A Prototype for Cloud Computing Data Security Risk Awareness and Training: a Cloud User's Perspective

Abubakar M. Tom[1], Wan Rozaini[2]
[1, 2]Institute for Advanced and Smart Opportunities, School of Computing Universiti Utara Malaysia,
06010, Sintok, Kedah, Malaysia.
Email: magiratom@gmail.com[1], wanrozaini57@gmail.com[2]

Article Info

Article history:

Received Jan 9, 2024
Revised Feb 20, 2024
Accepted Mar 11, 2024

Keywords:

Cloud Computing, Security
Risk
Awareness
Training.
Fourth keyword
Fifth keyword

ABSTRACT

Cloud Computing (CC), data security is a critical issue for all organizations and individuals alike. How- ever, despite all the benefits of CC, data security remains a problem and not well understood. Particularly, the cloud data storage security risks related to iCloud, Google Drive, Drop box and, One Drive. Less research focuses on cloud data/file storage risk awareness and training. From the standpoint of cloud users, this paper highlights the necessity of CC security of information knowledge and training. The prototype implementation of a CC, data security awareness, and training are all addressed in the study. The prototype will be created in accordance with current data security requirements set forth by the National Institute of requirements and Technology (NIST) and the International Standards Organization (ISO). This paper will contribute immensely to cloud users. Finally, contributions and future work are highlighted.

Corresponding Author:

Abubakar M. Tom,
Institute for Advanced and Smart Opportunities,
School of Computing Universiti Utara Malaysia, 06010, Sintok, Kedah, Malaysia.
Email: magiratom@gmail.com

1. INTRODUCTION

The ability of users to identify and refrain from actions that could jeopardize cyber security and to respond alertly and creatively when necessary to enhance cyber security is known as training and awareness about security [1]. Generally, awareness is used to remind people of basic security practices [2]. According to NIST, CC is a prototype that enables widespread, appropriate, and immediate entry to a mutual pool of network-based, reconfigurable computational resources, including servers, software, archived data, and the internet, that might be readily and swiftly provided [3]. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) are the three service models. Additionally, the secure cloud, the open cloud, collaborative cloud, and hybrid cloud are among the cloud service models. Users can develop, deploy, and maintain virtual machines and storage using the Infrastructure as a Service (IaaS) concept.

By enabling the user to install apps on the IaaS infrastructure, like the operating system, IaaS raises the user level. However, compared to SaaS and PaaS platforms, users are responsible for managing implementation patches and updates [4]. The program Programming Interface (API) and intermediary building are made possible by the PaaS, which enables the CU to launch the personalized program in the CC configuration [4]. Layers, creation of applications frameworks, middleware, which is functions, languages of programming, and tools are all integrated into the PaaS paradigm, which sits on top of IaaS [5]. SaaS enables businesses to save capital expenditures and just pay for the features they need, like maintenance. There is no need for control or upkeep, and it supports the pay per usage approach. The CSPs are responsible for managing the apps, data, application circumstances, intermediary software, operating system (OS), the use of virtualization privacy, servers, storage, and communication. The core IaaS and PaaS technologies serve as the foundation for SaaS [5]. The CC deployment models are shown in Figure 1.

