International Journal of Science and Engineering Applications
Volume 6–Issue 12, 350-359, 2017, ISSN:-2319–7560

Evaluating Security-as-a-Service (SECaaS) Measures to Increase the Quality of Cloud Computing

Khaled M. Musa

Sullivan University
Louisville, Kentucky, USA

Abstract: Cloud computing is the new theme of information technology. There are companies, agencies, and individual users that have adopted cloud computing at their work, and others are still considering adopting the new technology. The cloud environment is a virtual environment that offers services to various clients based on their need of service. Cloud computing offers services such as infrastructure (IaaS), platform services (PaaS), and software (SaaS). The providers of cloud computing services found that security measures are extremely needed to protect data and resources used by clients. Security-as-a service (SECaaS) is a new service implemented in the cloud computing environment to protect the IaaS, PaaS, and SaaS along with all data and resources that are used within the clouds. To provide secure environment, cloud computing providers are implementing several components of SECaaS that constitute security measures in cloud computing. IT managers and decision makers in various businesses aim to use adequate new technology to protect business data and resources. SECaaS in its various security services is a new technology for businesses to adopt for the protection of their data and resources. This research will evaluate identity and access management, data loss prevention, encryption capabilities, vulnerability management, and email security SECaaS measures and controls that would increase the quality of cloud computing. In this paper, there will be an evaluation to some of the common used SECaaS measures such as identity and access management, data loss prevention, encryption capabilities, vulnerability management, and email security on their importance to be key factors in the standardization of SECaaS measures of cloud computing.

Keywords: Cloud Environment, Cloud Computing, Software-as-a-service (SaaS), Platform-as-a-service (PaaS), Infrastructure-as-a-service (IaaS), Security as-a-service (SECaaS), Security Standards.

1. INTRODUCTION

Innovations in server centric computing have led to improved Internet-based structures called cloud computing (Mell & Grance, 2011). According to Mell & Grance (2011), cloud computing is described as Internet-based services accessed by different users, as shown in Figure 1. Cloud computing gives accessible visualized services such as software, storage, and programming capabilities from anywhere over the internet (Hussain & Abdulsalam, 2011), the cloud environment in its services allows organizations to avoid high investments in new computer networks, hardware, software and software licensing (Ardagna, Asal, Damiani, & Vu, 2015).

In this paper, there will be analyzation to how SECaaS specific measures of cloud computing would influence the adoption of cloud computing. It seeks to help cloud computing providers place emphasis on the implementation of stronger SECaaS measures and further standardizing SECaaS measures.

The results of this study are expected to provide information on key SECaaS measures, and their impact and significance to be included in SECaaS standardized measures offered by quality control bodies of cloud computing. In investigating the measures of SECaaS will yield information related to what measures implemented in SECaaS can be standardized for cloud providers to follow to provide safer and risk-free cloud environment.

The rest of this paper is organized as follows: section 2 presents an overview of the types of cloud computing services. Section 3 discusses the Security -as-a-Service (SECaaS) measures. Section 4 Evaluating SECaaS measures and controls. Finally, section 5 concludes the paper.

2. TYPES OF SOFTWARE TESTING

Although there are many cloud computing services, this paper will only include the following main services:

- **Software-as-a-service (SaaS):** a cloud computing model that provides software applications to be used by various clients via internet (Hussain & Abdulsalam, 2011).

- **Platform-as-a-service (PaaS):** a cloud computing model that provides users the ability to develop, customize and manage software applications (Hussain & Abdulsalam, 2011).

- **Infrastructure-as-a-service (IaaS):** a cloud computing model that provides clients top access, monitor, and manage their remote infrastructures such as storage, networks, and network services (Hussain & Abdulsalam, 2011).

- **Security-as-a-service (SECaaS):** a cloud computing model that provides IT security measures to protect information and software from any fraudulent and intruding issues (Hussain & Abdulsalam, 2011).

- **Security-as-a-Service (SECaaS) Measures**

SECaaS measures vary between simple antivirus measures to having large servers with firewalls to protect all attributes of the business that are important to various agencies, businesses, and persons. Tirado (2008) sought that security engineers should focus on the SECaaS measures that contribute to the failures or success of business processes and goals.
Integrating SECaaS measures and controls allow cloud computing to enforce common security measures to protect information and software systems in the cloud environment (Reddy & Kaylan, 2014).

