Journal of Theoretical and Applied Information Technology
31st December 2018. Vol.96. No 24
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FACTORS AND MODEL FOR SENSITIVE DATA MANAGEMENT AND PROTECTION IN INFORMATION SYSTEMS' DECISION OF CLOUD ENVIRONMENT

[1,3]HAIFAA JASSIM MUHASIN, [1,2] RODZIAH ATAN,
[1]MARZANAH BINTI A.JABAR, [1]SALFARINA BINTI ABDULLAH

[1]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
[3]College of Education for Pure Science Ibn-Al-Haitham, Department of Computer Science, University of Baghdad, Baghdad, Iraq

E-mail: haifaajassim@yahoo.com, rodziah@upm.edu.my, marzanah@upm.edu.my, salfarina@upm.edu.my

ABSTRACT

Cloud computing is a growing field, providing the need for enterprises and individuals to access cloud computing resources to meet their organizational computing requirements. The features of scalability, low cost and unlimited resources of cloud computing encourage many organizations and individuals to transfer their data including personal, financial or health data to the cloud. However, security and privacy are main issues in cloud computing because of the factors of confidentiality, integrity, availability and privacy. As well as access control, management and internal attacks. These fears become one of the biggest challenges in the cloud, especially when dealing with sensitive data.

This paper described a research done that proposed a framework to enhance information systems decision on managing sensitive information in cloud environment. The main factors are defining which are influencing on decision of management system on sensitive data in cloud and explain the model for these factors. Also, this paper explains shared responsibilities by all parties in the proposed framework which is one of our contribution for this study. The empirical study was conduct which is include expert-questionnaire, interview for pilot study and interviews validation. The proposed framework was evaluated through experts from academics and industries. The results of validation process confirmed the validity of proposed framework and the validity and reliability of the instrument proposed for the study. Empirical study was verified the proposed framework. This framework is enhanced information systems decision on managing sensitive information in cloud computing. This framework using multilevel related to Authorization, Authentication, classification and identity anonymity, and save and verify. The findings for this study by using anonymization technique and classifying the contents of the sensitive data file confirmed preserve privacy and security of sensitive data and enhanced the managing sensitive data.

Keywords: *Cloud Computing, Privacy, Confidentiality, Anonymity, Sensitive Data, Information System Decision*

1. INTRODUCTION

In this paper, the coverage will be emphasized into categories related to sensitive data in cloud computing. Cloud computing is a technology that helps access to resources such as networks, servers, services and applications. Common computing models are based on data traffic and organized by a third party [1]. For this reason, data security and privacy management are considered one of the biggest challenge for sensitive data in cloud environment [2].

The empirical study is conduct through expert interview, questionnaire for pilot study, proposed and implemented the modules of framework to enhanced information decision on managing sensitive information in cloud computing.

Privacy is one of the important issues in cloud computing, because all users have data stored on the cloud and to access them need connected to cloud servers. This information may be confidential or financial information. While, personal information is considered privacy to individual [2]. The optimal use of cloud - based services depends on the management of cloud security and the security of personal information of the organization or individuals. This is major concern for many cloud users and needs appropriate solutions [3]. The management sensitive data in cloud computing need many factors to enhance decision making in information systems.

Managing sensitive data requires many factors to enhance decision making in information systems. This paper explores the factors influencing decision making in information systems for sensitive data management, defining the model and proposed framework for managing and protecting sensitive data.

Hence, the purpose of this paper is to investigate the factors that effect on managing sensitive data for effective information system's decisions making and proposed the framework to enhance management of sensitive data in cloud computing.

The next section describes the related works of managing and protecting sensitive data in cloud, as well as review of factors affecting on managing sensitive data. In the following section, explains the factors that reviewed in the previous section and the hypotheses used for conduct the study. Then, section describes methods and design the modules for implementation proposed framework. The discussion section presents the results of the study. Finally, the conclusion with summary of the study are explained.

The main concerns discussed above are supported by various studies in similar context as found in literature review.

2. RELATED WORKS

The privacy and security of sensitive data in cloud computing are important issues. Margaret Rouse in [4] defined sensitive data as important data that must be protected from unauthorized access and managing the security and privacy of such data. There are three main types of sensitive data: personal information, personally identifiable information; such as medical information, financial information and unique identifiers such as passport or social security numbers. The second type of data is commercial information which includes information that leads to a risk to company if disclosed by the competitor such as trade secrets, completion plans, financial information, and customer information. The third type of data is classified information; this information related to a government and limited to the level of sensitivity such as confidential, secret and top secret [4].

