, TAM is specifically focused on examining behavioural intention to use information systems. TAM replaces many of TRAs attitude measures with the two technology acceptance measures, perceived ease of use, and perceived usefulness as illustrated in Figure 1.

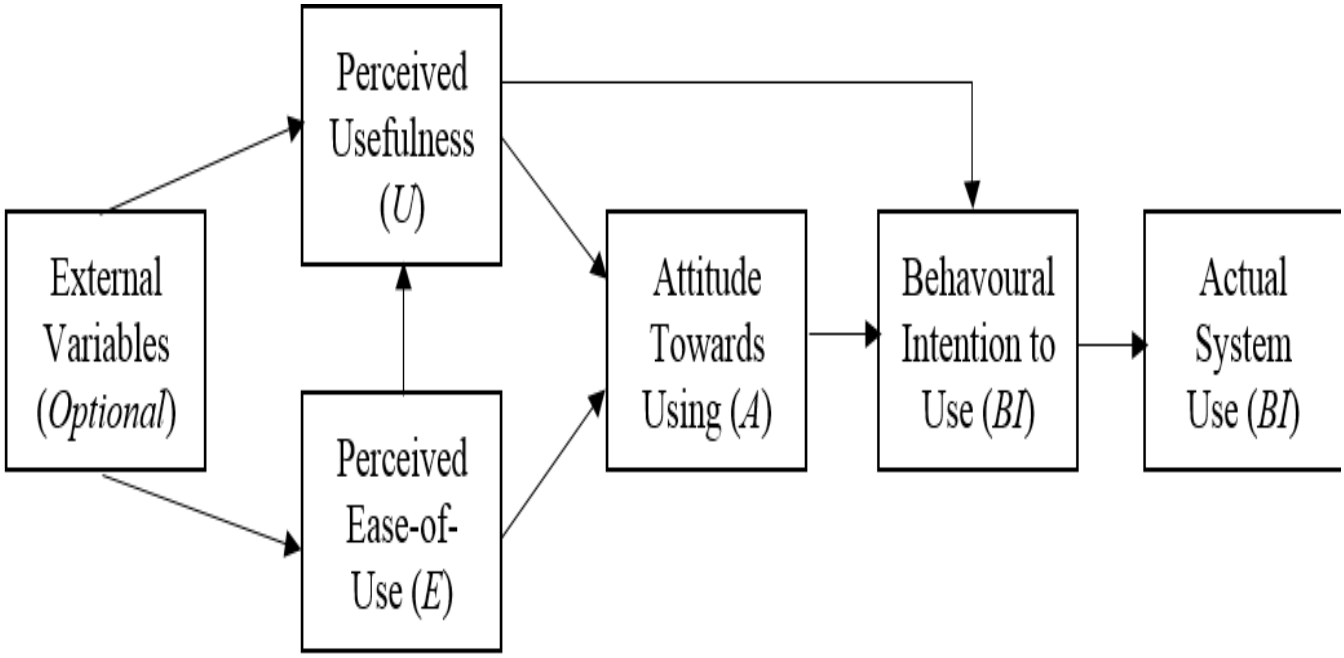

Figure 1: Technology Acceptance Model (TAM), Source: Davis et al., (1989)

Delone and McLean Adoption Model (DM)

Delone and McLean (1992) formulated an adoption model in an attempt to bring the different dimensions of IS adoption together in a comprehensive framework. Delone and McLean (1992) synthesized the views of earlier adoption models, including TAM, and categorized IS adoption into four major interrelated dimensions, namely, System Security, Information Privacy, User Trust and User Personal Innovativeness. Delone & McLean (1992) examined these four dimensions at one major level as defined by Shannon & Weaver (1949). This level is the user traits. The user traits level focuses on the information system itself by examining how users are characterized to use or reject it. The level also examines whether the information conveyed by the system is as intended to suit the user characteristics and how information from the system is impacted on the receiver. ***System security, examines*** the adoption of the system based on how users are concerned about security issues in information security while ***information privacy*** studies the system at the level at which users are concerned with privacy of their data collected by the information system, ***user trust*** has to do with the users' degree to disposition to trust and finally the ***user personal innovativeness*** measures the propensity of the user to accept or reject an information system based on how inventive they see the system. Figure 2 illustrates the four dimensions of the Delone and McLean (1992) successful adoption model.

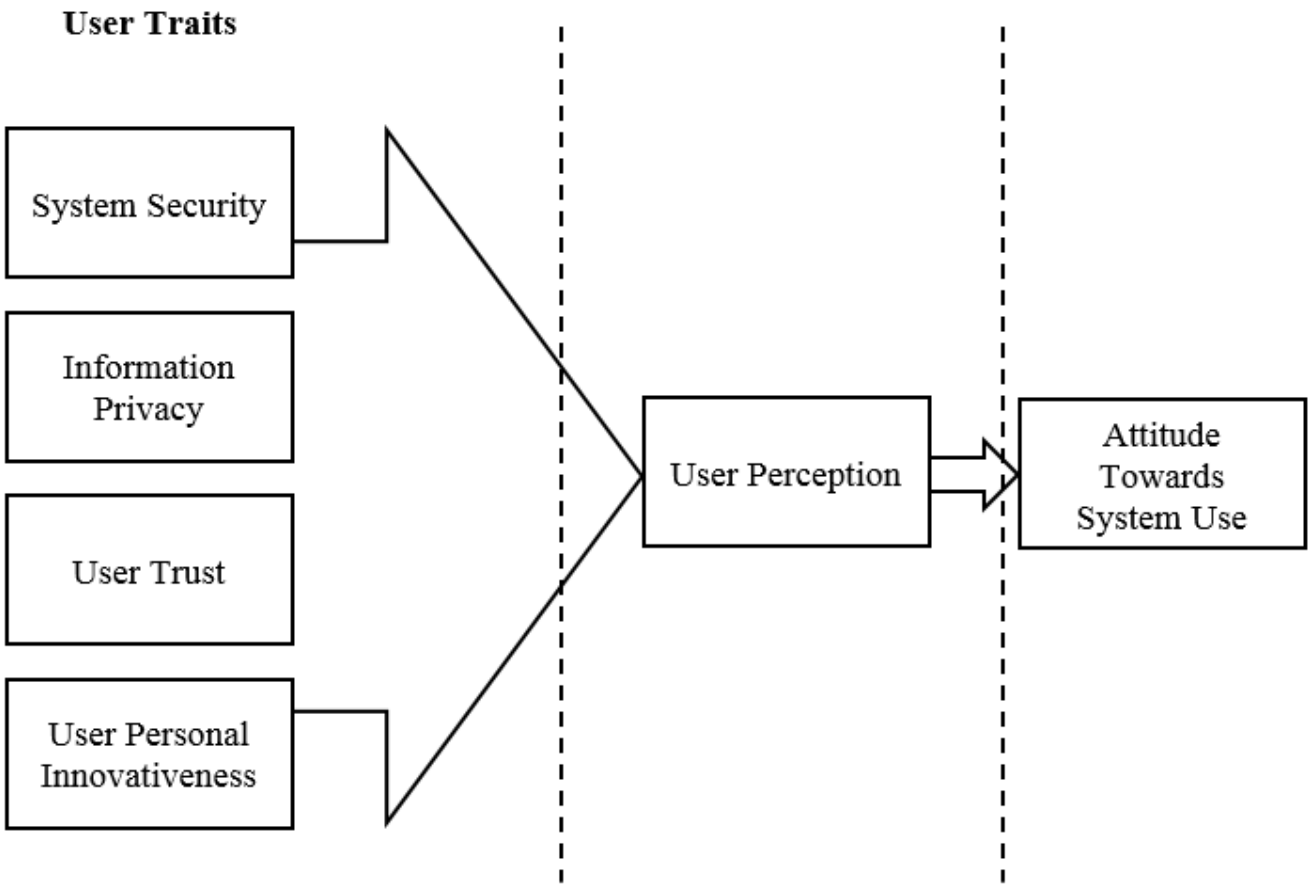

Figure 2: The Delone and McLean (1992) IS success adoption model

4.3 The Proposed Conceptual Model of the Research

This study seeks to update the Delone and McLean (1992) Success Adoption Model (DM), based on the evaluation of the contributions made by Seddon & Kiew (2007). In this updated model (see Figure 3), this research combined the TAM of Davis et al., (1989) with the success adoption model of DeLone and McLean (1992) where external variables for the TAM of Davis et al., (1989) were derived from the four dimensions considered in the model of DM. In this research model, seven variables were identified which are Privacy Concerns (P), Security Concerns (S), User Trust (T), User Personal Innovativeness (PI), the Perceived Usefulness (U), Perceived Ease-of-Use (EU) and Attitude Towards Using (A). In addition, the research grouped these variables into three levels which are ***user traits***, ***user perception*** and ***model outcomes***. Therefore, in the proposed model, privacy concerns, security concerns, personal innovativeness and trust were grouped under the user traits level, while perceived usefulness and perceived ease of use were variables grouped under user perception. The model outcome level had only one variable falling under it, being the attitude towards the use of the proposed keystroke biometric authentication.

