

THE USE OF FUZZY LOGIC TO MEASURE THE RISKS OF ICT IN E-AUDIT

Thabit Hassan Thabit*

Sid Ahmed HADJ AISSA**

Sinan Abdullah Harjan***

Abstract:

This research presents the role of information and communication technologies in enhancing the security of e-audit and the impact of these technologies on the development of the trend towards use of ICT in all areas of accounting and try to find solutions to the challenges faced by e-audit .

Keywords : ICT; e-audit; fuzzy logic; MatLab software; risks

Resumé

Notre recherché présente une etude sur le role des technologies de l'information et de la communication dans le remplacement de la sécurité de l'audit électronique et son impact sur le développement de la tendance à l'utilisation des TIC dans tous les domaines de la comptabilité en essayant de trouver des solution aux défis de l'audit électronique.

Mots-clés: TIC; E-audit; logique floue; Logiciel MatLab; les risques

الملخص:

يقدم هذا البحث دراسة حول دور تقنيات المعلومات والاتصالات في تعزيز أمن التدقيق الإلكتروني وتأثير هذه التقنيات على تنمية التوجه نحو استخدام تقنيات المعلومات والاتصالات في جميع مجالات المحاسبة ومحاولة إيجاد حلول للتحديات التي تواجه التدقيق الإلكتروني .
الكلمات المفتاحية : تقنيات المعلومات والاتصالات، التدقيق الإلكتروني، المنطق المضبط، المخاطر.

*Assistant Lecturer, Dept. of Accounting, Cihan University / Erbil - Iraq

**Assistant Professor, Dept. of Business and Management Sciences, University of Blida2, Algeria.

***Assistant Lecturer, Dept. of Finance, Cihan University / Erbil - Iraq

1. INTRODUCTION

The use of information and communication technology has become a necessity that should be met in our time because of the overlap of those techniques in all life facilities, social, economic and political, and therefore it was necessary to keep up with the advanced countries in the adoption of all what is better in their financial transactions, in particular, social and political in general

2. THE PREVIOUS STUDIES :

Many researches and studies about the relationship between ICT and E-Audit appeared in last decade. Table (1) summarized the main previous studies as following :

TABLE (2) :THE MAIN PREVIOUS STUDIES ABOUT E-AUDIT

The Authors	The Title	The Main Topics
Praseno, 2012	IT-Based Audit (e-Audit) Plan in Indonesia: An Analysis of the Program Logic, Feasibility, and Alternatives	• Criticizes the implementation of the e-Audit project • Explores the condition why e-audit is should not be implemented in this current stage • Assesses the condition of e-government progress • Evaluates the relation between state audit institution, and the e-audit project itself.
Nemec et al. , 2011	The e-Audit : The Road Map to Value Capture in e-Business's Second Wave	• Explains the challenges that facing e-audit. • Discusses the advantages and disadvantage of e-audit . • Shows the main functions of e-audit. • Evaluates the expected opportunities of using e-audit .
Bernier and Suire, 2014	Meeting the VAT e-audit challenge	• Depicts good practices for a relaxed e-audit . • Displays difficulties facing businesses in e-audit. • Identifies general information requested by the tax administration at the beginning of the e-audit.

3. THE CONCEPT OF E-AUDIT

Electronic auditing comprises the entire structure of the audit activities performed through electronic environment. The operation of that function is performed through electronic entries and documents. Establishments get rid of physical settlement boundaries while they provide goods and services.

The network information systems have provided the establishment, coordinate their abilities with the other establishments as virtual collaborations and virtual associations. This new concept is called virtual organizations as well as networked organizations. The function of electronic auditing will be comprehended more easily when it becomes necessary to audit these networked associations or organizations (Alptürk E, 2008).

4. THE APPROCHES OF E-AUDIT

There are two main approaches in auditing of firms' electronic information environments. Those approaches are auditing around the computer and auditing through the computer (Selvi et al., 2006):

4.1. Auditing around the computer :

In auditing around the computer approach, only entries made into computers from the source documents such as purchase and sales invoices as well as exits from computers such as journal or ledger are inspected. The computer's data processing function is omitted. For this reason, this approach is also called as the 'black box' or 'auditing by the computer' approach.

In this approach, when the inspection of inputs and outputs are in question, the auditor does not examine how all transactions as regards these inputs are executed in the computer as well as on what grounds the computer gives outputs. Today, as a consequence of improvements in information technologies and numerousness of transactions, the usage areas of this approach are rather confined, and the auditor chooses to implement it only

on quite rare occasions. In order to do that, the auditor needs to reach adequate source documents and the detailed list of outputs in a legible form.

