The Study about Risk Assessment on Cloud Computing Security among Small and Medium – Sized Enterprises (SMES) in Malaysia

Lim Jia Hui, Dhamayanthi Arumugam, Suresh Balasingam

Abstract: ***The primary objective of this research is to study the risk factors affecting on the cloud computing security among small and medium-sized enterprises (SMEs) in Malaysia. In this research, the researcher intends to discovery the risks on the use of cloud computing because they may affect the operating of the organisations in Malaysia. The researcher uses the primary method to conduct the data. In this research, five different variables that affect the cloud computing security significantly which include data confidentiality, data integrity, availability of data, mutual trust and auditability of data. The data was collected from the employees who use the cloud services in Malaysia. Statistical Package of the Social Sciences (SPSS) is used to assess the relationships between the five variables which able to influence the cloud security among SMEs in Malaysia. The findings discovered that all the variables have significant relationship with the cloud computing security among the SMEs in Malaysia. The conclusion have been discussed in this research that the providers and users of cloud services have responsibilities to ensure there have a safe cloud environment. This research creats the awareness of the use of cloud computing in order to avoid the risk of the data being stole or hacked and build a peace cloud environment.***

Keywords: Cloud Computing Security, Data Confidentiality, Data Integrity

I. INTRODUCTION

In this modern day, cloud computing has been widely used by most of the organisations. Cloud computing considers as a model that helps the organisations to obtain various types of computing resources through the network access (ISACA, 2011). It provides several services for file storage, applications, networks, and others. It benefits the organisations, especially for Small and Medium Size Enterprises (SMEs), by offering them a low cost information system to manage the data within the organisation as well as the interaction between the organisation and outsiders. It has replaced the traditional computing which requires the physical hardware to store the data or the use of software such as email to send the data. With the use of cloud, the organisations able to store a large amount of data with purchased amount of storage space that depends on the organisations (Huth & Cebula, 2011).

Exhibit 1 shows the statistics of respondents are applying cloud computing in 2016. Public cloud is preferred by small enterprises that allow users to share the data communally via Internet. Private cloud only can be accessed by specific groups or within the organisations. Community cloud is shared by several enterprises that have common concerns or requirements. Hybrid cloud is used with the combination of two or more cloud models which mentioned above to achieve the specific objectives. Furthermore, there consists of three models of cloud service delivery models which are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). SaaS can be a business application which facilitates the relationship between the organisation and customers over the Internet such as Google Apps (Rong, et al., 2013). PaaS is a computing tool that assists the deployment of cloud via Internet such as Google App Engine (Rong, et al., 2013). According to Kuyoro, Ibikunle and Awodele(2011) stated that IaaS is a virtual platform that enables organisations to handle the provisioning and management well such as Amazon Web Services.

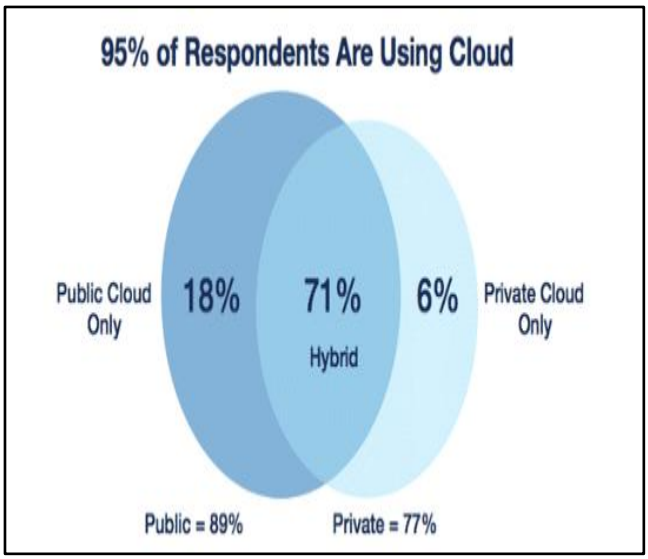

Exhibit 1: Statistic of Respondents are Applying Cloud Computing In 2016

Source: (Weins, 2016)

Revised Manuscript Received on January 19, 2019.
Lim Jia Hui Asia Pacific University, Malaysia.
Dhamayanthi Arumugam, Asia Pacific University, Malaysia.
Suresh Balasingam, Asia Pacific University, Malaysia.