The illegal use and disclosure of information can case non-acceptance of cloud services by users which are causing privacy and security problems. Many recent studies have shown that concerns and problems related to privacy and security are one of the most important reasons why cloud computing services are not adopted [5]. Some of these issues related to privacy such as loss of control, access control, data protection. Security of data is one of the concerns facing users of cloud computing. Many of these concerns related to personal information; information that may affect individuals and organizations. These concerns related to personal and sensitive data [6]. Researchers have proposed solutions for increasing accountability and secure access control methods to increase the storage security of privacy-sensitive data [7].

The authors propose the framework based on investigation on security factors effect adoption cloud computing. [8] discussed an adoption of cloud computing and problems associated with security and privacy issues. A study was conducted several interviews with cloud developers and security experts, and the related work was reviewed. Through this study, the current and future challenges are understood. The results lead to the identification of many security issues affecting cloud features. Other researchers explained the security factors that affect the adoption of cloud in the Saudi government agencies. A framework was proposed for three categories representing social factors, cloud security risks and cloud protection benefits that have known cloud security features. The initial framework was updated based on expert review and questionnaires. Quantitative and qualitative methods were used to ensure the validity of the results [9].

The privacy issues related to the user's secret data that stored in the cloud. The researchers discussed the need for general framework for maintaining privacy, which performs the task of maintaining user sensitive data. They are outlined the design of petri-net privacy preserving framework (PPPF) and moves the proposed technology and cooperates with privacy preserving cohesion technique (PPCT) to improve reliability and adaptability and increase the demand for information privacy [10].

Ali et al. in [11] discussed many security matters such as legal security, compliance and architectural security. This paper pointed out how authentication, licensing and integrity can provide web services in a safe method. In addition, it discusses the issue of security in cloud computing. The researchers in [12] provided a classification of security issues based on many security topics. This paper provides an explanation of some previous research. The authors provide many topics associated with security issues. This paper also makes some recommendations on the various challenges to be resolved later.

The researches provide an extensive study of privacy problems for cloud service providers and cloud security. The authors describe privacy problems separately from security. Initially, security terminology such as integrity, confidentiality, availability, access control, and audit characteristics are emphasized after that focusing on the methods used for privacy [13]. Research also provides some solutions on a multi-site storage server. Many problems related to cloud security such as sharing resources, controls, authentication, authorization and trust, as well as identity management, managing services related to security, privacy and data storage are discussed. But the authors did not provide solutions to these problems [14].

Abbas & Khan in [15] discuss the privacy issues only in the cloud of electronic health. They also explain open issues and countermeasures. Only the term cloud privacy is discussed. Another researcher proposed a system that contains double security for data on health records and proposed framework for storing these data by introducing isolation between cryptographic systems for sent data and stored data [16]. Many security issues associated with cloud computing and its advantages was described in the paper [17] but no solutions were identified for these issues.

Cloud computing is exposed to many security issues. Especially when the user sends his data to the cloud, there is a possibility of data loss. From the perspective of customer, security concerns for cloud computing still exist, particularly data security and privacy protection issues [18]. The problems related to security was verified through the perspective of privacy protection and information security.

Khan in [19] presents a survey of security issues in terms of security threats and their treatment. The study aims to contribute the analysis and classification of the working mechanisms of the main security issues and the possible solutions found in the literature. A comparison was made to the threats faced by the cloud platforms. In addition, intrusion detection and protection frameworks used to address security issues are compared. Trusted cloud computing and security compliance regulation mechanisms are also being developed between cloud service providers. Security mechanisms are still evolving. Thus, providing future orientation for security issues of cloud and possible countermeasures.

There are no suitable solutions for many questions related to managing and protecting the privacy of sensitive information [20]. Many of the existing solution use encryption methods by another party. These methods and techniques are based on the exchange of encryption keys, which may cause the detection of keys, and this leads to information penetration. In addition, encryption and decryption methods take a high cost of computing and a lot of time and space that can cause slower storage and retrieval of information [21], [22]. Therefore, the proposed framework permits verification of using the appropriate way to enhance information systems decision to managing protecting sensitive information in extensive environment such as cloud computing.

This research is done based on the factors found in previous work that are related to private and secured information sharing context.

3. SENSITIVE DATA MANAGEMENT FACTORS

The factors affecting the data privacy and security are discussed in many researches. The important factors affecting on sensitive data including authorization, confidentiality, authentication, integrity and availability.

This study was conducted to improve the management of sensitive data in public cloud in order to make effective decisions for information systems. This study explored factors affecting the decision of information systems on managing sensitive information in cloud computing environment. The study was initially based on structured interviews with many security experts working on cloud computing to investigate the main objectives of the proposed framework. Then a pilot study was conducted using a structured questionnaire.