4.2.Auditing through the computer :

In auditing through the computer approach, not the inputs or outputs, but the computer system en masse is examined. Therefore, softwares that operate inside the computer and execute all transactions are included in the auditing process. This approach requires the auditor to utilize from computer-aided auditing techniques, and the auditor primarily tries to recognise and comprehend the structure of internal controls in the computer system. Furthermore, three types of testing strategies, which are the data test, parallel simulation, and system-integrated auditing module, are involved in this approach.

5.RISKS OF USING ICT TECHNIQUES IN E-AUDIT

There are many risks that faced e-audit when using ICT techniques:

5.1.Risks associated with Portable Storage Devices

The convenience of using PSDs to store and transfer data has seen them increasingly used by agencies as part of their day-to-day work. However, there are a number of risks associated with their use, particularly due to their small size and portability. The risks include (ANAO , 2011); (GFI , 2011):

- external loss and theft—PSDs' size make them particularly susceptible to loss or theft by an unauthorized person. If the data is not encrypted it can be easily accessed;
- 'insider' data theft—PSDs provide a ready means by which data can be stolen from an ICT system, and because they are often small they can be moved in and out of a controlled environment without attracting attention. Additionally, because they are commonplace, theft of data can occur in plain sight (for example, using a CD/DVD or

USB flash drive at a desktop computer is not an uncommon sight);

- data loss—if data is stored only on a PSD, there is the risk of accidental or deliberate loss of the data if the device itself fails;
- introduction of viruses and malicious software ('malware')—PSDs can provide a conduit for viruses and malware to enter an ICT system, either deliberately by an attacker or unintentionally by a user;
- inadequate disposal—simply deleting data from PSDs does not completely erase it, and there are software and hardware products available that can recover deleted data which could be used by an unauthorised person;
- introduction of unwanted software—while not posing a security risk such as viruses and malware, unwanted software such as games may affect the performance of an ICT system and corporate productivity, or introduce illicit or illegal material such as pornography or media downloaded without copyright protections.

5.2.Risks associated with Cloud Computing

Cloud computing is a computing resource deployment and procurement model that enables an organization to obtain its computing resources and applications from any location via an Internet connection. Depending on the cloud solution model an organization adopts, all or parts of the organization's hardware, software, and data might no longer reside on its own technology infrastructure. Instead, all of these resources may reside in a technology center shared with other organizations and managed by a third- party vendor , The risks include (COSO , 2012) :

- Disruptive force – Facilitating innovation (with increased speed) and the cost-savings aspects of cloud computing can themselves be viewed as risk events for some organizations. By lowering the barriers of entry for new competitors, cloud computing could threaten or disrupt

some business models, even rendering them obsolete in the future. For example, streaming media over the Internet was a technology solution that significantly reduced the sales of CDs and DVDs and the need for physical retail stores. Existing competitors that fully embrace the cloud might be able to bring new ideas and innovation into their markets faster. Since cloud computing solutions yield considerable short-term cost savings due to reduced capital expenditures, an organization adopting the cloud might be able to extract better margins than its non-cloud competitors. Thus, when an industry member adopts cloud solutions, other organizations in the industry could be forced to follow suit and adopt cloud computing.

- Residing in the same risk ecosystem as the CSP and other tenants of the cloud – When an organization adopts third-party-managed cloud solutions, new dependency relationships with the CSP are created with respect to legal liability, the risk universe, incident escalation, incident response, and other areas. The actions of the CSP and fellow cloud tenants can impact the organization in various ways.
- Lack of transparency – A CSP is unlikely to divulge detailed information about its processes, operations, controls, and methodologies. For instance, cloud customers have little insight into the storage location(s) of data, algorithms used by the CSP to provision or allocate computing resources, the specific controls used to secure components of the cloud computing architecture, or how customer data is segregated within the cloud.
- Reliability and performance issues – System failure is a risk event that can occur in any computing environment but poses unique challenges with cloud computing. Although service-level agreements can be structured to meet particular requirements, CSP solutions might sometimes be unable to meet these performance metrics if

a cloud tenant or incident puts an unexpected resource demand on the cloud infrastructure.