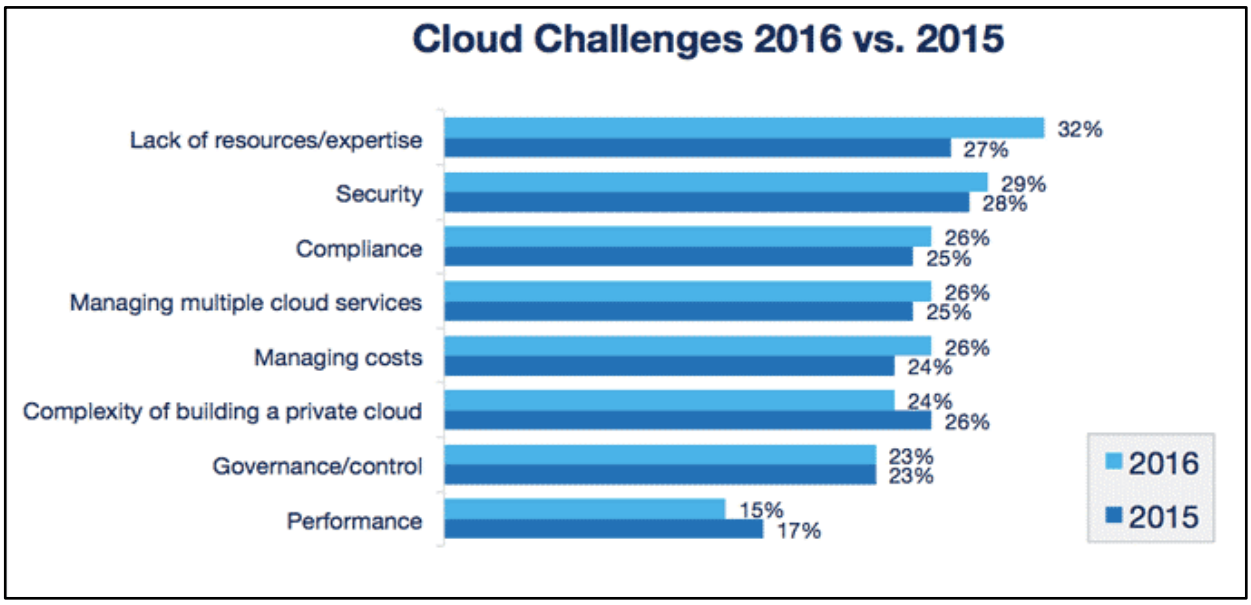

Exhibit 2: Cloud Challenges 2016 versus 2015
Source: (Lazar, 2016)

However, the organisations should consider the security cloud issues. The issue of data security will be arise as the organisations store their data in the cloud. They might think that whether their data will be secure and not be retrieved or stole from others, worsen the data stole will cause the loss of business. Besides that, the organisations also consider other challenges when using the cloud computing as shown in Exhibit 2.This research study is concentrating on the risk assessment for cloud computing security among small and medium-sized enterprises (SME) in Malaysia. The recent security issues will be discussed in the problem statements and followed by research objectives and research questions. The most important part is the discussion of the risk assessment on cloud security.

A. Problem statement

Nowadays, the cloud computing becomes a bigger issue that able to influence the organisations significantly. According to Chea, Duan, Zhan and Fan (2011) stated that cloud computing consists of seven security risks which are unknown risk profile, abuse use of the system, unsafety interfaces and APIs, vicious insiders, shared technology problems, illegal taking over account or service and the loss or divulge of data. Those risks will cause the organisations' crucial information being spread out. Hence, the competitors will take the advantages from it to against the organisations. According to Barron, Yu and Zhan (2013) discussed some facts about the offenders intrude into the system to modify and alter the setting, install vicious code of the system which influence the content of the system, trick other people, steal the crucial data, bring down the network and attack cloud users' account to conduct criminal. Example of these facts are XML signature wrapping attack, malware injection, social engineering attack, account hijacking, traffic flooding and Wireless Local Area Network (WLAN) Attack.