Chow, Golle, Jakobsson, Shi, Staddon, Masuoka, & Molina, (2009) examined the SECaaS measures that prevented companies from adopting cloud computing, but the security measures addressed in the study were based on the references of World Privacy Forum Report and Information Security magazine.

To increase the reliability of this research, this research will use the SECaaS measures and controls that match IT security standards that are shared between Cloud Security Alliance (CSA) organization, Cloud Standards Customer Council (CSCC), Open Data Center Alliance (ODCA), and National Institute of Standards and Technology (NIST).

The SECaaS security standards constituted by the common bodies of cloud computing standardization are identity and access management, data loss prevention, web security, email security, intrusion management, encryption capabilities, disaster recovery, network security, and vulnerability management. All these factors are equally important.

Looking at the different bodies that standardize the various cloud computing SECaaS measures, this research seeks to examine the common SECaaS measures the include the following measures:

- **The Identity and Access Management** component of SECaaS manages people, processes, and systems. The identity and access management ensure security as part of the cloud computing environment where it verifies identity, grant access levels to users to services and information (CSA, 2015).

- **Data Loss Prevention** or data loss protection describes the controls in SECaaS that ensure data resides for specific authorized users (CSA, 2015)

- **Information Encryption/ Decryption** capabilities is a SECaaS component that uses cryptography to protect data by providing encryption and decryption keys granted to authorized users to access their data only when needed (CSA, 2015).

- **Vulnerability Management** is a component of SECaaS that continually monitor the cloud computing components for deviation from enforced controls and standardize all inputs and outputs to enhance interoperability (Aros, n.d.).

- **Email Security** is a component of SECaaS to ensure security by monitoring and mitigating threats such as spam, phishing, malware propagation using emails. The email security component inspects, filter, and protect data using decryptions and digital signature (CSA, 2015)

3. EVALUATING SECAAS MEASURES AND CONTROLS

Evaluating the SECaaS measures using the IBM Statistical Package for Social Science (SPSS) statistics Version 22.0 software was performed using the on the completed survey responses. Using SPSS, descriptive analysis was calculated using numerical values of Likert scale where values range between 1 which is strongly disagree to 5 strongly agree. The resulting SPSS analysis of variance (ANOVA), on the 109-population sample, compared the values for each dependent variable with the values for the dependent variable. The descriptive statistics for the different variables addressed in the original responses of the survey are listed in the below table 1.

	N	Range	Minimum	Maximum	Sum	Mean	Mean	Std. Deviation	Variance
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
Identity and Access Management	109	4.00	1.00	5.00	472.25	4.3326	.07488	.78178	.611
Data Loss Prevention	109	4.00	1.00	5.00	473.25	4.3417	.07335	.76578	.586
Information Encryption/ Decryption	109	4.00	1.00	5.00	465.75	4.2729	.07173	.74887	.561
Vulnerability Management	109	4.00	1.00	5.00	466.50	4.2798	.07900	.82476	.680
Email Security	109	4.00	1.00	5.00	455.00	4.1743	.09150	.95531	.913
Valid N (listwise)	109								

Table 1. Descriptive Statistics Original Data.

In the descriptive statistics original data, there are five independent variables: identity and access management, data loss prevention, information encryption/decryption, vulnerability management, and email security. The descriptive statistical analysis table that contains the five variables show the range of values are between minimum 1 and maximum 5, and the mean which is the average of all values is between 4.17 to 4.34.

Each question addresses it's influence on the decision to adopt cloud computing. Each of all five dependent variables seem to have a mean that is greater than 4 which is the value of "Agree" to the importance of the variable to include in standardization requirements.to cloud computing. All variables are equally important on the decision to adopt cloud computing. The mean of every variable differs from another and the closer the values to the maximum value of 5, the more participants agree that it should be important to standardization of SECaaS measures of cloud computing.

The standard deviation measures the average distance from the mean or the dispersion of set of data from the mean (Burns & Burns, 2013) which found to be from .748 to .955. The variance measures how far data is spread, and its values are between .561 to .931.

Examining the standard deviation of the five independent variables, the four variables identity and access management, data loss prevention, information encryption/decryption, vulnerability management, seem to have relatively close variations from their mean with values between .749 and .824; whereas the variable email security seem to have larger deviation value of .955 from the mean. The closer the standard deviation to zero, the closer data points to the mean. None of the variables have a value that is close to zero, but all relatively close to each other's. The variable Email security, seem to have larger standard deviation or variance from each other.