- Vendor lock-in and lack of application portability or interoperability – Many CSPs offer application software development tools with their cloud solutions. When these tools are proprietary, they may create applications that work only within the CSP's specific solution architecture. Consequently, these new applications (created by these proprietary tools) might not work well with systems residing outside of the cloud solution. In addition, the more applications developed with these proprietary tools and the more organizational data stored in a specific CSP's cloud solution, the more difficult it becomes to change providers
- Security and compliance concerns – Depending on the processes cloud computing is supporting, security and retention issues can arise with respect to complying with regulations and laws such as the *Sarbanes-Oxley Act of 2002 (SOX)*, the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, and the various data privacy and protection regulations enacted in different countries. Examples of these data privacy and protection laws would include the *USA PATRIOT Act*, the *EU Data Protection Directive*, Malaysia's *Personal Data Protection Act 2010*, and India's *IT Amendments Act*. In the cloud, data is located on hardware outside of the organization's direct control. Depending on the cloud solution used (SaaS, PaaS, or IaaS), a cloud customer organization may be unable to obtain and review network operations or security incident logs because they are in the possession of the CSP. The CSP may be under no obligation to reveal this information or might be unable to do so without violating the confidentiality of the other tenants sharing the cloud infrastructure.
- High-value cyber-attack targets – The consolidation of multiple organizations operating on a CSP's infrastructure

presents a more attractive target than a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a CSP solution in most cases are higher with respect to confidentiality and data integrity.

- Risk of data leakage – A multi-tenant cloud environment in which user organizations and applications share resources presents a risk of data leakage that does not exist when dedicated servers and resources are used exclusively by one organization. This risk of data leakage presents an additional point of consideration with respect to meeting data privacy and confidentiality requirements.
- IT organizational changes – If cloud computing is adopted to a significant degree, an organization needs fewer internal IT personnel in the areas of infrastructure management, technology deployment, application development, and maintenance. The morale and dedication of remaining IT staff members could be at risk as a result.
- Cloud service provider viability – Many cloud service providers are relatively young companies, or the cloud computing business line is a new one for a well-established company. Hence the projected longevity and profitability of cloud services are unknown. At the time of publication, some CSPs are curtailing their cloud service offerings because they are not profitable. Cloud computing service providers might eventually go through a consolidation period. As a result, CSP customers might face operational disruptions or incur the time and expense of researching and adopting an alternative solution, such as converting back to in-house hosted solutions.

5.3.Risks of Digital Divine :

Many scholars have defined the digital divide almost exclusively in terms of a gap in physical access to ICT. , they said that it is " "Marketers, media, and governments often report

only the number of people who have access to the Internet" (Buente et al., 2008).

The U.S. Department of Commerce's description of the digital divide in 2000 was " Some individuals have the most powerful computers, the best telephone service and fastest Internet service, as well as a wealth of content and training relevant to their lives . Another group of people don't have access to the newest and best computers, the most reliable telephone service or the fastest or most convenient Internet services. The difference between these two groups is the Digital Divide " (Huang and Chen, 2010).

However , The digital divide often refers to two distinct issues: first, the gap in availability of broadband infrastructure (usually between densely populated urban areas and sparsely populated rural areas); and second, the gap in broadband take-up between certain demographic groups, with socio-economic factors often being key drivers , and the risks of digital divide include (Ali, 2011) :

- Market may not lead, as low socio-economic groups are seen as a lower revenue opportunity and a credit risk to operators
- No co-ordinated strategy to bridge the digital divide, hence unable to influence DAE targets
- Requires investment resources to aggregate demand and lead a procurement activity
- May not result in significantly reduced price broadband services as operators may use funds to offset risk and to increase profitability
- Requires significant upfront capital investment in infrastructure
- May be subject to state-aid challenges if public subsidy involved

6.SOLUTIONS ADOPTED BY ORGANIZATION INTERESTED WITH E-AUDIT

Many organizations interested with e-audit adopted various kinds of solutions to reduce the risks of using ICT in e-audit by contracting with specialized ICT security companies , and these solutions are :

6.1.Solutions that related to risks of using Portable Storage Devices :

Both of GFI¹ and NIST² companies presented many solutions to use PSDs safely , these solutions are (GFI , 2011); (NIST, 2007):

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed.
- Encryption is automatic, real-time and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.
- Provides plausible deniability, in case an adversary forces you to reveal the password.