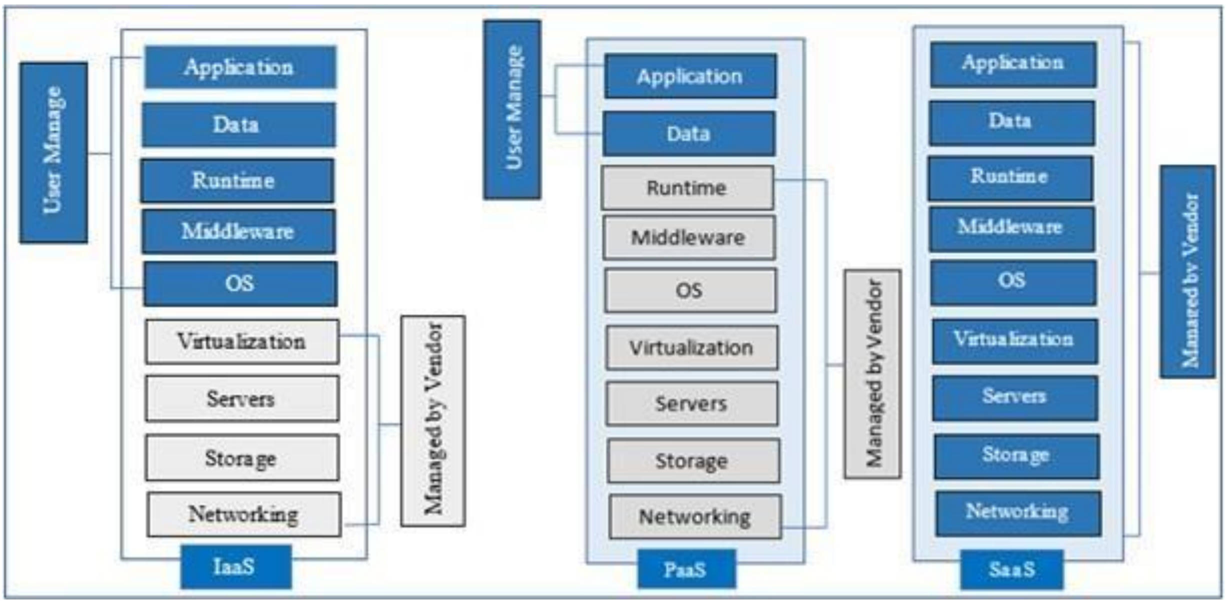

Figure 1. CC Deployment Models

However, CC deployment strategies are not impervious to vulnerabilities and security threats. Risks associated with SaaS could include the inability to move among cloud service providers, lock-in risks, privacy issues, access control, protection, guarantee of quality, data ownership, and inadequate standards [6]. Another major worry in the general cloud space is security. As a result, the public cloud restricts users' capacity to efficiently safeguard and manage their data in a specific area [7]. In addition to the basic computer safety knowledge techniques suggested by [1], [2], and [9], the current research emphasizes the necessity of risks associated with awareness in CC [8]. Raising awareness of the dangers posed by the rapidly expanding threats that target human behavior is the focus of the expanding field of information security awareness [10].

The purpose of training and education about security is to draw attention to safety and security issues and to develop their recognition. A developing area of information security is information security awareness, which focuses on improving perceptions of potential dangers posed by the rapidly expanding attacks focusing on human behavior [10]. Since information is the new oil, it is increasing in value likewise, attackers also strategize and develop sophisticated attack methods to lure users. Malicious users have effectively exploited individual human behavior to break an organization's networks as well as mission-critical infrastructures.

Security Awareness and Training

Toth and Klein [1] define awareness as the capability of users to identify or evade behaviors that would destroy cyber security as well as act vigilantly and ingeniously where exercising discernment is necessary to improve cyber security. The "Federal Information Security Management Act (FISMA)" mandates that IS users participate in awareness training. Training and awareness campaigns help mold individuals to be increasingly security-conscious. The most successful attacks on networks and computer systems nowadays frequently include taking advantage of human behavior [1]. Generally, awareness is used to remind people of basic security practices [2]. The cloud users should be enlightened vis-à-vis different attacks since the weakest link to security is often the user [11].

Users' links and actions about security should be altered by security training and awareness, measuring the success of the program and continually address the importance of security. Therefore, there are three distinct stages of learning: knowledge, instruction, and education [12]. Beyond raising awareness, training creates knowledge and produces capable security abilities. Competence for security professionals operating in the security area is created through education. The cloud users should be aware of threats, risks, and vulnerabilities as well as countermeasures before adopting the Cloud services. Therefore, the larger security awareness campaign should include CC protection knowledge and instruction.

Drawing the attention to this gap in the field of CC information security risk awareness from CUs perspective, this current the study aims to educate, train as well as evaluate CU's understanding using Animation and gaming to evaluate user's understanding of the data storage risks in CC respectively. One of the goals of awareness training is to change people's understanding of security risks as well as change their behavior [9]. The idea of this research came from the work of Furnell et al. [13], where users can use this software to perform awareness training on their own. However, our contribution lies in the development of a mobile application that will support both Android OS and IOS devices concurrently. The application will not only allow awareness training but also, provides users with feedback to understand their understanding of the cloud data/file storage security issues and counter measures.