The study extracted that the most influential factors are:

1. Data Confidentiality (DC) which deals with not disclosing data to unauthorized users, including cloud users, cloud service provider (CSP)- internal users, and malicious attackers and also includes secure deletion and transfer of data between authorized parties to prevent the data leakage.
2. Data Integrity (DI) that refers to the trust merit of the migrated resources. Especially, the data migrated into the cloud must only be adjustable by authorized users.
3. Data Privacy (DP) that refers to protect personally identifiable information (PII) within the cloud from antagonistic attacks that aim to find out the identity of the person that PII related to.
4. Data availability (DA) which refers to the migrated resources, such as data or applications, being reachable when needed and the cloud service being obtainable as soon as request.

Also, the mechanism of anonymity, found positive significance with three factors; namely, data confidentiality, data integrity and data privacy affect decision-making of information systems and supported. Also, the defining the responsibilities, found the importance of a positive factor with data privacy impact on the decision maker. And based on these factors, in order to make decision of information systems on sensitive data management in public cloud the organization management must improve and strengthen the mechanism of anonymity and defining the responsibilities in a good way to support the decision maker.

Figure 1 illustrates model have the four factors which are Data Confidentiality (DC), Data Integrity (DI), Data Privacy (DP), Data Availability (DA) that affecting on information systems decision on sensitive data management in proposed framework. In addition, this research model found four moderators that affect the main factors; authorization mechanism, authentication mechanism, anonymity mechanism and defining the responsibilities.

3.1 Hypotheses model

In this study Figure 2 explain Model hypothesis proposed of research, which were extract from literature review and pilot study. The main four factors Data confidentiality, Data Integrity, Data Privacy, and Data Availability are considered to be directly influential to enhance information system decision making on sensitive data management. Therefore, we hypothesized the main four hypotheses are as follows:

H1: Data confidentiality (DC) positively affects information systems decision on sensitive data management in public cloud.

H2: Data integrity (DI) is positively related to information systems decision on sensitive data management in public cloud.

H3: Data privacy (DP) positively affects information systems decision on sensitive data management in public cloud.

H4: Data availability (DA) positively influence the decision of information systems on sensitive data management in public cloud.

The four moderators which affect the main factors: authorization mechanism, authentication mechanism, anonymity mechanism and defining the responsibilities. Based on the pilot study on research work, hypotheses obtainable as follows:

H5: Authorization positively influences (DC, DI, DP, and DA) and the decision of information systems on sensitive data management in public cloud.

H6: Authentication positively influences (DC, DI, DP, and DA) and the decision of information systems on sensitive data management in public cloud.

H7: Anonymity positively influences (DC, DI, and DP) and the decision of information systems on sensitive data management in public cloud.

H8: Defining the responsibilities positively influences DP and the decision of information systems on sensitive data management in public cloud.

According to these factors and hypotheses, the study proposed a multi-level licensing framework (M2LF) to enhance information systems decision making on sensitive data management in cloud computing environment.

4. M2LF FRAMEWORK DESIGN IMPLEMENTATION

This study attempts to find if some of the factors influencing sensitive data security and privacy protection have to do with Authorization, Authentication, classification and Identity Anonymity, and Save and Verify. A survey was conducted to test the instrument for validity after investigate the main objective of proposed framework and suitability of instrument by interview with various security experts working on cloud computing security. The structured interview conducted and the results was analyzed. The proposed framework was revised according to the experts' feedback. Then the questioner was developing according to the revised framework. This pilot study is conducted with potential participants who fit the IT professional population being studied and working in IT department. The sample size to pilot test is small as normal, ranging from 15-30 respondents but it can be increased if the test requires several stages. So, a total of 32 copies of questionnaire was sending by using online survey and 29 were completed the questionnaire, the results were analyzed by SPSS 20. The process was achieved within three months from February-April 2017.

4.1 Structured Interview Measurement

Structured interviews were conducted with nine experts in cloud computing security from academics and industries. Five experts from academics and four from industries. Structured interview use 12 questions; 3 questions to verify the proposed framework feasibility enhance data confidentiality, privacy and improve the quality of security for public cloud, 2 questions to verify the proposed framework have appropriate confidentiality, integrity, and availability measures and include privacy-enhancing solutions for sensitive data protection, 2 questions to verify the proposed framework applicability and the procedure of access control and the procedures by the parties of framework support the protection of sensitive data, 3 questions to verify the proposed framework understandability, correctness, prevents data leakage, data loss, and providing protection of customer assets from unauthorized access, 2 questions to verify comprehensive of framework, the description of responsible parties and roles and security policies that used by the parties of framework enhance the protection of sensitive data. The data gathering in interview in office face-to-face. The interviews took place in personal offices and lasted between 30 to 45 minutes.

