Journal of Computer Science

Original Research Paper

Designing a Generic Information Systems Audit Framework to Improve the Quality of Audit in Higher Education

[1]Elfadil A. Mohamed, [2]Elgilani El. Elshareif and [3]Omer Ishag Eldai Mohamed

[1]Department of Information Technology,
College of Engineering and Information Technology, Ajman University, Ajman, UAE
[2]Faculty of Management, Canadian University, Dubai, UAE
[3]College of Computer Science and Engineering, University of Hafr Al-batin, Hafr Al-batin KSA

Article history
Received: 01-09-2018
Revised: 07-04-2019
Accepted: 09-05-2019

Corresponding Author:
Elfadil A. Mohamed
Department of Information Technology, College of Engineering and Information Technology, Ajman University, Ajman, UAE
Email: fadil_ali@yahoo.com

Abstract: There are some similarities between Financial Statement Audit (FSA) and Information Systems Audit (ISA). FSA is an examination of the reliability and integrity of financial statement records, whereas ISA is a review and evaluation of the controls, risks and system development within an information systems infrastructure to ensure that the safeguards protect against abuse, protect assets, maintain data integrity and operate effectively to achieve the organization's objectives. Decision makers need to ensure a reliable collection and evaluation of the evidence of an organization's information systems, practices and operations. Data manipulation can be caused by external or internal threat. Internal manipulation threat is the most dangerous because it is committed by authorized personnel, which makes it very difficult to detect. In particular, the framework introduces an anomaly detection technique, a data mining method, to determine if the suspected transactions arose from internal or external threats. Once the suspected transactions are identified, procedures and monitoring controls will be in place to minimize each threat. The proposed framework is expected to help university and ministry of higher education managers at all levels to make vital decisions based on reliable and accurate information.

Keywords: ISA Framework, Data Mining, Outlier Technique, Higher Education

Introduction

Most organizations and firms worldwide have replaced their manual systems with computerized ones in the form of information systems. These changes require close monitoring and auditing of the data generated by such systems.

Currently, higher education institutions such as universities and colleges are facing numerous challenges; for example, their information systems transactions have grown in volume and complexity. These institutions exist in a highly regulated environment. Therefore, there is a compelling need for controlling and monitoring mechanisms to evaluate and validate these transactions.

The data stored in information systems in higher education institutions is of paramount importance for both the institutions as well as the body represented by the ministry of higher education. Higher education institutions have to ensure the integrity of the data, which means the data must not be tampered with by external nor internal sources.

Auditing in financial accounting is concerned with the systematic verification of a company's or government unit's books of account transactions and it is conducted by external auditors. By contrast, Information Systems Auditing (ISA) must ensure that the data generated and stored by the information systems is safeguarded to protect against abuse, protect assets, maintain data integrity and allow the firms to continue successfully. ISA is more complex than financial auditing because the threats can come from either internal or external sources.

Authorities in the ministry of higher education have a greater role in monitoring and overseeing the activities of universities. They have to ensure that the data generated by information systems that relate to student marks, records and other personal information are accurate and

secure. Based on these requirements, there is strong need for ISA to guarantee the accuracy of the data provided by universities to the ministry of higher education.

A substantial body of research has already defined ISA. For example, Abdul Rahman *et al*. (2015) defined ISA as the assessment of various controls, risks and system developments within IS infrastructures.

The auditing process was originally manual but is now computer-based. Recently, the notion of Continuous Auditing (CA) was introduced as part of ISA, defined as a comprehensive electronic audit process that enables auditors to provide some degree of assurance on continuous information simultaneously with, or shortly after, the disclosure of that information (Rezaee *et al*., 2002).

Researchers have long pointed out the importance of Continuous Monitoring (CM) and auditing of information systems. To emphasize the importance of CA of organizational transactions, Marquesa *et al*. (2012) proposed a solution under a new vision for organizational auditing and monitoring. There is also increasing research on the applications of artificial intelligence in auditing. Kamil (2012) reviewed the main research efforts and current debates on auditors' uses of artificially-intelligent systems, with a view toward predicting future directions of research and software development in the area.

