Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 3, September 2018, pp. 1168~1175
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i3.pp1168-1175

The Factors Affecting on Managing Sensitive Data in Cloud Computing

Haifaa Jassim Muhasin[1], Rodziah Atan[2], Marzanah A.Jabar[3], Salfarina Abdullah[4]
[1,2,3,4]Department of Software Engineering & Information System, Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM), 43400 Selangor, Serdang, Malaysia
[2]Halal Research Products Institute, University Putra Malaysia, Serdang, Selangor, Malaysia
[1]College of Education for Pure Science Ibn-Al-Haitham, Department of Computer Science, University of Baghdad, Baghdad, Iraq

Article Info

Article history:

Received Apr 12, 2018
Revised Jun 13, 2018
Accepted Jun 27, 2018

Keywords:

Cloud Computing
Identity Anonymity
Privacy
Security
Sensitive Data

ABSTRACT

Cloud computing represents the most important shift in computing and information technology (IT). However, security and privacy remain the main obstacles to its widespread adoption. In this research we will review the security and privacy challenges that affect critical data in cloud computing and identify solutions that are used to address these challenges. Some questions that need answers are: (a) User access management, (b) Protect privacy of sensitive data, (c) Identity anonymity to protect the Identity of user and data file. To answer these questions, a systematic literature review was conducted and structured interview with several security experts working on cloud computing security to investigate the main objectives of proposed framework, a pilot study by using a structured questionnaire was conducted. Framework using multilevel to enhance management information system on sensitive data in cloud environment.

Corresponding Author:

Haifaa Jassim Muhasin,
Department of Software Engineering & Information System,
Faculty of Computer Science and Information Technology,
University Putra Malaysia (UPM), 43400 Selangor, Serdang, Malaysia.
Email: haifaajassim@yahoo.com

1. INTRODUCTION

Increasing internet users on web sites, or surfing the internet requires new ways to manage the size, diversity and availability of data, therefore, the users trend towards using cloud computing. Cloud computing has defined by National Institute of Standards and Technology (NIST) as follows: Cloud computing is a comprehensive and system-wide access model, which is a set of changes and configuration of permitted computing resources, including servers, networks, applications, storage space and services [1] .

The cloud computing model aims to provide a great deal of computing power in a virtual way by combining all services and resources into a one system. The paper [2] defines cloud deployment models that include public, private, hybrid, and community. It also talks about key features such as broadband access, fast flexibility, measured services, self-service demand and resource pooling. In terms of service models provided by NIST consist of Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service. Cloud computing like other IT fields, suffers from a lot of security and privacy issues, which must be addressed [3-5]. These risks related to policy and regulatory risks, technical risks, legal risks and others [6].

The main objective of this paper is improving and managing sensitive data in public cloud for effective information systems decisions making. This paper explains the factors influencing the decision of management systems on sensitive data and relations between these factors in cloud environment.

The remainder of this paper is as follows: The related works is discussed in section 2. The methodology used for conduct the research explained in section 3. In section 4 gives the results of the research. Section 5 gives the discussion. Finally, section 6 for conclusion.

2. RELATED WORKS

Privacy and security problems resulting from the illegal use of information, and disclosure of secret information, can hinder the acceptance of cloud services by users. Recent studies support this idea, this indicates to the fact that the primary reasons for non-adoption of cloud computing services for many users is privacy and security concerns.

The analysis of many research works in the information technology used in cloud computing includes many factors affecting the privacy and security of data including authorization, authentication, confidentiality, integrity, and availability. The authorization mechanism required from user some authorization to reach and use the cloud service. The provider problems some authority to the user which point out what type of processes that can be perform by user [7]. Authentication is identifying an authorized user before getting access to the service of cloud and the user used verification steps [7]. Confidentiality where the user of cloud is responsible for any process carried out that may cause data changes or loss by others in the cloud and specified to limit the confidential data access to intended user only [8]. Integrity is specified to guarantee the accuracy of the transmitted information without any change. Integrity is one of important issues related to cloud security [8]. Availability specified to make sure that the authorized users can access cloud resources anytime and anywhere upon request [9].

Many studies have addressed privacy and security vulnerabilities by proposing models that increase the effectiveness and strength of security and privacy in cloud computing environment. Paper [10] have identified several ways in which unauthorized or inappropriate access to personal information in the cloud provided, such as the lack of enforcement for access control or change of policies by un protected data or/and unauthorized entities within the cloud.