6.2.Solutions that related to risks of using Cloud Computing :

US-CERT³ organization presented many solutions to reduce the risks of using cloud computing, these solutions are (US-CERT, 2012):

- IT management and departments need to realize that cloud providers are an extension of their internal IT department. All of the risks apply equally to the provider as well. The key difference is that with internal departments, it can be easier to validate, enforce and administer controls to manage risk.
- Choosing a cloud provider who can demonstrate validation of controls. Some of these controls include SSAE audit, data, accessibility, data center security controls and data encryption.
- Opt for a private cloud, or a virtual private cloud, where systems are virtually separated from each other through an encrypted environment inside a public cloud.
- Analyze which legacy applications are appropriate for the cloud.
- Ask the cloud provider for a definitive disaster recovery plan. An internal revert strategy will also help to quickly move to an alternate IT service model.
- Maintain regular backups of critical cloud-based assets, and protect data through strong encryption.
- Ask for regular security-event alerts from cloud vendors, and ask them to flag specific mission-critical assets.
- Seek independent audit reports from service providers for greater transparency, and check industry certifications of cloud service providers such as ISO 27001 and 27002, ISO 31000, and Payment Card Industry Data Security Standard (PCI DSS) compliance certification.

6.3.Solutions that related to risks of Digital Divide :

Many suggested solutions were presented by (Dijk and Hacker) to reduce the digital divide in developing countries , such as (Dijk and Hacker, 2003):

- provide correct and accurate information on the digital divide and deal with them as a specific time and goals .
- Urge educational institutions to develop the curriculum to focus on the educational and technical sides , to use information technology optimizely .
- Provide information and communications technology to everybody , by a completely plan of community development .
- Develop the economical infrastructure to reduce the digital divide .

7.THE PRACTICES OF THE FOUR MAJOR AUDIT FIRMS

The four major audit firms in the world tried many solutions to enhance their practices in e-audit and to increase the level of trust for the customer. Table (2) shows the most important solutions which adopted by the four major audit firms in the world.

TABLE (2) :THE MOST IMPORTANT SOLUTION TO ENHANCE E-AUDIT

Firm	Practices
<i>Deloitte</i> ⁴	• Provides advices about how to protect the company from electronic threats . • Provides guidelines to protect the assets of electronic information from the risks of cybersquatting . • Meets the e-audit requirements by creating private servers related to the firm , without having to resort to cloud service provider.
<i>PwC</i> ⁵	• Provides the programs that deal with customers' electronic information with vital protection. • Identifies the staff that uses electronic information by special electrical identifier for each employee . • Provides specific criteria to deal with the electronic information of customers .
<i>Ernst &</i>	• Deals with a trusted cloud service provider,

<i>Young</i> ⁶	authorized by international standard organizations. • Customizes electronic records for each employee to keep track of the used electronic information. • Provides advice to costumers on how to handle with the security risks of electronic information.
<i>KPMG</i> ⁷	• Provides information security services in all aspects of the infrastructures of information and communication technologies to customers . • Protects the database bank of electronic information through electronic IDs, and identifies employees who are able to access them. • Improves a selective control by setting the level of confidence for the safety of electronic information used in the customers' companies.

8.FUZZY LOGIC

Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact. Compared to traditional binary sets (where variables may take true or false values). Fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false (Novák et al., 1999).

Furthermore , when linguistic variables are used, these degrees may be managed by specific functions. Irrationality can be described in terms of what is known as the fuzzjjective (Thabit, 2013).

The term "fuzzy logic" was introduced in the 1965 proposal of fuzzy set theory by Lotfi A. Zadeh. Fuzzy logic has been applied to many fields, from control theory to artificial intelligence (Toni and Tonchia, 2001).

In fact, Zadeh made the following statement in his seminar paper of 1965 : The notion of a fuzzy set provides a convenient point of departure for the construction of a conceptual framework which parallels in many respects the framework used in the case of ordinary sets, but is more general than the latter and, potentially, may prove to have a much wider scope of applicability, particularly in the fields of pattern classification and information processing . Essentially, such a framework provides a natural way of dealing with problems in which the source of imprecision is the absence of sharply defined criteria of class membership rather than the presence of random variables (Ross, 2010).

9. BENEFITS OF FUZZY LOGIC

There are many benefits of using fuzzy logic, such as (Al-Hubaity and Thabit, 2012):

- Fuzzy Logic describes systems in terms of a combination of numerics and linguistics (symbolic). This has advantages over pure mathematical (numerical) approaches or pure symbolic approaches because very often system knowledge is available in such a combination.
- Problems for which an exact mathematically precise description is lacking or is only available for very restricted conditions can often be tackled by fuzzy logic, provided a fuzzy model is present.
- Fuzzy logic sometimes uses only approximate data, so simple sensors can be used.
- The algorithms can be described with little data, so little memory is required.
- The algorithms are often quite understandable.
- Fuzzy algorithms are often robust, in the sense that they are not very sensitive to changing environments and erroneous or forgotten rules.