4.2 Measurement using pilot study

The Likert scales were utilized for measuring the security and privacy processes and procedures in framework (M2LF) towards factors influencing sensitive data security and privacy [23]. Examining factors that influencing sensitive data security and privacy by requesting from user to give the judgments value that is relevant to these factors and using in survey with the Likert scales to measure opinions, attitudes, and behaviors. The questionnaire consisting of multiple choice-questions. The instrument using a five-point Likert scale with values ranging from 1 Strongly Disagree to 5 for Strongly Agree. And used scale with values ranging from 1 Unimportant at all to 5 for Very Important to evaluate the important of activities. The questionnaire of the study is consisted from eight sections from 70 questions. Section 1: is a group of questions related to personal information about the respondents such as: name, job, country and the demographic information is included in this section. Section 2: is a group of nine questions for measuring Authorization Activities efficiency. Section 3: is a group of twelve questions for measuring Authentication Activities efficiency. Section 4: is a group of seven questions which aim for measuring the Classification and Identity Anonymity Activities efficiency. Section 5: is a group of four about Save and Verify Activities efficiency. Section 6: is a group of twelve questions which are target for measuring efficiency of activities according to objectives. Section 7: is a group of seven questions for measuring Activities Efficiency of framework. Section 8: is a group of ten questions for measuring Security Technologies Activity of framework.

4.3 The results of structured Interview and reliability test of pilot study

After the structured interviews undertook the results of interviews was analyzed. The results explain that there is 92.59% among experts agree with the proposed framework feasibility and the framework enhance data confidentiality, privacy and improve the quality of security, 94.45% among experts agree with the measures used by the proposed framework and the framework have appropriate confidentiality, integrity, and availability measures and include privacy-enhancing solutions for sensitive data protection, 94.44% among experts agree on the proposed framework applicability and the procedures used by the parties of framework support the protection of sensitive data, 92.59% among experts agree on the proposed framework understandability. Also 83.33% among experts agree on comprehensive and the description of responsible parties, roles and security policies that used by the parties of framework enhance the protection of sensitive data. The ranking of experts' interview results shown in table 1.

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 loading values are above 0.7 and suitable to proceed with the empirical study see table 2 for reliability results.

Table 1: Ranking of results from experts' interview

	Percent	Rank
Appropriate measures for confidentiality, integrity and availability and privacy enhancing solutions.	94.45 %	1
Framework applicability and procedures used by parties support the protection of sensitive data.	94.44 %	2
Framework feasibility and enhance data confidentiality and privacy	92.59 %	3
The framework understandability	92.59 %	4
The description of responsibility, roles and policies that used by the parties enhance the protection of sensitive data.	83.33 %	5

5. MODULES DESIGN FOR M2LF FRAMEWORK

The modules using to describe application of managing sensitive data in cloud computing. In this stage the modules of user part and cloud part are specifying the requirements of the tools, algorithms and procedures for data anonymity and digital signature in user part and user authorization, authentication and save and retrieve data file in cloud part. A module is a technique which explores a task managing sensitive data. Scenario of module specify actors, roles, processes, the goal(s) of the actor(s), and events that can occur in the course of attempting to achieve the goal. These are several modules formations the managing sensitive data in cloud computing.

M2LF is a framework proposed to managing sensitive data. The modules are divided into 2 sides; 1) the client side, 2) the cloud service side.

Table 2: Statistics of Reliability Coefficients

	Scale	N of Items	Cronbach's alpha	Results
1	**Authorization Activities efficiency**	**9**	**0.762**	Acceptable
2	**Authentication Activities efficiency**	**12**	**0.866**	**Good**
3	**Classification and Identity Anonymity Activities efficiency**	**7**	**0.893**	**Good**
4	**Save and Verify Activities efficiency**	**4**	**0.824**	**Good**
5	**Efficiency of Activities according to objectives**	**12**	**0.859**	**Good**
	a- Reduce high cost of calculations and storage time and space	4	0.825	**Good**
	b- Prevent Malicious insiders	4	0.788	Acceptable
	c- Prevent Data Breach and Data Loss	4	0.713	Acceptable

6	**Activities Efficiency of framework**	**7**	**0.812**	**Good**
7	**Security Technologies Activity of framework**	**10**	**0.872**	**Good**
	All Items	**61**	**0.959**	**Good**

N= Number of items

5.1 Part 1: User Modules

These modules describe all the processes for managing sensitive data by data owner. Actors in this module are user, and company agent. The functions set are data anonymity and generate signature.

- **Data Anonymity**

  data anonymization is a technique used to preserved the privacy of information and individuals while information is shared for many purposes. Data anonymization is a concept of hiding sensitive data items of the data owner such as personally identifying information (PII); name, social security number, phone number, email, address and anything that identifies the person directly [24].

- **Digital Signature Creating**

  The signature method used in this module Digital Signature Algorithm (DSA). DSA is based on the difficulty of computing discrete logarithms and is based on RSA cryptography. Discrete logarithms are analogous to ordinary logarithms but operate over modular arithmetic. Given the difficulty of taking discrete logarithms, it is infeasible for adversary to recover the secret key from the value of signature and using Hash value for the content of data file in digital signature give strong integrity for the data file that send to cloud. A digital signature is an authentication mechanism that enables the owner of the file to send an icon representing the signature of the data file.