The paper [11] explained reviewed issues of privacy, trust and analysis of threats related to privacy, trust and security. They provide a solution to achieve a reliable and secure cloud computing. This research provides the requirements of security for personal requirements, effective governance and some encryption techniques and a secure model for virtualization in the cloud computing system.

The paper [12] explains the framework that describes security problems of service delivery models. The researchers first explain the security of each delivery model. After the analysis of model, the authors find a lot of issues related to the SaaS model. Paper [13] describe deployment and service models in cloud computing. The researchers presented and explained cloud storage architecture and provide security and requirements of storage as a service. They also explain the security concerns related to storage in the cloud. A trusted environment for customers must be ensured the cloud service provider. The instructions and data stored in the cloud are accessible only to trusted users. Reliable execution techniques are provided a reliable method to check the integrity of the system [14], [15]. Also, the integrity of any system extends to software management, applications, and security policies. In paper discuss issues related to storage and data security in cloud computing. Also, discussed many issues, developments related to cloud computing data and the security of their storage. They also provided analysis of some issues related to authentication, web services, availability, authorization and accountability, the authors derived some of mechanisms and techniques for each feature to obtain privacy for data and secure storage.

In [17] present challenges and security issues related to private and public clouds. Some security issues such as multiple tenant service issues, identity issues, access control, availability of service and data storage issues have been discussed. All of these issues focus on aspects of data management and use. In [18] discussed the steps to deal with security and cloud problems before making the decision to adopt cloud computing, the need to develop a strategy of governance and technology, the strength of cloud computing, analysis of errors and profits and management of information security in the cloud. The paper [19] discusses the basic features of cloud, security problems, threats and appropriate solutions. The paper also discusses many topics related to cloud, namely cloud architecture, service, deployment models, technologies and concepts for cloud security, attacks and threats.

The main objective of the paper [20] is to offer security for the data stored in the cloud database from security threats related to cloud computing. The authors propose a new methodology that can effectively manage data security and provide privacy to users using cloud services. This paper provides additional control system that acts as an interface between the cloud user and the owner of the cloud. This approach gives security from view point of user and owner and giving flexibility to the infrastructure of cloud and has added feature of preventing a user account when doing a wrong activity. In the paper [21] a cloud security management model was proposed to address leakage of personal information to a network

selling security applications where personal information is divided into two types important and general information to ensure that private data does not leak and store it in a private cloud. The cloud-based membership service is provided and cloud-based system is also being applied to test the new model of framework and the results show that the model is viable.

The authors in paper [22] proposed a new method to protect security, access control, confidentiality and integrity of sensitive data for cloud users through the using of multiple cloud service providers. The organization encrypts sensitive data related to its security policy and procedures and storing encrypted data in reliable cloud. The keys used in encryption process are also encrypted and stored again in another area of the cloud and the organization have keys for encrypted data keys. Only the authorized entity can access and use the data and can prevent internal attacks by providing certain privileges. The paper [23] used a different approach to secure personal data and business data in the cloud. The authors proposed a system to prevent data access methods by classifying user behavior to determine if a person wants to access someone else's files in the cloud. They also used the technique of using dummy information in the system of files to mislead hackers who want to steal data from inside the cloud.

In paper [24] the researchers proposed approach to enable the protection of private data on personal health records (PHR) to control sensitive data and to address potential vulnerability to privacy. In addition to supporting accurate data access based on owner-specific privacy policies, it provides a cryptographic mechanism and key management approach to enforce privacy policies for PHR data.

3. METHODOLOGY

This research has been done literature review systematically according to guidelines that proposed by Kitchenham [25], [26]. 'The systematic literature review begins with the review plan, the research identifies, choosing the papers, the data extracting, data synthesis'. The systematic literature review was done to answer the research question of what the factors are affecting on managing sensitive data in cloud computing.

And a structured interview and survey was conducted to answer the question of which factors with significant effect on the decision of management systems on sensitive data in cloud environment.

3.1. The systematic Literature Reviews

The literature review has been done systematically according to guidelines that proposed by Kitchenham [25], [26]. 'The systematic literature review begins with the review planning, the identifying of research, choosing the papers, the data extracting, and data synthesis'. These steps shown in Figure 1.