According to Rabai, et. al. (2012) investigated the measure of cyber-security applied to evaluate cloud computing as a business model. The researcher stated that the unveiling of classified data has highly impact on the confidentiality of data which can be caused a high cost of unrecoverable loss. The security threats such as vicious action on cloud computing will lead to the loss of confidentiality. Hence, is the loss of confidential data will affect the cloud security?

According to Mohammadi and Jadidoleslamy(2011) discussed the security detection methods to control the link layer attacks of Wireless Sensor Networks (WSNs) effectively. Throughout the research, 76.9% of the attacks of WSNs are pointing integrity and availability which are most the highest percentage of attack threats among confidentiality, integrity, availability and authenticity. The researchers found out the clustering protocols is the best security solution for the attacks rather than encryption. Thus, how the data processing integrity influences the cloud security?

The availability, integrity, sensitivity, confidentiality and mission critical are considered when researching the substitute to the use of IT which more focused on cloud computing in order to enhance the universities' flexibility and save more (Mircea & Andreescu, 2011). After completing this research, the strategy for cloud security issues should be adopted to have the potential of reducing the universities' expenses. Therefore, is the cloud security will be affected by those consideration?Based on Pal, et. al. (2011) demonstrated about protecting cloud resources by using trusted security framework. The research found out the trust level of trusted user increases after conducting trusted communication with the cloud service provider. The framework can be included the method of identifying malicious activity to avoid unauthorized accesses to cloud data in order to increase the level of mutual trust between the cloud user and cloud service provider. Then how the mutual trust level will impact the cloud data?

According to Monfared(2010) determined the stages for researching security monitoring organisations in the cloud computing model. Mutual auditability is pursued by stakeholders to ensure there have assurance about the other parties. Cooperative organisations should communicate and examine every cloud layer. It enables to prevent the duplication of data in every layer and strengthen the accuracy. To what extent of mutual auditability will influence the cloud computing security?Therefore this paper analyse the risk assessment on Cloud Security among SMEs in Malaysia.

B. Objectives

- To identify how the data confidentiality affect cloud security in SMEs within Malaysia.
- To study about the data integrity impact on cloud security in SMEs within Malaysia.
- To discover the availability of data on cloud security in SMEs within Malaysia.
- To identify how the mutual trust between data owner and cloud service provider affect cloud security in SMEs within Malaysia.
- To study about the auditability of data on cloud computing in SMEs within Malaysia.
- To offer suggestion, conclusion and recommendation based on analysis in SMEs within Malaysia.

II. METHOD & MATERIALS

The Quantitative Research Method with primary data are applied in this research. Primary data can be defined as the data collected specifically and originally for the research (Kara, 2013). The primary data source will be collected by preparing questionnaires in respect of dependent variable and independent variables.The questionnaire consists of three sections. Section A is the list of questions that pertain the demographic questions such as gender, age, education level, job title and the nationality. Section B is regarding the current issues of cloud computing security. Section C is including the factors of risk assessment on the cloud computing security.