The five independent variables identity and access management, data loss prevention, information encryption/decryption, vulnerability management, and email security vary in their influences to adopt cloud computing. Analyzing the five variables to distinguish the difference in the influence the decision to adopt cloud computing, "Agree" will represent the "Strongly Agree or "Agree" responses whereas "Disagree" will represent "Strongly Disagree" or "Disagree".

4. EVALUATING IDENTITY AND ACCESS MANAGEMENT

Analyzing the identity and access management variable, we find that out of the 109 participants 89 agree which is a representation to strongly agree or agree, that the variable will influence the decision to include it in the standardization of SECaaS measures whereas 20 disagrees which is a representation to strongly disagree or disagree, that the variable influences to include it in the standardization of SECaaS measures, Figure 1.

Further, analyzing the identity and access management variable using the p-value (P) to determine the significance of the identity and access management variable. In table 2, the Significance is greater than .0005 (P < .0005) which means that the identity and access management is statistically significant element as SECaaS measures.

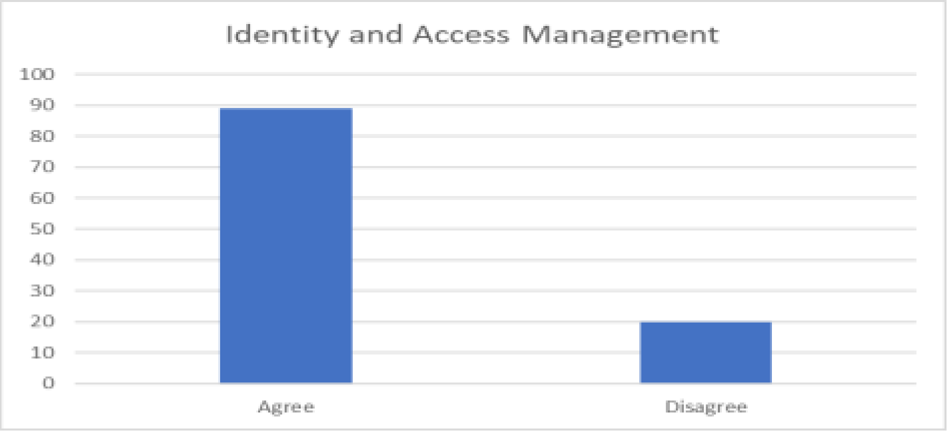

Figure 1. Identity and Access Management

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	42.340	1	42.340	409.046	.000[b]
	Residual	11.075	107	.104		
	Total	53.415	108			

Table 2. Identity and Access Management ANOVA Analysis

5. EVALUATING DATA LOSS PREVENTION

Analyzing the data loss prevention variable, we find that out of the 109 participants 91 agree, represent strongly agree or agree, that the variable will influence the decision to adopt cloud computing whereas 18 disagrees, represent strongly disagree or disagree, that the variable influences to include it in the standardization of SECaaS measures, Figure 2. Further, analyzing the data loss prevention variable using the p-value (P) to determine the significance of the data loss prevention variable.

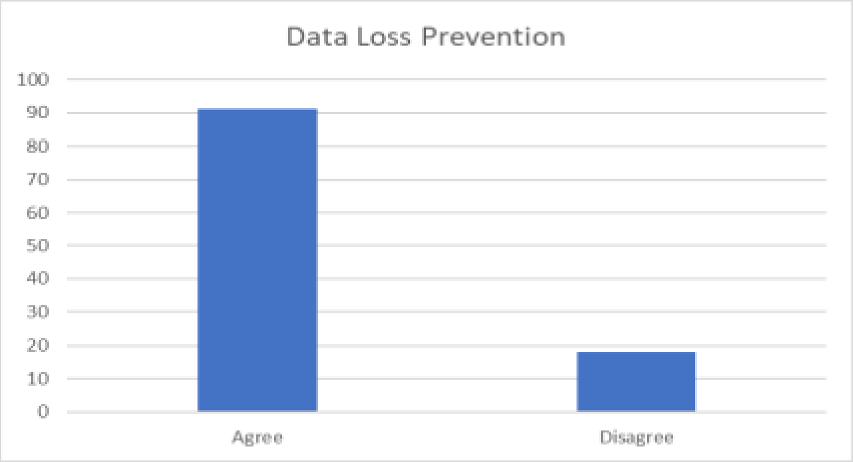

Figure 2: Data Loss Prevention

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	41.145	1	41.145	358.802	.000[b]
	Residual	12.270	107	.115		
	Total	53.415	108			

Table 3. Data Loss Prevention ANOVA Analysis

6. EVALUATING INFORMATION ENCRYPTION/ DECRYPTION

Analyzing the information encryption/ decryption variable, we find that out of the 109 participants 91 agree, represent strongly agree or agree, that the variable will influence the decision to adopt cloud computing whereas 18 disagrees, represent strongly disagree or disagree, that the variable influences to include it in the standardization of SECaaS measures, Figure 3.