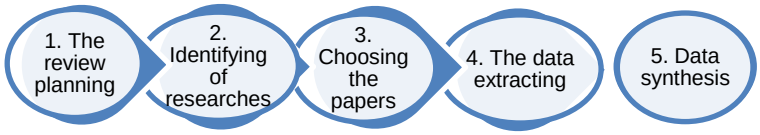

Figure 1. The steps of Systematic Literature Review

3.1.1. The Review Planning

The first step of the systematic literature review is defined and determine a strategic plan for research. The strategic plan that will be used in our research is the search for specific terms from specific sources such as journals, databases, e-books, and conferences.

3.1.2. Identifying of Researches

The research began by defining terms and keywords related to the subject of research. The keywords are used to search for many papers related to managing and protecting the privacy of sensitive data in cloud computing. The strategic plan for searching was to find published research in conferences, journals, and e-books stored in electronic databases, ACM, IEEE Explore, Elsevier's Science Direct, Springer Link, and Scopus.

3.1.3. Choosing the Papers

To identify papers related to the subject of research. The papers were selected from the papers published in scientific conferences and journals. At the beginning, a number of papers were selected,

summaries and conclusions were read. Then, a number of research papers were selected. In the second stage, the full selected research papers were read with details.

3.1.4. The Data Extracting

After choosing the papers, all information related to cloud data privacy and security and factors affecting on managing sensitive data in cloud computing were extracted.

3.1.5. Data Synthesis

After the relevant papers were selected, researchers started to understand the privacy and security of information in cloud computing and related definitions. In addition, researchers discussed the most important factors affecting the decisions of information systems in the management of sensitive data in the cloud computing.

3.2. The Collection of Data

The structure interview with several security experts and questionnaire was conducted. Structured interview uses 12 questions, and a total of 32 copies of questionnaire were sending by using online survey (Google Drive) and 29 were completed the questionnaire, the results were analyzed by Statically Package for Social Sciences (SPSS), Version 20. These interviews and survey will answer the research question of which factors with significant effect on the decision of management systems on sensitive data in cloud environment.

4. THE RESULTS OF RESEARCH

4.1 Systematic Literature Review Results

From the systematic literature review findings, the first question of research was answered. The factors affecting on managing sensitive data in cloud computing are: the data confidentiality, integrity, privacy, availability, data authentication and user authorization as shown in Figure 2.

The factor of Data Confidentiality deals with not disclosing data to unauthorized users, including customer, cloud service provider, internal users, and malicious insider and also transfer of data between authorized parties to prevent data leakage. Integrity refers to the trust merit of the migrated resources. In addition, the data migrated into the cloud must only be adjustable by authorized users [8]. Privacy refers to protect personally identifiable information (PII) within the cloud from any attacks that aim to find out the identity of the person that PII related to.

Availability refers to the migrated resources, such as data or applications, being reachable when needed and the cloud service being obtainable as per the agreement [9]. Authentication is a service for the classification of user accounts and data file. It performs setup an account, saving, storing, delete and manage individual user account and data file [8]. Other measures are such as authorization and access control [27].

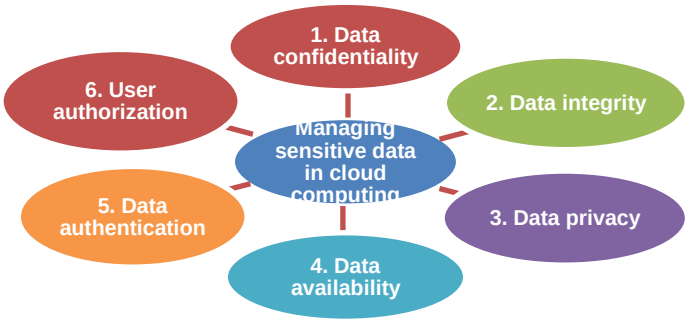

Figure 2. The factors affecting on managing sensitive data in cloud computing

The study proposed multilevel licensing framework (M2LF) according to the systematic literature review findings. The proposed framework applies methods deals with the challenges of privacy, confidentiality, integrity and availability to enhance managing information systems decision making on sensitive data in cloud environment as shown in Figure 3.