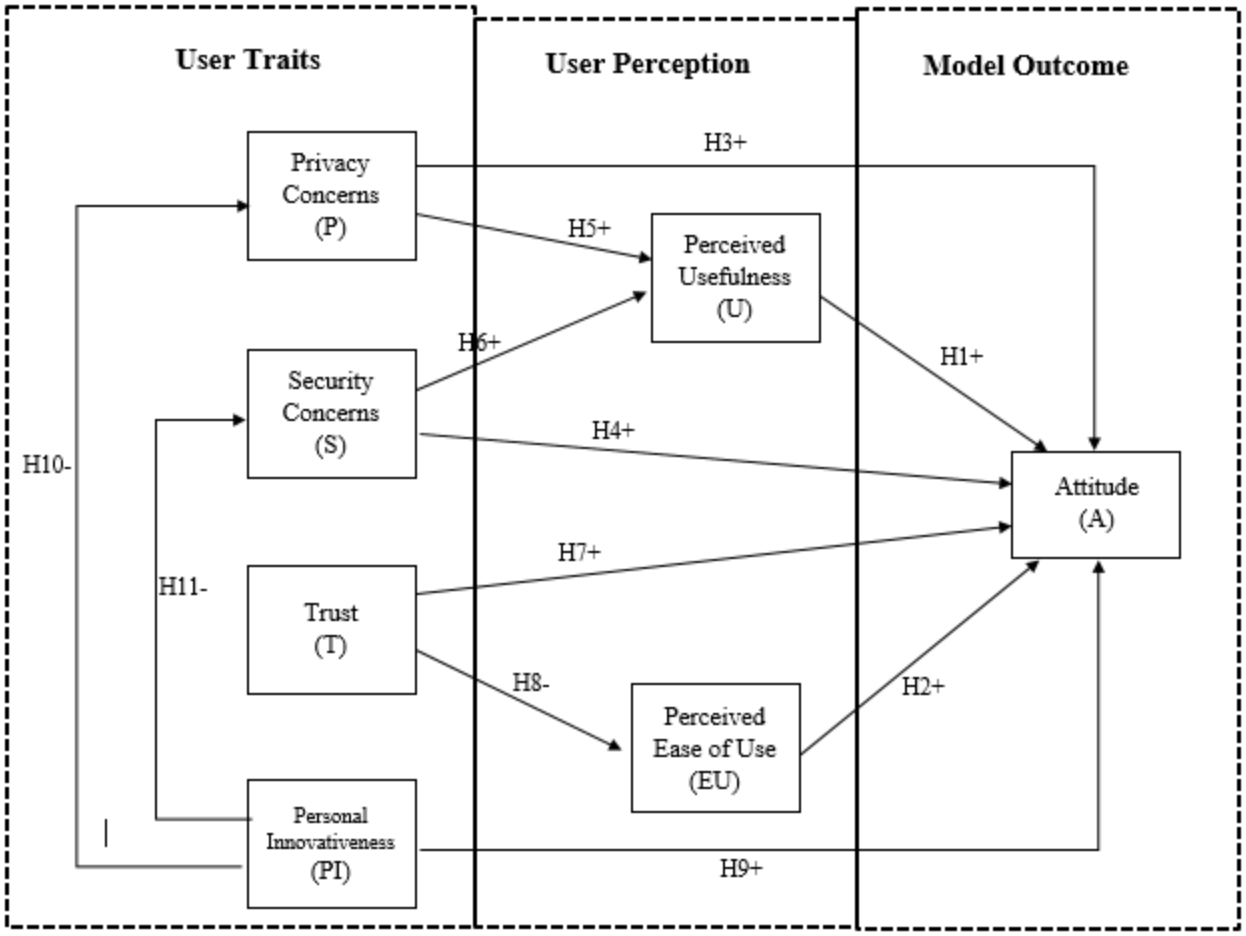

Figure 3: **Proposed Conceptual Model of the Research**

5. RESEARCH QUESTIONS:

What information security determinants influence the adoption of biometric authentication system? 1. What are the key determinants of end-user acceptance (or reject) of disruptive IT like biometric systems in healthcare environments? 2. What appropriate model influences the adoption of the proposed authentication technique in E-Health Systems?

The overarching questions are further developed into appropriate hypotheses.

H1: *Users with a higher degree of perceived usefulness will demonstrate a more positive attitude towards adopting keystroke biometric authentication technology for accessing the E-Health Systems.*

H2: *Users with a higher degree of perceived ease of use will demonstrate a more positive attitude towards adopting keystroke biometric authentication technology for accessing the E-Health System.*

H3: *Users with a higher degree of privacy concerns will demonstrate a high positive attitude towards adopting keystroke biometric authentication technology for accessing the E-Health System.*

H4: *Users with a higher degree of security concerns will demonstrate a high positive attitude towards adopting keystroke biometric authentication technology for accessing the E-Health System.*

H5: *Users with a higher degree of privacy concerns will demonstrate a higher degree of perceived usefulness towards keystroke biometric authentication technology for accessing E-Health System*

H6: *Users with a higher degree of security concerns will demonstrate a higher degree of perceived usefulness towards keystroke biometric authentication technology for accessing E-Health System.*

H7: *Users with a higher degree of trust will demonstrate a more positive attitude towards adopting keystroke biometric authentication technology for accessing the E-Health System.*

H8: *Users with a* ***very*** *high degree of perceived ease of use for the keystroke biometric authentication technology will demonstrate a lower degree of trust for the same authentication technology in protecting their information on the E-Health System.*

H9*: Users with a high degree of personal innovativeness will demonstrate a more positive attitude with respect to using keystroke biometric authentication technology for accessing the E-Health System.*

H10: *Users with a high degree of personal innovativeness will demonstrate a higher degree of perceived privacy concerns with respect to using keystroke biometric authentication technology for accessing the E-Health System.*

H11*: Users with a high degree of personal innovativeness will demonstrate a higher degree of perceived security concerns with respect to using keystroke biometric authentication technology for accessing the E-Health System.*

6. METHODOLOGY

Descriptive research was deemed appropriate for this phase, since it is better at collecting information that describes the world as it is (35). The research design in the current research is a self-administered survey design and the empirical part of the current research is quantitative. The aim of the empirical part is to test the fit of the conceptual model with received data from a questionnaire. This paper uses a cross-sectional approach that provides a "snapshot" of the secured system's usefulness and ease-of-use from the perspective of the end-users.

6.1 Data Collection Technique

The study targeted DHIMS2 users. These users primarily included the District Health Records and Information Officers (DHRIs), the Regional Health Records and Information Officers (RHRIs) and the Senior Health Records and Information Officers (SHRIs) who served as the managers at the MoH offices. Therefore, the sample was obtained from these users. The sample size was composed of 135 DHIMS2 users. Purposive sampling technique was being utilized in taking the 135 samples. A questionnaire was distributed to these sampled users of the DHIMS2.