The authors believe that data mining, specifically outlier analysis, could be a viable approach to facilitate auditing in information systems by highlighting suspicious transactions. In the present study, we intend to address the two questions: (1) what are the most appropriate techniques to detect fraudulent transactions in university information registration systems? (2) More specifically, what are the main components that reflect a generic approach to ISA used by universities and the ministry of higher education?

The main purpose of this paper is to introduce a framework for auditing information systems in higher education. The framework aims to provide the ministry of higher education with a system to evaluate, monitor and validate university registration system transactions in a non- disturbing way. The proposed model is expected to help both university management and the ministry of higher education to conduct a systematic verification of the validity of stored information that pertains to students.

Literature Review

Non-traditional auditing tools have long been used in the audit of information systems. For instance, the use of expert systems to facilitate the ISA process is documented in Comyn-Wattiau and Akoka (1996).

It is understandable that most professional auditors lack expertise in Information Technology (IT) that would allow them to implement generalized audit software. To bridge the gap between information systems and professional auditors, Li *et al*. (2007) proposed a systematic analysis approach that provides a framework for auditors to understand business processes and the data flow/structures of information systems effectively. Axelsen *et al*. (2017) developed an explanation theory that addresses the role of the information systems auditor in the public sector in supporting the financial audit and outlines key determinants that affect that role.

With the vast proliferation of data stored in an electronic form, there is a compelling need to ensure its validity and reliability. ISA is a necessity for most organizations seeking to compete in the market. In recent years, extensive research in the realm of ISA has explored suitable means to ensure the reliability of stored data. For example, Kim *et al*. (2015) proposed a model to bridge the gap between contemporary auditing practices and ISA. The authors included the auditor's expertise and role clarity as antecedent variables that affect audit responsiveness and audit reliability, which, in turn, affect audit satisfaction.

For higher education institutions, the presence or absence of CA/CM is an important characteristic that likely improves the reliability of the stored data and hence the credibility of the institution. Moreover, such auditing complies with the external regulations set up by the ministry of higher education. Marques *et al*. (2015) present a similar work, related to continuous assurance services in information systems that aim to improve the reliability of the business. The authors developed a prototype and consequent results analysis using real data, demonstrating the feasibility and effective use of the proposal.

CA and CM in information systems remains a hot research topic. For instance, Hardy and Laslett (2015) described a case study about the interpretation and implementation of CA and CM in a wholesale distribution and marketing company in Australia. They obtained interesting results from over 100 automated tests that were performed daily, a fully-integrated exception management system, advancement from data to predictive analytics and the use of visualization technologies to enhance reporting.

In many ways, ISA is similar to process auditing, a mechanism frequently used by many organizations to ensure the quality of their processes. To improve the quality of audit recommendations, Kurniati *et al*. (2015) suggested the use of process mining in auditing business processes based on data from event logs stored in information systems. CM of information systems data from external and internal threats is of paramount importance for top management. Many methods have been proposed to prevent external intruders from

accessing—and hence, tampering with—the data. Tao *et al.* (2018) present excellent work to detect external intruders; they proposed an alarm intrusion detection algorithm with Feature selection, Weight and Parameter optimization of Support Vector Machine (FWP-SVM-GA) based on the Genetic Algorithm (GA) and Support Vector Machine (SVM) algorithm for use in a human-centered smart IDS. Alles *et al.* (2018) emphasized that the use of computer algorithms derived from statistics, data mining and machine learning can help the auditing profession to remain relevant in these increasingly volatile times. Material transactions that deviate from the auditor's expectations are considered anomalous and require the auditor's attention.

Internal threats can cause huge damage for an organization because insiders have legitimate data access. Liu *et al.* (2018) identified several possible reasons for enormous loss: (1) the existing solutions do not pay enough attention to the early indications of an arising malicious insider, most of which do not raise alerts until damaging behaviors have occurred; (2) most of the solutions rely only on an individual audit data source, diminishing insights into the threats; and (3) conventional data analytics rely too heavily on domain knowledge to extract features and establish rules, resulting in a limited capability against evolving threats.

Some universities might opt for storing their data using a cloud storage system, but this approach requires more rigorous auditing to ensure the integrity of the data. Different schemes have been proposed to address such a problem. For example, Wang *et al.* (2017) proposed an Identity-Based Data Outsourcing (IBDO) scheme equipped with desirable features that are favorable to existing proposals for securing outsourced data.

