TALE 2019

Date & Venue

10–13 December 2019, Royal Ambarrukmo Hotel, Yogyakarta, Indonesia

Theme

"Creative & Innovative Education to Enhance the Quality of Life"

PROCEEDINGS

Conference Co-Chairs

Ford Lumban Gaol
Binus University, Indonesia

Ayu Purwarianti
Bandung Institute of Technology, Indonesia

Keynote Speakers

- Dr. Seiichi Kawata
- Prof. Minjuan Wang
- Dr. Henry Feriadi

Committees

Steering Committee

Chair

Manuel Castro
UNED/IEEE President Emeritus of the IEEE Education Society

Members

Preeti Bajaj
Lovely Professional University, Phagwara
Punjab, India

S H Bharati
REVA University
Bangalore, India

Dale Carnegie
Victoria University of Wellington
Wellington, New Zealand

Henry Chan
Hong Kong Polytechnic University
Hong Kong, China

Ford Lumban Gaol
Bina Nusantara University
Jakarta, Indonesia

Kai Pan Mark
Hong Kong Polytechnic University
Hong Kong, China

Nirmal Nair
University of Auckland
Auckland, New Zealand

Manoharan Sathiamoorthy
University of Auckland
Auckland, New Zealand

Gary Wong
The University of Hong Kong
Hong Kong, China

Minjuan Wang
The Education University of Hong Kong
Hong Kong, China

VICE-PRESIDENT ON CONFERENCES AND EVENTS
Diana Andone
University of Timisoara
Romania

IEEE REGION 10 DIRECTOR-ELECT
Takako Hashimoto
Chiba University of Commerce
Tokyo, Japan

Advisory Board

Current

PRESIDENT EMERITUS
Sorel Reisman
IEEE Computer Society and Former Managing Director, MERLOT

EDITOR-IN-CHIEF
John Mitchell
IEEE Transactions on Education

2021-22

PRESIDENT
Edmundo Tovar
IEEE Education Society

DIRECTOR
Deepak Mathur
IEEE Region 10

2019-20

PRESIDENT
Russ Meier
IEEE Education Society

Manuel Castro
UNED/IEEE President Emeritus of the IEEE Education Society

DIRECTOR
Akinori Nishihara
IEEE Region 10

IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)

2019 IEEE International Conference on Engineering, Technology and Education (TALE)
10-13 Dec. 2019

DOI: 10.1109/TALE48000.2019

Showing **1-25** of **188**

Quick Links

- Search for Upcoming Conferences
- IEEE Publication Recommender
- IEEE Author Center

Proceedings

The proceedings of this conference will be available for purchase through Curran Associates.

Engineering, Technology and Education (TALE), 2019 IEEE International Conference on

Print on Demand **Purchase at Partner**

Select All on Page   Sort By: Sequence

[Front matter]
Publication Year: 2019 , Page(s): i - lvii

Design, Development and Delivery of a Complimentary STEM Program for Primary School Pupils
LEE Kar Heng
Publication Year: 2019 , Page(s): 1 - 5
Cited by: Papers (2)
Abstract HTML

Engineerpreneurship: Engineers can be Entrepreneurs
LEE Kar Heng
Publication Year: 2019 , Page(s): 1 - 7
Abstract HTML

A literature review of trend in engineering education`s online laboratory-based tool, the past, now and its future since evolution of standards
Samuel Eneje
Publication Year: 2019 , Page(s): 1 - 8
Abstract HTML

Full Online Learning and Blended e-Learning: A Comparison of Students' Performance
Sze Kiu Yeung; Wee Leong Lee
Publication Year: 2019 , Page(s): 1 - 7
Abstract HTML

Numerical Control Plotter For Direct-To-Blank Substrate Tracing Of Conductive Ink For Electronic Education Purposes
Kent Edward David; Kenneth Jara; Ariel Joseph Lim; Jefferson Piñgol; Raymond Joseph Meimban; Kenneth Mervin Santos; Jaziel Soriano; Joseph Nalunat
Publication Year: 2019 , Page(s): 1 - 5
Cited by: Papers (1)
Abstract HTML

