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

Haifaa Jassim Muhasin*, 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

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.

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

1. THE WORK

Modern cloud computing technology enabled access 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)

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 and 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:

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

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


