Novel Risk Assessment Method to Identify Information Security Threats in Cloud Computing Environment

Ganthan Narayana Samy[1](✉), Sameer Hasan Albakri[1], Nurazean Maarop[1], Pritheega Magalingam[1], Doris Hooi-Ten Wong[1], Bharanidharan Shanmugam[2], and Sundresan Perumal[3]

[1] Advanced Informatics Department,
Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia,
Kuala Lumpur, Malaysia
ganthan.kl@utm.my

[2] School of Engineering and Information Technology,
Charles Darwin University, Casuarina, Australia

[3] Faculty of Science and Technology,
Universiti Sains Islam Malaysia, Nilai, Malaysia

Abstract. Cloud computing model brought many technical and economic benefits, however, there are many security issues. Most of the common traditional information security risk assessment methods such as ISO27005, NIST SP800-30 and AS/NZS 4360 are not fit for the cloud computing environment. Therefore, this study applies medical research approach to assess the information security threats in the cloud computing environment. This study has been conducted as a retrospective cohort study and the collected data has been analyzed by using the survival analysis method. The study has been conducted on the software as a service (SaaS) environment that has more than one thousand and seven hundred cloud customers. The survival analysis method is used to measure the significance of the risk factor level. The information security threats have been categorized into twenty-two categories. This study has proven that the medical research approach can be used to assess the security risk assessment in cloud computing environment to overcome the weaknesses that accompany the usage of the traditional information security risk assessment methods in cloud computing environment.

Keywords: Cloud computing security
Information security risk assessment method
Medical research design and method

1 Introduction

The cloud computing model bargains many economic and functional advantages, for small and medium-sized businesses (SMBs). The economic benefits include but not limited: Low cost, availability of resources, energy savings, and increased focus on business objectives [1–3]. International Data Corporation IDC in 2014 conducted a

F. Saeed et al. (Eds.): IRICT 2018, AISC 843, pp. 566–578, 2019.
https://doi.org/10.1007/978-3-319-99007-1_53

survey on cloud-related topics and published it in April 2015. The survey was conducted on 3,464 organizations across North America, Latin America, Europe, and Asia. In sub-report named 'IDC's European Enterprise Communications Survey' with sample size consisting of 933 interviews, IDC expected that cloud connectivity services market in Western Europe would grow from less than $100 million in 2013 to almost $1 billion by 2019. However, even with this large rate of growth, concerns over security in cloud computing are the main inhibitors of public cloud [4].

Cloud computing adds new challenges the ordinary information security challenges, as its model architecture was designed to outsource the essential services of the IT systems to a third party. Guaranteeing the data confidentiality, integrity, authenticity, auditability, availability and compliance in outsourcing scheme is a difficult task to achieve [5]. Furthermore, cloud computing virtualization environment requires the determination of new risks and the re-evaluation of well-known risks [6]. In addition, introducing multi-tenants or sharing resource services in the virtual environment of cloud computing adds new security challenges [7]. Moreover, cloud computing distinguished characteristics have raised many security risks and make the traditional risk assessment methods unsuitable for cloud computing environment. It is difficult to use most of the common traditional risk assessment methods (such as ISO27005, NIST SP800-30 and AS/NZS 4360) to assess the security risks in cloud computing environment due to its design and structure. These methods are designed for the traditional computer model; thus, it has some assumptions and risk level calculation approaches that are not suitable for the cloud computing model.

Many studies have investigated the similarity between the medical environment and the computing environment. The study has been designed as a retrospective study and the collected data has been analyzed by using the survival analysis method. The second section of this paper review the related work. The research methodology that we used in this study been discussed in Sect. 3. Section 4 presents the suggested categorization by this study for some of the security threats. The obtained results have been presented and discussed in Sect. 5. Finally, Sect. 6 concludes the paper.

