ISSN 2250-3153

Data Control Model for Secure Access of Customer Information

Abanti Cyrus and Nyasengo Caroline

Jomo Kenyatta University of Agriculture and Technology (JKUAT)

Abstract- This study was conducted with the aim of investigating how access control would secure customer information in Kenya. This study was guided by the set out objectives: first to determine how data control mechanisms enhance security access, secondly to investigate the security issues on access of customer information and thirdly to develop Secure Data Access Control (SEDAC) model. In achieving these objectives a self administered questionnaire was developed and distributed to randomly selected respondents. The findings of the study were analyzed using SPSS. The Security Data Access Control (SEDAC) model was developed for and recommended for adoption by the end users as a guide to enlighten the novice worker who constitutes a large number of the work force.

Index Terms- Access, Control, Secure, SEDAC, Data

I. Introduction

Access control is any type of control that regulates the entrance of a person in a given object. For instance, the personal identification number (PIN) code of your credit card is a type of everyday control that precedes the access to your bank account. The control can be done by a human being or it may be performed by a computerized machine using a suitable software program. This phenomenon is also widely used in everyday life to control the entrance and the exit of people in a certain building. Turban *et al.* (2009) has defined access control as the restriction of unauthorized user to access to a portion of a computerized user or to the entire system.

Access to a computer consist of physical, access to system and access to specific commands, control transaction privileges , programs and data. Password cracking is a technical vulnerability attacks to a system. According to Harriet (2011), the problem with passwords may include the vast number users are required to generate and remember. Passwords being the commonly used access control they have been identified to have their own weaknesses which lead to unauthorized access of customer information. Some of these weaknesses have been identified by different authors as seen here in. According to John Chew, (2011) he argues that a really strong password is one that nobody else has ever used and terms that as a fine hence strong password. Password authentication has a number of weaknesses making authentication to fail. This is due to the way to control password distribution, password which is simple and easy, naive implementation, brute force attack, eavesdropping and guessing (Pfleeger and Pfleeger 2007) . Kaufman et al (2011) argues that password based authentication is not who you know, it is what you know.

The above authors having mentioned some of the weaknesses of access control they left a research gap that is why the researcher wanted to investigate how to enhance security of customer information by the use of data access control mechanisms because as we all know customer information is the key asset in any organization.

II. Access Control Mechanisms and Security of Customer Information

Access control is the traditional center of gravity of computer security. It is where security engineering meets computer science. Its function is to control which principals (persons, processes, machines,) have access to which resources in the system which files they can read, which programs they can execute, how they share data with other principals, and so on. Gasser (2010) in his books, building a secure computer system, states that while implementing any access control, there are two driving factors that must be considered and they include: Least privilege principle that is the user should only have the minimum privileges to perform the tasks required. Segregation of duties is having more than one user to perform a critical task so as to reduce the risk of internal frauds.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The current security model for verification of identity, protection of information and authentication to access data or services is based on using a token or password, tied to and thereby representing an individual to either authenticate identity or allow access to information (Ann *et al*, 2007).

Prior to the work of Davis (1985) several studies had highlighted the importance of perceived ease of use and perceived usefulness of a person's behavior. Schultz and Selvin (1975) for instance carried out an explanatory study and found that perceived usefulness provided a reliable prediction for self-predicted use o a decision model. Robey (1979) later replicated the work of Schultz and Selvin and confirmed the high correlation that existed between perceived usefulness and system usage.

In the end Davis(1985) concluded that people tend to use or not use a system to the extent that they believe it will help them perform their job better(perceived usefulness) and also that the beliefs of the efforts required to use a system can directly affect system usage behavior(perceived ease of use). More formally he defined perceived usefulness and perceived ease of use as follows; Perceived usefulness: the degree to which an individual believes that using a particular system will enhance his/her

performance. Perceived ease of use: the degree to which an individual believes that using a particular system would be free of physical and mental effort.

Here in is figure 1 which is the proposed extended TAM for this research study.