Blended Design-based Learning (bDBL), An Innovative Approach to Cornerstone Engineering Design
Jac K. L. Leung; Paul D. Lavigne
Publication Year: 2019 , Page(s): 1 - 7
Cited by: Papers (1)
Abstract HTML

Understanding loops: a visual methodology
Anabela Gomes; Wei Ke; Chan-Tong Lam; Ana Rita Teixeira; Fernanda Brito Correia; Maria José Marcelino; António José Mendes
Publication Year: 2019 , Page(s): 1 - 7
Cited by: Papers (3)
Abstract HTML

Development of Mobile Learning Application as Scaffolds to Enhance Postgraduate-Level Statistical Literacy
Mohd Nihra Haruzuan Mohamad Said; Mohd Fadzli Ali; Lokman Mohd Tahir; Juhazren Junaidi; Norasyikin Mohd Zaid; Aini Zuhairnee Jasanuar; Fatimah Sarah Yaacob
Publication Year: 2019 , Page(s): 1 - 7
Abstract HTML

A Comparative Study of Teaching Problem-Solving in Mathematics Secondary Schools in Malaysia and South Korea
Abdul Halim Abdullah; Bomi Shin; Umar Haiyat Abdul Kohar; Dayana Farzeeha Ali; Norazrena Abu Samah; Zakiah Mohamad Ashari
Publication Year: 2019 , Page(s): 1 - 8
Cited by: Papers (1)
Abstract HTML

Towards Activity-Centered Gamification Design
Christo Dichev; Darina Dicheva; Keith Irwin
Publication Year: 2019 , Page(s): 1 - 9
Cited by: Papers (2)
Abstract HTML

Improving Student Engagement and Performance in Computing Final Year Projects
Usman Naeem; Syed Islam; Arish Siddiqui
Publication Year: 2019 , Page(s): 1 - 9
Cited by: Papers (1)
Abstract HTML

A Black Box Model of Academic Degree Knowledge System based Computer Network Course Construction Scheme for Postgraduates Students
Changqing Gong; Liang Zhao; Na Lin; Han Qi; Zhenzhou Guo; Xiguang Li
Publication Year: 2019 , Page(s): 1 - 6
Abstract HTML

Who Takes the Cake: Rethinking the Using of Student Teams-Achievement Division in Electronics Course
Pei-Hua Chang; Su-Fen Cheng; Chi-Wei Cheng; Ching-Biau Tzeng
Publication Year: 2019 , Page(s): 1 - 8
Cited by: Papers (1)
Abstract HTML

A Reflection on Teaching Design Thinking to First-Year Engineering Students
Kuntinee Maneeratana; Ratchatin Chancharoen; Peerapat Thongnuek; Potcharawan Sukmuen; Chamaiporn Inkaew; Praweenya Suwannatthachote
Publication Year: 2019 , Page(s): 1 - 8
Cited by: Papers (2)
Abstract HTML

Mirror-mirror on the Wall, Which Teachers Use Educational Technology in Mathematics Classroom-Malaysians or South Koreans?
Abdul Halim Abdullah; Bomi Shin; Nurul Farhana Jumaat; Umar Haiyat Abdul Kohar; Zakiah Mohamad Ashari; Sharifah Nurarfah S. Abd Rahman
Publication Year: 2019 , Page(s): 1 - 8
Abstract HTML

Priorities Dictate Practice – The Operation of Power in the Teaching and Learning Environment
Craig A. Watterson; Dale A. Carnegie; Marc Wilson
Publication Year: 2019 , Page(s): 1 - 8
Abstract HTML

Similarity Detection Techniques for Academic Source Code Plagiarism and Collusion: A Review
Oscar Karnalim; Simon; William Chivers
Publication Year: 2019 , Page(s): 1 - 8
Cited by: Papers (22)
Abstract HTML

The Intelligent Classroom Client Software Design
Tianping Deng; Xiaoyan Wang; Zhengguang Xu; Lin Zhang; Xiaojun Hei; Zhen Wang
Publication Year: 2019 , Page(s): 1 - 5
Cited by: Papers (3)
Abstract HTML