5.2 Part 2: Cloud Modules Design

Cloud module is the other side of the system implementation processes and cases for managing sensitive data in cloud from login until reach to user's data are included in this side of operation. Actors in these modules are user, company agent, cloud manager, security auditor party, cloud service provider. The functions set are update manager directory, identity data anonymity, enter encrypted code, user request, data authentication, save or retrieve data file.

This side of system is important due to its functionality for managing sensitive data. Algorithm created to download, upload, delete, and edit data file according to request of user. These processes need to authorization, authentication and save and retrieve modules.

The functions are described as follows:

- Update manager directory; in this function the contents of manager directory update according to access of user to cloud and this directory used in authorization level.

- Identity data anonymity; this function used by Security Auditor Party (SAP) to change user name and data file name to new values and save in SAP directory.

- Enter encrypted code; in this function request from user entered user encrypted code which generated by manager and send to user by email.

- User request; this function related to handles the user request such as upload, download, delete, or edit.

- Data authentication; this function related to processes of authentication for data file that will be downloaded, uploaded, deleted, or edited in cloud computing.

- Save or retrieve data file; this function related to the processes of save or retrieve data file according to user request.

5.2.1 User Authorization Module

This module ensure that no unauthorized user can reach to user's data in cloud computing and handles log in and log out and checks for access permissions. It interfaces with cloud manager.

This module describes the process of log into the cloud, gives and checks access permissions for many types of users and companies. Actors in this module are user, company agent, cloud manager. The functions set are login, check authorization information, update manager directory, create encrypted code. The activity diagram explains the steps of primary scenario of User Authorization in cloud computing as shown in Figure 3 :

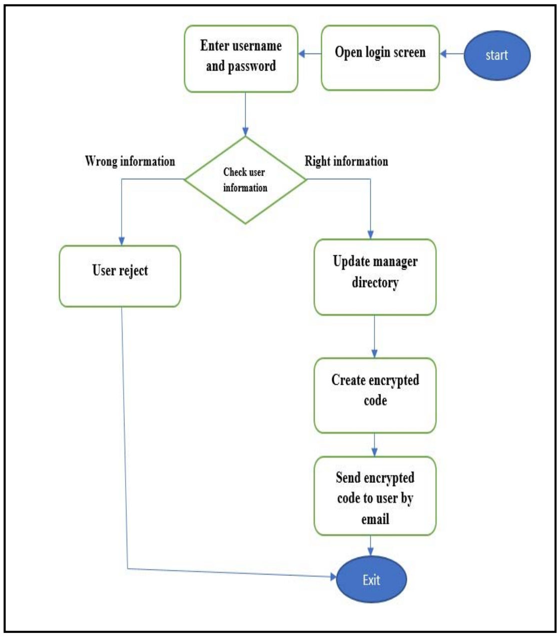

Figure 3: User Authorization Primary Scenario

The authorization level using policy between the user and the cloud manager depend on the number of attributes to be provided to confirm the security and privacy of the user data. The authorization level has policy attributes such as: number of access control from manager (NoAcM), number of access user (NoAu) can used the data, certificate symbols lists (CSLs), number of encrypted codes (NoEncCs). These attributes are the content of manager directory discussed in [25].

5.2.2 Authentication module

This module describes the processes of authentication for download data file, upload data file, delete data file and edit data file into cloud computing. Actors in this module are user, company agent, and security auditor party (SAP). The functions set are entered encrypted code, upload data file, download data file, delete file, edit file, update SAP directory.

The security and privacy level have many policy attributes to ensure that the data of user not modified or changed by unauthorized users and protect the privacy of personal sensitive data. These attributes are: Number of security and privacy mechanism (NoSecPrM), Number of data types (NoDTs), Number of resources (NoRs), Number of Authorized Users (NoAUs). These attributes were explained in [25].

The directory of SAP contains number of authorized users, user's codes, data file name, data file codes, data type, new user identity, new name of data file.

5.2.3 Save or Retrieve data file

This module describes the processes of save or retrieve data file according to user request. Actors in this module are user, company agent, cloud service provider (CSP). The functions set are check user and data file codes, save data in data center, update CSP directory.

The save and verify level has policy attributes to ensure of data safety and protect the privacy of user's data. These attributes are: Number of data types (NoDTs), Number of data centres (NoDCs), Number of Authorized users (NoAUs), these attributes were discussed in [25].

The directory of cloud service provider (CSP) contains number of authorized users' codes, data file codes, number of data types, new user identity, new name of data file, and number of data centers that use for save data files.