The issue with raising awareness regarding security is the reality that it is expensive and mostly targeted at SMEs and enterprises. But the previously mentioned could potentially used in a major organization with financial and human resources to carry out the awareness campaign. Smaller firms have a different perspective on security [13]. Although it is often acknowledged that cloud users require security knowledge and training, in this paper we focus on individual cloud clients who utilize any of the open-source and free data storage programs like Dropbox, iCloud, One Drive, etc.

2. RELATED WORK

According to Mazur et al. [14], according to the security level specified in the SLA agreement, cloud users are accountable for making sure that appropriate security measures are implemented. This is particularly difficult because most users aren't even aware of the security criteria they need, let alone how to monitor cybersecurity in the decentralized internet space. Similarly, the primary issue in CC, according to the "European Community Directorate for Network as well as Information Security (ENISA)," is a lack of security knowledge. Cloud consumers are unaware of the hazards associated with cloud migration, especially those produced by clouds-specific risks such data lock-in and loss of control [15]. Furnell et al. [13] proposed a prototype software tool to pursue self-paced security training. The prototype is implemented in visual basic with a database and a selection of interaction scenarios. However, the software focused on general security. Also, the prototype is not tailored to CC data security. Kruger provided an early version for measuring security-related knowledge and Kearney (2006). An worldwide mining business's privacy knowledge is measured using the working model.

The prototype was applied to the Australian regional offices.

However, practical data from the system is not utilized and the system is designed for an organization, not for individual usage the tool is not automated.

Security Awareness Models and Standards

An information security awareness capability models (ISACM) was proposed by Poepjes and Lane [16]. The model integrates the concept of awareness of circumstances with ISO/IEC 27002. Finding a strong base of knowledge, identifying the detailed knowledge points that might be evaluated, constructing the survey instrument coupled with awareness importance ratings, altering the specific knowledge concerns to a practical level, and developing the remaining components of the model are the steps involved. The model maps awareness of importance, awareness capability as well as awareness of risks into "situation-awareness" in dynamic decision making. [17] presented an incident knowledge framework for risk management for information security (SA-ISRM). Through a company-wide collection of information-related hazard analysis and reporting, this framework tackles the shortcomings in the methodology of the risk of information security assessment. It is adapted from Ends leys situation awareness model as well as USNSIE. A role-based paradigm for integrated IT/cyber security training, NIST SP-900, was put forth by [1]. The phases include of experience, role-based instruction and training, cyber security fundamentals, and security awareness. Similarly, NIST SP:800-12: An introduction to computer security was proposed by [18]. Behavior, and responsibility, consciousness, formation, instruction, execution, interdependence, and financial conditions are some of the stages. The handbook aids in securing computer-based resources by explaining concepts cost consideration & interrelation of security controls.

Security of Data Knowledge and Learning Aspects

Siponen [19] proposed five dimensions of information security awareness. The organizational in nature, open to everyone, socio-political, computer-ethical, and academic aspects are among them, as are the categories (or target groups) that fall under each of these dimensions. However, the paper's focus is restricted to establishing information security aspects in terms of target groups and forms, as well as security issue preventative techniques not included in this study, like how to prevent certain dangers. There are no clear borders between the above dimensions. For instance, within the organizational dimensions, issues of general public dimensions are discussed. Each component doesn't figure in the main topic of security problems. A three-dimension of security, People dimensions, policy dimension and enforcement dimension (monitoring of the working) was proposed by Saleh [20]. They include the solution that looks at the aspects of people, policy, and enforcement. The biggest danger to a the company's protection is its workforce. Security is heavily reliant on technology, but the risk and vulnerabilities are caused by users. this could be because users are not involved in policy writing and due to lack of training to the users [20]. However, it is designed for creating an information security plan for an organization. The dimensions are non-technical. Some important dimensions such as the CC dimension is not considered. An empirical analysis of information security awareness in the business and public sector of Hungary was proposed by [21]. The authors also contend that consumers' lack of security awareness is the primary cause of today's security issues. The awareness dimension includes the organizational, individual and infrastructural dimension. However, there is no distinction between the individual dimension and the infrastructural dimension as well as too abstract.