2 Related Work

The main features of the cloud computing (i.e. Resource pooling, broad network access, rapid elasticity, on-demand self-service, and measured service) of the cloud computing model [8] have raised several new security risks and call for many past, well defined risks to be re-evaluate and redefine according to the cloud computing model [9]. Several studies have been conducted that define cloud computing risks. In this section, we present some of these studies to address the security risks in cloud computing environment. Munir and Palaniappan (2013), listed some of the potential security threats they found in cloud computing environment. Examples of these threats include changes to business models, abusive use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues and the nature of multitenancy nature, data loss and leakage, service hijacking, risk profiling, and identity theft. They also mentioned security attacks such as zombie service injection Man-in-the Middle, Metadata spoofing, Phishing, and Backdoor channel attacks as well as attacks on virtualization, VM Escape, and Rootkit in Hypervisor, [10].

Tanimoto et al. in 2014, covered some cloud computing risks in their research on assessing cloud computing risks. They evaluated twenty-three risks including wrongly used data, data being deleted after cloud service use, regulatory non-compliance by the service provider, and service providers limiting information disclosure [7]. Alruwaili and Gulliver in 2014, listed eight types of the security threats that must be assessed during the security risk assessment process for cloud computing environment. These security threats were hardware failure or errors, software failure or errors, quality of service and policy deviation, compromise of intellectual property (IP), deliberate software or hardware attacks, human error or failure, obsolete technology, and acts of nature [11]. Al-Anzi et al. in 2014, mentioned some of the prominent security threats they found in cloud computing environment. Those threats included, abuse and nefarious use of cloud computing, insecure application programming interfaces, malicious insiders, customer-data manipulation, data loss/leakage, account, service and traffic hijacking, data scavenging and malicious VM creation [12]. Jafarpour and Yousefi in 2016, listed some of the security risk in cloud computing such as difficulty to guarantee data privacy and data integrity, losing of control of data, lack of trust, inadequate of security control, malicious or ignorant tenants, single point of failure due to the sharing services, controls misconfigurations, commingled tenant data, and performance risks [13].

Most of the popular risk assessment standards such as ISO27005, NIST SP800-30 and AS/NZS 4360 are designed with main assumption, which is the organization's assets exist in the organization's data center and the information security risk assessor can grant full access to the information assets by the organization itself [14, 15]. However, the cloud computing model has some distinguishing characteristics that make this assumption unfit for the cloud computing [9]. For example, cloud service provider is not the real owner for the information assets but the cloud customer. There is a sharing for the hardware and software ownership, access and control authorities, and security responsibilities between the cloud service provider and the cloud customers.

3 Research Methodology

Most statistical methods used in medical research have better and more accurate results. For instance, survival analysis is more efficient and provides more accurate results compared to other methods such as neuron network, fuzzy logic, and decision trees [16, 17]. The medical studies can be classified as a primary study which usually conducted be using primary data or as a secondary study which use a secondary data that has been produced by other studies [16, 18]. One of the most popular medical studies approaches is the epidemiological studies, this type of studies focuses on specific population and investigate the patterns and frequencies, and relationship between risk factors. There are four forms of the epidemiological studies: cohort, case control, cross-sectional, and ecological studies [18, 19]. The term 'cohort' in medical studies refers to a part of pre-defined population with common characteristics and the 'cohort study' is a study that depends on the observation as a method for data collection to answer the research questions by selecting appropriate samples [20].

There are two approaches to conduct a cohort study; prospective and retrospective approach. Prospective approach starts the observation (i.e. data collection) at baseline time and follow up to the specific time in the future or until specific condition is satisfied. Retrospective approach starts the observation (i.e. data collection) at baseline time and follow up to the specific time in the past [21]. There are many advantages for this approach such as it is required short time and less expenses because it depends on historical data. Besides, it is efficient to discover new findings based on existing data and it is able to combine the data from different sources [22, 23].

This study has been designed as retrospective study, the historical raw data that collected by our previous study for the information security risks in cloud computing environment [24]. The original study has been conducted on the software as a service (SaaS) environment that has more than one thousand and seven hundred cloud customers. In this study, the information security threats have been categorized into twenty-two categories as explained in the next section. All the collected data has been analyzed by the survival analysis method within R software. The survival analysis method is used to decide the significance of the risks' factors.