Implementation of modules for the framework and results achieved have verified the validity and credibility of factors affecting the management of sensitive data in the cloud. The empirical study to verify the final framework has proved its results and implementation of the modules related to the operations of the framework and the credibility of the mechanisms of licensing, authorization, authentication and identity anonymity on the factors of protection of data security, integrity, maintaining their privacy and availability affecting the decision of information systems.

6. RESULTS AND DISCUSSION

The experimental validity and data analysis was carried out to validate the research work. In this stage the experts' interviews are conducted. The validity questions divided into three parts include: the framework part, implementation program and contributions. Experts' interview was conducted with 6 experts and analyzed the results.

Validation questions are divided into three parts. The first concerns the proposed framework and consists of four questions. The second part concerns the tool used for implementation and consists of three questions. The third part relates to contributions related to the work of the research consisting of four questions. The interviews for validation research work were conducted with 6 experts, and the results of interviews were analyzed.

The minimum number of experts are three, as recommended by [26]. The results of the interviews confirmed the experts' agreement on the possibility of the framework and the quality of its performance in the management of sensitive data in the cloud and the results of tool implementation contributed to enhance the decision of information systems of managing sensitive data.

An analysis of the qualitative data and experts' viewpoint covered in this study are positive evidence that the validation and evaluation of the proposed framework has clearly shown its applicability and easy to use in context of managing sensitive data and enhancing the protecting of privacy and security for sensitive data in cloud environment. The validation of proposed framework meets the requirements and objectives of managing sensitive data in cloud for effective information systems decisions.

The factors that effect on the decision of information systems on sensitive data management in cloud environment are implemented in experiment and the results of experiment and interview with experts confirmed the validity of the study and all the participants interviewed sharing responses on benefits and risks of factors influence on protecting and managing sensitive data and contributes of publishing experiment evidence of them and all of the experts confirm the framework helps firms and individuals to achieve their goals about managing sensitive data.

M2LF framework is accepted by experts in terms of contributes to enhance the managing and protecting sensitive data in public cloud computing. The objectives of validation are; 1) Confirm the effectiveness of framework, 2) Confirm ability and performance of the implementation tool, and 3) Achieving the study's contributions.

In general, the evaluation and evidence from experts' feedback support and agree to the proposed model and framework as evident below;

- For effectiveness measure; i) the framework offers good methods for managing sensitive data, ii) the framework improved procedures to enhanced performance of managing sensitive data.

- For ability and performance of the implemented tool; i) the framework and implementation tool are easy to use, ii) the implementation tool is effective for managing sensitive data, iii) the techniques used in framework are suitable for managing sensitive data.

- For achieving the study's contributions; i) this study contributes to enhance management of sensitive data, ii) this study contributes to publish experiment evidence of factors influencing protecting and managing sensitive data.

The qualitative data that collected through discussions with six information systems privacy and security experts, using qualitative data lead to a more insightful understanding of the field. This resulted to acceptances of the factors, model and framework proposed in order to make decisions with regards to sensitive data management and its protection.

7. CONCLUSION

This study conducts to improve the quality of managing sensitive data in cloud computing for effective on information system's decisions making. Therefore, the study explains the factors model to management information systems decision on sensitive data. The results of structured interview and pilot study found the factors with significant effect are; data confidentiality, integrity, privacy, and availability. The framework is proposed to enhance information systems decision making on sensitive data management in cloud computing. Execution the modules in the framework using to describe application of managing sensitive data in cloud computing. The experimental validity and data analysis were carried out to validate the research work. One obvious limitation in this work is the files sent to public cloud must be an exact match to the original file for it to be opened.

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] Kumar, S. N., & Vajpayee, A., "A Survey on Secure Cloud: Security and Privacy in Cloud Computing", *American Journal of Systems and Software*, 4(1), 2016, 14-26.

[2] Loganayagi, B., & Sujatha, S., "Enhanced cloud security by combining virtualization and policy

monitoring techniques", *Procedia Engineering*, 30, 2012, 654-661.

[3] Albugmi, Ahmed, Alassafi, Madini O., Walters, Robert, Wills, Gary, "Data Security in Cloud Computing", *Fifth International Conference on FGCT IEEE*, 2(1), 2016, 1–169.

[4] Rouse, M., "Sensitive Information", *Available: http://whatis.techtarget.com/*2014.

[5] Whitley, E. A., Willcocks, L. P., & Venters, W., "Privacy & security in the Cloud", *Journal of International Technology and Information Management*, 22(3), 2013, 5.

[6] Kaur, S., & Singh, A., "The concept of cloud computing and issues regarding its privacy and security", *International Journal of Engineering Research & Technology (IJERT)*, 1(3),2012.

[7] Tong, Y., Sun, J., Chow, S. S., & Li, P., "Cloud-assisted mobile-access of health data with privacy and auditability", *IEEE Journal of biomedical and health Informatics*, 18(2), 2014, 419-429.