The electronically questionnaires are being used in this research as the participants of the research are computer literate. Then the questionnaires will be sent to the respondents of employees in SMEs. The responses from the respondents will be described in detailed to come out the analysis of the results. This research takes the sample size of 120 employees which the sample size is calculated with the use of Raosoft Sample Size Calculator. The Simple Random Sampling is used to select the sample size randomly from the population. The margin of error can be accepted is 8% and the level of confidence set is 92% to show a favourable results.Multiple linear regression model is being used in this research to investigate the how the factors affect the cloud computing security via SPSS. This model allow the researcher to predict the outcome of a variable in accordance with the outcome of another variable (Lund Research Ltd, 2013). In this research, the predicted variable is known as criterion variable which represented by Y while the predictor variable is represented by X.

$$\mathbf{Y = B_0 + B_1X_1 + B_2X_2 + B_3X_3 + B_4X_4 + B_5X_5}$$

In this research,
Y = Cloud Computing Security (Dependent Variable)
X_1 = Data Confidentiality (Independent Variable)
X_2 = Data Integrity (Independent Variable)
X_3 = Availability of Data (Independent Variable)
X_4 = Mutual Trust (Independent Variable)
X_5 = Auditability of Data (Independent Variable)

When the p-value < 0.05 which is less than the alpha level, hence the null hypothesis, H_0 will be rejected while the alternative hypothesis, H_A is accepted (Dunlop & Baillie, 2009).

III. RESULTS

Table 1:Model Summary[B] of Multiple Linear Regression

Model	R	R^2	Adjusted R^2	Standard Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Significant F Change
1	.466[a]	.217	.183	.54166	.217	6.438	5	116	.000

a. Predictors: (Constant), Auditability of Data, Data Confidentiality, Mutual Trust, Availability of Data, Data Integrity
b. Dependent Variable: Cloud Computing Security

The R in Model Summary acts as a multiple correlation value between the real and estimated values of dependent variable (Field, 2000). The range from -1 to 1 for R value demonstrates whether the relationship is positive or negative. Whereas R^2 measures the rate of the variance in the dependent variable expressed by the linear regression model (Frost, 2017). Based on Table 1, the correlation coefficient, R value is 0.466 which shows that there is a positive relationship between the variables. Moreover, R^2 value in Table 5.6 is 0.217 which means the five different independent variables able to explain 21.7% of dependent variables in this study. It also can be defined that there is a significant correlation between cloud computing security with independent variables which include data confidentiality, data integrity, and availability of data, mutual trust and auditability of data. In addition, the remaining 78.3% of cloud computing security variable can be affected or contributed by other factors.

Table 2: Analysis Of Variance (Anova[A])

Model		Sum of Squares	df	Mean Square	F	Significance
1	Regression	9.445	5	1.889	6.438	.000[b]
	Residual	34.033	116	.293		
	Total	43.478	121			

a. Dependent Variable: Cloud Computing Security
b. Predictors: (Constant), Auditability of Data, Data Confidentiality, Mutual Trust, Availability of Data, Data Integrity

Source: Primary Data

According to Field (2008), the significance level of estimating the result can be tested through Analysis of Variance (ANOVA). It able to compare the samples for numerical dependent variables and also determine whether the results are being explained concisely (O'Donoghue, 2013). Based on Dallal(2012), the Regression Sum of Squares in ANOVA is the discrepancy between Total Sum of Squares and Residual Sum of Squares. Besides that, the Total Sum of Squares refers to the sum of variability amount in the response and Residual Sum of Squares that not able to be considered after the regression model is adopted while the Regression Sum of Squares refers to the variability amount in the response that is considered by the regression model. The df is represent the degrees of freedom which is the number of independent variables. The df is calculated by subtracting 1 from the number of variables (df = n-1) (Statistic How To, 2018). Moreover, F ratio is used to describe the variances between the variables. The significance level (p-value) of ANOVA should be less than or equal to 5% (p-value ≤ 0.05) which indicates that the relationship between two variables is significant and the null hypothesis should be rejected (Minitab Inc, 2016).