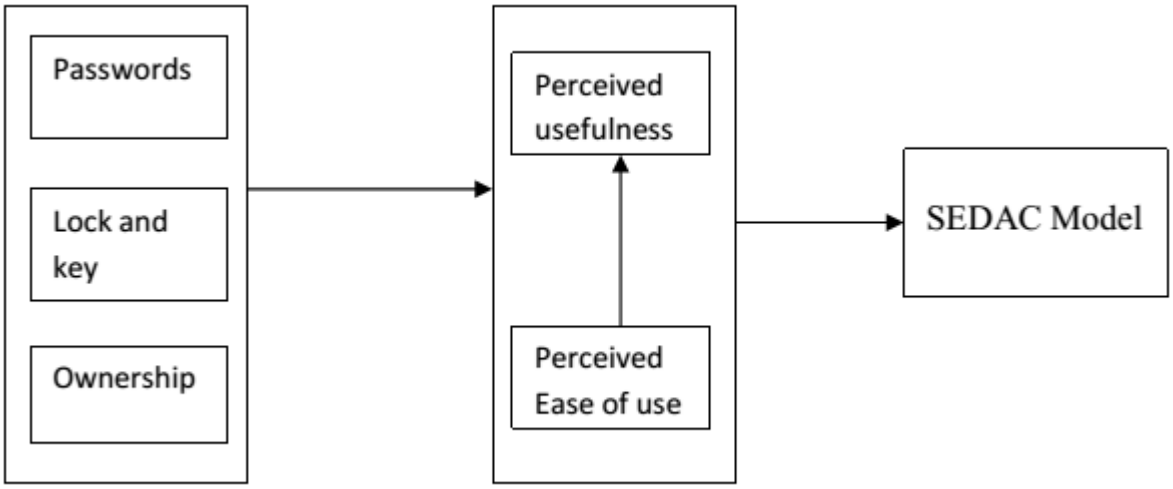

Figure 1: The Proposed Extended Technology Acceptance Model

The above figure 1 shows the extended technology that the researcher intends to use with the two specified variables; perceived usefulness and perceived ease of use. If the attitude of the user towards the PU and PEOS is positive then the actual system is put in use.

The researcher placed the conceptual model into test in order to establish the significance of the proposed relationships. In this case the independent variable is control access and the dependent variable is secure customer information. Figure 3 shows how these variables are related.

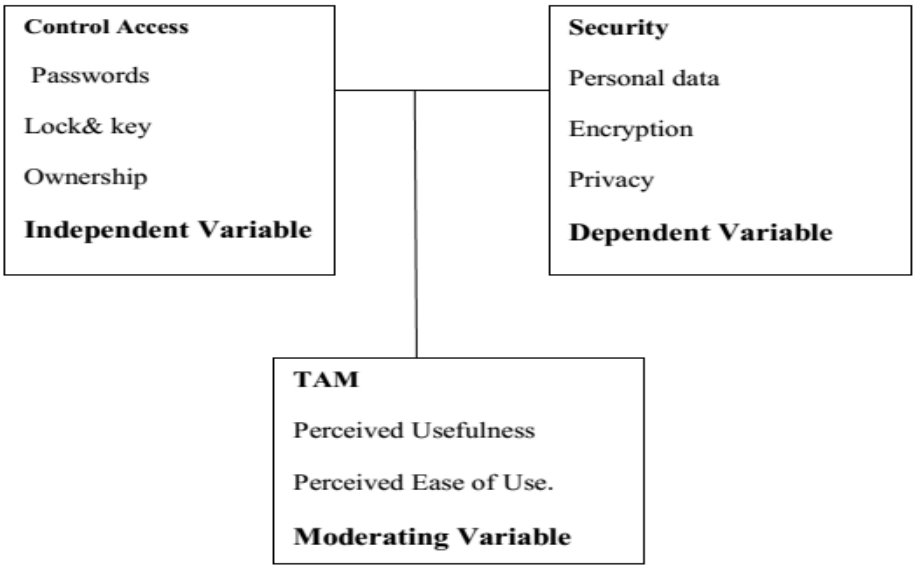

Figure 3: Conceptual Framework.

The above figure 3 shows the relationship between the independent variable and dependent variable and how they are related to the technology acceptance model which is TAM. Under independent variable we have attributes such as passwords, lock and key and ownership. Below is a brief explanation of the above mentioned attributes.

Passwords-Password is information associated with an entity that confirms the entity's identity. This is an example of authentication mechanism based on what the people know. The user supplies a password, and the computer validates it. If the password is one associated with the user's identity, the identity is authenticated. If not the password is rejected and authentication fails. The main disadvantage of password is that they can be stolen and forgotten.