Information Systems in Higher Education Institutions

Information and Communication (ICT) infrastructure investment in emerging countries still lags behind. Kunda *et al.* (2019) gathered evidence from both public and private higher education institutions in Zambia to investigate factors that impact Zambian lecturers' attitudes about incorporating ICTs in research and teaching activities. They found a positive correlation between the important factors that influence lecturers to assimilate ICTs in an academic environment. Other researchers have highlighted the importance of integrating IT governance in higher education institutions (Khouja *et al.*, 2018).

In the United Arab Emirates, there are currently 68 accredited universities and colleges and the majority are private institutions (www.mohesr.gov.ae). All these institutions use information systems to handle a variety of things, including student academic information. The reliability of the generated data is a crucial part of the management of these institutions, which have to deal with both internal and external threats. Management requires close monitoring and thorough auditing of the information systems to ensure the trustworthiness of academic data. Higher education institutions, especially private ones, exist in a very tough, competitive and regulated environment that necessitates maintaining their reputation in the academic field. The ministry of higher education requires all accredited universities and colleges to adhere to a strict set of rules and regulations. The ministry of higher education desperately needs mechanisms to monitor, audit and ensure the integrity of the academic data generated by these systems.

Information systems in higher education institutions have peculiar characteristics compared with other types of information systems. For example, the pattern of transactions is unique; transactions are particularly heavy in certain time periods, such as during student registration, student admission and mark entries. The proposed model attempts to close the research gap by providing an easy method to detect and highlight suspected fraudulent transactions and facilitate the decision process.

Methods

Information systems are composed of hardware, software, users and data. Auditing in information systems is entirely different from other types of auditing. In this study, the auditing process will be confined to data and information. Ioan (2015) identified seven characteristics of information:

- Availability—the information must be available at any time during the decision process
- Integrity—the content and accuracy of the data must be in accordance with the rules and expectations of the organization
- Compliance—the logical structure of information and its concrete values must reflect the actual level of processes it characterizes
- Reliability—the information must relate to the specific decision-making process that it serves
- Efficiency—the information must be provided with the lowest consumption of resources
- Effectiveness—the information must be relevant, accurate and provided in a timely manner for decision making
- Confidentiality—the information must be provided only to the intended users

Figure 1 shows the proposed framework processes, which use data mining techniques to audit and detect suspected fraudulent transactions for referral to the management of the higher education institution and the ministry of higher education.

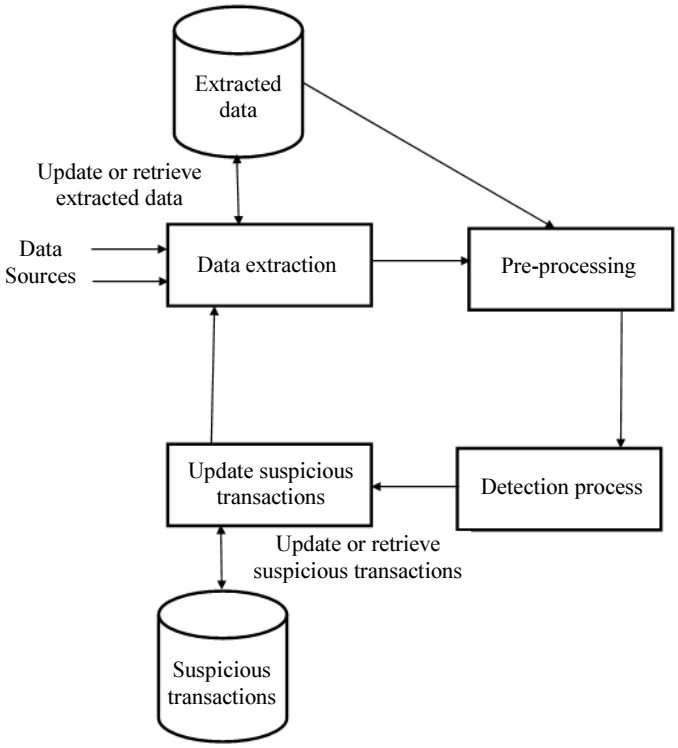

Fig. 1: The proposed framework processes

The proposed framework indicates five phases:

Data Extraction Phase

This phase uses the log file from information systems to extract data and to prepare and extract features that are valuable for detecting suspected fraudulent transactions.