[8] Khan, N., & Al-Yasiri, A., "Identifying cloud security threats to strengthen cloud computing adoption framework", *Procedia Computer Science*, 94, 2016, 485-490.

[9] Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B., "A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies", *Telematics and Informatics*, 34(7), 2017, 996-1010.

[10] Chandramohan, D., Vengattaraman, T., Rajaguru, D., & Dhavachelvan, P., "A new privacy preserving technique for cloud service user endorsement using multi-agents", *Journal of King Saud University-Computer and Information Sciences*, *28*(1), 2016, 37-54.

[11] Ali, M., Khan, S. U., & Vasilakos, A. V., "Security in cloud computing: Opportunities and challenges", *Information sciences*, *305*, 2015, 357-383.

[12] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R., "Security issues in cloud environments: a survey", *International Journal of Information Security*, *13*(2), 2014, 113-170.

[13] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A., "Security and privacy in cloud computing: A survey", *In Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on 2010*, pp. 105-112. IEEE

[14] Takabi, H., Joshi, J. B., & Ahn, G. J., "Security and privacy challenges in cloud computing environments", *IEEE Security & Privacy*, 8(6), 2010, 24-31.

[15] Abbas, A., & Khan, S. U., "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds", *IEEE Journal of Biomedical and Health Informatics*, 18(4), 2014, PP. 1431-1441.

[16] Deshmukh, P., "Design of cloud security in the EHR for Indian healthcare services", *Journal of King Saud University-Computer and Information Sciences*, *29*(3), 2017, 281-287.

[17] Rong, C., Nguyen, S. T., & Jaatun, M. G., "Beyond lightning: A survey on security challenges in cloud computing", *Computers & Electrical Engineering*, 39(1), 2013, 47-54.

[18] Shariati, S. M., & Ahmadzadegan, M. H., "Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection", *In Knowledge-Based Engineering and Innovation (KBEI), 2015 2nd International Conference on* 2015, pp. 1078-1082. IEEE.

[19] Khan, M. A., "A survey of security issues for cloud computing", *Journal of network and computer applications*, 71, 2016, 11-29.

[20] Kelbert, F., "Data usage control for the cloud. In Cluster, Cloud and Grid Computing (CCGrid)", 13*th IEEE/ACM International Symposium on* 2013, pp. 156-159. IEEE.

[21] Zhao, F., Li, C., & Liu, C. F., "A cloud computing security solution based on fully homomorphic encryption", *In Advanced Communication Technology (ICACT), 2014 16th International Conference on 2014*, pp. 485-488. IEEE.

[22] Tebaa, M., & Hajji, S. E., "From single to multi-clouds computing privacy and fault tolerance", *IERI procedia*, 10, 2014, 112-118.

[23] Likert, R., "A technique for the measurement of attitudes", *Archives of Psychology*,1932.

[24] Saranya, M., & Senthamil Selvi, R., "Data Anonymization Approach for Privacy preserving in cloud", *International Journal of Computer Science & Engineering Technology (IJCSET)*, Vol. 6 No. 04, 2015, pp. 193-197. ISSN:2229-3345.

[25] Muhasin, H. J., Atan, R., Jabar, M. B. A., & Abdullah, S. B., "Cloud computing sensitive data protection using multi layered approach", *In Proceeding - 2016 2nd International*

Conference on Science in Information Technology, ICSITech 2016: Information Science for Green Society and Environment.

[26] Asarani, N. A. M., & Ab Rahim, N. Z., "Preliminary study of online training implementation from multiple respective in Malaysia public sector", *Journal of Theoretical and Applied Information Technology*, *90*(1), 2016, 77.