- The reasoning process is often simple, compared to computationally precise systems, so computing power is saved This is a very interesting feature, especially in real time systems.
- Fuzzy methods usually have a shorter development time than conventional methods.

10. METHODOLOGY

The researchers distributed 40 questionnaires with 40 questions to 40 scholars and academic researchers in accounting and IT. 20 questions are about the risks of ICT on the security of e-audit, and the other 20 questions are about the best solutions to protect the e-audit information from thieving and hacking. All the answer are linguistic variables, so that the fuzzy logic is the best method to analyze the results.

To analyze the results of the questionnaire by fuzzy logic, the results are processed by fuzzy logic function, built in Matlab ver. 6.5 according the following steps:

- Step 1 : determining the required ratios of the results.
- Step 2 : determining the weights of ratios and questions
- Step 3 : calculating all the ratios, based on the data of the questionnaires.
- Step 4: calculating all the ratios according to their weights which resulted from step 3.
- Step 5: calculating the rate of the linguistic variables by assuming a rated value to each linguistic variable by dividing the weight of each ratio into the number of linguistic variables (weak = 0.01, acceptable = 0.02, good = 0.03, very good = 0.04 and excellent = 0.05).
- Step 6: calculating the rate of triangular fuzzy numbers by using the function of fuzzy logic in MatLab ver.6.5.

- Step 7: computing the weighted rates of triangular fuzzy numbers.
- Step 8: Determining the fuzzy Distance of each ratio by using the equations (1) and (2) (El-Hossainy, 2011).

$$D^2(\tilde{X}, M) = (b - M)^2 + \frac{1}{3}(b - M)[(c + a) - 2b] + \frac{1}{18}[(c - b)^2 + (b - a)^2] - \frac{1}{18}[(c - b)(b - a)] f(\alpha) \approx \alpha \dots (1)$$

$$D^2(\tilde{X}, M) = (b - M)^2 + \frac{1}{2}(b - M)[(c + a) - 2b] + \frac{1}{9}[(c - b)^2 + (b - a)^2] - \frac{1}{9}[(c - b)(b - a)] f(\alpha) \approx 1 \dots (2)$$

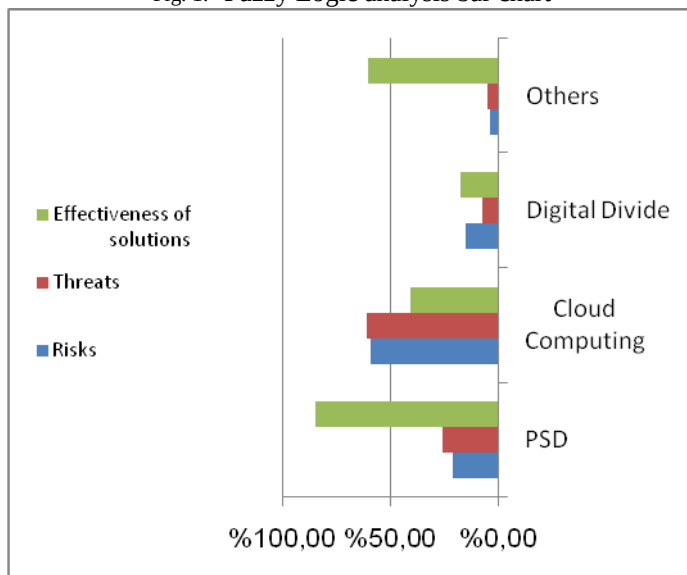
Table (3) shows the results of analysis :

TABLE (3) :FUZZY LOGIC ANALYSIS RESULTS

	PSD	Cloud Computing	Digital Divide	Others
Risks	21.25%	59.20%	15.34%	4.21%
Threats	25.85%	60.77%	7.95%	5.43%
Effectiveness of solutions	84.55%	40.95%	17.88%	60.54%

Fig. 1 illustrates the results of analysis by bar chart to show the clear effect of ICT on e-audit.