Lock and Key-This is the physical way of protecting information inside a room from unauthorized access. In the middle ages castles and fortress were building to protect the people and the valuable properties inside (Pfleeger and Pfleeger

2007). This traditional way of providing security was characterized by strong gate or door to repel invaders; heavy walls to withstand objects thrown or projected against them; surrounding moats, to control access; arrow slit to let arches shoot approaching enemies; crenulations to allow inhabitants to lean out from the root and pour hot or vile liquids on attackers; draw bridge to limit access to authorized people; and gatekeepers to verify that only authorized people and goods could enter (Abanti, 2009).

Ownership-Determining ownership in an organization involves determining who has certain rights and duties over some information. The dependant variable attributes such as personal data; Encryption and privacy. They are as described below;

Encryption-Encryption is the process of changing information in such a way as to make it unreadable by anyone except those possessing special knowledge (usually referred to as a "key") that allows them to change the information back to its original, readable form. Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Businesses use it to protect corporate secrets, governments' use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.

Privacy.-Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed (William Stallings 5th edition). The employees working at the sacco should therefore keep high privacy of customer information and avoid revealing account details such as account balance to other people.

Personal Data-This refers to the customer information and it should therefore be highly secured from unauthorized access to avoid tampering with it to guard it against things like identity theft.

The technology model TAM is associated with two attributes; PU and PEOU which means; Perceived usefulness **(PU)** is the degree to which an individual believes that using a particular system will enhance his/her performance while Perceived ease of use (PEOU) is the degree to which an individual believes that using a particular system would be free of physical and mental effort. The next chapter describes the methodology the researcher used in achieving the objectives

III. Research Methodology

The researcher adopted open ended, multiple choice and declarative questions and used tables, graphs, and charts to analyze and present findings from where conclusions and recommendations were drawn. The researcher targeted the employees who were the users of the, system administrators and management of Wakenya Pamoja Sacco. In the targeted group, the researcher had questionnaires for the employees at the clerical level, middle management level and top management level.

IV. Result Presentation, Analysis and Discussion.

Descriptive statistical analysis was used to identify frequencies and percentages to answer all of the questions in the questionnaire. Questionnaires were used as data collection instruments and employees, management, and the database administrators were targeted for the study. The research was done on both the independent and dependent variable and the turnout was100%. Questionnaires helped the researcher to collect data on the variables for later analysis.

According to Turban *et al*, (2009), access control is the restriction of unauthorized user to access to a portion of a computerized user or to the entire system. The researcher investigated the relevant of the attributes of access control and results represented as follows. Question 5 in the questionnaire wanted to know if there was any access control mechanism in their current system. The response is as shown in Figure 8.

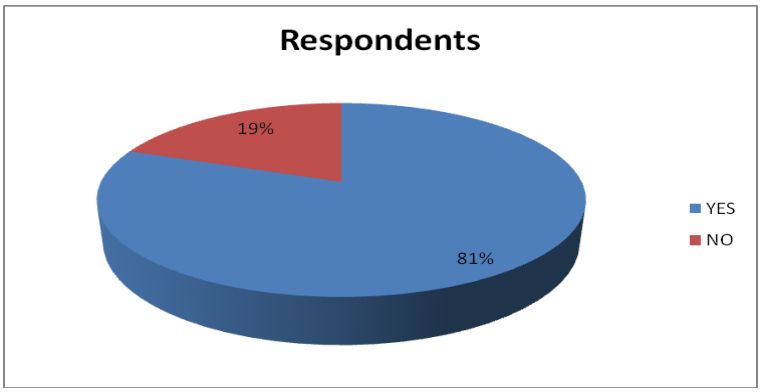

Figure 8: Presence of Access Control Mechanism

Figure 5 shows that 81% response accepted the existence of access control mechanism while13% disagreed. This meant that there was an access control mechanism in place.

In question 6 of the questi**o**nnaire, the researcher wanted to know the way various respondents rated the available access control mechanism i.e very weak, weak, strong, and very strong. The response is as shown in figure 9.

