Assessment Of User Authentication Risks In A Healthcare Knowledge Management System

Oluwole Adekanmbi, Durban University of Technology, South Africa
Paul Green, Durban University of Technology, South Africa

ABSTRACT

Risk management is a concept which has becomes very popular with a number of national and international businesses. Many companies often establish a risk management procedure in their projects for improving performance and increasing profits. Projects undertaken in the construction sector are widely complex, often having significant budgets; therefore, reducing risks associated with projects should be a priority for each project manager. Patient information security has become a matter of interest to healthcare professionals, governments and researchers worldwide.

This paper proposes a comprehensive risk assessment methodology that provides a decision support tool, directed to a healthcare system, which can be utilized for evaluating risk involved during user authorization and authentication procedures. Within this context, a process technique was implemented to develop a risk assessment model, which is used to derive the relative priorities of the risk factors associated with a healthcare knowledge management system. The study showed risks involved when users are accessing a healthcare system. It proposes a model for assessing each risk occurring during the user authorization and authentication process. The results of the knowledge generated from the risk assessment provide a basis for deriving a system performance that is desirable for evaluating risk.

Keywords: Assessment; Healthcare; Knowledge; Management; Risk, Knowledge Management Systems

1. INTRODUCTION

Information security is important to organizations. This is most common in a healthcare system where patient records and information are considered very sensitive. Patients are the most important actors in a healthcare system and, as a result, patients' record information should be kept secured from breaches (Ward and Chapman, 2003). Simultaneously, the information must be available when needed in order to provide patients with the best care. The accessibility and availability of information has become imperative as the healthcare system moves toward an environment where patients can obtain care from various healthcare providers in cross-border healthcare systems (Smith et al., 2013). Several researches have been conducted in the last decade to evaluate the severity, prevalence and causes of a large variety of adverse events in hospitals, as well as the efficiency of several methods used to reduce adverse events and risks.

Risk is a multi-faceted concept that has substantial impact on knowledge management projects' performances in terms of quality, time and cost. Once a knowledge management project becomes more complex, the ability to manage potential risk through the healthcare process will become a crucial section for averting unwanted threats. According to Bergman et al. (2011), the five main processes in a healthcare system are identified as: 1) diagnosing diseases, 2) detecting health problems, 3) treating diseases, 4) keeping healthy, and 5) providing for a good end of life. Knowledge management in a healthcare system involves optimization of information by processing data and technology, collaboration of experience and expertise to achieve organizational optimal growth and performance (Alavi and Leidner, 2001; Gold et al., 2001).

The success of a healthcare system depends on three essential processes: 1) collection and analysis of data, 2) continuous exchange of billing, clinical information, and 3) utilization of the information. The vast and ever-growing amount of information and knowledge, both public and proprietary, has made it imperative that organizations, especially those in a competitive environment, make highly efficient use of their existing knowledge and information base. This has resulted in a huge demand for automated processes and systems that can manage these challenges. This, in turn, has fueled the explosive growth of the field of knowledge management. Patient records are critical factors in healthcare, possibly even the most vital information to be secured in a healthcare system (The Royal Society, 2006). Dwivedi et al. (2003) argue that electronic patient information will be the norm in the future. The claim is validated by the fact that several governments and health organizations worldwide have set up similar schemes, with the goal of providing patient information in electronic format.

2. LITERATURE REVIEW

2.1. Knowledge Management

Knowledge Management is a fast-rising discipline bridging several fields of research, including computer science, economics, education, philosophy, management, information and technology, psychology, and business. Knowledge management is a subject field of several literature, planning, discussion and action. Scholars and practitioners in various fields have turned their attention to knowledge management systems as a means of sharing knowledge in organizations. As a result, there is no general definition for knowledge management as there is no general acceptance of what knowledge consists of. In large, knowledge management can be defined as a multi-disciplined approach to improving, evaluating, collecting, integrating, cataloguing, and generating value from the organization's knowledge-based asset (Alavi and Leidner, 2001). According to Holsapple (2004), it can be considered as a process of acquiring, capturing, creating, sharing and utilizing the knowledge to achieve organizational capability. The increasing amount of knowledge and information, both proprietary and public, has made it essential that competitive organizations make effective use of their information and knowledge base (Perez-Araos et al., 2007). The huge demand for automated systems and processes to manage difficult challenges has resulted in the enormous growth of the knowledge management field.