Table 2 shows the df is 5 (df = 6-1 = 5) which means the degree of freedom generated by six variables involve cloud computing security, data confidentiality, data integrity, availability of data, mutual trust and auditability of data. In addition, the residual of degree of freedom is in accordance to the sample size for responses received which is 122. From this 122 of sample size, the 6 variables are deducted from the sample size to obtain 116. Next, the aggregate of 5 for degree of freedom calculation and 116 produce the outcome of 121 for the total of degree of freedom. Hence, it can be concluded that when the sample size increases, the degree of freedom, df also increases.Furthermore, the F-ratio which presented in Table 2 is 6.438 which is calculated by using the Regression of Mean Square divides with the Residual of Mean Square (1.888974/.293392=6.438). Besides that, based on Table 2, it indicates the significance level is 0.000 which is lower than 0.05, so that the relationship between the dependent variable and independent variables which included data confidentiality, data integrity, availability of data, mutual trust and auditability of data is significant among SMEs in Malaysia. Hence, the null hypothesis should be rejected.

IV. CONCLUSION

The cloud computing security is important for the individual users, organisations and cloud services providers. The secured cloud environment able to enhance the security of users' data. The risk assessment is an essential tool to examine the security of cloud computing. A lot of researchers have conducted the studies and discovered that the security of cloud computing and risk assessment factors have a positive relationship. When the thorough risk assessment is being conducted, the risk on cloud security can be reduced or avoided. Since the objectives of cloud computing system is to store and secure the users' data, then awareness of risk assessment is one of the consideration to improve the cloud security. Hence, the information of organisation can be secured in order to strengthen the internal control system of the organisation. In this study, the researcher propose five variables of risk assessment on cloud computing security to create the particular awareness among SMEs in Malaysia.

This research have focused on the degree of risk assessments which includes the data confidentiality, data integrity, data availability, mutual trust and data auditability influence towards the cloud computing security. Throughout the research, it figured out that all the five independent variables which mentioned above have a positive and significant impact on the cloud computing security. It can be defined that the level of risk assessment factors increase, the degree of cloud security also increases. In this research, the most significant relationship is between the mutual trust variable and cloud computing security. However, the other four variables also have its own significant impact on cloud security which should be taken into consideration by the users.

V. RECOMMENDATIONS

In this advanced technology era, the cloud computing is being used widely. It able to replace the use of compact disc (CD), flash drives, USB and others. It is convenient which allow the people to store and exchange information through this platform. Now, the more organization sutilise the cloud to keep their documents and other confidential data. However,

some of the organizations feel hesitant to adopt cloud

computing to run the business due to there have risk on cloud information is unsecured. They afraid their privacy information will be invaded and theft by the unauthorized parties. It becomes the global issues currently which should be taken into consideration by everyone when applying cloud services.

To address the shortage when using the cloud services, there have some recommendation to protect the privacy of users and also reduce the issues of cloud security. First, the employees of the organisation should be serious about the encryption in the cloud service (Ivey, 2013). To strengthen the encryption, it can be conducted by creating a secured password for the cloud. The employees need to ensure their passwords are stronger enough which also able can be remembered by themselves. The strong passwords should be included the small and big capital letters as well as the numbers. It may difficult to be invaded by the hackers into the employees' accounts to steal their information in order to protect their privacy. Also, the information of the organisation is being protected.

Second, the organisations should take responsibility to protect the data in cloud environment. The rules of cloud governance practice should be obeyed by all the workers of the organisation. The organisation should include the method of managing risks of cloud security into Enterprise Risk Management (ERM) in order to prevent the vulnerability in cloud environment. The internal auditor ought to take the responsibility to enhance the ERM system and ensure the compliance is existed when engaging cloud services. Internal auditors can discuss the information process lifecycle in cloud to understand which information should be updated, kept and terminated in order to facilitate the cloud operation. To ensure the business operations is continuing due to uncertainty, the knowledge and skills of disaster recovery in cloud environment should be improved. It able to provide the guidelines for the organisation when there is damaged data. The data centre operations of organisation also need to provide the method to assess the data process and reliability in cloud (Cuschieri, 2013). The internal control in cloud platform should be concerned by the organisation to ensure the data and other resources are protected and not leaked out.