In their proposal, Schlienger and Teufel [22] shifted the standard model beyond a technical to a behavioral approach, making people the asset instead of a threat. The human element is largely overlooked in security of information [22].

A human dimension to information security is proposed by the author. A model of analysis based on IS, an organizational dimension, and an institutional dimension based on institutional theory was suggested by Albuquerque and Santos [23] to allow the study of all the components that contribute to the acceptance of information security among scientific institutions. The institution dimension focuses on internal factors that lead to the adoption of measures in public research institute. While the organizational dimension focuses on the view of information security governance as well as the environmental factors. Hence, the institutional dimension is supported by the institutional theory. The proposed dimension includes organization, institutional, government, regulatory organizations and funding organizations, Information Technology and information security professionalization as well as other organizations. However, only factors that lead to the adoption of IS measures are identified, as well as the lack of guidelines and metrics to evaluate the security measures that are missing.

Cloud-Based Data Storage Security Issues

SaaS supports organizations to create applications for data storage like Google Drive, iCloud and Dropbox. Dropbox is one of the leading players in cloud storage services [24]. Around 200 million users are using Drop-box in the world. however, security over the years has plagued Dropbox. However, security over the years has plagued Dropbox. There are many security breaches of the cloud- based data storage that affect millions of users. For example, the recent Dropbox data breach leaks account details of 68 million users in 2012 [25]–[32]. The data stolen are user email and password. "The data beach contains encrypted passwords and details of around two- thirds of CUs, has been leaked." [32]. Therefore, this hack highlighted the need for high-security conscience from CUs end.

Google Drive has the following limitations: weak file- sharing security, lacks of private encryption options and no block-level synchronization [33]. On the other hand, Dropbox paid storage is expensive (free 2GB), does not allow sharing of files with non-members, has bad customer ratings and compliant, it allows tracking (privacy policy) and based in the U.S.[33]. Some nude pictures of celebrities are exposed from the Apple iCloud accounts [34]. Additionally, over a billion users store their personal files on cloud-based storage [35]. Whether consumers of cloud storage are conscious of all the data they've been collecting online is still unclear. Their investigation revealed that cloud users kept private images in online storage even though they had no intention of uploading. There is still a lacking of security awareness in CC [36]. The CUs should also know about protecting their data against administrative access by the CSPs as well as comprehend the data encryption methods which are applied to the data [37]. In this new context, the CUs must be alert and aware of the potential consequences of data breaches [38], [39].

3. PROPOSED MOBILE APPLICATION

The proposed mobile application for self-security awareness and training in CC will comprise of components, resources, modules, content and progress report. The mobile application will use Animation to teach cloud users a brief introduction of the cloud data storage issues and its counter-measures. The gaming aspect will allow cloud users to play games, as well as solving challenges upon passing stages. In the process, they will become security conscious and the score will be registered in the database for future assessment. The proposed mobile app will support both Android and IOS devices. The app will train as well as access users' understanding of the CC data storage security issues by completing obstacles.

4. CONCLUSIONS AND FUTURE WORK

So far, less attention has been paid to the security risk awareness in CC. In a CC setting, cloud users will relinquish and hand over the control of their data to cloud service providers. Numerous problems related to SaaS such as iCloud, Dropbox, Google Drive, etc. applications have been identified. Therefore, cloud users must understand the data security risks by using the proposed application for self-security awareness and training. This can be achieved using an Animation and gaming application to help users undertake security awareness and training in this new paradigm. Cloud users are not adequately trained or aware of the security risks associated with cloud computing.

We intend to focus on proposing an application to educate as well as train cloud users on how to protect their data in this new paradigm. Progress will be recorded in our database to access and see the understanding of security. That is to say, are users more aware now that they use our app? This question will be answered in our future work.

REFERENCES

[1] P. Toth and P. Klein, “A role-based model for federal information technology/cyber security training,” NIST Spec. Publ. 800, vol. 3, no. 16, p. 163, 2014.

[2] B. Guttman and E. Roback, “Sp 800-12. An introduction to computer security: The NIST Handbook," pp. 1–297, 1995.