The concept of information technology allowed knowledge management to suffer from the unreliability in enforcing the traditional technique of processing information on the strategic needs of present-day organizations. The traditional knowledge management model accentuates compliance and convergence to achieve the predefined organizational objectives (Gupta et al., 2000). Knowledge management systems were modelled on the same standard to ensure adherence to organizational processes developed into information technology. Several companies are becoming conscious of the fact that they are suffering from "information overload" and "excess duplicating data" as a result of necessities to maintain and gather data. As a result of the information overload and excess accumulation of data, information is not easily accessible for decision-making and analysis. Recently, an explosion of interest, writing, research and application of knowledge management occurred to solve these challenges. New information is created, older information is extracted, and old information is made obsolete. Knowledge management provides techniques and methodologies to build up task-oriented services for solving strategic needs of different organizations. Knowledge management provides the means to achieve a designated function or task to address the knowledge gaps intrinsically within the distribution process. Knowledge management offers a wide spectrum of services that cover the knowledge needs for the entire continuum of a delivery process. It is essential to emphasize that data-driven activities provided by knowledge management systems are predicated on the effectiveness of knowledge management services (Ahmad et al., 2007); as such, enabling knowledge management services can be viewed as providing the 'knowledge platform' to develop high-level services. Therefore, the design of an efficient knowledge management service needs to incorporate four interacting dimensions (as shown in Figure 1); namely, Knowledge, Technology, Workflow, and Stakeholder stipulations for service needs and usage preferences.

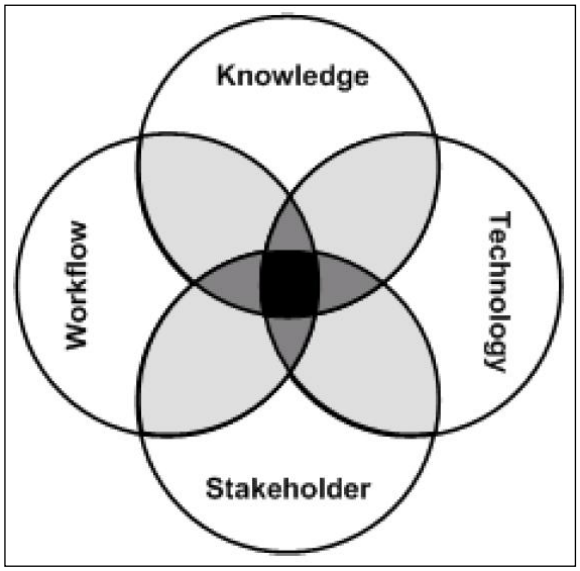

Figure 1: The Four Design Dimensions Of Knowledge Management Services

2.2. Knowledge Management System

The term "knowledge management system" (KMS) has been used in different meanings through the literature. In knowledge management literature, the terms knowledge management system and knowledge systems are used interchangeably to refer to the technology or software components of knowledge management (Raftery, 2003). For example, Alavi and Leidner (2001) define knowledge as "IT-based systems developed to support and enhance the organizational processes of knowledge creation, storage/retrieval, transfer, and application". Furthermore, Gupta et al. (2000) define it as "A class of information systems applied to managing organizational knowledge". Knowledge management systems help organizations to select, find, disseminate, organize and transfer vital information and expertise necessary for activities such as dynamic learning, decision-making, problem-solving, and strategic planning. However, other researchers have expanded those definitions by incorporating strategy, services, processes, and user components to the KMS, not just the IT components (Haimes, 2005). So, the terms of KMS and knowledge system in this research are used to refer to the technological and/or non-technological components of knowledge management that may include knowledge management software, hardware, networks, individuals, groups, organizations, resources, tools, services, activities, procedures, methods and other environmental factors and activities that may compose, relate to or affect knowledge management in an organization. Readers interested in knowledge management systems should refer to the text by Gupta et al. (2000), Copperman et al. (2004) and King and Marks, Jr. (2008).

2.3. Risk Management

Recently, knowledge security experts have used risk analysis and assessment methods to identify and categorise the level of security to be implemented. Security has to provide sufficient bulwark and be practicable to implement. Before designing information security for a system, it is imperative to know how risks in organizations are perceived. As a result, risk perception becomes vital to implementing and designing security techniques in a knowledge management system. Several definitions and explanations of risks and risk management have been recently developed. As a result, there is no universal definition of risk management as there is no universal acceptance of what risk consists of. Each author provides his own definition of what risk means and his perception of risk management. The perception depends on the type of business, project and profession (Samson et al., 2009).