6.2 Data Analysis and Method of Analysis

Descriptive statistics including some of the measures of central tendencies such as mean, median was employed to describe the data. Other descriptive measures used in analyzing the data included frequency tables and Structural Equation Modelling (SEM). These statistical methods were employed in establishing the effect of some factors contributing to the adoption of keystroke biometric authentication incorporated into DHIMS2.

6.3 Ethical Considerations

As this study required the participation of human respondents, specifically users of a critical computer system within the health sector and some senior management staff, certain ethical issues were addressed. The consideration of these ethical issues is necessary for the purpose of ensuring the privacy as well as the safety of the participants. Among the significant ethical issues that were considered in the research process includes consent and confidentiality. In order to secure the consent of the selected participants, the researcher relayed all important details of the study, including its aim and purpose. By explaining these important details, the respondents were able to understand the importance of their role in the completion of the research. With this, the participants were not forced to participate in the research. The confidentiality of the participants was also ensured by not disclosing their names or personal information on the research. Only relevant details that helped in answering the research questions were included.

7. DATA ANALYSIS AND RESULTS:

7.1 Research Question 1: Is the proposed authentication technique efficient enough to influence its adoption, as an enhanced authentication in E-Health Systems?

Table 1 summarizes the responses on the adoption of the proposed keystroke authentication system, subject to users' perceived ease of use (EU-*X1*), perceived usefulness (U-*X2*), and attitude (A-*X3*). Using the information in Table 1, there are three (3) explanatory variables which are of interest. These variables are EU, U, A. The coefficients which ought to be determined are *b1*, *b2*, and *b3*. To answer how these variables, relate to the adoption of the proposed keystroke authentication system (*Y*), which is the response variable, as indicated in Table 1. A multiple regression analysis was performed with 'Adoption of Keystroke Authentication', hereafter, referred to as 'The Technology' as the dependent variable and perceived usefulness, perceived ease of use and altitude as the predictor variables. Table 1 present values of these measures generated. There is a straightforward interpretation of the coefficients. The predictor variables which were examined are EU, U and A. In multiple regression, the model is expressed as

$$\mathbf{Y = b0 + b1.X1 + b2.X2 + \ldots\ldots + bk.Xk}$$

The research object was to know how well the DHIMS2 users' perceptual and attitudinal variables (EU, U and A) account for the variance in the adoption of keystroke authentication module**.** To answer, a reference is made to formulate the estimated regression model as expressed by;

$$\mathbf{Y = b0 + b1.EU + b2.U + b3.A}$$

Where b1, b2, and b3, are called the regression coefficients of the predictors while the b0 is the constant. The regression coefficients of the predictors quantify the amount of linear trend in 'The Technology' (*Y*) integration. Now using the information from Table 1, the regression coefficients of the predictors can be estimated.

Table 1: SPSS Output for variables in equation

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	**(b0)**	8.015	17.324		.463	.000
	EU	.139	1.073	.161	.409	.023
	U	1.25	.547	.850	2.29	.002
	A	.336	.739	.155	.155	.017

a. Dependent Variable: Technology Integration (Y)

b. Predictors: (Constant), EU (X1), U (X2), A (X3)

The coefficients of perceived ease of use (b1), perceived usefulness (b2) and attitude (b3) correspond to 0.44, 1.25 and 0.34 respectively. This is indicated under the 'B' column of Table 1. Replacing them with the values of the regression coefficients, the fitted estimated model is now expressed by;

Y = 8.02 + 0.44(EU) + 1.25(U) +0.34(A)

The coefficients for perceived ease of use (b1), perceived usefulness (b2) and attitude (b3) which are found to be 0.44, 1.25 and 0.34 respectively, represent the amount of change in adoption of proposed keystroke authentication module (Y) corresponding to a one unit change in a predictor while all other predictors are held fixed at some specified levels. The signs of the coefficients are non-negative, implying there is positive relationship between the response variable and the explanatory variables. This means that suppose there is an observed increase in perceived usefulness (U) of the proposed keystroke authentication module (Y) by one unit, then there will be a corresponding increase in its adoption by users of DHIMS2 for about 1.25 times. Adoption of proposed keystroke authentication module, thus, related positively to all the determinants. As the elements of determinants increase, more users would hold onto the proposed keystroke system by adopting as their main authentication module for DHIMS2. Perceived Ease of Use (EU), Perceived Usefulness (U) and Attitude (A) are then described as factors that determine a complete, partial or no adoption of the proposed keystroke authentication system into DHIMS2, but among these determinants, perceived usefulness has the most prominent influence. Again, all these three elements of regression were significant at $p<0.001$, $p<0.005$ and $p<0.05$, respectively.

Also, the research objective wants to know how well the DHIMS2 users' personality traits (P, S, T and PI) account for the variance in the adoption of keystroke authentication module. To answer, a reference is again made to formulate the estimated regression model as expressed by;

Y = b0 + b1.P + b2.S + b3.T + b4.PI

Where b1, b2, and b3, are called the regression coefficients of the predictors while the b0 is the constant. The regression coefficients of the predictors quantify the amount of linear trend in Technology (*Y*) integration. Now using the information from Table 2, the regression coefficients of the predictors can be estimated.

Table 2: SPSS Output for variables in equation

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	**(b0)**	6.290	13.825		.897	.000
	P	-1.347	.602	.887	.601	.001
	S	-1.205	.652	.468	.562	.001
	T	.869	.577	.657	.696	.029
	PI	.141	.709	.553	.613	.634

a. Dependent Variable: Technology Integration (Y)
b. Predictors: (Constant), P(X1), S(X2), T(X3), PI(X4)

The coefficients of privacy (b1), security (b2), trust (b3) and personal innovativeness (b4) correspond to -1.35, -1.21 and 0.87 and 0.34 respectively. This is indicated under the 'B' column of Table 2. Replacing them with the values of the regression coefficients, the fitted estimated model is now expressed by;

Y = 6.290 + 0.35(P) + 0.21(S) + 0.87(T) + 0.34(PI)

The coefficients of privacy (b1), security (b2), trust (b3) and personal innovativeness (b4) corresponds to 0.35, 0.21, 0.87 and 0.34 respectively, representing the amount of change in the adoption of keystroke authentication module (*Y*), corresponding to a one unit change in a predictor while all other predictors are held fixed at some specified levels. The signs of the coefficients for privacy concerns (b1), security concerns (b2) are negative whilst the signs of the coefficients for trust (b3) and personal innovativeness (b4) are non-negative, implying that, whilst there is negative relationship between privacy and security concerns and the explanatory variable, the adoption of keystroke authentication module, there is however a positive connection between trust and personal innovativeness and the adoption of keystroke authentication module. This means that suppose there is an observed increase in privacy and security concerns of users towards keystroke authentication, its integration into DHIMS2 will decrease correspondingly for about 1.347 or 1.205, respectively. Again, if there is an assumed increase in trust and personal innovativeness on the part of the users, there will be a correspondingly observed increment in the integration keystroke authentication module into DHIMS2 for about 0.869 and 0.141 times respectively. Technology integration is, thus, related positively to two of the users' personality traits (privacy and security concerns) but negatively to another two of the users' personality traits (trust and personal innovativeness). However, among these users' personality traits, privacy concerns have the most prominent influence followed by security concerns. Trust can be termed to have an average influence of keystroke authentication module adoption in DHIMS2. Again, all these elements of regression or paths were significant at either $p<0.001$ or $p<0.05$, except the significant level between Personal Innovativeness (PI) and Keystroke Authentication integration, which was not significant at these p-values

7.2 Research Question 2: What appropriate model influences the adoption of the proposed authentication technique in E-Health Systems?