In table 3, the Significance is greater than .0005 (P < .0005) which means that data loss prevention is statistically significant element as SECaaS measures

Further, analyzing the identity and access management variable using the p-value (P) to determine the significance of the information encryption/ decryption variable. In table 3, the Significance is greater than .0005 (P < .0005) which means that the information encryption/ decryption is statistically significant element as SECaaS measures.

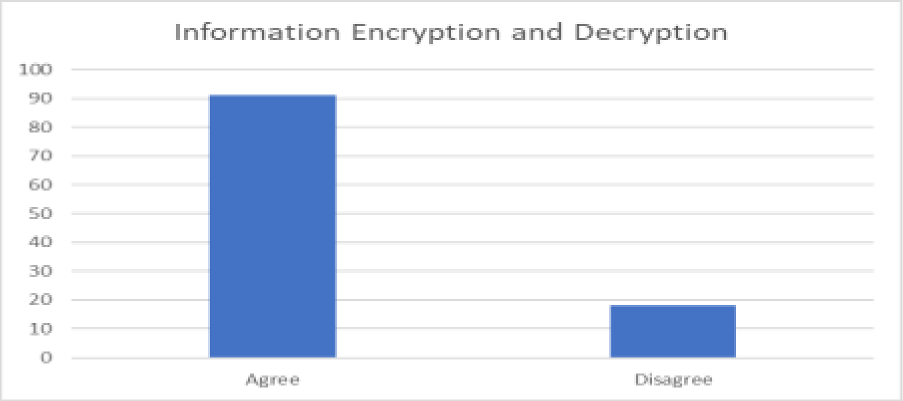

Figure 3. Information Encryption/ Decryption

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	38.996	1	38.996	289.377	.000[b]
	Residual	14.419	107	.135		
	Total	53.415	108			

Figure 1. Identity and Access Management

7. EVALUATING VULNERABILITY MANAGEMENT

Analyzing the vulnerability management variable, we find that out of the 109 participants 103 agree, represent strongly agree or agree, that the variable will influence the decision to adopt cloud computing whereas 6 disagrees, represent strongly disagree or disagree, that the variable influences to include it in the standardization of SECaaS measures, Figure 4.

Further, analyzing the vulnerability management variable using the p-value (P) to determine the significance of the information encryption/ decryption variable.

In table 5, the Significance is greater than .0005 (P < .0005) which means that the vulnerability management is statistically significant element as SECaaS measures.

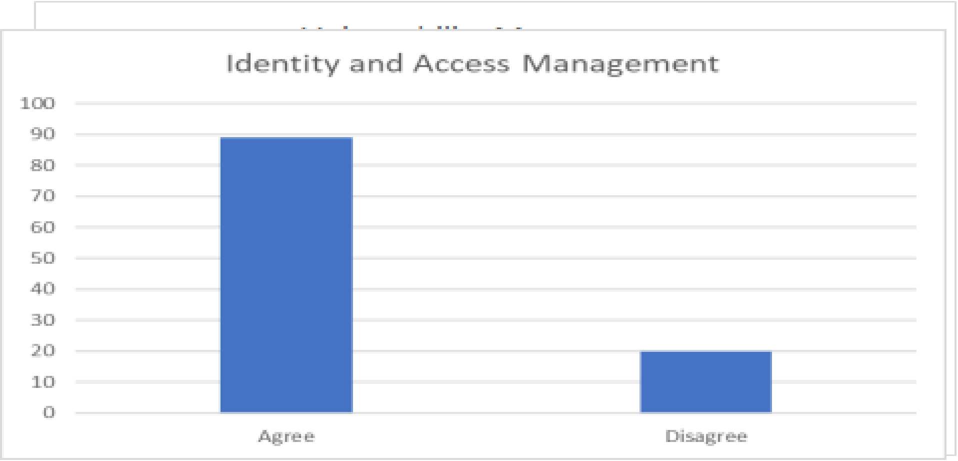

Figure 4. Vulnerability Management

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	42.214	1	42.214	403.255	.000^b
	Residual	11.201	107	.105		
	Total	53.415	108			