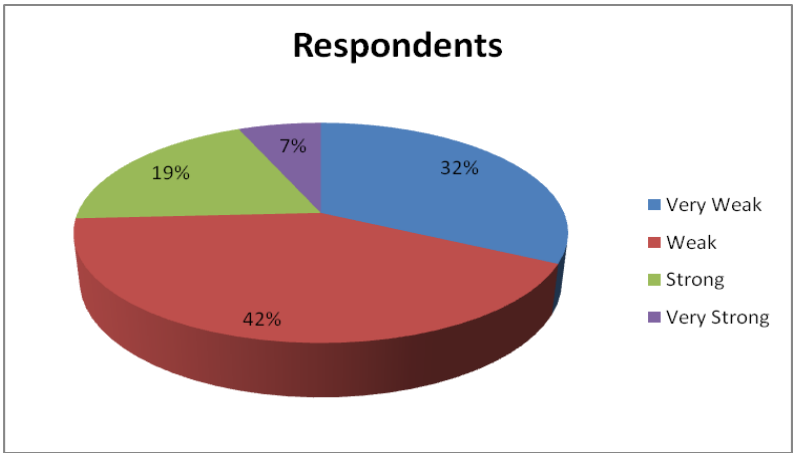

Figure 9: Measure of the Presence of Access Control Mechanism.

From figure 6 it showed that most of the respondents were not satisfied with the available access control mechanism in place because74% of them agreed that the mechanism weak

hence the need to enhance / improve the mechanism as seen in the table 1 below.

Table 2: Respondent's on the Need for Improvement

Respondents	Number
Yes	23
No	5
Undecided	5
Total	31

Table 1 showed that most of the respondents were for improvement of the available access control mechanism which had the largest percentage and this is shown in the figure 10.

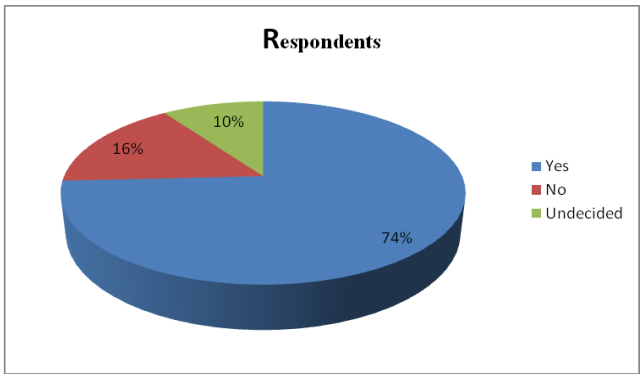

Figure10: Respondents' on the Need for Enhancement.

In figure 7, 74% responded positively indicating that there is a strong need of improving the available access control mechanism while 16% were against improvement according to them they were satisfied with the current security of their system and 10% were those who were undecided as this showed that they were not sure of either the current access control and the enhancement of the same.

In question eight of the questionnaire the researcher was interested in finding out which access control mechanism was the most appropriate to be implemented in their system and they included discretionary access control, Mandatory access control, Role based access control and Access control lists. The respondents gave the following responses as shown in figure 11.

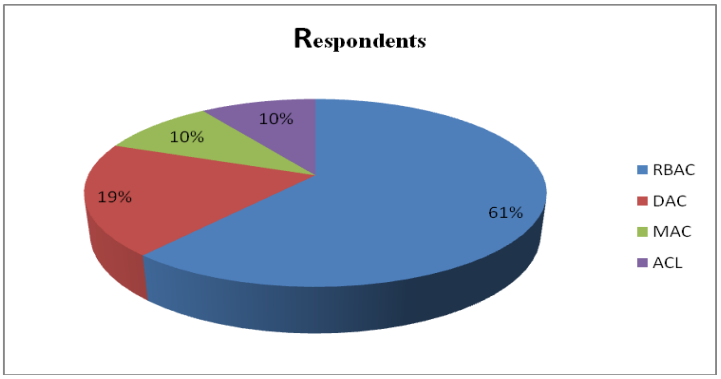

Figure11: Measure on the Appropriate Access Control Mechanism.

Figure 11 illustrated that most of the respondents preferred the Role Based Access Control mechanism which had 61% compared to others. This is because in this model the access to a resource is governed based on the role that the subject holds within an organization. RBAC enables the user to inherit privileges that are tied to his/her role. The user does not have a control over the role that he/she will be assigned. This meant those who will be given the rights to access their system will have their roles tied unto them thus restricting unauthorized access.