Student's Perception on Usage of Online Social Network and Difficulties in Learning Social Science Research
Fatimah Sarah Yaacob; Norasykin Mohd Zaid; Jamalludin Harun
Publication Year: 2019 , Page(s): 1 - 6
Abstract HTML

Tuklas: Design, Development and Testing of an Augmented Reality Experience for a Children's Museum
Ma. Mercedes T. Rodrigo; Eric Cesar E. Vidal; Ingrid Yvonne D. Herras; Jenilyn L. Agapito; Walfrido David Diy; Victor Antonio Ortega; Nicole Anne Bugayong; Aaron Ong; John Michael Santos; Luis Raphael Tomas Lim
Publication Year: 2019 , Page(s): 1 - 6
Cited by: Papers (2)
Abstract HTML

Do Students Prefer Puzzles To Conventional Assessment Methods?
Roderick Lottering; Robert Hans; Manoj Lall
Publication Year: 2019 , Page(s): 1 - 6
Abstract HTML

Understanding Several Adaptive Filter Algorithms Based on the Weight-update Strategy
Qun Wan; Qi Wu; Lin Zou
Publication Year: 2019 , Page(s): 1 - 4
Cited by: Papers (1)
Abstract HTML

Figure Drawing Method Based on Human Motion Using Pictogramming
Kazunari Ito
Publication Year: 2019 , Page(s): 1 - 6
Cited by: Papers (2)
Abstract HTML

Microwave Engineering Course for Engineering Education Accreditation: Exploration and Practice in SUSTech
Yijun Liu; Qingsha S. Cheng
Publication Year: 2019 , Page(s): 1 - 4
Cited by: Papers (1)
Abstract HTML

Risk Assessment on Cloud Computing for The Learning System in The Education Environment

Maniah
Computer Science Department, BINUS Graduate Program - Doctor of Computer Science, Bina Nusantara University
Jakarta, Indonesia 11480
maniah@poltekpos.ac.id

Benfano Soewito
Computer Science Department, BINUS Graduate Program - Doctor of Computer Science, Bina Nusantara University
Jakarta, Indonesia 11480
benfano@gmail.com

Ford Lumban Gaol
Computer Science Department, BINUS Graduate Program - Doctor of Computer Science, Bina Nusantara University
Jakarta, Indonesia 11480
ford.gaol@gmail.com

Edi Abdurachman
Computer Science Department, BINUS Graduate Program - Doctor of Computer Science, Bina Nusantara University
Jakarta, Indonesia 11480
edia@binus.edu

***Abstract*—**Purpose **- Cloud computing as a service facility in online learning systems provides good solutions for educational institutions. Reasons for educational institutions to use cloud computing as a means of learning include cloud service providers providing sizable hardware and software resources, so educational institutions do not have to pay a large amount of money to buy hardware and software as an investment. But as long as this online learning system runs there will definitely be risks, for example performance problems from internet network connections. This study aims to discuss this problem.** Methodology/approach **- In this study, firstly identifying dangerous or harmless activities to the activities carried out in cloud computing, then determining the impact, aspects, likelihood and severity of risks, and finally determining the level of risk from these activities using a risk matrix.** Finding **- By using a risk register in the learning system, risk analysis and evaluation can show the Incident, Cause, impact, risk type, risk category, aspect, likelihood, severity, and risk level for each dangerous or non-hazardous activity.** Originality/value **- The tools used to measure the level of risk for dangerous or non-hazardous activities for the learning system can be used for more extensive research aimed at measuring institutional-level risks in the education sector**

Keywords— risk assessment, learning system, risk register, risk level

I. INTRODUCTION

Cloud Computing is a subscription-based service where service users can obtain network storage space and computer resources from service providers by using internet connections as access media [1]. . Cloud computing technology certainly provides many benefits for companies as users of cloud services, so it is possible that many companies will soon switch from intranet applications (On-Premise Software) to Cloud Computing, but besides that it also raises a variety of security and confidential issues that need to be considered [2].