4 Threats Categorization

In this study, eighty-one information security threats have been identified during literature review for the previous studies. These information security threats have been grouped into twenty-two categories. These security threats categories include Natural Disasters, Environment, Accidental Accidents, Hardware Problems, Software Problems, Application Design, Human Sabotage, Human Errors, Users Awareness, Unauthorized Access, Unauthorized actions, Security Attack on the Server, Security Attack on the Clients, Application Security Risks, Security Attack on the Administration, Security Attack on the Network, Loss of Communication Services, Loss of Essential Services, Cloud Risks, Organizational Risks, Administration Problems, and Location.

The security threats T08 (Freezing), T09 (Flood), T10 (Climatic phenomenon), T11 (Volcanic phenomenon), T12 (Meteorological phenomenon), and T13 (Seismic phenomenon) have been categorized as 'Natural Disasters'. This category includes all the security threats that beyond the human control and usually have catastrophic effects. This category is equivalent to 'Natural events' category in ISO27005 [25]. The 'Environment' category includes the security threats T02 (Water damage), T03 (Pollution), T06 (Dust), and T07 (Corrosion). This category involves the security threats that related to the environments and its effects can be controlled or limited by human action. This category is equivalent to 'Physical damage' category in ISO27005 [25]. The 'Accidental Accidents' category includes the security threats T01 (Fire), and T04 (Major accident). This category includes the security threats that occurred accidentally such as fire or any physical damage in way that cause partially or completely stop the cloud service provider system. The 'Hardware Problems' category includes the security threats T18 (Equipment failure), and T20 (Equipment malfunction). This category involves the security threats that usually effect on the hardware in the cloud service provider's system without any human interfering such as failure and malfunction.

This category is equivalent to 'Hardware failure or error' category in Alruwaili and Gulliver (2014) study.

The 'Human Sabotage' category involves the security threats T05 (Destruction of equipment or media), T51 (Tampering with hardware), T52 (Tampering with software), T33 (Backups lost, stolen), T35 (Theft of computer equipment), T46 (Theft of media or documents), and T48 (Retrieval of recycled or discarded media). This category includes the damage that my occurred to the hardware in the cloud service provider system because the human interfering. It also involves all the stealing actions that might occur for the cloud service provider assets. The category 'Software Problems' contains the security threats T19 (Software malfunction), T72 (Outdated application software), T28 (Use of counterfeit or copied software), and T47 (Operating System Failure). This category includes the security threats that accompany the software in the cloud service provider system. The 'Application Design' category includes T21 (Saturation of the information system) and T80 (Using Known Vulnerable Components). The 'Application Design' category involves the security threats that accompany the improper software design (i.e. it may work perfect but the security threat come from its design), while the 'Software Problems' category covers the well-known software problems that may accompany any software [26].

The category 'Human Errors' includes the security threats the occurred by human unintentionally such as T56 (Error in use), regardless the level of the user experience. This category is equivalent to 'human error or failure' category in Alruwaili and Gulliver (2014) study. The category 'Users Awareness' involves the security threats T58 (Loss of encryption keys), T59 (Loss authentication keys), and T60 (Lack of user technical expertise). These security threats usually occurred because the lake of the user awareness, it may be happened intentionally or unintentionally. The 'Unauthorized Access' category includes the security threats T26 (Unauthorized use of equipment), T32 (Forging of rights), and T34 (Unauthorized access to premises). This category involves the unauthorized access to the cloud service provider's assets. The 'Unauthorized actions' category contains the security threats T25 (Abuse of rights), T27 (Fraudulent copying of software), T30 (Illegal processing of data), T31 (Denial of actions), and T49 (Disclosure). This category involves any actions that violate the cloud service provider's rules. This category is equivalent to 'Unauthorised actions' category in ISO27005 [25].