In contrast to DAC or MAC systems, where users have access to objects based on their own and the object's permissions, users in a Role-based Access Control (RBAC) system must be members of the appropriate group, or Role, before they can interact with files, directories, devices. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

The researcher here wanted to investigate the security issues on customer data and the results are summerized in table 2.

Table 3: Main causes of insecurities

Security issues	Frequency
Unauthorized change of passwords and usernames	15
User error	8
Staff misuse	4
Theft(hardware or software	3
TOTAL	**31**

Table 3 showed that organization was experiencing unauthorized change of passwords and usernames which had the largest percentage and this is shown in the figure below

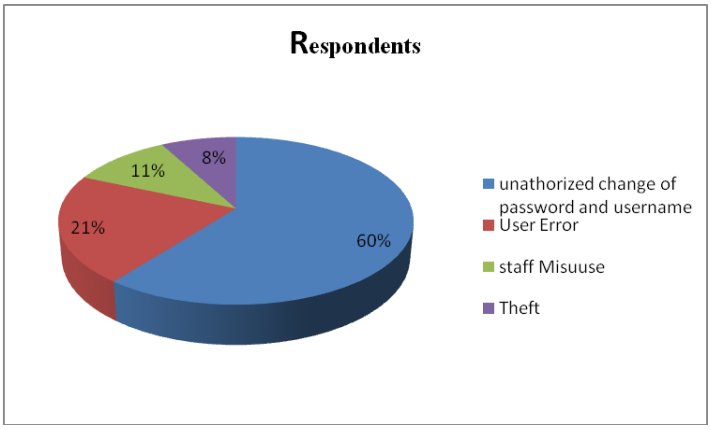

Figure 12: Measure on Security Issues.

In figure 12 most of the respondents related the insecurities with the following breaches as shown in the table 2 which indicated that most of their system is experiencing unauthorized change of passwords and usernames which had the largest percentage and this is shown in figure9 this is because the usernames and passwords were not changed by the database administrator from time to time thus if unauthorized user knew the password he/she could log into the system without permission thus tampering with important records of customers.

The researcher also realized that the organization has not put in place policies that deter unauthorized access which amounted to 74%. This is shown through the way the respondents answered question 13 of the questionnaire. From the figure it was then concluded that the organization needed policies and strategies to be put in place so as to bar off any form of unauthorized access. Strategies of enhancing relevant skills for those responsible in managing access to the system needed to be implemented.

Table 3 shows response on the mediating variable TAM and the two variables which were Perceived Ease of Use and Perceived usefulness. Here the researcher wanted to know if the respondents knew PU has positive effect on user attitude and if PEOU has positive effect on user adaptation. The response was summarized as shown below.

Table 4: Respondents' on Technology Acceptance Model.

TAM		**Response**		
Mediating	**Elements**	**Yes**	**No**	**Not Sure**
Perceived Usefulness	Positive effect on user attitude	20	5	6
Perceived Ease Of Use	Positive effect on user adaptation	18	10	3

A scale of 1 to 3 was used (1=Yes, 2=No, 3=Don't Know). From table 3 20 respondents were for yes which wanted to know if PU has positive effect on user attitude and this meant that users believed that using a particular system will enhance their performance while again majority were for PEOU which also was testing if perceived ease of use has positive effect on user adaptation and the response was yes giving a clear indication that using a particular system would be free of physical and mental effort hence user adaptation would be very easy.

According to George(2012), analysis is the process of evaluating data using analytical and logical reasoning to examine each component of the data provided. This form of analysis is just one of the many steps that must be completed when conducting a research experiment. Data from various sources is gathered, reviewed, and then analyzed to form some sort of finding or conclusion. The research was analyzed according to the objectives of the study as discussed below. According to the respondents unauthorized change of password and usernames was the most common security breach that their systems experienced amounting to 60% as seen in figure 9 above. This is because the usernames and passwords were not changed by the database administrator from time to time thus if unauthorized user knew the password he/she could log into the system without permission thus tampering with important records of customers. As shown in figure 10 this security breach amounted to 21%. This occurred as a result of users imposing different errors on the system sometimes without their consent or knowledge thus tampering with important records of the customer data.