The aim of the second research question was to gather information on how easy, simple and secured the proposed system was from the users' perspective, as this is assumed to influence their acceptance or attitude of use and adopt the proposed authentication technique incorporated into DHIMS2. The findings of this research question can be an indication as to either the proposed system is advantageous or detrimental to e-health system users. The views of the users were solicited assessed the validity of the structural model and the associated hypotheses

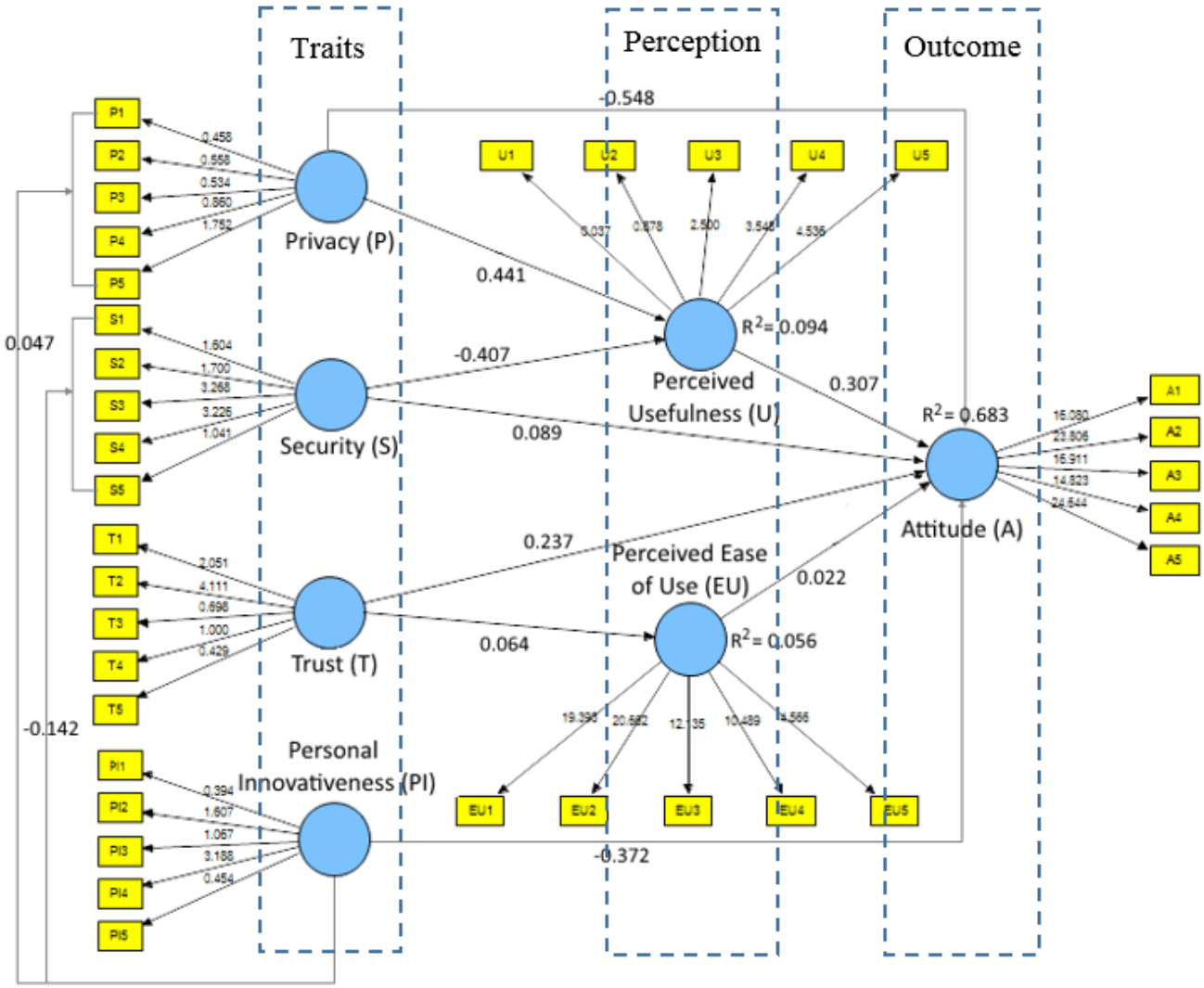

Figure 4: Proposed Adoption Model with its SmartPLS Results

The adoption model was proposed and further evaluations were made to SmartPLS (v. 2.0.M3) as shown in Figure 5. The proposed adoption model was verified by using the bootstrapping calculation approach, a nonparametric technique available to estimate the significance of the path coefficients (36). The bootstrapping estimation approach used, drew a number of samples to attain a certain set of bound estimates (with each sample containing the same number of cases as the original sample. From Figure 5, the hypotheses, paths, path coefficients, etc. are detailed in Table 3.

Using these responses from users of DHIMS2, an appropriate adoption model that influences the integration of keystroke authentication into DHIMS2, was then drawn. The model was used to decipher the hypotheses set for this study. The hypotheses are either supported or rejected using the weight ratings of the model drawn. This is shown Table 3.

Table 3: Summary of Results to Verify Hypothesis.

Hypothesis	Path	Beta	Standard Error	t-statistic	p-value	Validation
H1	U→A	0.307	0.052	5.852	< 0.001***	Supported
H2	EU→A	0.022	0.039	2.445	<0.05*	Supported
H3	P→A	-0.548	0.043	12.914	< 0.001***	Supported
H4	S→A	0.089	0.043	2.054	< 0.05*	Supported
H5	P→U	0.441	0.045	9.764	<0.001***	Supported

H6	S→U	-0.407	0.055	7.470	< 0.001***	Supported
H7	T→A	0.237	0.053	4.447	< 0.001***	Supported
H8	T→EU	0.064	0.066	0.280	0.328 (n.s.)	Rejected
H9	PI→A	-0.372	0.062	0.355	0.401 (n.s)	Rejected
H10	PI→P	0.047	0.041	0.144	0.254 (n.s.)	Rejected
H11	PI→S	-0.142	0.058	0.571	0.568 (n.s.)	Rejected

Significance levels: ***significant @ p<0.001, **significant @ p<0.01, *significant @ p<0.05, (n.s.) not significant @ p>0.05

There was a need to then simplify the model after the hypothesized relationships were developed. It must be distinguished here that not all the paths were significant, and hence not all hypotheses were supported. More specifically, three hypotheses were rejected in the model evaluated in above. All innate paths within the user traits were insignificant (H10 and H11). Adding to these insignificant paths is the path between the constructs '*trust (T)*' and '*Perceived ease of use (EU)*', thus H8. Also, the path that examined the relationship

Among health workers with '*Personal Innovativeness (PI)*' and their '*Attitude (A)*' with respect to using keystroke biometric authentication technology for accessing the DHIMS2, was insignificant. As such, the intention was that a model needed to be re-run in a simplified manner, in which all non-significant paths were removed and the contextual construct of '*Personal Innovativeness (PI)*' was eliminated, and dropped. '*Personal exploring effect sizes.*

Innovativeness (PI)' was removed as its three hypothesized paths were all not significant.

Therefore, a model was drawn with these features incorporated into it. Then, this simplified structural model was again evaluated using bootstrapping technology in SmartPLS with 135 samples. The results are shown in Figure 6 and Table 4. Comparing Figure 5 with Figure 6, one can see that the overall predictive power of attitude of the simplified model (R2 = 0.679) is virtually unchanged from the original model (R2 = 0.683) and that the same can be said for the R-squared values for trust, privacy and security concerns, and usefulness. Looking at Table 4, one can also see that all the remaining paths are significant. The simplified model will be used for the purpose of

Table 4: Summary of Simplified Model to Verify Hypothesis.

Hypothesis	Path	Beta	t-statistic	p-value	Significance	Validation
H1	U→A	0.321	6.065	< 0.001	***	Supported
H2	EU→A	0.022	2.761	<0.05	*	Supported
H3	P→A	-0.548	11.885	< 0.001	***	Supported
H4	S→A	0.089	3.158	< 0.05	*	Supported
H5	P→U	0.463	10.006	<0.001	***	Supported
H6	S→U	-0.432	6.587	< 0.001	***	Supported
H7	T→A	0.237	5.528	< 0.001	***	Supported

Significance levels: ***significant @ p<0.001, **significant @ p<0.01, *significant @ p<0.05.