The category 'Security Attack on the Server' includes the security threats, T44 (Remote spying), T61 (Distributed denial of service (DDoS)), T62 (Economic denial of service (EDOS)), T63 (Undertaking malicious probes or scans), T64 (Compromise service engine), T67 (Loss or compromise of operational logs), T68 (Loss or compromise of security logs), and T69 (SQL Injection). This category involves the security attacks that might occur against the cloud service provider's system. The 'Security Attack on the Clients' category includes the security attacks on the cloud customers such as T65 (Social engineering attacks) [27]. The 'Application Security Risks' category involves the security threats T50 (Data from untrustworthy sources), T29 (Corruption of data), T75 (Insecure Direct Object References), T78 (Cross-Site Scripting (XSS)), T79 (Cross-Site Request Forgery (CSRF)), and T81 (Un-validated Redirects and Forwards). This category includes the security attacks that targeting the application interface. The category 'Security Attack on the Administration' contains the security attacks that targeting the system administrators, including T55 (Breach of personnel availability), T57 (Administrator's email attack), T70 (Account lockout attack), and T71 (Login brute force attack). The category 'Security Attack on the Network' involves T45 (Eavesdropping), T54 (Interception of compromising interference signals), and T66 (Modifying network traffic). This category include the security attacks that targeting the network and the data traffic within the system network [26]. The 'Loss of Communication Services' category includes the security threats that cause the communications failure such as T17 (Failure of telecommunication equipment). The category 'Loss of Essential Services' involves the security threats that cause losing one of the essential services for the data center such as T14 (Loss of power supply), T15 (Failure of air-conditioning system), and T16 (Failure of water supply system).

The category 'Cloud Risks' includes the security threats that accompany the cloud computing implementation such as T22 (Resource exhaustion), T23 (Isolation failure), T24 (Conflicts between customer hardening procedures and cloud environment), and T74 (Insecure or Ineffective Deletion of Data). The category 'Organizational Risks' involves T36 (Lock-in), T37 (Loss of governance), T38 (Compliance challenges), T39 (Loss of business reputation due to co-tenant activities), T40 (Cloud service termination or failure), T41 (Cloud provider acquisition), T42 (Supply chain failure), and T43 (Risk from changes of jurisdiction). This category includes the security threats that accompany the organization's sustainability, legitimacy and how it manages the cloud infrastructure. This category is equivalent to 'Policy and organizational' in the categories proposed by [27]. The category 'Administration Problems' includes the security threats T73 (Long time for system recovery), T76 (Security Misconfiguration), and T77 (Missing Function Level Access Control). This category involves the security threats that occur because of the administration actions. The last category 'Location' includes the security threats that related to the organization location such as T53 (Position detection).

5 Results and Discussion

This section presents the results that obtained by this study. It also discusses how adapting the medical research design and methods to assess the security risk in cloud computing environment fit for cloud computing security field. There are two main popular data layout for the survival data; basic data layout and counting process [21], in this study, we used counting process (CP). The survival analysis method has been used to analysis the collected data. This section presents the results that obtained from data analysis according to their categorization as discussed in the previous section. Multiple security incidents have been recorded for seventeen security threats, these security threats are T18 Equipment failure, T19 Software malfunction, T22 Resource exhaustion, T28 Use of counterfeit or copied software, T29 Corruption of data, T37 Loss of governance, T49 Disclosure, T56 Error in use, T57 Administrator's email attack, T60 Lack of user technical expertise, T63 Undertaking malicious probes or scans, T64 Compromise service engine, T68 Loss or compromise of security logs, T71 Login brute force attack, T72 Outdated application software, and T73 Long time for system recovery. There are some categories have no recorded security incidents. These categories are Natural Disasters, Environment, Accidental Accidents, Application Design, Human Sabotage, Unauthorized Access, Security Attack on the Clients, Security Attack on the Network, Loss of Communication Services, Loss of Essential Services, and Location.

In the category of hardware problems only T18 Equipment failure has some recorded incidents. As shown in the Table 1 below, it is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 5.51 higher than zero. Moreover, the hazard ratio value is quite high, 245 which means the group that exposed for the security threats has a potential to get affected, 245% higher than the unexposed group. Usually the security incident of T18 Equipment failure will cause many other security threats.