Fig. 1. Fuzzy Logic analysis bar chart



11. CONCLUSION

In this paper the results of Fuzzy Logic analysis of the questionnaires indicate the following:

- The strengthening of e-audit security will lead to facilitate the audit process and increase the reliability and the speed of implementation.
- The expenses of reducing the collateral damage will increase the profits of audit firms in the future.
- The availability of national CSP will help to increase the customers' confidence in cloud computing and thus it increases the confidence in e-business environment.
- Finally, the proposed algorithm has the capability to deal with similar types of the same situations such as : ranking the best decisions to be dealt with, the best financial ratio in the bank , choosing the best applications in environmental sustainability , etc. therefore, the proposed method provides accurate selection and can be used easily in many sectors.

REFERENCES

- [1] Al-Hubaity , Qasim M. and Thabit , Thabit H. , (2012), The Use of Fuzzy Logic Model for Decision Making Depending on Multiple Linguistic Criteria: An Accounting Study in Ways of Pricing Products , journal of Tanmiatalrafiain , administration and economic collage , University of Mosul , 110(34) , pp: 105-122.
- [2] Ali , Amir Hatem , (2011) , The Power of Social Media in Developing Nations: New Tools for Closing the Global Digital Divide and Beyond , Harvard Human Rights Journal , Vol. 24 , issue 1 .
- [3] Alptürk E (2008), Electronic Auditing Guide. Kurtiş press, Ankara, Turkey
- [4] ANAO , (2011) , Audit Report No. 18 , Australian National Audit Office , Information and Communications Technology Security : Management of Portable Storage Devices , Barton , Commonwealth of Australia .
- [5] Bernier, Gwenaëlle, and Suire, Julien, (2014), Meeting the VAT e-audit challenge, Indirect tax briefing, Issue 11 .
- [6] Buente, Wayne, and Robbin , Alice. (2008), Trends in Internet Information Behavior, 2000-2004 , Journal of the American Society for Information Science and Technology , 59(11) Available on www.interscience.wiley.com.
- [7] COSO , (2012) , Enterprise Risk Management for Cloud Computing , Committee of Sponsoring Organizations of the Treadway Commission , USA .
- [8] Dijk , Jan van and , Hacker , Kenneth ,(2003) , The Digital Divide as a Complex and Dynamic Phenomenon , The Information Society, 19 , Taylor & Francis Inc. , USA .
- [9] El-Hossainy , T.M., (2011), A Fuzzy Model for Multi-Criteria , JKAU: Eng. Sci., 1(22) , pp: 99-118.
- [10] GFI , (2011) ,The threats posed by portable storage devices , Available on www.gfi.com .
- [11] Huang, Chun-Yao; Chen , Hau-Ning , (2010) , Global Digital Divide: A Dynamic Analysis Based on the Bass Model , Journal of Public Policy & Marketing 29 (2).
- [12] Nemec, Joseph Jr., Germany, Rhonda, and Weinberg, Jim, (2011), The e-Audit : The road map to value capture in e-business's second wave, e-Insights, Booz, Allen & Hamilton Inc.
- [13] NIST , (2007) , Guide to Storage Encryption Technologies for End User Devices , U.S. Department of Commerce , Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology , USA.
- [14] Novák, V., Perfilieva, I. and Močkoř, J., (1999) , Mathematical principles of fuzzy logic , Dodrecht: Kluwer Academic.
- [15] Praseno, Arief, (2012), IT-Based Audit (e-Audit) Plan in Indonesia: An Analysis of the Program Logic, Feasibility, and Alternatives, International Institute of Socail Studies (ISS), The Hague, The Netherlands.
- [16] Ross, Timothy J. , (2010), Fuzzy Logic with Engineering Applications , Third Edition , John Wiley & Sons, Ltd.

- [17] Selvi Y, Türel A, and Senyigit B , (2006) , Accounting Auditing in Electronic Information Environments , I. International Turkish Financial Auditing Symposium, VII. Turkish Financial Auditing Symposium. Istanbul, Turkey.
- [18] Thabit , Thabit H. , (2013), Adoption The Fuzzy Logic To Enhance The Quality Of The Accounting Information To Operate Balanced Scorecard - Applied on Mosul Bank For Development & Investment in Nineveh Province" , M.Sc. thesis in accounting , University of Mosul , Mosul , Iraq.
- [19] Toni, A. D. and Tonchia, S., (2001), Performance measurement systems models , characteristics and measures , International Journal of Operations & Production Management , 2(1/2).
- [20] US-CERT , (2012) , US-CERT Security Trends Report : 2012 in Retrospect , Homeland Security , USA.