[3] P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.

[4] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, “Benefits and challenges of three cloud computing servicee models," in 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), 2012, pp. 198–205.

[5] B. Arinze and M. Anandarajan, “Adapting cloud computing service models to subscriber requirements,” 6th Int. Symp. Wirel. Pers. Multimed. Commun., pp. 1–5, 2013.

[6] M. Janssen and A. Joha, “Challenges for adopting cloud-based software as a service (saas) in the public sector.,” ECIS, 2011.

[7] O. Ghazali, M. T. Abubakar, M. T. Hatim, H. Suhaidi, A. N. Shahrudin, and H. M. S. Ahmad, “Security Measurement as a Trust in Cloud Computing Service Selection and Monitoring - Volume 8, No. 2, May 2017 - JAIT,” Journal of Advances in Information, 2017. [Online]. Available: http://www.jait.us/index.php?m=content&c=index&a=sh ow&catid=179&id=997. [Accessed: 30-Sep-2017].

[8] R. Kalaiprasath, R. Elankavi, and R. Udaya- kumar, “A Cloud Security and Compliance-A Semantic Approach in End to End Security,” Int. J. Mech. Eng. Technol., vol. 8, no. 5, 2017.

[9] L. Spitzner, “How to build an effective information security awareness program - Information Security Magazine,” 2017. [Online]. Available: http://searchsecurity.techtarget.com/magazineContent/Ho w-to-build-an-effective-information-security-awareness- program. [Accessed: 05-Dec-2017].

[10] Wikipedia, “Information security awareness,” 2017. [Online]. Available: https://en.wikipedia.org/wiki/Information_security_aware ness.

[11] D. Lukan, “The top cloud computing threats and vulnerabilities in an enterprise environment - Cloud Tech News,” 2014. [Online]. Available: https://www.cloudcomputingnews.net/news/2014/nov/21/ top-cloud-computing-threats-and-vulnerabilities- enterprise-environment/. [Accessed: 22-Dec-2017].

[12] S. K. Katsikas, “Health care management and information systems security: awareness, training or education?,” Int. J. Med. Inform., vol. 60, no. 2, pp. 129– 135, Nov. 2000.

[13] S. M. Furnell, M. Gennatou, and P. S. Dowland, “A prototype tool for information security awareness and training,” Logist. Inf. Manag., vol. 15, no. 5/6, pp. 352– 357, Dec. 2002.

[14] S. Mazur, E. Blasch, Y. Chen, and V. Skormin, “Mitigating Cloud Computing security risks using a self-monitoring defensive scheme,” in Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON), 2011, pp. 39–45.

[15] ENISA, “Cloud Computing Benefits, risks and recommendations for information security,” 2009.

[16] R. Poepjes and M. Lane, “An information security awareness capability model (ISACM),” 10th Aust. Inf. Secur. Manag. Conf. (SECAU 2012), Dec. 2012.

[17] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, “A situation awareness model for information security risk management,” Comput. Secur., vol. 44, pp. 1–15, Jul. 2014.

[18] B. Guttman and E. A. Roback, “SP 800-12. An Introduction to Computer Security: the NIST Handbook.” National Institute of Standards & Technology, 1995.

[19] M. T. Siponen, “Five dimensions of information security awareness,” ACM SIGCAS Comput. Soc., vol. 31, no. 2, pp. 24–29, Jun. 2001.

[20] M. F. Saleh, “The Three Dimensions of Security,” Int. J. Secur., vol. 5, no. 2, pp. 1–9, 2011.

[21] A. Nemeslaki and P. Sasvari, “Empirical Analysis of Information Security Awareness in the Business and Public Sectors of Hungary PDF Logo,” In Central and Eastern European eDem and eGov Days 2015. Time for a European Internet?, 2015, pp. 1–29.

[22] T. Schlienger and S. Teufel, “The Socio- Cultural Dimension in Information Security,” Secur. Inf. Soc. Visions Perspect., vol. 86, p. 191, 2002.