This breach consisted of 11% and it was caused by the various staff members who logged into the system without having access rights hence tampering with crucial information. This amounted to 8% and it included both the staff and intruders thieving different parts of the computer hence tampering with the processing of information.

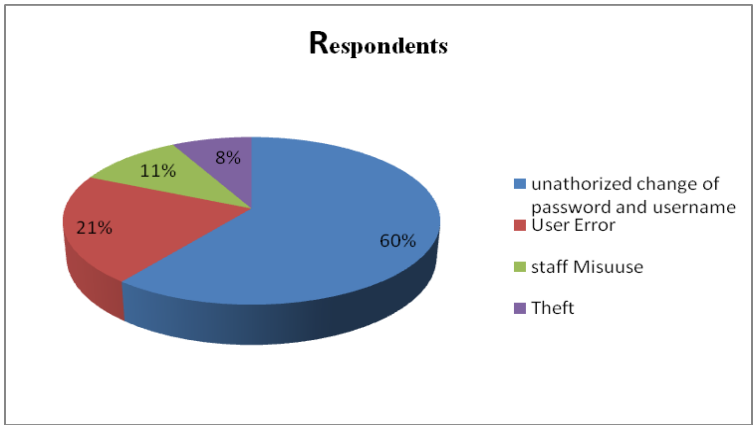

Figure 12: Measure on Security Issues.

Figure 9 above summarizes all the information on security issues on customer information as gathered from the respondents. This research study purposively adopted the Technological Acceptance Model (TAM) as described by Davis (1985). However not all variables did the researcher major in, she only looked at two and these are Perceived Usefulness (PU) and Perceived Ease of Use

Perceived usefulness was as the degree to which an individual believes that using a particular system will enhance his/her performance while Perceived ease of use is the degree to which an individual believes that using a particular system would be free of physical and mental effort(Gilbert 2012). In table 3 above majority of 20 respondents agreed that perceived usefulness has positive effect on user adaptation and also 18 of them agreed that perceived ease of use has positive effect on user adaptation.

V. Discussion

Based on the data collected and analyzed in this study, the researcher arrived at some conclusions reflecting the objectives of the study. According to Turban *et al*,(2009) defined access control as the restriction of unauthorized user to access to a portion of a computerized user or to the entire system.

From the questionnaire that was distributed it was evident that most of the respondents were not satisfied with the available access control it was found that 74% agreed that the mechanism was weak hence the need to enhance it while 16% were against the improvement since they said they were comfortable with it and the other 10% were undecided.

Since the main objective was to investigate how enhanced access control will secure customer information one way was to find out how to improve the available access control of which they use passwords and is discussed as below;If users are not allowed to generate their own passwords, they cannot pick easy-to-guess passwords. Some generators create only pronounceable non-words to help users remember them. However, users tend to write down hard-to remember passwords. Many operating systems can be configured to lock a user ID after a set number of failed log-in attempts. This helps to prevent guessing of passwords.

Users can be instructed, or the system can force them, to select passwords with a certain minimum length, with special characters, that are unrelated to their user ID, or to pick passwords which are not in an on-line dictionary. This makes passwords more difficult to guess.Periodic changing of passwords can reduce the damage done by stolen passwords and can make brute-force attempts to break into systems more difficult. Too frequent changes, however, can be irritating to users.

Information Security (InfoSec)) has become increasingly important in an era in which information is recognized as a key asset by many organizations. The number and severity of security breaches grows. In 2007, the TJX Company lost, according to different sources, from 36.2 to 94 million customers' credit and debit cards records (Shaw, 2010). In 2011, Sony reported a data breach that had resulted in the loss of personal information of 77 million customers (Sony, 2011). According to the *Information Security Breaches Survey 2010* (PwC, 2010), the number of large companies in the UK that suffered a security incident during 2010 increased up to 92%, in comparison to 72% in 2008. As a result, the spending on security is expected to grow from $55 billion in 2011 to $86 billion in 2016 (Gartner, 2012).

It was therefore concluded that Organizations should pay increasing more attention to information protection because the impact of security breaches today has a more tangible, often devastating effect on business. To enhance information security, the research proposes a regular system audit to be done by trained personnel. The research also suggested that all employees should be made aware of security threats and their potential risks through the provision of Incident Response Plan (IRP) manual and quarterly appraisals relating to cyber intelligence and computer forensics.