Last but not least, the agreement between the cloud service providers and users creates a significant issues in cloud environment. The cloud service providers and users should be aware of and accept the contents in the agreement when the users really want to use the cloud service to prevent the misunderstanding. If the users meet the technical issues when using the cloud service, they should contact to cloud service providers to discuss the issues together. This is because the users can explain clearly about the issues which facilitate the cloud service providers to solve the issues effectively and efficiently in order to ensure the users' data are not being lost but able to be stored safely and protracted.

REFERENCES

1. Ahmed, M. & Hossain, M. A., 2014. Cloud Computing And Security Issues In The Cloud. International Journal of Network Security & Its Applications (IJNSA), 6(1), pp. 25-36.
2. Alam, M. K. & K, S. B., 2013. An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds. International Journal of Scientific and Research Publications, 3(4).
3. Aldossary, S. & Allen, W., 2016. Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. International Journal of Advanced Computer Science and Applications, 7(4), pp. 485-498.
4. Asma, A., Chaurasia, M. A. & Mokhtar, H., 2012. Mousmi Ajay Chaurasia. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 1(2).
5. Barron, C., Yu, H. & Zhan, J., 2013. Cloud Computing Security Case Studies and Research. World Congress on Engineering, Volume 2.
6. Chadha, K. & Bajpai, A., 2012. Security Aspects of Cloud Computing. International Journal of Computer Applications, 40(8), pp. 43-47.
7. Chea, J., Duan, Y., Zhan, T. & Fan, J., 2011. Study on the security models and strategies of cloud computing. International Conference on Power Electronics and Engineering Application, Volume 23, pp. 586-593.
8. Chen, Y., Paxson, V. & Katz, R. H., 2010. What's New About Cloud Computing Security?. Electrical Engineering and Computer Sciences.
9. Chen, Y., Paxson, V. & Katz, R. H., 2010. What's New About Cloud Computing Security?. Electrical Engineering and Computer Sciences, pp. 1-8.
10. Cuschieri, D., 2013. Cloud Encryption and Key Management Considerations. pp. 1-125.
11. Demirkan, H. & Delen, D., 2013. Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud. Decision Support Systems, Volume 55, pp. 412-421.
12. Department of Statistics, Malaysia, 2017. SME Annual Report 2016/17. Malaysia, SME Corp. Malaysia.
13. Djemame, K., Armstrong, D. J., Kiran, M. & Jiang, M., 2011. A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. Cloud Computing 2011 : The Second International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 119-126.
14. Drew, C. J., Hardman, M. L. & Hosp, J. L., 2008. Designing and Conducting Research in Education. United States of America: SAGE.
15. Drissi, S. & Medromi, H., 2013. A New Risk Assessment Approach for Cloud Consumer. Journal of Communication and Computer 11, Volume 11, pp. 52-58.
16. Field, A., 2008. Multiple Regression. Research Methods in Psychology, pp. 1-11.
17. Field, A. P., 2000. Discovering Statistics Using SPSS for Windows: Advanced Techniques for the Beginner. London: SAGE Publications Inc.
18. Frost, J., 2017. How To Interpret R-squared in Regression Analysis. Statistics By Jim, 15 April.
19. Gawande, M. M. R. & Kapse, M. A. S., 2014. Analysis of Data Confidentiality Techniques in Cloud Computing. International Journal of Computer Science and Mobile Computing, 3(3), pp. 169-175.
20. Gholami, A. & Laure, E., 2015. Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments. Computer Science & Information Technology, pp. 131-150.
21. Gliem, J. A. & Gliem, R. R., 2003. Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales. Midwest Research to Practice Conference in Adult, Continuing, and Community Education, pp. 82-88.
22. Habiba, U., Masood, R., Shibli, M. A. & Niazi, M. A., 2014. Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive SystemsModeling, 2(5), pp. 1-37.
23. Hair, J. F. et al., 2006. Multivariate Data Analysis. 6th ed. New Jersey: Pearson Prentice-Hall International.