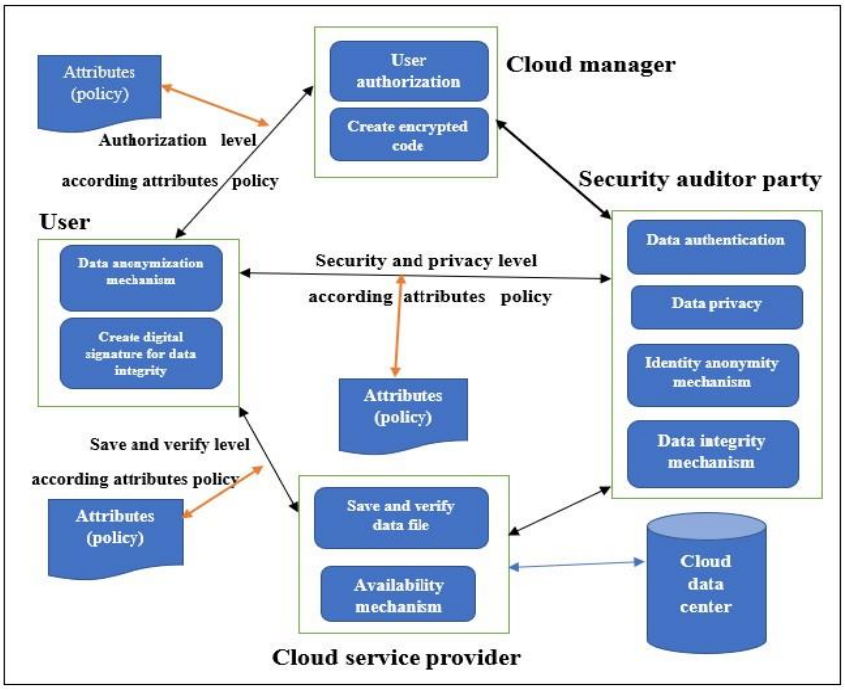

Figure 3. The proposed framework

4.2 Statistical Analysis Results for Interviews and Survey

4.2.1. Validity of Proposed Framework

After the structured interviews were conducted, the results of interviews were analyzed. The results show that there is 92.59% among experts agree with the framework viability and the framework enhances the privacy and security of sensitive data in cloud, and 94.45% among experts agree with processes used in proposed framework and the framework have suitable confidentiality, integrity, and availability procedures that support the privacy of sensitive data, and 94.44% among experts agree on the applicability of proposed framework and the procedures for the parties of framework enhance the protection of sensitive information, also 92.59% among experts agree on the understandability for proposed framework. As well 83.33% among experts agree with the description of responsible parties, and policies that used in proposed framework.

4.2.2. The Test of Reliability

After the validation of the framework through the interviews and the framework was adjusted according to the results of interviews with experts. The questionnaire was developed according to the revised framework. This pilot study was conducted with potential participants from the population of IT professionals who work in the IT field. A total of 32 copies of questionnaire was sending online by using survey (Google Drive). 29 were completed the questionnaire, the results were analyzed by SPSS 20.

The reliability of survey instrument according the hypotheses for (M2LF) framework. The reliability of survey was computed with Cronbach's alpha (a) to illustrate the mean versus the median and rank for the research hypotheses [28,29]. The pilot test results indicate that the Cronbach's alpha for all coefficients ranged from (a=0.825) for data confidentiality, (a=0.846) for data integrity, (a=0.859) for data availability, (a=0.912) for data privacy. With an overall reliability of (a=0.959).

The reliability measurements of the scales examined using Cronbach's alpha (a) gave a strong reliability result with (a=0.959) for alpha. This finding indicates that all the instruments are valid. All the factors values are above 0.7 and suitable to proceed with the empirical study later the results shown in Table 1.

The statistical results of the pilot study for respondents' characteristics showed that there was 51.7% of respondents were female and 72.41% of respondents were Asian. Also 34.6% were academic experts. And 69% have experience less than 10 years, as well 65.6% working less than10 years in the IT, and 96.6% have work experience less than 10 years. Lastly, 86.2% working less than 10 years with security issues. Table 2 gives the details of information about respondents' demographic data.