Table 1. Hardware Problems

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T18	Equipment failure	5.51	246.00	<0.05
T20	Equipment malfunction	NA	NA	NA

In the category of software problems, T19 Software malfunction, T28 Use of counterfeit or copied software, and T72 Outdated application software have recorded incidents. As shown in the Table 2 below, T72 Outdated application software is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 12.56 higher than zero. Moreover, the hazard ratio value is extremely high, 284900. The T72 Outdated application software leads to many other security threats such as software malfunction and data disclosure. The security threat T19 (Software malfunction) also is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 3.91 higher than zero. Moreover, the hazard ratio value is 49.73 which means the group that exposed for the security threats has a potential to get affected, 48.73% higher than the unexposed group. The security threat T28 Use of counterfeit or copied software is not statistically significant where p-value is greater than 0.05.

Table 2. Software Problems

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T19	Software malfunction	3.91	49.73	<0.05
T28	Use of counterfeit or copied software	1.31	3.72	>0.05
T47	Operating System Failure	NA	NA	NA
T72	Outdated application software	12.56	284900.00	<0.05

In the category of human errors, the T56 Error in use has some recorded incidents. As shown in the Table 3 below, it is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 11.61 higher than zero. Moreover, the hazard ratio value is extremely high, 110400 which means the group that exposed for the security threats has a potential to get affected higher than the unexposed group.

Table 3. Human Errors

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T56	Error in use	11.61	110400.00	<0.05

In the category of user awareness only T60 Lack of user technical expertise has some recorded incidents. As shown in the Table 4 below, it is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 0.65 higher than zero. Moreover, the hazard ratio value is slightly high, 3.15 which means the group that exposed for the security threats has a potential to get affected, 2.15% higher than the unexposed group.

Table 4. Users Awareness

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T58	Loss of encryption keys	NA	NA	NA
T59	Loss authentication keys	NA	NA	NA
T60	Lack of user technical expertise	0.65	1.91	<0.05

In the category of unauthorized actions, T49 Disclosure has some recorded incidents. As shown in the Table 5 below, it is not statistically significant where p-value is equal 0.05, even it has a positive regression coefficient value, which is higher 1.15 higher than zero. Moreover, the hazard ratio value is slightly high, 1.91 which means the group that exposed for the security threats has a potential to get affected, 0.91% higher than the unexposed group.

Table 5. Unauthorized actions

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T25	Abuse of rights	NA	NA	NA
T27	Fraudulent copying of software	NA	NA	NA
T30	Illegal processing of data	NA	NA	NA
T31	Denial of actions	NA	NA	NA
T49	Disclosure	1.15	3.15	0.05

In the category of security attack on the server, only T63 Undertaking malicious probes or scans, T64 Compromise service engine, and T68 Loss or compromise of security logs have recorded incidents. As shown in the Table 6 below, T64 Compromise service engine is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 6.80 higher than zero. Moreover, the hazard ratio value is extremely high, 899.70. The occurrence of T64 Compromise service engine leads to many security consequences. The security threat T63 Undertaking malicious probes or scans also is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 2.25 higher than zero. Moreover, the hazard ratio value is 9.51 which means the group that exposed for the security threats has a potential to get affected, 8.51% higher than the unexposed group. The security threat T68 Loss or compromise of security logs is not statistically significant where p-value is greater than 0.05.

Table 6. Security Attack on the Server

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T44	Remote spying	NA	NA	NA
T61	Distributed denial of service (DDoS)	NA	NA	NA
T62	Economic denial of service (EDOS)	NA	NA	NA
T63	Undertaking malicious probes or scans	2.25	9.51	<0.05
T64	Compromise service engine	6.80	899.70	<0.05
T67	Loss or compromise of operational logs	NA	NA	NA
T68	Loss or compromise of security logs	1.34	3.81	>0.05
T69	SQL Injection	NA	NA	NA

In the category of application security risks, T29 Corruption of data has some recorded incidents. As shown in the Table 7 below, it is not statistically significant where p-value is greater than 0.05, even it has a positive regression coefficient value, which is higher 6.69 higher than zero. Moreover, the hazard ratio value is extremely high, 801.10 which means the group that exposed for the security threats has a potential to get affected.