Risk management generally is a very comprehensive subject of many literatures. In this paper, one definition of risk and risk management is selected so as to possess a clear understanding of the concepts in the healthcare sector. Miller and Lessard (2001) define risk as "an uncertain event or condition that, if it occurs, has a

positive or negative effect on a project's objectives". Ward and Chapman (2003) extensively discuss the concept of risk and suggest using a more universal concept for explaining risk uncertainty. They argue that the term 'risk' is often associated with adversity and focuses on threats, not opportunities. As shown in Figure 2, risk management encompasses three processes: 1) risk identification, 2) analysis or assessment, and 3) risk evaluation.

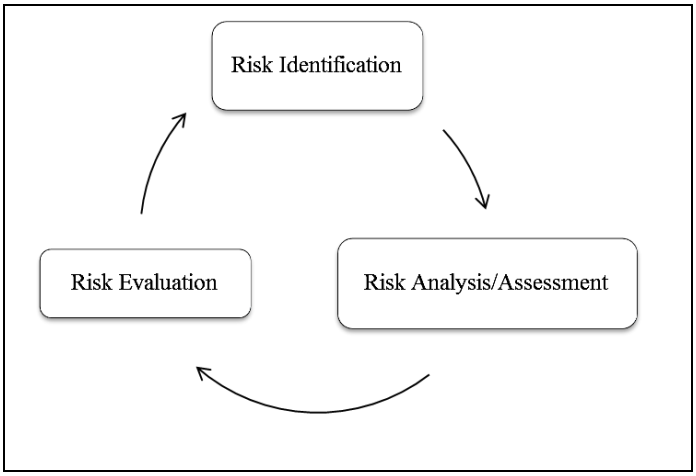

Figure 2: Risk Management Process Lifecycle

2.3.1. Risk Identification

Risk identification analyses the knowledge management system to detect information security risk and its source. It identifies security risk that occurs during an organization's daily operation by employing several information-gathering methods such as interviews and brainstorming (Raftery, 2003; Vose, 2008). Preferably, this phase should incorporate vulnerability and threat analysis of each asset and develop an accurate profile of the assets' feasible attacks and their medium (Visintine, 2003; Haimes, 2005). Vulnerability is defined as the exploitation of the intrinsic weakness in a knowledge asset (Peltier, 2005), while a threat is defined as any element that can exploit that asset - for example, viruses, human errors and hacking (Visintine, 2003). The outcome of this phase is to obtain a list of feasible threats to knowledge assets of the organization provided that the vulnerabilities in the knowledge asset are identified and control methodologies are in place.

2.3.2. Risk Assessment

Risk assessment is the process by which the vulnerabilities and threats are assessed in terms of likelihood and consequence (Peltier, 2005). Risk Identification produces a list of potential threats, but not all of these threats deserve or require attention. Some are inconsequential and therefore can be overlooked, while others present severe consequence to the welfare of a knowledge management system. Range analysis, scenario analysis, probability analysis, hybrid analysis and failure mode and effect analysis are the techniques utilized in assessing risk. Risk analysis or assessment can be quantitative, semi-quantitative, or qualitative (Nikolic and Ruzic-Dimitrijevic, 2009).

In quantitative approach, numerical values are assigned to both likelihood and impact of threat. The quantitative measure of threat computed by using a statistical model is utilized to estimate the acceptability of the threat. Quantitative approach employs a metric representation of the threat to determine the risk level – "critical", "high", "medium" and "low". The threat impacts are assigned with values of 1.00 – critical, 0.75 – high, 0.50 – medium, and 0.25- low. The likelihood of occurrence of the threat is categorized into "almost certain", "likely", "moderate", and "unlikely" with the following assigned: 100 – almost certain, 75 – likely, 50 – moderate and 25 – unlikely. The risk level can be calculated by multiplying the assigned values of the threat impact with the assigned values of the threat likelihood, thereby forming a 4×4 risk-level matrix as shown in Table 1. Risk scale is presented as Critical (>75 to 100), High (>50 to 75), Medium (>10 to 50), and Low (1 to 25).

Table 1: Risk-Level Matrix

Threat Likelihood	**Threat Impact**			
	Low (0.25)	Medium (0.50)	High (0.75)	Critical (1.00)
Unlikely (25)	Low (6.25)	Low (12.50)	Low (18.75)	Low (25.00)
Moderate (50)	Low (12.50)	Low (25.00)	Medium (37.50)	Medium (50.00)
Likely (75)	Low (18.75)	Medium (37.50)	High (56.25)	High (75.00)
Almost Certain (100)	Low (25.00)	Medium (50.00)	High (75.00)	Critical (100.00)

In semi-quantitative, the threats are classified in accordance to the probabilities and the consequence of their occurrence. The approach is predicated on the opinion of the people making an assessment (Nikolic and Ruzic-Dimitrijevic, 2009). In Qualitative approach, a detailed description of the likelihood of occurrence and consequence is provided. This approach is used in events where it is difficult to measure the threat or risk numerically (Nikolic and Ruzic-Dimitrijevic, 2009). The risk assessment methodology encompasses nine primary steps shown in Figure 3.