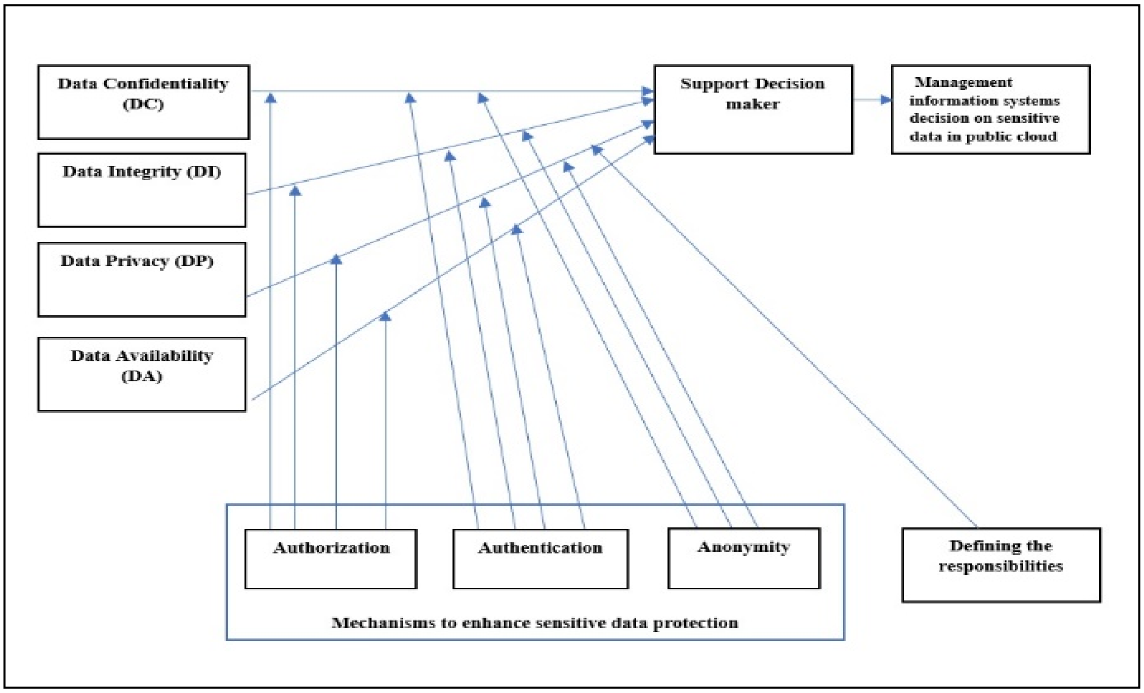
Data Confidentiality (DC)
Data Integrity (DI)
Data Privacy (DP)
Data Availability (DA)
Support Decision maker
Management information systems decision on sensitive data in public cloud
Authorization
Authentication
Anonymity
Defining the responsibilities
Mechanisms to enhance sensitive data protection

Figure 1: Research factors model of information systems decision on sensitive data management

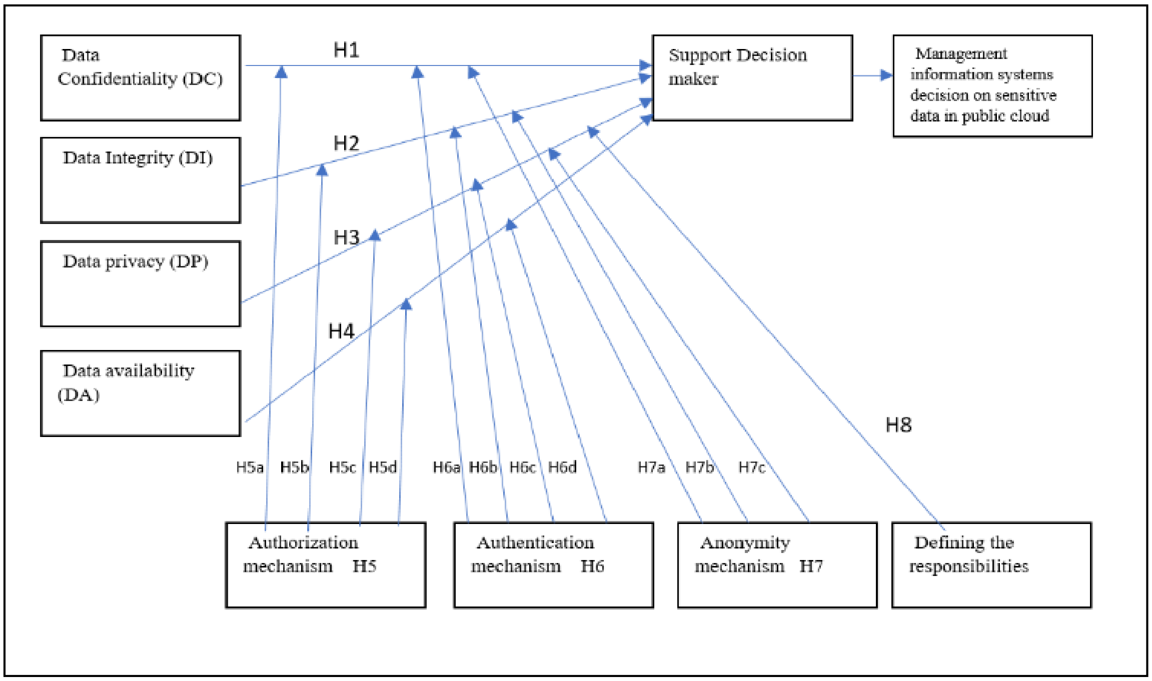
Data Confidentiality (DC)
Data Integrity (DI)
Data privacy (DP)
Data availability (DA)
Support Decision maker
Management information systems decision on sensitive data in public cloud
H1
H2
H3
H4
H5a H5b H5c H5d
H6a H6b H6c H6d
H7a H7b H7c
H8
Authorization mechanism H5
Authentication mechanism H6
Anonymity mechanism H7
Defining the responsibilities

Figure 2: Model hypothesis proposed