Table 7. Application Security Risks

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T29	Corruption of data	6.69	801.10	>0.05
T50	Data from untrustworthy sources	NA	NA	NA
T75	Insecure Direct Object References	NA	NA	NA
T78	Cross-Site Scripting (XSS)	NA	NA	NA
T79	Cross-Site Request Forgery (CSRF)	NA	NA	NA
T81	Un-validated Redirects and Forwards	NA	NA	NA

In the category of security attack on the administration, T57 Administrator's email attack, and T71 Login brute force attack have recorded incidents. As shown in the Table 8 below, T57 Administrator's email attack is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 9.86 higher than zero. Moreover, the hazard ratio value is extremely high, 19210. T71 Login brute force attack is statistically significant where p-value is less than 0.05, and it has a positive regression coefficient value, which is higher 1.90 higher than zero. Moreover, the hazard ratio value is slightly high, 6.66 which means the group that exposed for the security threats has a potential to get affected, 5.66% higher than the unexposed group.

Table 8. Security Attack on the Administration

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T55	Breach of personnel availability	NA	NA	NA
T57	Administrator's email attack	9.86	19210.00	<0.05
T70	Account lockout attack	NA	NA	NA
T71	Login brute force attack	1.90	6.66	<0.05

In the category of cloud risks only T22 Resource exhaustion has some recorded incidents. As shown in the Table 9 below, it is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 5.09 higher than zero. Moreover, the hazard ratio value is quite high, 161.90 which means the group that exposed for the security threats has a potential to get affected, 160.90% higher than the unexposed group.

Table 9. Cloud Risks

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T22	Resource exhaustion	5.09	161.90	<0.05
T23	Isolation failure	NA	NA	NA
T24	Conflicts between customer hardening procedures and cloud environment	NA	NA	NA
T74	Insecure or Ineffective Deletion of Data	NA	NA	NA

In the category of organizational risks only T37 Loss of governance has some recorded incidents. As shown in the Table 10 below, it is statistically significant where p-value is less than 0.05 and it has a positive regression coefficient value, which is higher 1.62 higher than zero. Moreover, the hazard ratio value is slightly high, 5.06 which means the group that exposed for the security threats has a potential to get affected, 4.06% higher than the unexposed group.

Table 10. Organizational Risks

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T36	Lock-in	NA	NA	NA
T37	Loss of governance	1.62	5.06	<0.05
T38	Compliance challenges	NA	NA	NA
T39	Loss of business reputation due to co-tenant activities	NA	NA	NA
T40	Cloud service termination or failure	NA	NA	NA
T41	Cloud provider acquisition	NA	NA	NA
T42	Supply chain failure	NA	NA	NA
T43	Risk from changes of jurisdiction	NA	NA	NA

In the category of administration problems application security risks, T73 Long time for system recovery has some recorded incidents. As shown in the Table 11 below, it is not statistically significant where p-value is greater than 0.05, even it has a positive regression coefficient value, which is higher 4.14 higher than zero. Moreover, the hazard ratio value is high, 62.71 which means the group that exposed for the security threats has a potential to get affected.

Table 11. Administration Problems

ID	Security threats	Regression coefficient	Proportional hazard ratio	Significance
T73	Long time for system recovery	4.14	62.71	>0.05
T76	Security Misconfiguration	NA	NA	NA
T77	Missing Function Level Access Control	NA	NA	NA

6 Conclusion

This study used the medical approaches to assess the security risks in the cloud computing environment. The study has been designed as retrospective study and the collected data has been analyzed by using the survival analysis method. The collected data were analyzed using R statistical analysis software, which identified a list of information security risks. The regression coefficient and proportional hazard ratio has been calculated by using survival analysis method. The regression coefficient and proportional hazard ratio give an estimation for the future potential occurrence for each security threat. This study confirms that the medical research design and method can be adapted into cloud computing environments to overcome the weaknesses of the traditional risk assessment methods.

Acknowledgements. The authors would like to thank Universiti Teknologi Malaysia (UTM) for supporting this work through the Tier 1 GUP Grant Scheme under Grant vote number Q.K130000.2538.14H18.