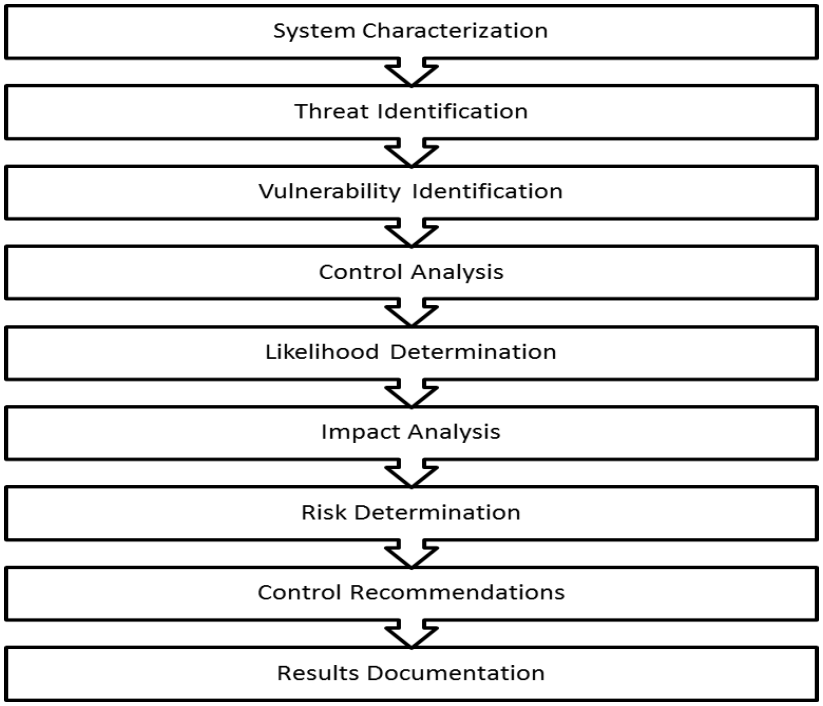

Figure 3: Risk Assessment Methodology

2.3.3. Risk Evaluation

Risk evaluation is the process by which the vulnerabilities and threats are evaluated by comparing the results of the risk assessment phase with the evaluation criteria. Organizations critically rate in order to prioritize the risk in terms of urgency; i.e., which risk deserves immediate attention, which risk can be overlooked, and which risk can be treated at a later date (King and Marks, Jr., 2008). As soon as this phase is completed, a new risk management process life cycle will occur.

3. METHODOLOGY

This section presents a comprehensive risk assessment methodology that provides a healthcare knowledge management system the ability to evaluate risk involved during user authorization and authentication procedures. The prototype system provides basic related functions such as capturing patient and doctor information, managing the information on the medical history of patients. Figure 4 presents the activity diagram for the overall process in the proposed healthcare system which is logically divided into three main sections; namely, 1) user authentication

and authorization section, 2) administrator section, and 3) user section. The user authentication and authorization section comprises of where the user authorization and authentication is put to test in order to ensure the safety and security of the system. The administrator section is made up of where the administrator registers new users and patients, performs the operation of assigning a doctor with a new patient and view of the patient to the assigned doctor. The administrator checks the update of every user and progress in the system. The user section comprises of where the doctor and nurses attend to existing and new patients. After the recognition and identification of risk in the system, assessment of the risk is an important issue to be discussed. In Nikolic and Ruzic-Dimitrijevic (2009), the impact of the risk was classified into five levels as shown in Table 2.

Table 2: Evaluation Of Risk Based On The Value Of The Risk

Risk Impact	Range
Negligible	Risk value = 0
Low but significant	0 < risk value < = 2.5
Moderate	2.5 < risk value <= 5.0
High	5.0 < risk value <= 7.5
High Unacceptable	7.5 < risk value <= 12.5

As stated in the literature, risk value can be calculated by multiplying the assigned values of the threat impact with the assigned values of the threat likelihood, but in this research, the formula was modified to have:

$$\text{Risk Value} = P \acute{} N \acute{} D$$

where P is the likelihood of occurrence, N is the number of times the risk occurs for a particular user, and D is the degree of the risk. The ease of accessing technology and the ability to interface the technology with statistical analysis software makes surveys a valuable research tool. The increasing use of surveys to gather information has led to work on benefits and limitations, incentives, and how to improve response rates. The performance of the risk assessment and implementation was evaluated by the distribution of the questionnaires. Participants' satisfaction on the risk assessment step involved in the healthcare system was measured using one statement ranked on a 5-point Likert scale, including excellent, very good, good, average, and poor. Using a multidimensional item to measure satisfaction was preferred over single satisfaction constructs in order to keep the survey concise. The 5-point Likert scale is shown in Table 3.