24. Harshitha, T. C., Aditya, G. & Teja, G., 2014. Security Issues In Cloud Computing. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11(2), pp. 56-59.
25. Hashizume, K., Rosado, D. G., Fernández-Medina, E. & Fernandez, E. B., 2013. An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5), pp. 1-13.
26. Higgins, J., 2005. The Correlation Coefficient. In: The Radical Statistician. California: The Management Advantage, Inc., p. 11.
27. Hussain, W., Hussain, F. K. & Hussain, O. K., 2014. Maintaining Trust in Cloud Computing through SLA Monitoring. International Conference on Neural Information Processing, pp. 690-697.
28. Information Technoogy Services, 2016. Part 1: Descriptive Statistic. In: IBM SPSS Statistic 23. Los Angeles: Information Technoogy Services, p. 7.
29. ISACA, 2011. IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. United States of America: ISACA Professional Guidance Publications.
30. Ismail, U. M., Islam, S. & Mouratidis, H., 2015. Cloud Security Audit for Migration and Continuous Monitoring. pp. 1-6.
31. Ivey, V., 2013. 5 Tips to Keep Your Data Secure on the Cloud. Cloud Security, 16 December.
32. Jain, P., 2012. Security Issues and their Solution in Cloud Computing. International Journal of Computing & Business Research.
33. Kara, H., 2013. Collecting primary data: A time-saving guide. s.l.:Policy Press.
34. Kateeb, I. & Almadallah, M., 2014. Risk Management Framework in Cloud Computing Security in. Joint International Conference, pp. 1-15.
35. Kim, H. J., 2012. Online Social Media Networking and Assessing Its Security Risks. International Journal of Security and Its Applications, 6(3), pp. 11-18.
36. Krishnan, I. G., 2017. Impact of Emotional Intelligence on Work Life Balance Among Female Nurses Serving in Private Multi speciality Hospitals in Kerala with Special Reference to Ernakulam District. pp. 86-131.
37. Kuyoro, S. O., Ibikunle, F. & Awodele, O., 2011. Cloud Computing Security Issues and Challenges. International Journal of Computer Networks, 3(5), p. 250.
38. Lee, K., 2012. Security Threats in Cloud Computing Environments. International Journal of Security and Its Applications, 6(4), pp. 25-32.
39. Li, C., Peters, G. F., Richardson, V. J. & Watson, M. W., 2012. The Consequences Of Information TechnologyControl Weaknesses On Management Sarbanes–Oxley Internal. MIS Quarterly, 36(1), pp. 179-204.
40. Lin, G., Bie, Y. & Lei, M., 2013. Trust Based Access Control Policy in Multi-domain of Cloud Computing. Journal Of Computers, 8(5), pp. 1357-1365.
41. Lionel Dupré, T. H., 2012. Cloud Computing: Benefits, risks and recommendations for information security. .
42. Liu, W., 2012. Research on Cloud Computing Security Problem and. International Conference on Consumer Electronics, Communications and Networks, p. 1218.
43. Mircea, M. & Andreescu, A. I., 2011. Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis. Communications of the IBIMA, p. 15.
44. Mohammadi, D. S. & Jadidoleslamy, H., 2011. A Comparison Of Link Layer Attacks On Wireless Sensor Networks. International journal on applications of graph theory in wireless ad hoc networks and sensor networks, 3(1), pp. 35-56.
45. Mohammadi, S. & Jadidoleslamy, H., 2011. A Comaparison of Link Layer Attacks on Wireless Sensor Networks. International journal on applications of graph theory in wireless ad hoc networks and sensor networks, 3(1), pp. 35-56.
46. Monfared, A. T., 2010. Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments. Seminar on Network Security.
47. Nirmala, S., Bhanu, S. S. & Patel, A. A., 2012. A Comparative Study Of The Secret Sharing Algorithms For Secure Data In The Cloud. International Journal on Cloud Computing: Services and Architecture(IJCCSA), 2(4), pp. 63-71.