Data Pre-Processing Phase

The step may include data cleaning, normalization, transformation and feature selection to prepare the data for analysis.

Detection Process Phase

As shown in Figure 1, this phase includes two processes:

- Mining: This phase uses a suitable outlier analysis algorithm to detect suspected fraudulent transactions
- Post-processing: This phase intends to evaluate the generated patterns after the mining process

Generating Suspected Fraudulent Transactions Phase

This phase uses the tested pattern to generate suspected fraudulent transactions. This phase is the actual experimental work. The result will be delivered to the institution's management for further investigations.

These steps or phases will be detailed further when the actual data is prepared and the model is tested.

Conceptual Design of the Proposed Framework

Figure 2 shows the conceptual design of the proposed framework. The proposed design consists of the following services/components:

- User Interface Service: This service helps the users to navigate the different services, as detailed in the rest of this section
- Naming and Location Service: This service stores information about the names and locations of the registered services. This service can be implemented as a centralized or distributed service
- Detection Service: This service can be implemented as an extensible class that can be extended by the developer to add a new detection service, such as for the academic institution or for the regulatory institution
- Reporting Service: This service stores suspicious transactions in a special database that can be accessed and investigated by different users through the user interface service
- Data Sources: These encompass the databases and files that include information about the academic regulations, registration information, policies, processes/procedures, student information, regulatory rules and any other data that is relevant to the purpose of audit
- Suspicious Transactions Database: This database stores only the suspicious transactions detected by the

detection service. This database can be implemented as a centralized or distributed database as required

Framework Model Formulation

The proposed framework will be based on outlier analysis, a data mining technique that can detect suspected fraudulent transactions. An outlier is generally defined as an object that deviates from the rest of the objects in the dataset.

As explained in Han *et al*. (2012), there are many outlier detection methods in practice, such as supervised, semi-supervised and unsupervised methods. In this research, we intend to use supervised method for detecting the suspected fraudulent transaction. The supervised method needs to model data normality and abnormality. It requires a domain expert to label the sample data. In this research, we have designed an algorithm to act as a domain expert for labeling the transactions (Transactions Labeling Algorithm). Two classes can be labeled: legitimate transaction and suspected fraudulent transaction. Figure 3 shows the algorithm steps.

After the data is extracted and pre-processed a model should be designed to predict the suspected fraudulent transactions. The model can be formulated by utilizing Support Vector Machine (SVM), a prominent classification technique for predicting illegal transactions. SVM (Vapnik and Vapnik, 1998) is a non-probabilistic binary linear classifier that constructs a hyperplane or set of hyperplanes in a high or infinite dimensional space. It can be used for classification, regression, or other tasks. The main idea underlying SVM for transactions classification is to find a hyperplane that divides the transactions into fraudulent or legitimate.

In order to discriminate between "fraudulent" and "legitimate" transactions, the SVM learns a classification function from a set of positive examples (fraudulent) χ_+ and set of negative examples (legitimate) χ-. Following (Ismail *et al*., 2018; Zaki *et al*., 2004; 2006), the classification function takes the form shown in Equation (1):

$$f(x) = \sum_{i:x_i \in \chi+} \lambda_i K(x, x_i) - \sum_{i:x_i \in \chi-} \lambda_i K(x, x_i) \quad (1)$$

where, the non-negative weights λ_i are computed during training by maximizing a quadratic objective function and the kernel function $K(x, x_i)$. In this case, Gaussian Radial Basis Function kernel (RBF kernel) can be used.