Table 3: Likert Scale

Likert Scale	Excellent	Very Good	Good	Average	Poor
Values	5.0	4.0	3.0	2.0	1.0

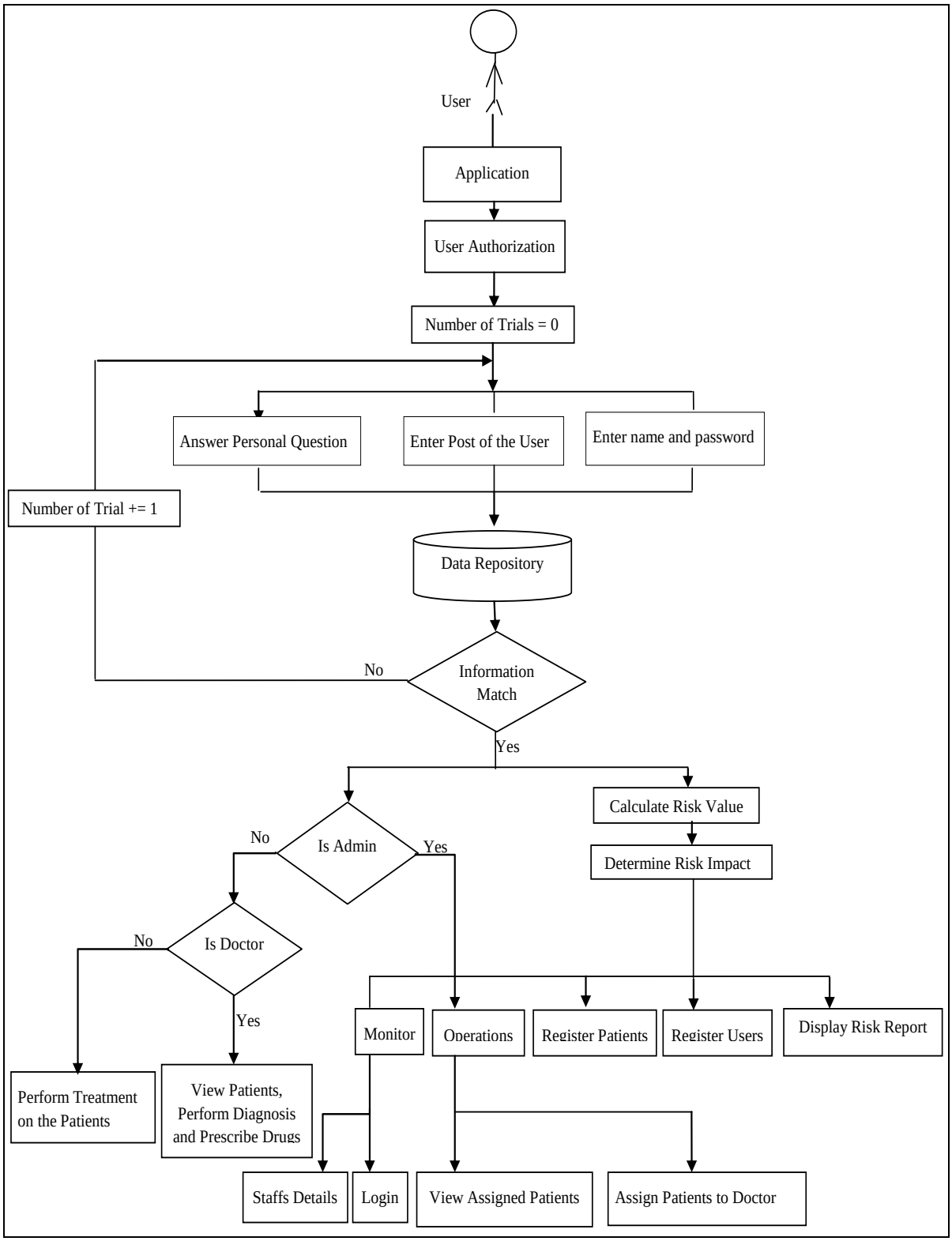

Figure 4: The Proposed Healthcare System Process Flow

Analysis of the quantitative data was performed using the SPSS statistical analysis package. Data were collected through the distribution of questionnaires. A total of 100 questionnaires was distributed, but 82 were administered, completed and received from staff at three different hospitals, where one is a private and public hospital. The responses were verified and validated by a follow-up with some interviews and all responses were manually entered into a spreadsheet. Relevant descriptive statistics and frequencies were calculated for the independent variables.