48. O'Donoghue, P., 2013. Statistics for Sport and Exercise Studies: An Introduction. New York: Routledge.
49. Pal, S., Khatua, S., Chaki, N. & Sanyal, S., 2011. A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security. Cryptography and Security, p. 12.
50. Pinto, A. A. et al., 2011. Securing Cloud System via Internal Control Management. World Congress on Engineering, Volume 1, p. 3.
51. Popa, R. A. et al., 2011. Enabling security in cloud storage slas with cloudproof. Berkeley, USENIX Association.
52. Qin, T. L., Chuang, L. & Yang, N., 2010. Evaluation of User Behavior Trust in Cloud Computing. International Conference on Computer Application and System Modeling, pp. 567-572.
53. Rabai, L. B. A., Jouini, M., Aissa, A. B. & Mili, A., 2012. A cybersecurity model in cloud computing environments. Computer and Information Sciences, Volume 25, pp. 63-75.
54. Rong, C., Nguyen, S. T. & Jaatun, M. G., 2013. Beyond lightning: A survey on security challenges in cloud computing. Computers and Electrical Engineering, 39(1), p. 49.
55. Sabahi, F., 2011. Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges. International Journal on Advances in ICT for Emerging Regions, 4(2), pp. 12-23.
56. Salazar, D., 2016. Cloud Security Framework Audit Methods. pp. 1-25.
57. Sawyer, S. F., 2009. Analysis of Variance: The Fundamental Concepts. The Journal of Manual & Manipulative Therapy, 17(2), pp. 27-38.
58. Sengupta, S., Kaulgud, V. & Sharma, V. S., 2016. Cloud Computing Security – Trends and Research Directions.
59. Sen, J., 2013. Security and Privacy Issues in Cloud Computing. pp. 1-42.
60. Shereek, B. M., Muda, Z. & Yasin, S., 2014. Improve Cloud Computing Security Using RSA Encryption. IOSR Journal of Engineering (IOSRJEN), 4(2).
61. Sinha, M., Silakari, S. & Pandey, R., 2016. Trust based Mechanism for Secure Cloud Computing Environment: A Survey. International Journal of Engineering Science Invention, 5(3), pp. 2319-6726.
62. Sun, Y. C., Zhang, J. S., Xiong, Y. P. & Zhu, G. Y., 2014. Data Security and Privacy in Cloud Computing. International Journal of Distrubuted Sensor Networks, pp. 1-9.
63. Talib, A. M., Atan, R., Abdullah, R. & Murad, M. A. A., 2011. Multi Agent System Architecture Oriented Prometheus Methodology Design to Facilitate Security of Cloud Data Storage. Journal of Software Engineering, 5(3), pp. 78-90.
64. Tavakol, M. & Dennick, R., 2011. Making sense of Cronbach's alpha. International Journal of Medical Education, Volume 2, pp. 53-55.
65. Ullah, S., Zheng, X. F. & Zhou, F., 2013. TCloud: A Dynamic Framework and Policies for Access Control across Multiple Domains in Cloud Computing. International Journal of Computer Applications, 62(2), pp. 1-7.
66. Wang, C., Chow, S. S.-M. & Wang, Q., 2010. Privacy-Preserving Public Auditing for. INFOCOM, 2010 Proceedings IEEE.
67. Zanoon, N., Al-Haj, A. & Khwaldeh, S. M., 2017. Cloud Computing and Big Data is there a Relation between the Two: A Study. International Journal of Applied Engineering Research, 12(17), pp. 6970-6982.
68. Zhang, X., Wuwong, N., Li, H. & Zhang, X., 2010. Information Security Risk Management Framework for the Cloud Computing Environments. IEEE International Conference on Computer and Information Technology, Volume 10, pp. 1328-1334.
69. Zissis, D. & Lekkas, D., 2012. Addressing cloud computing security issues. Future Generation Computer Systems, Volume 28, pp. 583-592.

AUTHORS PROFILE

Lim Jia Hui is working as Asia Pacific University, Malaysia.

Dhamayanthi Arumugam is working as Asia Pacific University, Malaysia.

Suresh Balasingam is working as Asia Pacific University, Malaysia.