Cloud Computing Security is a domain of information security that refers to a series of policies, technologies, and controls used to protect data, applications, and related Cloud Computing infrastructure [3]. The way to maintain security against cloud computing infrastructure from external threats is by maintaining access [4]. When we are going to switch to Cloud Computing technology, as stated by [5], is to provide initial signs for users in making good decisions for migrating to cloud computing, while explaining about the processes that must be done . And when the process of migrating to the cloud has been done, of course the next problem is how to maintain the security of our information to avoid threats from outside that can damage the company's reputation [6]. Including how the strategies and procedures for cloud migration are also a concern for cloud users [7].

Cloud computing in the education environment is nothing new, such as the use of email which has a top-level domain extension .edu means the name of a domain for educational sites. Another example of cloud computing for education is the use of virtual machines and e-learning services [8].

Online learning systems require a lot of hardware and software resources provided by cloud computing services [9]. This is certainly a serious concern for educational institutions that implement it. Including the risk problems that may arise during the online learning system process. To answer this problem, it is necessary to conduct a risk assessment of the online learning system process in the educational environment, which aims to provide information to the leaders of educational institutions whether the activities in this online learning system have low, medium or high risk.

This paper presents a reference in calculating the risk of information technology in cloud computing for education.

This paper is structured with the following writing structure. Section 2 provides information related to risk assessment process and cloud computing for education. In the second part, it also reviews existing papers and analyzes the processes used in risk assessment in the context of cloud computing. Section 3 explains the methodology used in this study. In section 4 explains the risk assessment process on cloud computing for education. The conclusions of this paper convey the steps in the risk assessment process and submit our next research plan delivered at the end of this paper.

II. FUNDAMENTAL CONCEPT

A. Risk Assessment

Risk is a variation of the possibility of an event and consequence [10]. In everyday life the risk is always there, the risk cannot be eliminated but the possibility of the emergence of risks can be reduced as small as possible. Risk can mean a process that includes the process of identifying hazards according to their nature, the likelihood of occurring, their potential impact, then can be assessed and controlled [11].

In general, risk assessment is part of the risk management process, as described in the ISO 31000-2018 standard, that

the risk management process includes: (1) communication and consultation, (2) scope, context and criteria, (3) risk assessment, (4) risk treatment, (5) monitoring and review, (6) recording and reporting [12].

Risk assessment is more likely to use quantitative methods, where the assessment is based on the magnitude of the possibility of the occurrence of risks, and the impact of risk, which can be used by decision makers to determine the prevention cost plan and the necessary resources.

In detail the risk assessment can be divided into 3 stages, namely: [12]

1. Risk identification
   This stage determines the risk factors that are the main causes of the emergence of risks and risk categories.
2. Risk analysis
   This stage determines risk characteristics including the level of risk and control.
3. Risk evaluation
   Risk evaluation is used to help determine decisions based on comparison of the results of risk analysis with predetermined risk categories.

B. Cloud Computing

Cloud Computing is an innovative technology that can provide data transaction facilities for manufacturing, financial, distribution, sales, customer service activities that can share information and work with trading partners [13].

The National Institute of Standards and Technology (NIST) provides an example of Cloud Computing services for all three services that are in the cloud (PaaS, SaaS, IaaS), as shown in figure 1 below:

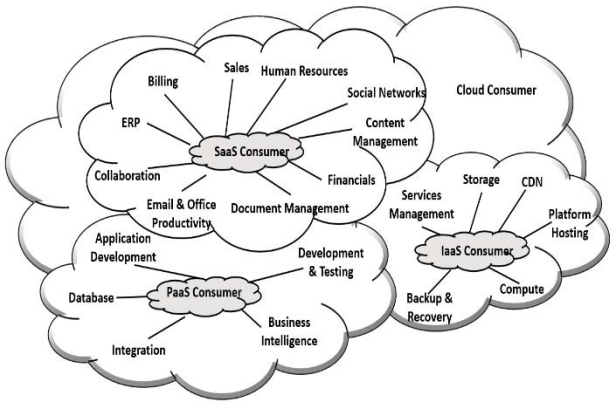

Fig. 1. Cloud Computing Services [14]

Cloud Computing technology revolution provides many benefits for the organization, but on the other hand there is a paradigm shift that causes security and privacy problems that must also be considered [2]. Despite the many benefits provided by Cloud Computing, there are still many companies or individuals who do not want to apply this innovative technology, this is due to many issues of security, privacy and trust [15]. Companies, businesses, government institutions, transportation systems, hospitals, and in some cases, even power plants around the world have been affected by high-level cyber attacks in 2017 [16]. The closest threat to the organization is the presence of cyber attacks [17].