[23] A. E. de Albuquerque and E. M. dos Santos, “Adoption Of Safety Measures Information: An Analysis Model For Public Research Institutes,” Proc. Brazilian Symp. Inf. Technol. (SBTI 2014), vol. 5, no. 2, pp. 1–14,2014.

[24] Cloudwards,“Dropbox Review – Updated 2017,” 2017. [Online]. Available: https://www.cloudwards.net/review/dropbox/. [Accessed: 22-Dec-2017].

[25] K. Turner, “Hacked Dropbox login data of 68 million users is now for sale on the dark Web - The Washington Post,” 2016. [Online].Available: https://www.washingtonpost.com/news/theswitch/wp/201 6/09/07/hacked-dropbox-data-of-68-million-users-isnow- or-sale-on-the-dark-web/?utm_term=.1b8cc69383f1. [Accessed: 17-Dec-2017].

[26] K.Conger and M. Lynley, “Dropbox employee’s password reuse led to theft of 60M+ user credentials | TechCrunch,”2016. [Online]. Available: https://techcrunch.com/2016/08/30/dropbox-employees- password-reuse-led-to-theft-of-60m-user-credentials/. [Accessed: 17-Dec-2017].

[27] BBC, “Dropbox hack ‘affected 68 million users’- BBC News,” 2016. [Online]. Available: http://www.bbc.com/news/technology-37232635. [Acce ssed: 17-Dec-2017].

[28] Telegraph, “Dropbox hackers stole 68 million passwords - check if you’re affected and how to protect yourself,” 2016. [Online]. Available: http://www.telegraph.co.uk/technology/2016/08/31/dropb ox-hackers-stole-70-million-passwords-and-email- addresses/. [Accessed: 17-Dec-2017].

[29] W. Ashford, “Lessons from the Dropbox breach,” 2016. [Online]. Available: http://www.computerweekly.com/news/450303585/Lesso ns-from-the-Dropbox-breach. [Accessed: 17-Dec-2017].

[30] T. Mendelsohn, “Dropbox hackers stole e-mail addresses, hashed passwords from 68M accounts | Ars Technica,” 2016. [Online]. Available: https://arstechnica.com/informationtechnology/2016/08/d ropbox-hackers-stole-email-addresses-hashed-passwords- 68m-accounts/. [Accessed: 17-Dec-2017].

[31] J. Rogers, “Dropbox data breach: 68 million user account details leaked,” Fox News, Fox News, 31- Aug- 2016.

[32] S. Gibbs, “Dropbox hack leads to leaking of 68m user passwords on the internet | Technology | The Guard- ian,” 2016. [Online]. Available: https://www.theguardian.com/technology/2016/aug/31/dr opbox-hack-passwords-68m-data-breach. [Accessed: 17- Dec-2017].

[33] R. Tiwari, “Dropbox vs Google Drive 2017: Deep Dive &amp; Comparison,” 2017. [Online]. Available: https://www.cloudwards.net/dropbox-vs- google-drive/. [Accessed: 31-Dec-2017].

[34] Cbsnews, “Apple patches iCloud security gap after celebrity photos hacked, reports say - CBS News,” 2017. [Online]. Available: https://www.cbsnews.com/news/apple-patches-icloud- security-gap-after-celebrity-photo-hacks-reports-say/. [Accessed: 31-Dec-2017].

[35] J. W. Clark, P. Snyder, D. McCoy, and C. Kanich, “& quot;I Saw Images I Didn’t Even Know I Had & quot;,” in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI ’15, 2015, pp. 1641–1644.

[36] S. S. M. Kassim, M. Salleh, and A. Zainal, Cloud Computing: A General User’s Perception and Security Awareness in Malaysian Polytechnic. Springer, Cham, 2015.

[37] P. Dhir and S. Garg, “Survey on Cloud Compu- ting and Data Masking Techniques,” Int. J. Innov. Adv. Comput. Sci., vol. 6, no. 4, pp. 1–7, 2017.

[38] S. Subashini and V. Kavitha, “A survey on secu- rity issues in service delivery models of cloud compu- ting,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[39] M. A.-A. G. Ahmed and Y. A. Mohammed, “A novel approach for data integrity protection in cloud,” Int.J. Comput. Sci. Inf. Technol., vol. 5, pp. 07–12, 2017.