4. IMPLEMENTATION

In Figure 5, a user wants to access the system. The user identifies himself as the administrator, so he enters his username and password and then clicks on 'next'. Since the administrator has the right of access to view and perform updates or change some information in the system, the user is allowed to view and perform major operations in the system which are registering of user and patients, assigning of patients to doctors and monitoring the log in and detail of the user of the system.

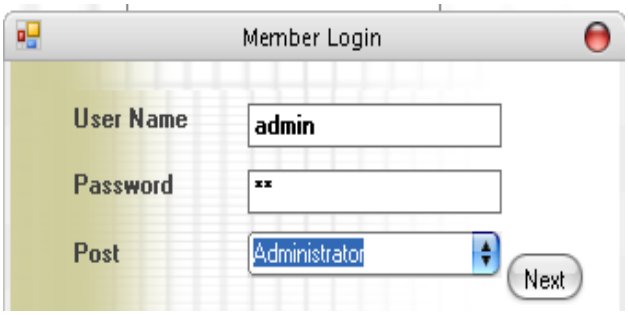

Figure 5: Login Form For Administrator

In Figure 6, a registered user tries to log in to the system and perform some operation. The user enters his username, password, selects the post being held in the system, and is required to answer a personal question to show more authentication and authorization.

Figure 6: Login Form For A Registered User

In Figure 7, the MonitorStaffDetails form enables the administrator to view and monitor the information of the user of the system, including the key characters in the system. The password of each user is encrypted and the administrators do not know the password of the user, except if it is decrypted.

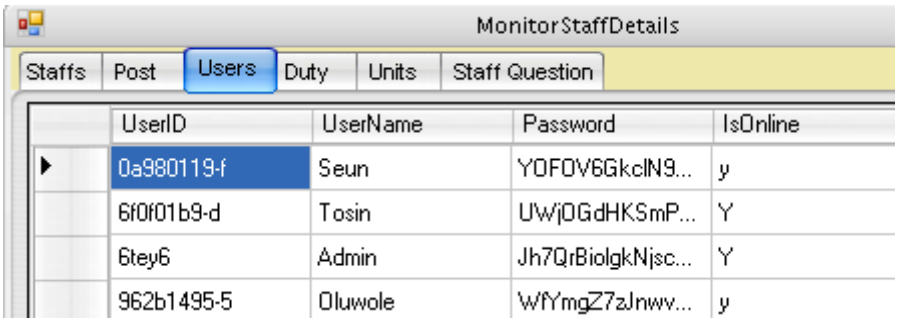

Figure 7: Monitor Staff Form

In Figure 8, the risk value and risk impact are displayed and viewed by the administrator to make some important changes and notification to the users whose information is accessed or to be corrupted. This form explains the main objective of the paper in which the risk was assessed using a risk assessment methodology.

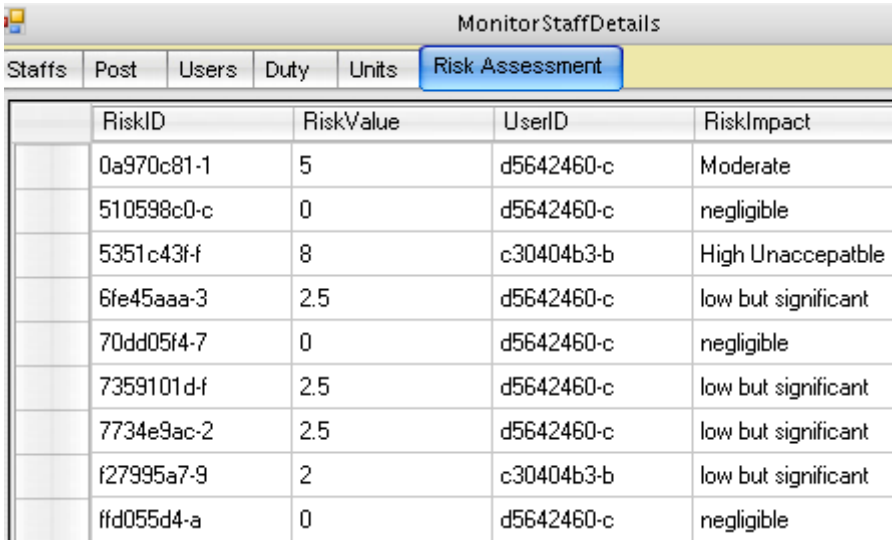

Figure 8: Risk Assessment Form

4.1. ANALYSIS OF RESULTS

The objective of this project is to evaluate the performance of risk assessment in a healthcare system. The statistics of the data collected is presented in Table 4 showing the valid percentage of a linguistic variable with respect to the risk assessment steps involved in the healthcare system.