C. Cloud Services for Education Environment

Cloud computing provides sophisticated innovations in the world of education, for example with e-learning systems. Cloud computing services implemented in education for Infrastructure as a Service (IaaS) services are mostly for creation of customized on-demand virtual machines, while for Platform as a Service (PaaS) services such as servlet container platforms, while for Software as a service Services (SaaS) such as using email, web servers, collaborative workspaces [8].

Research conducted by [18] Create an architecture in the cloud environment for education as shown in Figure 2 below:

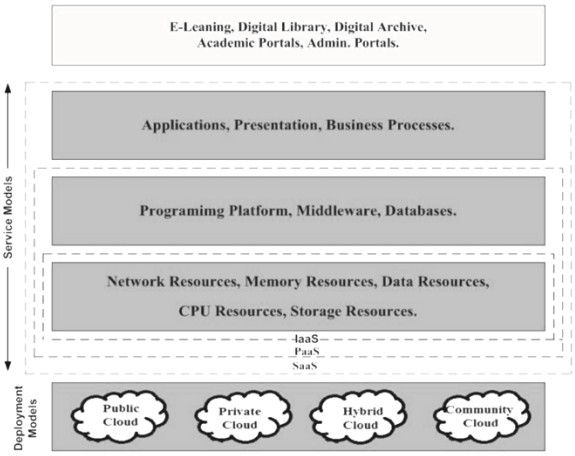

Fig. 2. Architecture on Cloud Computing for Education [18]

From Figure 2 we can see that IaaS is the foundation of all cloud services, containing APIs that will manage interactions with user infrastructure.

The cloud computing architecture for education developed is a guide for decision making in education to migrate to the cloud. Migration strategies that are usually used in an educational environment start from: [19]

a. Develop a knowledge base about Cloud computing;
b. Evaluating the present stage of university from the point of view IT needs, structure and use;
c. Experimenting with Cloud Computing solution;
d. Choose a Cloud Computing solution;
e. Implementation and management Cloud Computing Solution.

After migration to the cloud, the hope is to be able to ensure that learning and teaching become more interactive, but in fact the challenges of cloud services must be faced by users in the education environment. Some challenges include: security, data privacy, insufficient network, and data handling [20]. If we discuss the challenges of cloud computing, we can almost meet in several sectors, such as challenges or failures in implementing cloud computing in the following organizations or institutions:

1. There is failure in the use of digital forensic, this is because the cloud works on wireless networks and all of its resources are distributed, this is not suitable for digital forensics [21].
2. One of the largest cloud service providers in the world is China, but for cloud technology users in China, for example online gaming fields are still skeptical of

services from the cloud because there is still a lack of transparency regarding data security in the cloud [22].

3. Surveys in several institutions in Indonesia (LKPP, BIG, BPPT Institute of Science and Technology and the Ministry of Communication and Information) that have implemented cloud computing, from the 4 agencies said that the lack of cloud service providers is the unavailability of dashboards for service settings especially for IaaS and PaaS services [23].

III. Methodology

The steps undertaken in this study begin with (1) Identifying an activity; (2) Determine the impact, aspects, likelihood and severity of each activity; (3) Determine the level of risk.