Table 1. Statistics of Reliability Coefficients

No	Scale	N of Items	Cronbach's alpha	Results
1	Data Confidentiality	13	0.825	Good
	a- User Authorization	7	0.702	Acceptable
	b- Data Authentication	3	0.713	Acceptable
	c- *Data Anonymity*	3	0.710	Acceptable
2	Data Integrity	9	0.846	Good
	a- User Authorization	3	0.730	Acceptable
	b- Data Authentication	3	0.704	Acceptable
	c- *Identity anonymity*	3	0.748	Acceptable
3	Data Privacy	28	0.912	Good
	a- Defining the responsibilities	10	0.771	Acceptable
	b- Identity Management	15	0.848	Good
	b1- User Authorization	5	0.704	Acceptable
	b2- Data authentication	4	0.717	Acceptable
	b3- Identity anonymity and Data classification	6	0.724	Acceptable
	c- *Data anonymity*	3	0.748	Acceptable
4	Data Availability	11	0.859	Good
	a- Authorization mechanism	2	0.726	Acceptable
	b- Authentication mechanism	3	0.739	Acceptable
	c- *Storage mechanism*	6	0.750	Acceptable
	All Items	61	0.959	Good

N = Number of items

Table 2. Respondents Demographic Data

		Frequency	percent
1	Gender		
	Male	14	48.3%
	Female	15	51.7%
2	Nationality		
	Asian	21	72.41%
	Middle East	5	17.24%
	African	3	10.35%
3	Professional role		
	Academic expert	10	34.6%
	User of cloud	9	31.0%
	Technical expert	6	20.8%
	Researcher	1	3.4%
	Senior analyst	1	3.4%
	Web developer	1	3.4%
	Technical IT	1	3.4%
4	Experience		
	Less than 10 years	20	69%
	Between 10-20 years	9	31%
5	Number of years working in the IT		
	Less than 10 years	19	65.6%
	Between 10-20 years	9	31.0%
	More than 20	1	3.4%
6	Number of years working with cloud computing		
	Less than 10 years	28	96.6%
	Between 10-20 years	1	3.4 %
7	Number of years working with security issues		
	Less than 10 years	25	86.2%
	Between 10-20 years	4	13.8%

5. DISCUSSION

According to literatures and the results of statistical analysis and the reliability test, the factors which enhancing the management of information system decision making on sensitive data in cloud computing; Data Confidentiality (DC), Data Integrity (DI), Data Privacy (DP), and Data Availability (DA). Using four mediators based on pilot study results as follows: Authorization positively influences (DC, DI, DP, and DA). Authentication positively influences (DC, DI, DP, and DA). Anonymity positively influences (DC, DI, and DP). Defining the responsibilities positively influences DP. All of these factors influence on the decision of management information systems on sensitive data in public cloud.

6. CONCLUSION

The literatures in this research was identified and explained the factors affecting on the decision of management information systems on sensitive data in public cloud such as: Data Confidentiality, Data Integrity, Data Privacy, Data Availability, Authorization, Authentication, Anonymity, and Defining the responsibilities. Interviews and survey were conducted to explain the influence of these factors on the decision of management information systems on sensitive data in cloud environment.

ACKNOWLEDGEMENT

This paper is sponsored by Ministry of Higher Education Malaysia through Fundamental Research Grant Scheme Project no.: FRGS/1/2015/ICT04/UPM/02/2 Vote no.: 5524829 on Establishing Theory for Cloud Platform Measure Based on SLA Management and Enforcement.