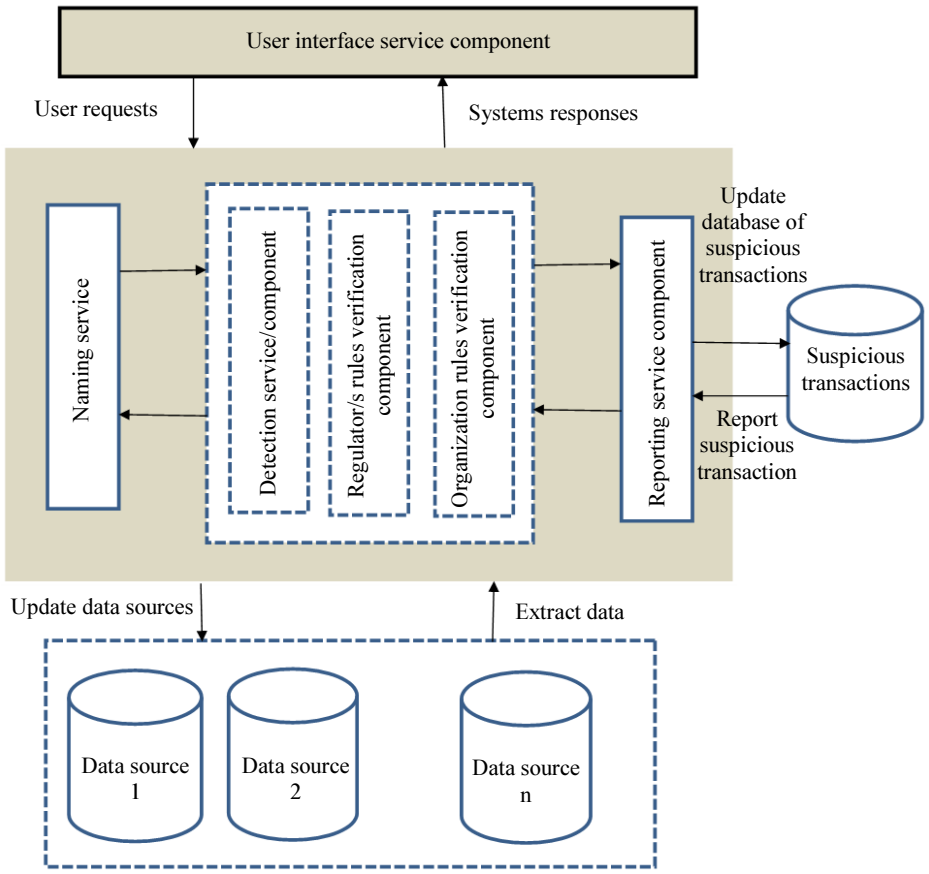

Fig. 2: The proposed framework components

Transactions Labeling Algorithm
1. Scan the database file
2. Read the transaction, if not end of file, go to step 3, otherwise go to step 5
3. Check transaction
   3.1 Check transaction timing validity, if it not valid, label the transaction as fraudulent. Otherwise…
   3.2 Check the transaction location validity, if it is not valid, label the transaction as fraudulent. Otherwise…
   3.3 Check university regulation violation, if there is a violation, label the transaction as fraudulent. Otherwise…
   3.4 Check ministry of higher education regulation violation, if there is a violation, label the transaction as fraudulent. Otherwise…
   Label the transaction as legitimate
4. Repeat step 2
   5. End of labeling

Fig. 3: Transactions Labeling Algorithm

The RBF kernel allows pockets of data to be classified, which is more powerful approach than simply using a linear dot product (Zaki *et al*., 2006). Any new transaction, x, is then predicted to be positive or negative if the function, $f(x)$. is fraudulent or legitimate, respectively. More details about how the weights, λ_i, are computed and the theory of SVM can be found in Vapnik and Vapnik (1998).

Model Evaluation

After building the classification model using SVM, the next step is the model evaluation. The literature is abundant with descriptions of the use evaluation measures such as accuracy, sensitivity (or recall), specificity, precision and F1 measure (Han *et al*., 2012). In this framework model, we intend to use Precision, Recall, F1 measure and accuracy as model evaluation measures. The following assumptions are made:

- Positive transaction means the transaction is fraudulent
- Negative transaction means the transaction is legitimate

The formulation of the measures are as follows:

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

$$Recall = \frac{TP}{TP + FP} \tag{3}$$

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{4}$$

$$Accuracy = \frac{TP + TN}{P + N} \tag{5}$$

where, TP, TN, FP, FN, P and N are defined as:
TP: Fraudulent transaction classified as Fraudulent.
TN: Legitimate transaction classified as Legitimate.
FP: Legitimate transaction classified as Fraudulent.
FN: Fraudulent transaction classified as Legitimate.
P: Total number of fraudulent transactions.
N: Total number of legitimate transactions.