VI. Model Development

Constructs Reliability-In reference to Wikipedia Reliability is the overall consistency of a measure. A measure is said to have a high reliability if it produces similar results under consistent conditions. Construct reliability measures the internal consistency of a set of measures rather than the reliability of a single variable. It captures the degree to which a set of measures indicate the common latent construct (Abanti, 2014)

The model under study entailed ten latent variables and three study variables which were modeled using LISREL software. From the ten latent variables of this four were independent constructs, four dependent constructs and two moderating constructs. Two of the dependent constructs (scale RATEACC (0.59), and scale APPROPRI (0.54)) have Structural Equation Modeling (SMC) that exceeds 0.5. Also one moderating construct (usefulness (0.98)) also had SMC exceeding 0.5. In the path diagrams, squares represent observed used to imply a variable and circles represent the latent concepts. Single-headed arrows are direction of assumed causal influence, and double-headed arrows are used to represent covariance between two latent variables.

Model Estimation-The model under study entailed ten latent variables with three study variables namely latent independent variables, latent mediating variables and latent dependent variables. A latent variable is an unobserved construct composed of multiple survey items, or indicators (Raafat *et al*. 2007; Morton, 2008).These variables were modeled using LISREL software. First both dependent and dependent latent variables were modeled with the corresponding attributes to confirm whether there existed a relationship.

The hypothesized conceptual path model showed that there existed a direct relationship between access control and two of its attributes. The attributes RATE and APPROPI had direct relationship with dependent latent variable (Data Control model).When the conceptual path model was analyzed using LISREL software, some of the hypothesized relationships were proved to converge while others not converging. Those latent variables whose path model failed to converge were excluded from the final model.

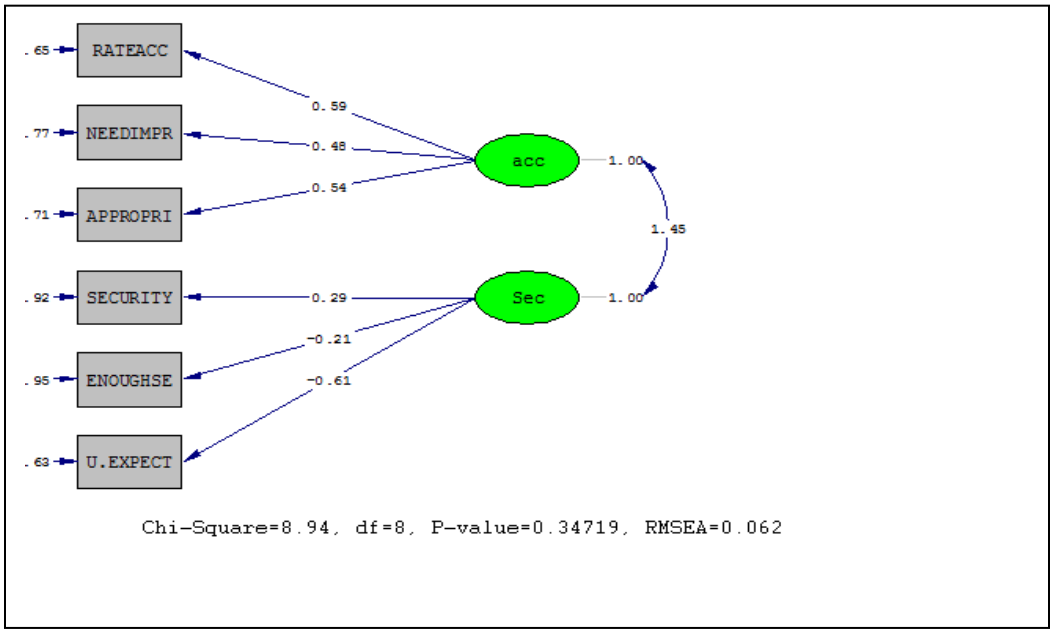

Figure 14: Path Model

Figure 14 was out to taste if there existed a relationship between the independent variable and dependant variable and results presented as discussed above.

The next latent and mediating variables that were modeled (Figure 14) were TAM, Access control and security. One of the two major constructs in TAM, perceived ease of use is often studied in technology acceptance constructs. Defined as the degree to which a person believes that using particular system would be free of effort. The perceived ease of use is hypothesized to have a significant direct relationship on security and access control as seen in figure11. Therefore between two systems that are meant to perform the identical set of finding, a user should find the one that is easier to use more useful. Some of the hypothesized relationships were proved to converge while others not converging. Those latent variables whose path model failed to converge were excluded from the final model.