REFERENCES

[1] Zhang Q, Cheng L, Boutaba R. Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*. 2010 May 1;1(1):7-18.
[2] Mell P, Grance T. *The NIST definition of cloud computing, recommendations of the national institute of standards and technology*. National Institute of Standards and Technology. 2011 Sep:800-145.
[3] Coppolino L, D'Antonio S, Mazzeo G, Romano L. Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*. 2017 Apr 1; 59:126-140.
[4] Ramachandran M. Software security requirements management as an emerging cloud computing service. *International Journal of Information Management*. 2016 Aug 1;36(4):580-590.
[5] Ramachandra G, Iftikhar M, Khan FA. A Comprehensive Survey on Security in Cloud Computing. *Procedia Computer Science*. 2017 Jan 1; 110:465-472.
[6] Catteddu D. Cloud Computing: benefits, risks and recommendations for information security. In *Web application security* 2010 (pp. 17-17). Springer, Berlin, Heidelberg.
[7] Sen J. Security and privacy issues in cloud computing. *Architectures and protocols for secure information technology infrastructures*. 2013 Sep 30:1-45.
[8] Zissis D, Lekkas D. Addressing cloud computing security issues. *Future Generation computer systems*. 2012 Mar 1;28(3):583-592.
[9] Tebaa M, Hajji SE. From single to multi-clouds computing privacy and fault tolerance. *IERI procedia*. 2014 Jan 1; 10:112-118.
[10] Pearson S, Charlesworth A. *Accountability as a way forward for privacy protection in the cloud*. In IEEE International Conference on Cloud Computing 2009 Dec 1 (pp. 131-144). Springer, Berlin, Heidelberg.
[11] Saripalli P, Walters B. *Quirc: A quantitative impact and risk assessment framework for cloud security*. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on 2010 Jul 5 (pp. 280-288). IEEE.
[12] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*. 2011 Jan 1;34(1):1-11.
[13] Kulkarni G, Waghmare R, Palwe R, Waykule V, Bankar H, Koli K. *Cloud storage architecture*. In Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on 2012 Oct 30 (pp. 76-81). IEEE.
[14] Futral W, Greene J. *Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters*. Apress; 2013 Oct 8.
[15] Computing SC. *Building Trust and Compliance in the Cloud with Intel® Trusted Execution Technology*. media13.connectedsocialmedia.com
[16] Aguiar E, Zhang Y, Blanton M. An overview of issues and recent developments in cloud computing and storage security. In *High Performance Cloud Auditing and Applications* 2014 (pp. 3-33). Springer, New York, NY.
[17] Tari Z, Yi X, Premarathne US, Bertok P, Khalil I. Security and privacy in cloud computing: Vision, trends, and challenges. *IEEE Cloud Computing*. 2015 Mar;2(2):30-38.
[18] Krishna BH, Kiran S, Murali G, Reddy RP. Security issues in service model of cloud computing environment. *Procedia Computer Science*. 2016 Jan 1; 87:246-251.
[19] Singh A, Chatterjee K. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*. 2017 Feb 1; 79:88-115.
[20] Mishra S, Tripathy AK, Joshi P. Making a Cloud Data Secure and Effective for Better Performance of Services. *Indonesian Journal of Electrical Engineering and Computer Science*. 2016 Jun 1;2(3):695-702.
[21] Qiong S, Liu M, Pang S. Cloud Computing Application of Personal Information's Security in Network Sales-channels. *Indonesian Journal of Electrical Engineering and Computer Science*. 2013 Dec 1;11(12):7331-7338.
[22] Gunasekhar T, Rao KT, Reddy VK, Kiran PS, Rao BT. Mitigation of Insider Attacks through Multi-Cloud. *International Journal of Electrical and Computer Engineering*. 2015 Feb 1;5(1):136.
[23] Sastry KN, Rao BT, Gunasekhar T. Novel Approach for Control Data Theft Attack in Cloud Computing. *International Journal of Electrical and Computer Engineering*. 2015 Dec 1;5(6).
[24] Leng C, Yu H, Wang J, Huang J. Securing personal health records in the cloud by enforcing sticky policies. *Indonesian Journal of Electrical Engineering and Computer Science*. 2013 Apr 1;11(4):2200-2208.

[25] Kitchenham B. Procedures for performing systematic reviews. Keele, UK, Keele University. 2004 Jul; 33 (2004):1-26.
[26] Kitchenham B, Pretorius R, Budgen D, Brereton OP, Turner M, Niazi M, Linkman S. Systematic literature reviews in software engineering–a tertiary study. *Information and Software Technology*. 2010 Aug 1;52(8):792-805.
[27] Wang Z. *Security and privacy issues within the Cloud Computing*. In Computational and Information Sciences (ICCIS), 2011 International Conference on 2011 Oct 21 (pp. 175-178). IEEE.
[28] Walpole RE, Myers RH, Myers SL, Ye K. Probability and statistics for engineers and scientists. New York: Macmillan; 1993 Jan.
[29] Soja P. Examining the conditions of ERP implementations: lessons learnt from adopters. *Business Process Management Journal.* 2008 Feb 8;14(1):105-123.