Identifying an activity carried out by functions that exist in the organization. The activity was chosen based on dangerous or harmless. From each activity selected, then determine what impact will arise due to the activity, what aspects affect the activity, then determine the level of its likelihood criteria, and determine the severity of the risk. The final step is to determine the level of risk by mapping the likelihood of risk to the severity of the risk using a risk matrix. The steps undertaken in this study can be illustrated as shown in Figure 3 below:

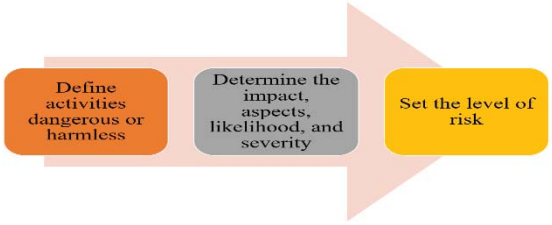

Fig. 3. Methodology

IV. Risk Assessment Process on Cloud Computing

This section will explain some of the meanings of risk assessment in the context of the cloud. The explanations presented here are the results of a survey of papers related to the risk assessment process in the cloud environment.

A. Related Work

Risk management is intended for stakeholders in the company to create value and to protect assets, besides that it can be in the form of compliance with the rules that apply. In general, the risk management process based on the ISO 30001: 2018 standard is shown in the following figure 4:

Fig. 4. Risk Management Process [12]

As done by [11] conducting surveys and analyzing of several risk assessment models with the aim of providing a reference to cloud service users in assessing risk when deciding to migrate to cloud computing environments.

Although this approach is enough to help cloud users in making decisions to migrate to cloud computing, but here is still less transparent in the process of calculating the value of risk that appears both before and after migration to cloud computing, so there is still no risk gap that occurs.

The next risk assessment process can be seen in the risk management framework created by [5], where the framework created aims to assist cloud service users in making decisions when migrating to cloud computing environments. In the risk assessment process, it is explained how to identify risks, then conduct a risk analysis by calculating the risk value determined by the average value of risk factors. Unlike the case in [24], his research[24] conducts risk assessments in selecting certain cloud service providers (CSPs) based on security, privacy and service risks to users. This model is enough to help cloud users to decide which cloud service provider to choose according to the safest level of risk for cloud service users.

Specifically, risk assessment from [25] with a quantitative approach is carried out on infrastructure security and cloud services, where risk assessment is based on: (i) Service assessment, (ii) Config assessment, and (iii) Image assessment. The results of this risk assessment produce scores from Common Vulnerability and Exposures (CVE), Impact, Likelihood, and Criticality. Whereas in [26] it is more specific to carry out risk assessments of security in the context of cloud computing. The risk assessment model developed adopts a number of pre-existing risk assessment models, but is more focused on security in the cloud computing environment, so cloud service providers and cloud service users can jointly maintain security in the cloud environment.

Furthermore, in [27] defines there are seven steps in the risk assessment process in the cloud environment, namely:

1. risk inventory
2. vulnerability identification
3. threat identification
4. Monitoring data
5. event Analysis
6. Quantitative Risk Analysis (risk of event calculation and risk aggregation)
7. assessed risk - Decision making

The above processes are somewhat different from several processes that have been proposed by other researchers. The approach used in this risk assessment process is a combination of qualitative and quantitative. For a quantitative approach, it is used to calculate risks based on vulnerabilities and threats on an asset.

B. Analysis of Risk Assessment Process

From several papers related to the risk assessment process in the Cloud context, model approaches are used: (i) qualitative, (ii) semi quantitative, or there are also (iii) a combination of qualitative and semi-quantitative.

Especially for papers that use a semi quantitative model approach, the following are given the different models used:

1. This first model is used to calculate the risk value of an asset based on its vulnerability and threat [27]:
   a. The likelihood of threats to vulnerability can be defined as follows:
   $$Lj,i = (Tj,Vi) \quad (1)$$
   Where: *L* is the likelihood value, *T* is the threat and *V* is the vulnerability value.
   b. Furthermore, the general risk value can be calculated by:
   $$Rj,i = Lji * \ Ii \quad (2)$$
   Where: *R* is the risk value of an asset, *L* is the the likelihood value, and *I* is the impact of the risk.
   c. For each asset, the risk value can be calculated as follows:
   $$RE = 1 - \prod_{j=1}^{m}(1 - Rj,i) \quad (3)$$
   Where: *E* is the element of risk to each asset.
   d. Finally, calculate of the aggregate risk of all individual risks:
   $$Ragg = 1 - (RE1 * RE2 * \dots REk) \quad (4)$$
   R_{agg} is the aggregate risk value of all individual risks.
2. The model used to calculate the total risk value (net risk calculate) [5]:
   $$ri = P(ri)xI \quad (1)$$
   $$Ri = \frac{1}{n}\sum\{ri1, ri2, \dots, rin\} \quad (2)$$
   Where: *ri* is the value of the risk factor, *P(ri)* is the risk factor probability, *I* risk impact, *ri1, ...*, is an influential risk factor. So that *Ri* can finally be calculated, namely the value of risk.
3. The next model is used to calculate the level of risk and the level of risk control [6]:
   a. First determine the type of threat to an activity, its vulnerability, and damage, then calculate the risk value based on the probability of the level of vulnerability, the probability of the threat level, and the level of damage:
   $$R = p(T)p(V)D \quad (1)$$
   Where: *R* the risk value of an asset, *p(T)* is the probability of the threat level, *p(V)* is the probability of the level of vulnerability, and *D* is the level of damage.
   b. Next, calculated the value of the level of risk control by adding the existing risk control.
   $$R = \frac{\mathrm{p(T)p(V)D}}{\mathrm{Kc}} \quad (2)$$
   Where: *R* is the risk value after adding the control value, *Kc* is the control value of the asset.

Based on several formulas for calculating risk in the cloud context above, it can be concluded that the elements or components used in calculating risk are:

1. Level of risk vulnerability [6], [27]
2. Risk threat level [6], [27]
3. Value of risk factors [5]
4. Value of the impact of risk [5]
5. Level of risk of damage [6]
6. Level of risk control [6]

C. Risk Assessment Process for Education

The risk assessment process for education aims to determine the level of risk based on the Likelihood of Risk and Severity of Risk, where to know the likelihood of risk is seen based on likelihood criteria, while the severity of risk is seen based on the criteria of risk impact. Risk impact criteria are the level of impact that occurs based on its aspects, where the component aspects can be: performance, financial, reputation, confidentiality of information and human resources. While the likelihood criterion is the level of qualitative criteria based on frequency of occurrence. Table 1 shows the existing risk impact criteria, and table 2 shows the likelihood criteria.

TABLE I. RISK IMPACT CRITERIA

Level	Impact	Aspect				
		Performance	***Financial***	***Reputation***	***Confidentiality of information***	***Human resources***
1	Very small	1. Achievement of Target ≤ 90% 2. Pending Work max. 1 week 3. Declining Performance ≤ 90%	1. Financial loss < USD 100 2. Additional costs ≤ USD 100	Verbal complaints through the hotline	Don't lose the database	Annual employee turnover <10%
2	Small	1. Achievement of Target ≤ 70% 2. Pending Work max. 4 week 3. Declining Performance ≤ 70%	1. Financial loss < USD 200 2. Additional costs ≤ USD 200	Complaints via email	Database loss permanently> 10%	Annual employee turnover <20%
3	Medium	1.Achievement of Target ≤ 50% 2.Pending Work max. 8 week 3.Declining Performance ≤ 50%	1. Financial loss < USD 500 2. Additional costs ≤ USD 500	Complaints through local media	Permanently lost database> 20 %	Annual employee turnover <30%
4	Large	1.Achievement of Target ≤ 30% 2.Pending Work max.12 week 3.Declining Performance ≤ 30%	1. Financial loss < USD 1000 2. Additional costs ≤ USD 1000	Complaints through online media and / or lawsuits	Permanent database loss ≥ 30%	There was a mass strike followed by <40%
5	Very large	1.Achievement of Target ≤ 10% 2.Pending Work max. 16 week 3.Declining Performance ≤ 10%	1. Financial loss < USD 2000 2. Additional costs ≤ USD 2000	Complaints received national attention	Permanent database loss ≥ 40%	There was a mass strike followed by <50%

TABLE II. LIKELIHOOD CRITERIA

Level	Qualitative Criteria	Frequency
1	Rarely	At least 1 time per semester
2	Possible Small	At least 2 time per semester
3	Possible Medium	At least 3 time per semester
4	Possible Large	At least 4 time per semester
5	Almost certainly	At least 5 time per semester

The results of the mapping between risk impact criteria and likelihood criteria produce a heat map in the form of a risk matrix, as shown in Figure 5. There are 2 types of risk, namely: opportunities and threats. Opportunity is the ability to manage risk that aims to find innovation [28], threat is the possibility of vulnerability to a system that is running [25]. Risk categories include: strategy, operational, financial, people, regulator or governance.