Table 4: Performance Results Of The Implementation Of Risk Assessment In A Healthcare System

Risk Assessment Steps	**Valid Percent**				
	Excellent	**Very Good**	**Good**	**Average**	**Poor**
System Characterization	5.0	22.5	40.0	25.0	7.5
Threat Identification	0.0	25.0	45.0	22.5	7.5
Vulnerability Identification	2.5	27.5	45.0	12.5	12.5
Control Analysis	5.0	10.0	42.5	35.0	7.5
Likelihood Determination	2.5	27.5	37.5	20.0	12.5
Impact Analysis	0.0	20.0	55.0	25.0	0.0
Risk Determination	0.0	37.5	37.5	22.5	2.5
Control Recommendation	2.5	17.5	50.0	22.5	7.5
Results Documentation	5.0	17.5	50.0	22.5	5.0

In Figure 9, the Likert scale "Good" has the highest valid percent of the risk assessment steps. This implies that the implementation, in some way, was able to assess risk or threat and that this assessment can be rated to be of good performance.

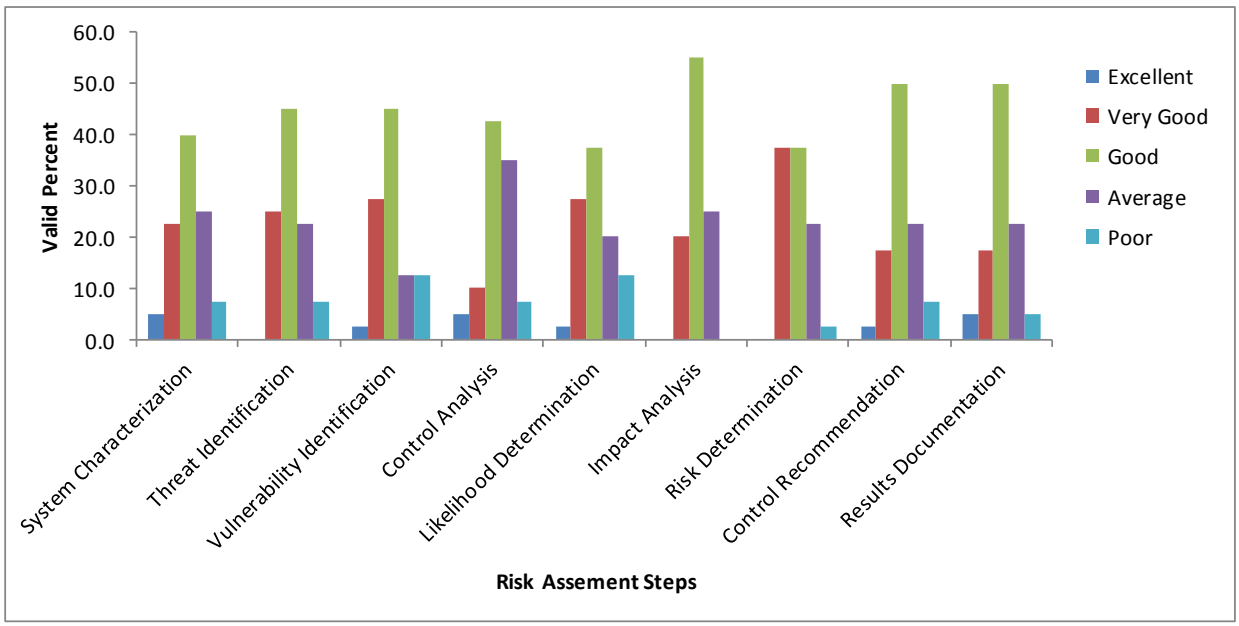

Figure 9: Performance Evaluation Histogram

5. CONCLUSION

The goal of the paper was to assess risk in a healthcare system - risk caused by malicious attackers who are trying to launch into a system. The attacker is the outsider and the target is the medial data of patients stored in the healthcare system. It is hard for a healthcare facility to protect against this sort of attack. Even a detailed management of access rights may be useless if there are underlying vulnerabilities. From the assessment point of view, the implementation of the risk shows that risk assessment in healthcare systems reduces the unauthorized user to have access to the system. The authors believe that if a risk assessment in a healthcare system is encouraged in all knowledge management systems, it has increased the identification and evaluation of threats, vulnerabilities and safety characteristics of the knowledge management system.