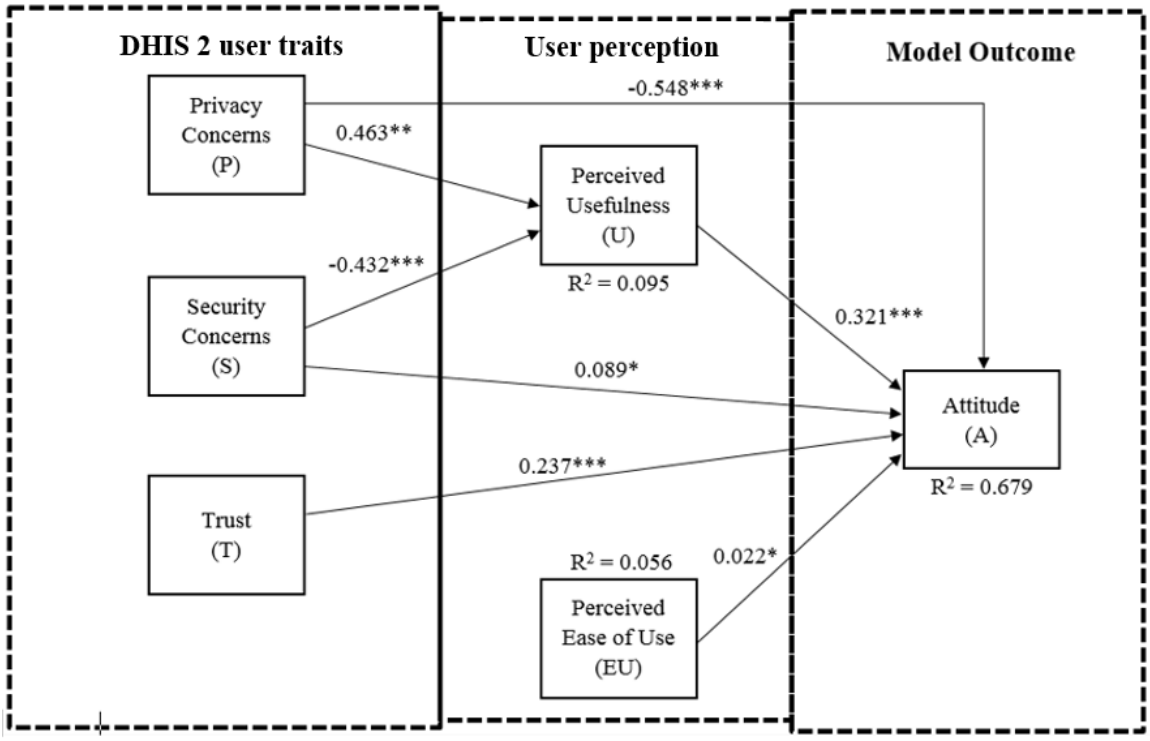

Figure 5: **Proposed Simplified Model SmartPLS Results**

Further, evaluations were made to the proposed model to come out with a more refined saturated model, with the simplified model, serving as the foundation. A saturated model was developed and tested to investigate the possibility of the existence of additional relationships not previously included. The saturated model is not shown due to the fact that the excessive links make it somewhat unruly and convoluted. The saturated model contains 15 paths in total. While some of these paths were part of the original model, they have been reintroduced in the interests of completeness. All the hypothesized paths in the simplified model, and their corresponding coefficients, t-statistics, etc., for both the simplified and saturated model are shown in Table 5. The findings for the new paths created in the saturated model are shown in Table 6. There were essentially no differences in the hypothesized paths between the simplified model and saturated simplified model; and no new significant paths were noted

Table 5: Summary of Saturated and Simplified Models

Hyp.	Path	Non-Saturated Model				Saturated Model				Δ*β*
		β	t-val.	p-val.	Valid.	*β*	t-val.	p-val.	Valid.	
H1	U→A	0.321	6.065	< 0.001	☐	0.317	5.842	< 0.001	✓	0.004
H2	EU→A	0.022	2.761	<0.05	☐	0.019	2.528	<0.05	✓	0.003
H3	P→A	-0.548	11.885	< 0.001	☐	-0.538	11.901	< 0.001	✓	-0.010
H4	S→A	0.089	3.158	< 0.05	☐	0.085	2.975	< 0.05	✓	0.004
H5	P→U	0.463	10.006	<0.001	☐	0.458	9.5	<0.001	✓	0.005
H6	S→U	-0.432	6.587	< 0.001	☐	-0.423	6.596	< 0.001	✓	-0.009
H7	T→A	0.237	5.528	< 0.001	☐	0.229	5.114	< 0.001	✓	0.008

✓ = Supported, ***β*** = Beta, **Δ*β*** = Delta Beta

Table 6: Summary of Findings for Saturated Model for New Relationships

Hyp.	Path		Beta	t-statistic	p-value	Significance	Status
	From	To					
-	P	EU	0.113	1.675	0.095	n.s.	Rejected
-	S	EU	0.025	0.410	0.682	n.s.	Rejected
H8	T	EU	-0.007	0.108	0.914	n.s.	Rejected
-	PI	EU	0.032	0.909	0.364	n.s.	Rejected
-	PI	U	-0.002	0.027	0.978	n.s.	Rejected
H9	PI	A	-0.372	0.355	0.401	n.s.	Rejected
H10	PI	P	0.047	0.144	0.254	n.s.	Rejected
H11	PI	S	-0.142	0.571	0.568	n.s.	Rejected

The impact of individual constructs was then examined to assess the predictive power and quality of a model. This is known as the effect size (37; 38). The calculation of effect size (F^2) allowed to determine the contributions of independent variables upon the R-squared of dependent variables (Chin 1998). Using Chin's (37) formula and Ellis's (38) guidelines with respect to effect sizes, ≥0.02 is interpreted as '*small*', ≥0.15 is interpreted as '*medium*', and ≥0.35 is interpreted as '*large*' impact of each of the independent variables upon their corresponding dependent variables. This is shown in Tables 7 and Table 8. Table 7 demonstrates that usefulness, privacy concerns and security concerns have a significant impact upon attitude, while the impact of trust and ease of use on attitude is minimal. Turning to privacy and security concerns, paths into these constructs are large. While trust has a medium impact the remaining construct, ease of use has only a small influence. Finally, looking at usefulness, the effect of privacy and security is medium. Therefore, the most dominant paths, in order of strength, are from privacy and security concerns and usefulness to attitude, privacy and security concerns to usefulness, and trust to attitude and ease of use to attitude, in that order.

Table 7*: Effect Sizes of Antecedents of Attitude*

R^2 (included} =0.679	Privacy(P)	Security(S)	Trust(T)	Usefulness(U)	Ease of Use (EU)
R^2 (excluded)	0.473	0.572	0.103	0.508	0.661
F^2	0.640	0.618	0.315	0.530	0.06
Effect	large	large	medium	large	small

From Table 7, the attitudinal effect sizes (F^2) of Privacy Concerns (P), Security Concerns (S) and Perceived Usefulness (U) 0.640, 0.618 and 0.53 respectively, whiles that of Trust (T) was 0.315, and Ease of Use (EU) being 0.06. Ellis' (38) guidelines with respect to effect sizes (F^2), if $0.02 \leq F^2 < 0.15$, then F^2 is interpreted as having a small effect, else if $0.15 \leq F^2 < 0.35$, then F^2 is interpreted as having a medium effect, else if $0.35 \leq F^2$ or $F^2 \geq 0.35$, then F^2 is interpreted as having a large effect. From the Table 7, since the effect sizes of Privacy Concerns (P), Security Concerns (S) and Perceived Usefulness (U) satisfies the last condition such that 35≤F2 or F2≥0.35. However, the Trust (T) as a personality trait of DHIMS2 users satisfied the second condition such that $0.15 \leq F^2 < 0.35$ whereas Ease of Use (EU) as a perceptual trait of DHIMS2 users satisfied the first condition such that $0.02 \leq F^2 < 0.15$. Therefore, it can be interpreted that the privacy, security and usefulness concerns of DHIMS2 users about proposed keystroke authentication will very largely influence their attitude towards its use and hence finally influence its full integration into DHIMS2. But the effect size of Trust (T) on attitude of DHIMS2 users is medium which interprets that, if these users of DHIMS2 have higher level of trust, it will averagely strongly influence their attitude towards the use an influence the integration proposed keystroke authentication into DHIMS2. Lastly the effect size or Perceived Ease of Use (EU) is small, which interprets that if users of DHIMS2 perceive proposed keystroke authentication to be easy and simple to use, their perception does not necessarily influence their attitude towards the use or adoption of the proposed keystroke authentication module into DHIMS2.