References

1. Amini, A., et al.: A fuzzy logic based risk assessment approach for evaluating and prioritizing risks in cloud computing environment. In: International Conference of Reliable Information and Communication Technology. Springer (2017)
2. Li, J., Li, Q.: Data security and risk assessment in cloud computing. In: ITM Web of Conferences. EDP Sciences (2018)
3. Ali, K.E., Mazen, S.A., Hassanein, E.E.: Assessment of cloud computing adoption models in e-government environment. Int. J. Comput. Intell. Stud. **7**(1), 67–92 (2018)
4. Bakkers, J.H., Eibisch, J.: Cloud Connectivity Services in Europe in Industry Developments and Models. International Data Corporation IDC (2015)
5. Xuan, Z., et al.: Information security risk management framework for the cloud computing environments. In: 10th IEEE International Conference on Computer and Information Technology (CIT 2010), Bradford (2010)
6. Fito, J.O., Macias, M., Guitart, J.: Toward business-driven risk management for cloud computing. In: 2010 International Conference on Network and Service Management (CNSM), Niagara Falls. IEEE (2010)
7. Tanimoto, S., et al.: A study of risk assessment quantification in cloud computing. In: 2014 International Conference on Network-Based Information Systems, Salerno (2014)

8. Mell, P., Grance, T.: The NIST definition of cloud computing. NIST Spec. Publ. **800**(145), 7 (2011)
9. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Gener. Comput. Syst. **28**(3), 583–592 (2012)
10. Munir, K., Palaniappan, S.: Framework for secure cloud computing. Int. J. Cloud Comput. Serv. Archit. **3**(2), 21–35 (2013)
11. Alruwaili, F.F., Gulliver, T.A.: Safeguarding the cloud an effective risk management framework for cloud computing services. Int. J. Comput. Commun. Netw. (IJCCN) **4**(3), 6–16 (2014)
12. Al-Anzi, F.S., Yadav, S.K., Soni, J.: Cloud computing: security model comprising governance, risk management and compliance. In: International Conference on Data Mining and Intelligent Computing (ICDMIC), New Delhi (2014)
13. Jafarpour, S., Yousefi, A.: Security Risks in Cloud Computing: A Review (2016)
14. Almorsy, M., Grundy, J., Ibrahim, A.S.: Collaboration-based cloud computing security management framework. In: 2011 IEEE International Conference on Cloud Computing (CLOUD), Washington, DC (2011)
15. Zhao, G.: Holistic framework of security management for cloud service providers. In: 2012 10th IEEE International Conference on Industrial Informatics (INDIN), Beijing. IEEE (2012)
16. Samy, G.N.: Analysing information security threats in healthcare information systems using survival analysis method. Faculty of Computer Science and Information Systems Universiti Teknologi Malaysia (2012)
17. Ma, Z., Krings, A.W.: Competing risks analysis of reliability, survivability, and prognostics and health management (PHM). In: 2008 IEEE Aerospace Conference. IEEE (2008)
18. Röhrig, B., et al.: Types of study in medical research: part 3 of a series on evaluation of scientific publications. Deutsches Arzteblatt Int. **106**(15), 262–268 (2009)
19. Allen, L.A., Horney, J.A.: Methods: study designs in disaster epidemiology. In: Disaster Epidemiology, pp. 65–74. Elsevier (2018)
20. Bhopal, R.S.: Concepts of Epidemiology an Integrated Introduction to the Ideas, Theories, Principles and Methods of Epidemiology, vol. 38, 1st edn. Oxford University Press, New York (2002)
21. Kleinbaum, D.G., Klein, M.: Survival Analysis: A Self-Learning Text, 3rd edn. Springer, Cham (2012)
22. Van Stralen, K.J., et al.: Case-control studies—an efficient observational study design. Nephron Clin. Pract. **114**(1), c1–c4 (2009)
23. Cox, D.R.: Analysis of Survival Data. Routledge, Abingdon (2018)
24. Albakri, S.H., et al.: Security risk assessment framework for cloud computing environments. Secur. Commun. Netw. (2014)
25. BS.ISO/IEC27005:2011: Information Technology-Security Techniques-Information Security Risk Management: The British Standards Institution (2011)
26. Owasp, T.: The Ten Most Critical Web Application Security Risks (2013)
27. ENISA: Cloud computing: benefits, risks and recommendations for information security. The European Network and Information Security Agency (ENISA) (2009)