Table 5. Vulnerability Management ANOVA Analysis

8. EVALUATING EMAIL SECURITY

Analyzing the email security variable, we find that out of the 109 participants 87 agree, represent strongly agree or agree, that the variable will influence the decision to adopt cloud computing whereas 22 disagrees, represent strongly disagree or disagree, that the variable influences the decision to include it in the standardization of SECaaS measures, Figure 5.

Further, analyzing the email security variable using the p-value (P) to determine the significance of the information encryption/ decryption variable.

In table 6, the Significance is greater than .0005 ($P < .0005$) which means that the email security is statistically significant element as SECaaS measures.

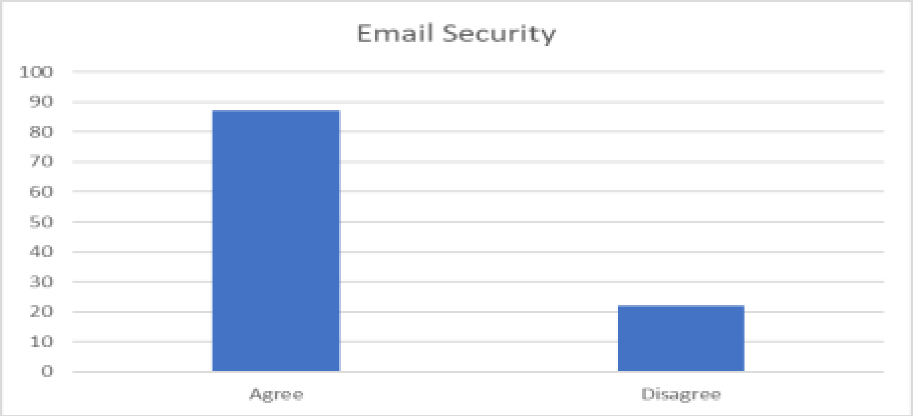

Figure 5: Email Security

ANOVA^{a}

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	35.168	1	35.168	206.219	.000^{b}
	Residual	18.247	107	.171		
	Total	53.415	108			

Table 6. Email Security ANOVA Analysis

4. CONCLUSION

The common five SECaaS measures that include identity and access management, data loss prevention, information encryption/ decryption, vulnerability management, and email security. The 109 participants agreed on the importance that all five SECaaS measures which signify the purpose to include them in standardizing SECaaS. The ANOVA analysis for each measure indicated the high significance of each variable to SECaaS standards. The analysis of all variables shows close results to their importance to cloud computing, despite the different readings they give. Many of all participants agreed that data loss prevention and information encryption/ decryption have the highest votes to its importance, following identity and access management, following email security.

REFERENCES

[1] D. Galin, Software Quality Assurance: From Theory to Implementation, Addison Wesley, New York, NY, USA, 2003.

[2] ISO, ISO/IEC TR 19759: Guide to the Software Engineering Body of Knowledge (SWEBOK), International Organization for Standardization, Geneva, Switzerland, 2005.

[3] S. Chat, Performance Management of Software Architecture, online: http://www.findwhitepapers.com/whitepaper2373/, visited on July 4, 2009.

[4] G. J. Myers, T. Badgett, T. M. Thomas, and C Sandler, the Art of Software Testing, Wiley, USA, 2004.

[5] ApTest, Web QA Test Tool Links, online: http://www.aptest.com/webresources.html, visited on April 15, 2009.

[6] INSECURE, Top 100 Network Security Tools online: http://sectools.org/, visited on April 20, 2009.

[7] Java-Source, Open Source Testing Tools in Java, online: http://java-source.net/open-source/testing-tools, visited on April 20, 2009.

[8] Ranorex, Web Testing, online: http://www.ranorex.com/support/user-guide-20/web-testing.html, visited on April 22, 2009.

[9] Bright-Hub, Sniffing Data with Ettercap for Linux and Windows, online: http://www.brighthub.com/computing/smb-security/articles/35545.aspx, visited on April 22, 2009.

[10] QFS, Facts & Features, online: http://www.qfs.de/en/qftest/, visited on April 23, 2009.