Table 8*: Effect Sizes of Antecedents of Usefulness*

R^2 (included}= 0.168	**Privacy**	**Security**
R^2 (excluded)	0.008	0.147
F^2	0.19	0.16
Effect	medium	medium

Then again, the level of effects of privacy and security concerns were individually tested on DHIMS2 users' perceptual usefulness of integrating keystroke authentication into DHIMS2. From the Table 8, the effect sizes (F^2) of Privacy Concerns (P) and Security Concerns (S) on DHIMS2 users' perceptual usefulness were 0.19 and 0.16 respectively. Ellis' (38) guidelines with respect to effect sizes (F^2), these values for effect sizes satisfies the second condition such that $0.15 \leq F^2 < 0.35$. Therefore, it can be interpreted that the privacy and security concerns of DHIMS2 users about the proposed keystroke authentication will at an average, influence their perceptual usefulness in adopting the use of proposed keystroke authentication module integration in DHIMS2 at their hospitals.

Table 9*: Summary of Most dominant paths, in order of strengths*

Hypothesis	**Path**	**F^2**	**Effect / Impact Level**
H3	P→A	0.640	Large
H4	S→A	0.618	Large
H1	U→A	0.530	Large
H7	T→A	0.315	Medium
H5	P→U	0.19	Medium
H6	S→U	0.16	Medium
H2	EU→A	0.06	Small
Average Effect Size		**0.359**	**Large**

A summary on the effect sizes of all the supported hypotheses are presented in Table 9. From previous the findings, H3 with the path P→A scored an effect size (F^2) of 0.640 therefore it was first on the list as having a large impact level, followed by H4, with the path S→A, and an F^2 of 0.618, then by H1 with the U→A and an F^2 of 0.530. All these hypotheses were interpreted as having large influence on attitudinal change of DHIMS2 users towards the adoption and use of the proposed keystroke authentication in DHIMS2. In terms of medium influence, hypotheses H7 with path T→A, H5 with path P→U and H6 with S→U, fell under this category in that order. Hypothesis H2 with path EU→A scored an F^2 of 0.06, and therefore was the last on the list as it constituted small influence on attitudes of DHIMS2 users. Overall, the average effect size of all paths combined, on the adoption of the proposed keystroke authentication, score 0.359, which is interpreted as a general large impact, per the guidelines of Cohen (1988). All these findings are summarized in model which is seen in Figure 6.

8. DISCUSSION

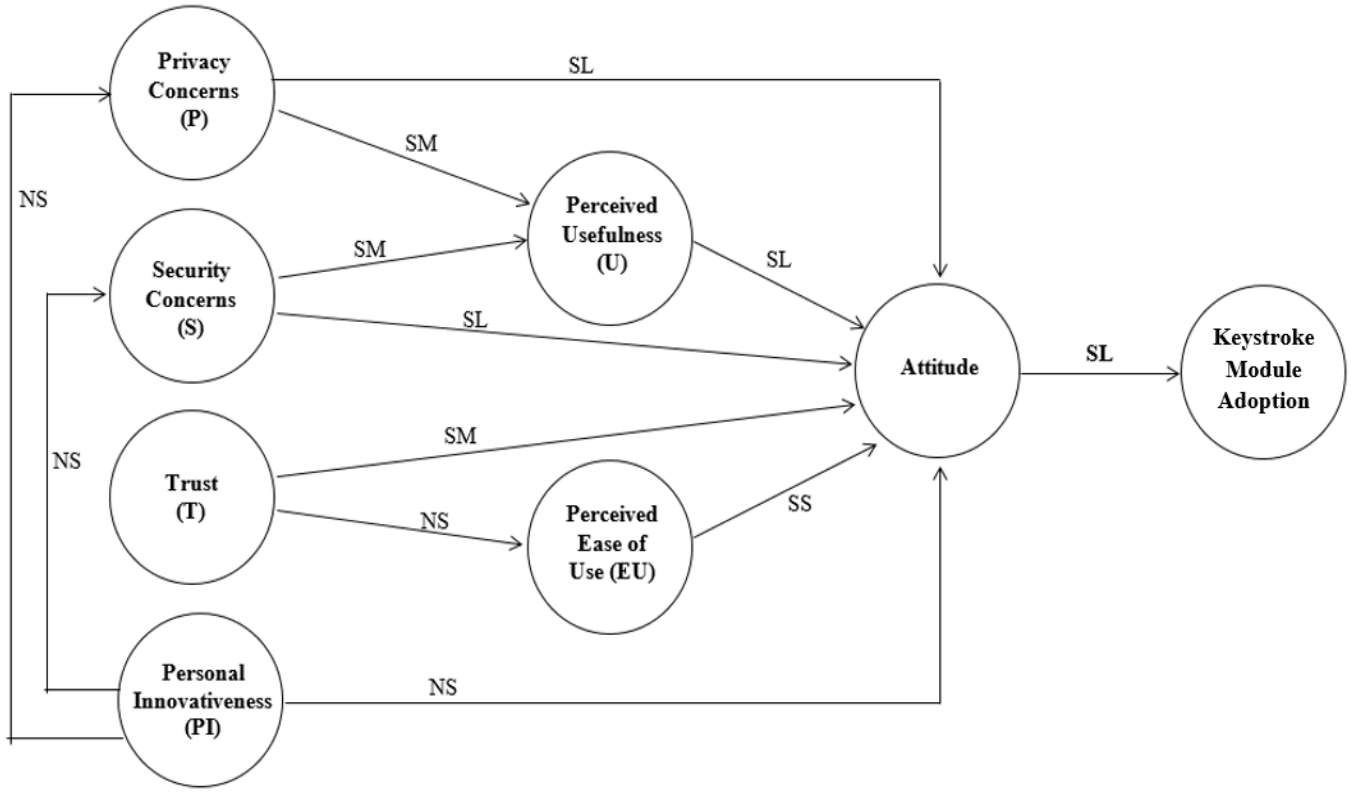

Figure 6: **Summary of Adoption Model**

Note: SL=Significantly Large, SM=Significantly Medium, SS=Significantly Small, NS=Not Significant; Significant levels at p<0.001, p<0.005 and p<0.05;

Figure 7 graphically summarises the regression model of the impact the perceptions and personality traits of users on their level of adopting keystroke authentication modules into DHIMS2. From the figure, and from the previous findings from analysis, it can be realized that, all significant levels either satisfies one of the condition p<0.001, p<0.005 and p<0.05. These are further elaborated in Table 10.