The first measure that we intend to discuss for the evaluation of our framework model is precision, which is a measure of exactness; i.e., the percentage of transactions labeled as fraudulent that are actually fraudulent. The calculation of precision is shown in Equation (2). Precision alone is not sufficient for model evaluation because it does not tell us anything about the mislabeled classes.

A complement of precision measure is a recall, which is a measure of completeness; i.e., what percentage of fraudulent transactions are labeled as such. Equation (3) shows the computation of recall value. To evaluate the model, precision and recall values are used together in a way in which the precision values are compared with a fixed value of recall or the recall values are compared with a fixed precision value.

A widely used and better model evaluation measure that combines both precision and recall is the F measure or F_1, or F-score measure. The F measure uses harmonic mean of precision and recall and gives equal weight to both. Equation (4) shows the calculation of the F_1 measure.

The last and the most important model evaluation measure is accuracy, which is the percentage of test set transactions that are correctly classified by the classifier. Equation (5) explains the computation of the classifier accuracy.

During the experimental work, the values of precision, recall, F measure and accuracy will be calculated. The extent to which the values of precision, recall, F1 measure and accuracy determine the quality and use of a model depend on the aim of the study. For example, if the model aims to predict whether a patient has cancer or not, then the false negative will have a devastating impact for the patient; hence, high model accuracy is very important.

The aim of this study is to develop a generic information systems audit framework model. As such, the evaluation of the model should be generic (matching concept). Thus, the model evaluation criteria should go hand in hand with the materiality concept in auditing. The values of precision, recall, F1 measure and accuracy that determine the acceptance of the model depend on the level of materiality as a function of relative size and importance of the higher education.

Discussion

Internationally, universities recognize the importance of registration systems, one categories of information systems. These systems store huge amounts of data about students, courses, grades, etc. Maintaining the integrity of such data is of paramount importance for both universities and the ministry of higher education, which has the responsibility to oversee and monitor the activities of universities and to guarantee the accuracy of the data stored by such systems.

ISA represents a challenging issue for most organizations, especially higher education institutions, the reputations of which play an important role in improving their market share. Maintaining data integrity is an important characteristic sought by most organizations operating in a very competitive environment. The audit framework aims to establish whether university registration systems are safeguarding corporate assets, maintaining the integrity of stored and communicated data, supporting university objectives effectively and operating efficiently. To achieve such an uphill task, the framework algorithm first extracts the transactions from the university registration system and then utilizes outlier analysis (Han *et al*., 2012), a data mining technique, to identify possible fraudulent transactions. The algorithm considers different types of events, stages and relationships that constitute the essence of each university registration system transaction.

It is recognized that university registration systems have a peak time period during which there is a larger volume of generated transactions. For example, during registration at the beginning of the semester and at the end of the semester, the marks and grades of every student are recorded by the instructors and employees of the registration office. The framework uses different factors to identify suspected fraudulent transactions and one of the most important factors is the timing of the transactions. In a university registration system, some transactions can only be generated during certain time periods. For example, as explained above, transactions related to student marks and grades should only occur at the end of the semester or within certain periods of time and should be performed only by certain types of users. If the auditing system detects that such transactions were generated outside these times, the system immediately flags these transactions as suspicious for fraudulent transactions, thus adding them to a separate file for further investigation.

The framework accounts for factors other than timing, such as the specific rules of the university or ministry of higher education. Transactions that violate these rules should be marked as suspicious as well. In addition, the location of the transaction is important; most universities restrict the locations for the execution of transactions related to student marks and grades. Any transactions carried out by individuals outside these locations should be flagged by the auditing system.

The framework also aims to address issues related to ostensibly legal transactions. For example, a transaction may be performed by authorized personnel from the right place, from the right machine and at the right time, but nevertheless is fraudulent. This is an example of internal threat and the framework can respond by using the concept of transaction consistency. In such a scenario, transactions can be grouped based on certain characteristics. For example, after an instructor finishes entering the marks of the students for certain course section, if the auditing system discovers that some transactions were later updated by another user, these transactions will be flagged by the system.

The Confidentiality, Integrity and Availability (CIA) triad model is used in a variety of information systems, such as health information (Azadi *et al*., 2018). The model is helpful for evaluating factors related to choosing vendors and this can be considered an important component of the proposed ISA framework. The confidentiality component of the CIA triad model ensures that the university information systems' data are protected from unauthorized access. The integrity component provides assurance that the university data is not modified or destroyed. The ISA framework will be able to detect whether an authorized or unauthorized person modifies the data.