Those that didn't converge included appropri, enoughsec, sec.priv, and Policies values at the level below 0.05, implying that they don't fit well in the model. The final model that was developed included three latent variables that are dependent variable, independent variable and PU. This model illustrates the relationship between Data control and security access of customer Information and this is moderated by PU. The model was called Security Data Access Model (SEDAC) model

VII. Conclusion

The research concludes that for a state of access control to said to be safe is when no permission can be leaked to an unauthorized or uninvited principal therefore to assure the safety of an access control system, it is essential to make certain that the access control configuration such as access control model will not result in the leakage of permissions to an unauthorized principal hence secure customer information. The SEDAC model developed was with the objective of securing customer information and adoption by the end users which will be used as a guide to enlighten the novice worker who constitutes a large number of the work force in any organization.

References

[1] Abanti. C (2009). Integration of Biometrics with Cryptographic Techniques for Secure Authentication of Networked Data Access.

[2] Ann et al,(2007). Principles of Computer security.

[3] Calvasina, G. E., Calvasina, R. V. & Calvasina, E. J. (2007). Preventing employee identity fraud.

[4] Charlie Kaufman (2nd edition) Network security.

[5] Charles P. Pfleeger and Shari Lawrence Pfleeger (4thed) (2007). Security in Computing. Pearson

[6] Education.

[7] Davis F. D. (1986). Perceived Usefulness, Perceived Ease of Use and User Acceptance

[8] Gramm-Leach-Bliley Act (2011) Protecting Customer's Personal Data

[9] Gasser (2010) .Building a secure computer system

[10] Gartner (2012) Security Breaches- Security Growth Expenses

[11] Gilbert Maiga and Elizabeth Asianzu,(2012), The Perspective of the Technology Acceptance.

[12] George (2012), Analysis in Statistics.

[13] Goldwasser, J., & Anderson, T. M. (2007). Passwords+ pictures = security? Kiplinger's,June,

[14] Gregory, A. (2008). Conserving customer value: Improving data security measures.

[15] G.S. Raafat, N. Fassil & T. Weiwei (2007), "Viability of the Technology Acceptance Model in

[16] Multimedia Learning Environments: A Comparative Study", Interdisciplinary Journal of Knowledge and Learning Objects, Pp. 175–184

[17] Harriet (2011). Passwords authentication.

[18] Lee, kozar, &Larsen (2013).Technology acceptance models

[19] Matt (2004). Computer Security Art and Science. Pearson Education. India.

[20] Morton M.E (2008), "Use and Acceptance of an Electronic Health Record: Factors Affecting

[21] Physician Attitudes", PhD Thesis. Drexel University

[22] Pfleeger, C. (2007) .Security in Computing. Prentice Hall
[23] PwC (2010) Information Security Breaches Survey
[24] Schultz and selvin (1975, Perceived Usefulness, Perceived Ease of Use.
[25] Steven (2008). Access control configuration of rights and permissions.
[26] Tayloy (2008). IT Security in computer systems.
[27] Turban et al (2009). Access control and information security.
[28] Turban E. et al, (2011). Business Intelligence.
[29] William Stallings (2011). Cryptography and Network security Principles and practice.
[30] Wilson, James M. (2008). Gantt charts: A centenary appreciation.
[31] Wilson Mizne (2013). Access control as a center of gravity in computer security.

AUTHORS

First Author – Abanti Cyrus is lecturer at Jomo Kenyatta University of Agriculture and Technology [JKUAT]. His area of interest is health informatics, biometric technologies, Information Systems Security, Design and Analysis of Algorithms. He is currently associate chairman Information Technology and Mathematics JKUAT Kisii CBD Campus. He has completed his PhD Research Information Technology, supervised by Prof Miph and Dr Maiga from Nkumba University.

Second Author – Ogega Caroline Nyasengo is Information Technology student at Jomo Kenyatta University of Agriculture and Technology. Her research interest is on the Access control, Information Systems Management, Programming, Modelling and Systems Security. Her research work was supervised by Abanti Cyrus.