AUTHOR INFORMATION

Oluwole Adekanmbi received his BSc degree from the Department of Computer Science at the University of Agriculture in Abeokuta, Nigeria, in 2010. He completed his Master's Degree in Information Technology in 2014 from Durban University of Technology in South Africa. He is currently a lecturer at Durban University of Technology, Pietermaritzburg Campus in the Department of Finance & Information Management. His research interests include machine learning, neural networks, evolutionary algorithms, differential evolution, and applications of evolutionary algorithms, data mining and knowledge management. Email: adekanmbioluwole@gmail.com

Paul Green is a Senior Lecturer in the Faculty of Accounting & Informatics at the Durban University of Technology. He has a PhD from the University of KwaZulu-Natal. He has published in peer-reviewed journals and presented papers at international and national conferences. His research interests include Systems Thinking, Evaluation, Service Quality, and Universities of Technology.

REFERENCES

1. Ahmad, H. S., An, M., & Gaterell, M. (2007). Development of KM model to simplify knowledge management implementation in construction projects. *Management*, 515: 524.
2. Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*: 107-136.
3. Bergman, B., Neuhauser, D., & Provost, L. (2011). Five main processes in healthcare: a citizen perspective. *BMJ quality & safety*, 20 (Suppl 1): i41-i42.
4. Copperman, M., Angel, M., Rudy, J. H., Huffman, S. B., Kay, D. B., & Fratkina, R. (2004). *System and method for implementing a knowledge management system*. Google Patents.
5. Dwivedi, A., Bali, R. K., Belsis, M. A., Naguib, R. N. G., Every, P., & Nassar, N. S. (2003). Towards a practical healthcare information security model for healthcare institutions. In: Proceedings of *Information Technology Applications in Biomedicine, 2003. 4th International IEEE EMBS Special Topic Conference on.* IEEE, 114-117.
6. Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: an organizational capabilities perspective. *J. of Management Information Systems*, 18 (1): 185-214.
7. Gupta, B., Iyer, L. S., & Aronson, J. E. (2000). Knowledge management: practices and challenges. *Industrial Management & Data Systems*, 100 (1): 17-21.
8. Haimes, Y. Y. (2005). *Risk modeling, assessment, and management*. John Wiley & Sons.
9. Holsapple, C. (2004). *Handbook on knowledge management 1: Knowledge matters*. Springer.
10. King, W. R., & Marks, Jr., P. V. (2008). Motivating knowledge sharing through a knowledge management system. *Omega*, 36 (1): 131-146.
11. Miller, R., & Lessard, D. (2001). Understanding and managing risks in large engineering projects. *International Journal of Project Management*, 19 (8): 437-443.
12. Nikolic, B., & Ruzic-Dimitrijevic, L. (2009). Risk assessment of information technology Systems. *Issues in Informing Science & Information Technology*, 6.
13. Peltier, T. R. (2005). *Information security risk analysis*. CRC press.
14. Perez-Araos, A., Barber, K. D., Munive-Hernandez, J. E., & Eldridge, S. (2007). Designing a knowledge management tool to support knowledge sharing networks. *Journal of Manufacturing Technology Management*, 18 (2): 153-168.
15. Raftery, J. (2003). *Risk analysis in project management*. Routledge.
16. Samson, S., Reneke, J. A., & Wiecek, M. M. (2009). A review of different perspectives on uncertainty and risk and an alternative modeling paradigm. *Reliability Engineering & System Safety*, 94 (2): 558-567.
17. Smith, N. J., Merna, T., & Jobling, P. (2013). *Managing risk in construction projects*. John Wiley & Sons.
18. The Royal Society. (2006). *Digital healthcare: the impact of information and communication technologies on health and healthcare.* London, UK.
19. Visintine, V. (2003). An introduction to information risk assessment. *SANS institute*, 8.
20. Vose, D. (2008). *Risk analysis: a quantitative guide*. John Wiley & Sons.
21. Ward, S., & Chapman, C. (2003). Transforming project risk management into project uncertainty management. *International Journal of Project Management*, 21 (2): 97-105.

NOTES