Table 10: **Summary of Hypothesis Support Levels**

S/N	*Hypothetical Statement*	Sig. Level	Effect Level
H1	*Users with a higher degree of perceived usefulness (U) will demonstrate a more positive attitude (A) towards adopting keystroke biometric authentication module in DHIMS2.*	**Sig**	**Large**
H2	*Users with a higher degree of perceived ease of use (EU) will demonstrate a more positive attitude (A) towards adopting keystroke biometric authentication module in DHIMS2*	**Sig**	**Small**
H3	*Users with a higher degree of privacy concerns (P) will demonstrate a high positive attitude (A) towards adopting keystroke biometric authentication module in DHIMS2*	**Sig**	**Large**
H4	*Users with a higher degree of security concerns (S) will demonstrate a high positive attitude (A) towards adopting keystroke biometric authentication module in DHIMS2.*	**Sig**	**Large**
H5	*Users with a higher degree of privacy concerns (P) will demonstrate a higher degree of perceived usefulness (U) towards keystroke biometric authentication module in DHIMS2.*	**Sig**	**Medium**
H6	*Users with a higher degree of security concerns (S) will demonstrate a higher degree of perceived usefulness (U) towards keystroke biometric authentication module in DHIMS2*	**Sig**	**Medium**
H7	*Users with a higher degree of trust (T) in the DHIMS2 will demonstrate a more positive attitude (A) towards adopting keystroke biometric authentication module in DHIMS2*	**Sig**	**Medium**
H8	*Users with a higher degree of perceived ease of use (EU) for the*	**Not Sig**	**-**

	keystroke biometric authentication module will demonstrate a lower degree of trust (T) for its adoption into DHIMS2		
H9	*Users with a high degree of personal innovativeness (PI) will demonstrate a more positive attitude (A) with respect to using keystroke biometric authentication module in DHIMS2*	**Not Sig**	**-**
H10	*Users with a high degree of personal innovativeness (PI) will demonstrate a higher degree of perceived privacy concerns (P) with respect to using keystroke biometric authentication module in DHIMS2*	**Not Sig**	**-**
H11	*Users with a high degree of personal innovativeness (PI) will demonstrate a higher degree of perceived security concerns (S) with respect to using keystroke biometric authentication module in DHIMS2*	**Not Sig**	**-**

Note: Sig.=Significant, Not Sig.= Not Significant; Significant levels at $p<0.001$, $p<0.005$ and $p<0.05$;

This study developed and proposed a model that explains the users' intention to adopt keystroke biometric authentication in an e-health system. This model has specified eleven hypotheses describing relationships between users' intention to adopt keystroke biometric authentication. The hypotheses depicted a comprehensive view of the key drivers influencing keystroke biometric adoption and what aspects to highlight to increase the usage. Through the specification of these relationships, it addresses an important gap in the adoption research.

First, the research objective was to know how well the DHIMS2 users' perceptual and attitudinal variables (Perceived Ease of Use, Perceived Usefulness and Attitude) account for the variance in the adoption of keystroke authentication module**.** The coefficients for perceived ease of use, perceived usefulness and attitude which are found to be 0.44, 1.25 and 0.34 respectively, implying there is positive relationship between the response variable and the explanatory variables. Hence, adoption of the proposed keystroke authentication module is positively significant, as the elements of determinants increase, more users would hold onto the proposed keystroke system by adopting as their main authentication module for DHIMS2. These findings match with results from reviewed literature (39; 40).

Also, the research wants to know how well the DHIMS2 users' personality traits account for the variance in the adoption of keystroke authentication module. The coefficients of Privacy, Security, Trust and Personal Innovativeness were -1.35, -1.21 and 0.87 and 0.34 respectively, implying that, whilst there is negative relationship between privacy and security concerns and the explanatory variable, there is however a positive connection between trust and personal innovativeness. This means that an increase in privacy and security concerns of users towards keystroke authentication, its integration into DHIMS2 will decrease correspondently for about 1.347 or 1.205, respectively. Again, if there is an increase in trust and personal innovativeness on the part of the users, there will be a correspondently observed increment in the integration keystroke authentication module into DHIMS2 for about 0.869 and 0.141 times respectively. Keystroke authentication integration is thus, related positively to two of the users' personality traits (privacy and security concerns) but negatively to other two of users' personality traits (trust and personal innovativeness). However, among these users' personality traits, privacy concerns have the most prominent influence followed by security concerns. This result proved that security challenges, and privacy issues were the significant concerns while adopting a new authentication technique, which was consistent with the past studies (41; 42; 43). Trust can be termed to have an average influence of keystroke authentication module adoption in DHIMS2. The result of this research was consistent with Gao, L., & Bai, X. (44) study, which also found that the trust had no major role in the attitude towards use of adopting new technologies.

With regards to the appropriate model influences the adoption, As seen in Table 10 and Figure 7, hypotheses 1 to 7 (H1 to H7) were supported at significant levels, whereas hypotheses 8 to 11 (H8 and H11) were not supported at all. Among these, hypotheses 1, 3 and 4 were supported by the model at a larger score. It implies, first, users with a higher degree of perceived usefulness of keystroke biometric authentication will at a very large extent, demonstrate a more positive attitude towards its adoption. Likewise, users with a higher degree of privacy and security concerns about the proposed keystroke biometric authentication module will at a very large extent, demonstrate a high positive attitude towards its integration into the main DHIMS2 (H3 and H4). The result of this research was consistent with (45) study, which also found Higher Usage Intentions, Perceived Usefulness were found to be the key factors influencing attitude towards use of adopting new technologies.

9. CONCLUSIONS AND RECOMMENDATION

Based on empirical findings, this study reached several conclusions. First, results of the empirical analysis indicated that user perception has a strong significant influence on attitude. Thus, system designers should make full use of the completeness and accuracy of information to increase behavioral attitude to use the proposed authentication technique. Second, system designers should actively seek methods of improving system security and system privacy; since these elements significantly affect attitude to use authentication techniques. Third, the improvement of information system through enhancing information quality; perceived usefulness; and perceived ease of use will foster user involvement; behavioral intention and attitude. Finally, the proposed model and its elements as agreed by (46) proves that it can be a useful tool for decision makers in healthcare institutions in evaluating authentication techniques in e-health systems.

This study suggests directions for future research. First, like the conventional authentication system, most of the biometric-based systems, whether physical, behavioral, or the multi-biometric, are susceptible to attacks (47). These attacks broadly fall in two categories: direct (or presentation) attacks, and indirect attacks. Researchers (2; 48) suggest that despite various

countermeasures these issues are still prevalent and new techniques are required to deal with the associated threats. Thus, an authentication system that is capable of providing high performance and spoof resistance, along with non-obtrusiveness and cost-effectiveness, is highly desirable.

10. LIMITATIONS

The study has a limitation as to which type of the e-Health system users were concentrated. Majority of the users are officers in charge of data entry and data management at public sector government hospitals who use the system routinely. Therefore users of DHIMS 2 from other organizations were not studied. The users were divided into two, primary and secondary. The primary users, the core users of DHIMS 2, are the District Health Records and Information Officers (DHRIOs) who interact with DHIMS 2 frequently. The secondary users do not use DHIMS 2 as frequently as the Regional Health Records and Information Officers (RHRIOs). The bulk of the respondents of this study were DHRIOs who at the time of the data collection were mostly based at the district level. However, few respondents came from the regional health officers as well as a very few who were Senior Health Records and Information Officers (SHRIs) serving as managers at the MoH offices. Lastly, the limitation had to do with the sampling procedures. A big part of the target population in this study was DHRIOs who are distributed over the 216 districts in Ghana. Though our plan was to derive a representative sample through random sampling, this was not the case.

11. REFERENCES

[1] Jain, A, Flynn, P and A, Ross. A Handbook of Biometrics. US : Springer US, 2008, pp. 1-2.

[2] Bolle, Ruud M., et al. Guide to biometrics. s.l. : Springer Science & Business Media, 2013.

[3] Biometric authentication and identification using keystroke dynamics: A survey. Banerjee, S. P. and Woodard, D. L. 2012, Journal of Pattern Recognition Research, pp. 7(1), 116-139.

[4] Health Professionals' readiness to implement electronic medical record system at three hospitals in Ethiopia: a cross sectional study. Biruk, Senafekesh , et al. 2014, BMC Med Inform Decis Mak, p. 14(1): 1.

[5] Privacy and biometrics: An empirical examination of employee concerns. Carpenter, D., et al. 2018, Information Systems Frontiers, pp. 20(1), 91-110.

[6] Exploring biometric technology adoption in a developing country context using the modified UTAUT. Akinnuwesi, B. A., et al. 2016, International Journal of Business Information Systems, pp. 23(4), 482-521.