Concluding Remarks and Future Research Directions

Prior research in CA and CM of data demonstrates the existence of a solid connection between contemporary auditing practices and ISA. With the objective of ensuring the validity and reliability of all data stored in an electronic form, ISA will remain a controversial research topic. This paper highlights the theoretical aspects of a framework to detect and identify suspected fraudulent transactions in the information systems of higher education institutions. Our literature review revealed that this is the first attempt to propose a viable technique—the outlier analysis algorithm—to improve the auditing of university information systems.

In this paper, we have proposed a theoretical framework to support ISA in higher education institutions. The findings of our research contribute to the previous literature in various ways. First, the consequences of this research indicate that the higher the quality and integrity of the stored data, the better the performance of the university. Second, the quick detection of fraudulent transactions allows universities to take swift measures to correct these transactions and avoid any punishment imposed by the ministry of higher education. Third, the identification of suspected fraudulent transactions in university information systems

helps both universities and the ministry of higher education senior executive to make complex decisions around efficient, effective resource use to ensure quality education in mutual manner.

At this point, we acknowledge that there is a need for further investigations. To create recommendations for implementation of this framework, researchers should collect real data from university information systems. Moreover, the outlier analysis (the proposed data mining technique) detects outlier objects by employing several different techniques: Clustering-based techniques, nearest-neighbor classification techniques and statistical methods. There is a convincing need for future research to determine the best outlier analysis technique for improving the auditing of information systems.

Acknowledgment

The authors would like to acknowledge the assistance and support provided by Ajman university library and Canadian university library for procuring most of the papers and the books used in the article.

Author's Contributions

Elfadil A. Mohamed: He participated in creating the research idea, conceptual design and validating of the ISA framework. He also participated in the writing of the abstract, introduction, literature, results and discussion. He has significant contribution in the research intellectual content.

Elgilani Elshareif: He significantly contributed in validating the research idea, research methods and the ISA framework. He is also contributed in the process of drafting, writing, and reviewing the article.

Omer Ishag Eldai Mohamed: He participated in the conceptualization of the research idea and gearing the direction of the paper towards the creation of a generic ISA framework. He has made considerable contributions in the entire design and description of the proposed ISA framework and the proposed framework processes.

All authors have made significant contributions in this article.

Ethics

This article is original and was not published before. All the authors have read and approved the manuscript.

References

Abdul Rahman, L., S. Islam and A. Ai-Nemrat, 2015. Measuring sustainability for an effective information system audit from public organization perspective. Proceedings of the 9th IEEE International Conference on Research Challenges in Information Science, May 13-15, IEEE Xplore Press, Athens, Greece, pp: 42-51. DOI: 10.1109/RCIS.2015.7128862

Alles, M., G. Brennan, A. Kogan and M.A. Vasarhelyi, 2018. Continuous Monitoring of Business Process Controls: A Pilot Implementation of a Continuous Auditing System at Siemens. In: Continuous Auditing: Theory and Application, Chan, D.Y., V. Chiu and M.A. Vasarhelyi (Eds.), Emerald Publishing Limited, pp: 219-246.

Axelsen, M., P. Green and G. Ridley, 2017. Explaining the information systems auditor role in the public sector financial audit. Int. J. Account. Inform. Syst., 24: 15-31. DOI: 10.1016/j.accinf.2016.12.003

Azadi, M., H. Zare and M.J. Zare, 2018. Confidentiality, Integrity and Availability in Electronic Health Records: An Integrative Review. In: Information Technology-New Generations. Advances in Intelligent Systems and Computing, Latifi, S. (Ed.), Springer, Cham, ISBN-13: 978-3-319-77027-7, pp: 745-748.

Comyn-Wattiau, I. and J. Akoka, 1996. Logistics information system auditing using expert system technology. J. Expert Syst. Applic., 11: 463-473. DOI: 10.1016/S0957-4174(96)00062-0

Han, J., M. Kamber and J. Pei, 2012. Data Mining: Concepts and Techniques. 3rd Edn., Morgan Kaufmann, Waltham, MA., ISBN-10: 0123814804, pp: 744.

