



MANAGING SENSITIVE DATA IN CLOUD COMPUTING FOR EFFECTIVE INFORMATION SYSTEMS' DECISIONS

Haifaa Jassim Muhasin^{1*}, Marzanah A. Jabar¹, Salfarina Abdullah¹, Hanayanti Hafit²

¹Department Software Engineering and Information Systems, Faculty of Computer Science & Information Technology, Universiti Putra Malaysia

²Soft Computing and Data Mining Centre, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn, Johor, Malaysia

*Corresponding author email: haifaaajassim@yahoo.com

This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ARTICLE DETAILS

Article history:

Received 07 August 2017

Accepted 18 October 2017

Available online 7 December 2017

Keywords:

cloud computing, privacy, sensitive data, confidentiality, integrity, availability

ABSTRACT

The purpose of this research is defining the main factors influencing on decision of management system on sensitive data in cloud. The framework is proposed, a structured interview with experts working on cloud computing and a pilot study conduct to explore the main objectives of framework. The framework using multilevel to enhance management information system on sensitive data in cloud.

1. THE WORK

Modern cloud computing technology enabled accesses to required resources such as servers, applications, network and services. The process utilizes common computing models that are based on data traffic, and regulated by a third party [1]. Hence, security and privacy remain the biggest challenge for sensitive information in cloud environment [2]. Sensitive information is defined as data that must be protected from unauthorized access to safeguard privacy and security of individual or organization [3].

There are three main types of sensitive data: personal information which is sensitive, personally identifiable information; such as medical information, financial information and unique identifiers such as passport or social security numbers. The second type of sensitive data is business information; which includes any information with risk to affect the company if discovered by competitor or the public such as trade secrets, achievement plans, financial data, supplier and customer information. The third type of sensitive data is classified information; this data related to a government and is limited to level of sensitivity such as confidential, secret and top secret [3].

In order to improve the management of sensitive data in public cloud domain for effective information systems decisions making, this study is conducted. This study offers to examine the factors influencing the decision of management systems on sensitive data in cloud environment. The structured interview with several security experts working on cloud computing security to investigate the main objectives of framework, a pilot study by using a structured questionnaire was conducted. The results found that factors with a significant effect are; the data confidentiality, integrity, privacy, and availability. In addition, anonymity mechanism, positive significance was found with three factors; which are data confidentiality, data integrity and data privacy are influencing and supporting IS decision making. Also, defining the responsibilities, positive significance was found with the factor data privacy influence on decision maker. Based on research findings, in order for management information systems decision on sensitive data in public cloud the organization management should improve and enhance the anonymity mechanism and defining the responsibilities in a good way to support the decision maker.

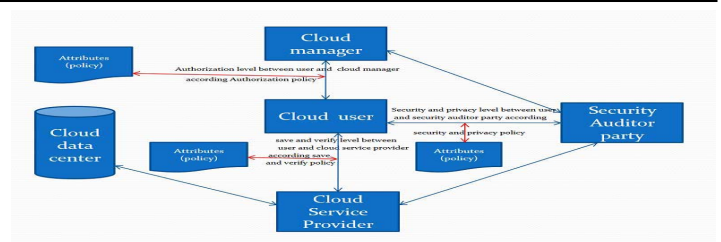


Figure 1: The proposed Framework (M2LF)

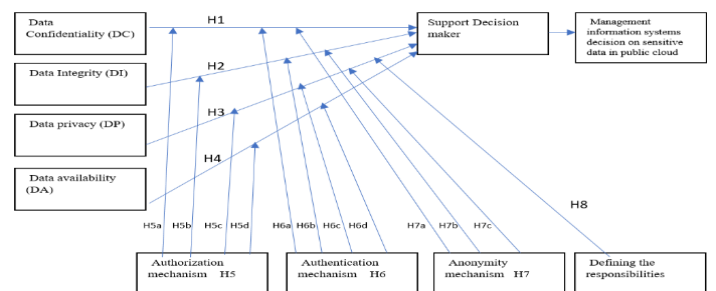


Figure 2: Hypotheses model to management information systems decision on sensitive data in cloud computing

According to these factors, the study proposed a multi layered framework (M2LF) to enhance management information systems decision making on sensitive data in cloud computing environment as depicted in Figure 1. Figure 2 explains the hypotheses and factors which enhancing the management of information system decision making.

This study defined several terminologies necessary for the formation of the framework as; data Confidentiality 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. Integrity refers to the trust merit of the migrated resources. Especially, the data migrated into the cloud must only be adjustable by authorized users. Privacy 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. 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. To evaluate the framework this study hypothesized a few hypotheses as follows:

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

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

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

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

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

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

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

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

The last four hypotheses; **H5**, **H6**, **H7**, and **H8** represent the mediators based on research results. Most of the existing solutions to improve the performance of security and privacy for storing sensitive information in public cloud using limited methods such as data encryption by third party, and this technique need to be used exchange of encryption keys, which may expose the keys to detection and penetration and this leads to the possibility of data breaches [4,5]. In addition, the encryption process takes high computations and need more time and space this leads to slower in store and retrieval the data [4,5]. And also, the encryption method is expensive and renders the information in an unusable format. Therefore, the proposed framework permits verification of using the appropriate way to enhance management information systems decision to protect sensitive information in the cloud computing environment.

2. 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 influencing the decision of management systems 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 management information systems' decision making on sensitive data in cloud computing.

REFERENCES

- [1] Kumar, S., Vajpayee, A. 2016. A Survey on Secure Cloud: Security and Privacy in Cloud Computing. American Journal of Health-System Pharmacy, [Internet]. [cited 2017 Jun 24]; Available from: <http://pubs.sciepub.com/ajss/4/1/2/>
- [2] Loganayagi, B., Sujatha, S. 2011. Enhanced cloud security by combining Virtualization and Policy Monitoring Techniques. International Conference on Communication Technology and System Design.
- [3] Rouse, M. 2014. Sensitive Information, Available: <http://whatis.techtarget.com/2014>.
- [4] Zhao, F., Li, C., Liu, C.F. 2014. A cloud computing security solution based on fully homomorphic encryption, ICACT 2014, February 16-19.
- [5] Tebaa, M., Hajji, S.E. 2014. From Single to Multi-Clouds Computing Privacy and Fault Tolerance. IERI Procedia, 10,112-118.