[7] PMI . Ghana's Innovative Health Information Management System Gains African Recognition. [Online] PMI, April 2014. [Cited: October 06, 2019.] https://www.pmi.gov/news/stories-from-the-field/stories-from-the-field---detail/ghana-s-innovative-health-information-management-system-gains-african-recognition.

[8] Poppe, O. Health Information Systems in West Africa: Implementing DHIS2 in Ghana (Master's thesis). Accra, Ghana : UNIVERSITY OF OSLO, 2012.

[9] DHIS2 Documentation Team. Rolling Out A Nationwide Web-Based District Health Information System, DHIMS2-The Ghana Experience. [Online] 2012. dhis2.org/doc/snapshot/en/implementer/dhis2..

[10] A literature review and meta-synthesis of its strengths and operational challenges based on the experiences of 11 countries. Dehnavieh, R., et al. 2019, Health Information Management Journal, pp. 48(2), 62-75.

[11] Nyonator, F., Ofosu, A. and Osei, D. District Health Information Management System DHIMS II: The Data Challenge For Ghana Health Service. NetHope Solutions Center Case Studies. [Online] 2013. https://solutionscenter.nethope.org/assets/collaterals/dhims2_crs_presentation.ppt.

[12] Response option for attacks detected by intrusion detection system. Anwar, S., et al. 2015. In Software Engineering and Computer Systems (ICSECS), 2015 4th International Conference. pp. 195-200.

[13] Coley, S. C., et al. Use of Password System for Primary Authentication. CWE Version 2.9. 2015, p. 601.

[14] Securing passwords against dictionary attacks. Pinkas, B. and Sander, T. s.l. : ACM, 2002. In Proceedings of the 9th ACM conference on Computer and communications security. pp. 161-170.

[15] Offline dictionary attack on password authentication schemes using smart cards. Wang, D. and Wang, P. Berlin, Germany : s.n., 2015. In Information Security; Springer. pp. 221–237.

[16] Understanding password choices: How frequently entered passwords are re-used across websites. Wash, R., et al. 2016. In Symposium on Usable Privacy and Security (SOUPS). pp. 175-188.

[17] A study of personal information in human-chosen passwords and its security implications. Li, Y., Wang, H. and Sun, K. s.l. : IEEE, 2016. In INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. pp. 1-9.

[18] User practice in password security: An empirical study of real-life passwords in the wild. Shen, C., et al. 2016, Computers & Security, pp. 61, 130-141.

[19] Who Is Reusing Stolen Passwords? An Empirical Study on Stolen Passwords and Countermeasures. Missaoui, C., et al. s.l. : Springer, Cham., 2018. In International Symposium on Cyberspace Safety and Security. pp. 3-17.

[20] Scaling Up: The Challenges of eHealth Systems in Developing Countries. Kwao, Lazarus, et al. X, s.l. : IJRASET, October 2019, International Journal for Research in Applied Science & Engineering Technology, Vol. 7, pp. 815-823. 2321-9653.

[21] Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. Miltgen, C. L., Popovič, A. and Oliveira, T. 2013, Decision Support Systems, pp. 56, 103-114.

[22] Towards understanding user perceptions of authentication technologies. Jones, L. A., Antón, A. I. and Earp, J. B.

2007. In Proceedings of the 2007 ACM workshop on Privacy in electronic society. pp. 91-98.

[23] Perceived acceptability of biometric security systems. Deane, F., et al. 1995, Computers & Security, pp. 14(3), 225-231.

[24] Biometrics and e-identity (e-passport) in the European Union: end-user perspectives on the adoption of a controversial innovation. Ng-Kruelle, G., et al. 2006, Journal of Theoretical and Applied Electronic Commerce Research, pp. 1(2), 12-35.

[25] Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. Orlikowski, W. J and Iacono, C. S. 2001, Information systems research, pp. 12(2), 121-134.

[26] Technology acceptance model 3 and a research agenda on interventions. Venkatesh, V. and Bala, H. 2008, Decision sciences, pp. 39(2), 273-315.

[27] User acceptance of information technology: Toward a unified view. Venkatesh, V., et al. 2003, MIS quarterly, pp. 425-478.

[28] Verification of computer users using keystroke dynamics. Obaidat, M. S. and Sadoun, B. 1997, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), pp. 27(2), 261-269.

[29] Biometric personal authentication using keystroke dynamics: A review. Karnan, M., Akila, M. and Krishnaraj, N. 2011, Applied Soft Computing,, pp. 11(2), 1565-1573.

[30] Gagbla, K. G. Securing E-Business Applications. Using Keystroke Dynamics as a Biometric Authentication Technique. 2005.

[31] Evaluating the reliability of credential hardening through keystroke dynamics. Bartlow, N. and Cukic, B. s.l. : IEEE, 2006. In 2006 17th International Symposium on Software Reliability Engineering. pp. 117-126.

[32] Journal of management information systems. Hu, P. J., et al. 2, 1999, Examining the technology acceptance model using physician acceptance of telemedicine technology, Vol. 16, pp. 91-112.

[33] Why do people use information technology? A critical review of the technology acceptance model. Legris, P., Ingham, J. and Collerette, P. 3, 2003, Information & management, Vol. 40, pp. 191-204.

[34] User acceptance of computer technology: a comparison of two theoretical models. Davis, F. D., Bagozzi, R. P. and Warshaw, P. R. 1989, Management science, pp. 35(8), 982-1003.

[35] Sekaran, Uma and Bougie, Roger. Research methods for business: A skill building approach. s.l. : John Wiley & Sons, 2016.

[36] A bridge between PLS path modeling and multi-block data analysis. In Handbook of partial least squares. Tenenhaus, M. and Hanafi, M. s.l. : Springer, Berlin, Heidelberg., 2010, pp. 99-123.

[37] The partial least squares approach to structural equation modeling. Chin, W. W. 2, s.l. : Modern methods for business research, 1998, Vol. 295, pp. 295-336.

[38] Ellis, P. D. The essential guide to effect sizes: Statistical power, meta-analysis, and the interpretation of research results. s.l. : Cambridge University Press, 2010. p. 94. Vol. 90.

[39] The DeLone and McLean model of information systems success: a ten-year update. Delone, W. H. and McLean, E. R. 4, s.l. : Journal of management information systems, 2003, Journal of management information systems, Vol. 19, pp. 9-30.

[40] Does the technology acceptance model predict actual use? A systematic literature review. Turner, M., et al. 5, s.l. : Information and software technology, 2010, Vol. 52, pp. 463-479.

[41] The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Shin, D. H. 5, s.l. : Interacting with computers, 2010, Vol. 22, pp. 428-438.

[42] Privacy and data security in E-health: Requirements from the user's perspective. Wilkowska, W. and Ziefle, M. 3, s.l. : Health informatics journal, 2012, Vol. 18, pp. 191-201.

[43] Investigating factors influencing the adoption of e-Health in developing countries: A patient's perspective. Hoque, M. R., Bao, Y. and Sorwar, G. 1, s.l. : Informatics for Health and Social Care, 2017, Vol. 42, pp. 1-17.

[44] A unified perspective on the factors influencing consumer acceptance of internet of things technology. Gao, L. and Bai, X. 2, s.l. : Asia Pacific Journal of Marketing and Logistics, 2014, Vol. 26, pp. 211-231.

[45] Factors influencing consumer adoption of USB-based Personal Health Records in Taiwan. Jian, W. S., et al. 1, s.l. : BMC health services research,, 2012, Vol. 12, p. 277.

[46] An integrated success model for evaluating information system in public sectors. Zaied, A. N. H. 6, s.l. : Journal of Emerging Trends in Computing and Information Sciences, 2012, Vol. 3, pp. 814-825.

[47] Multimodel Biometric Authentication Based on Finger Print and Keystroke Dynamics Using Fuzzy Set. Venko, Chandrasekar, Shanmugavalli, V and Krishna, Sankar P. 2014, Australian Journal of Basic and Applied Sciences, p. 8(5).

[48] I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphone. De Luca, A., et al. Seoul, Korea : ACM: New York, NY, USA,, 2015. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. 18–23 April 2015. pp. 1411–1414.