Hardy, C.A. and G. Laslett, 2015. Continuous auditing and monitoring in practice: Lessons from Metcash's business assurance group. J. Inform. Syst., 29: 183-119. DOI: 10.2308/isys-50969

Ioan, R., 2015. Technologies and methods for auditing databases. Proc. Econom. Finance, 26: 991-999. DOI: 10.1016/S2212-5671(15)00921-1

Ismail, H.M., B. Belkhouche and N. Zaki, 2018. Semantic Twitter sentiment analysis based on a fuzzy thesaurus. Soft Comput., 22: 6011-6024. DOI: 10.1007/s00500-017-2994-8

Kamil, O., 2012. The application of artificial intelligence in auditing: Looking back to the future. J. Expert Syst. Applic., 39: 8490-8495. DOI: 10.1016/j.eswa.2012.01.098

Khouja, M., I.B. Rodriguez, Y.B. Halima and S. Moalla, 2018. IT governance in higher education institutions: A systematic literature review. Int. J. Human Capital Inform. Technol. Profess., 9: 52-67. DOI: 10.4018/IJHCITP.2018040104

Kim, S.L., T.S.H. Teo, A. Bhattacherjee and K. Nam, 2015. IS auditor characteristics, audit process variables and IS audit satisfaction: An empirical study in South Korea. Inform. Syst. Frontiers, pp: 1-15.

Kunda, D., C. Christopher and M. George, 2019. Factors that influence Zambian higher education lecturer's attitude towards integrating ICTs in teaching and Research. J. Technol. Sci. Educ., 8: 360-384. DOI: 10.3926/jotse.338

Kurniati, A.P., G.P. Kusuma and G.A. Ary Wisudiawan, 2015. Designing application to support process audit using process mining. J. Theor. Applied Inform. Technol., 80: 473-480.

Li, S.H., S.M. Huang and Y.C.G. Lin, 2007. Developing a continuous auditing assistance system based on information process models. J. Comput. Inform. Syst., 48: 2-13.
DOI: 10.1080/08874417.2007.11645990

Liu, L., O. De Vel, Q.L. Han, J. Zhang and Y. Xian, 2018. Detecting and preventing cyber insider threats: A survey. IEEE Commun. Surveys Tutorials, 20: 1397-1417.
DOI: 10.1109/COMST.2018.2800740

Marques, R.P., H. Santos and C. Santos, 2015. Monitoring organizational transactions in enterprise information systems with continuous assurance requirements. Int. J. Enterprise Inform. Syst., 11: 13-32. DOI: 10.4018/ijeis.2015010102

Marquesa, R.P., H. Santosa and C. Santosb, 2012. A solution for real time monitoring and auditing of organizational transactions. Proc. Technol., 5: 190-198. DOI: 10.1016/j.protcy.2012.09.021

Rezaee, Z., A. Sharbatoghlieb, R. Elam and P.L. McMickle, 2002. Continuous auditing: Building automated auditing capability. Auditing: J. Practice Theory, 21: 147-163.
DOI: 10.2308/aud.2002.21.1.147

Tao, P., Z. Sun and Z. Sun, 2018. An improved intrusion detection algorithm based on GA and SVM. IEEE Access, 6: 13624-13631.
DOI: 10.1109/ACCESS.2018.2810198

Vapnik, V.N. and V. Vapnik, 1998. Statistical Learning Theory. 1st Edn., Wiley, New York,
ISBN-10: 0471030031, pp: 736.

Wang, Y., Q. Wu, B. Qin, W. Shi and R.H. Deng *et al*., 2017. Identity-based data outsourcing with comprehensive auditing in clouds. IEEE Trans. Inform. Forens. Security, 12: 940-952.
DOI: 10.1109/TIFS.2016.2646913

Zaki, N.M., S. Deris and H. Alashwal, 2006. Protein-protein interaction detection based on substring sensitivity measure. Int. J. Biomed. Sci. 1: 148-154.

Zaki, N.M., S. Deris and R. Illias, 2004. Feature extraction for protein homology detection using hidden Markov model combining scores. Int. J. Comput. Intell. Applic., 4: 1-12.
DOI: 10.1142/S1469026804001161