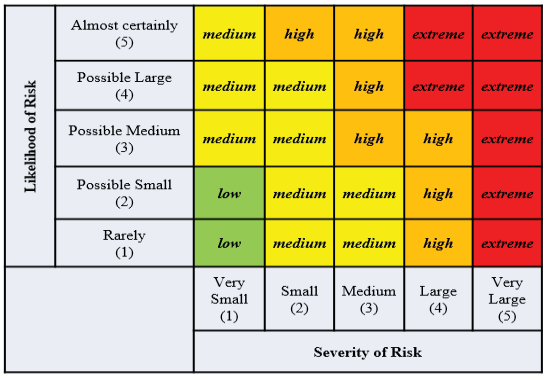

Fig. 5. Risk Matrix

For example: One of the learning activities in education is the application of cloud computing to the implementation of SAP (System, Application and Product in Data Processing) software in the SAP University Alliance Program. The learning process is carried out practically in a computer laboratory that uses internet connection facilities to connect the application server with the client computer. The performance of the SAP practicum learning process is measured based on the level of risk. Measurement of the level of risk uses risk impact criteria and likelihood criteria by adding risk types and risk categories. The results of risk measurement are shown in the following table 3

TABLE III. RISK REGISTER

No	Process/ Activity	Risk Identification					Risk Analysis & Evaluation			
		Incident	*li*	*Impact*	*Risk type*	*Risk category*	*Aspect*	*Likelihood*	*Severity*	*Risk level*
1	Implementation of SAP Certification	The process of practicum does not run according to the target in the module used.	SAP software used runs slowly, because internet traffic is very congested. Often even internet network connections are lost.	Practicum activities are hampered, not according to the learning target	Threat	Operational	Reputation	Possible Small	Very Small	Low
2	Internet Down	Loss of internet connection without the knowledge of the provider	The presence of viruses, natural phenomena	Learning activities especially those that use internet connections are disrupted	Oppor tunity	Operational	Performance	Possible Medium	Small	Medium

The results of the risk register table can then be used to periodically monitor the improvement of the learning system, so as to minimize the possibility of dangerous risks in teaching and learning activities in the field of education.

V. CONCLUSION

This paper explains the process of assessing the risk level of online learning systems that implement cloud computing in the field of education. The results of this study can provide the following conclusions:

1. In the form of risk assessment research can be done with a qualitative or quantitative approach or a combination of the two.
2. In the online learning system aspects used to determine the criteria for risk impact are performance, financial, reputation, confidentiality of information, and human resources.

3. Risk register can be applied to measure the risk of online learning activities through risk analysis and evaluation.

VI. Limitation and Future Research

The results of this survey are still very limited and still allow it to develop more perfect. This is because search results related to references that are very relevant to the research topic are still very limited. Therefore, this research is still very open to be developed more fully, especially to explore in more detail about the risks of security, privacy, and trust, especially in the educational environment. The benefits of this survey will be used as reference material for further research which will examine in more detail about the risks of information technology in the context of cloud computing.

Acknowledgment

Our sincere gratitude to Politeknik Pos Indonesia and Doctor of Computer Science Programs with the support to complete this research.

References

.

[1] A. Huth and J. Cebula, "The Basics of Cloud Computing," pp. 1–4, 2011.

[2] A. Gholami and E. Laure, "Security and Privacy of Sensitive Data in Cloud Computing : A Survey of Recent Developments," pp. 131–150, 2015.

[3] Mahesh, "Data Security and Security Controls in Cloud Computing," pp. 11–13, 2016.

[4] C. Esposito and A. Castiglione, "Challenges of Connecting Edge and Cloud Computing : A Security and Forensic Perspective," pp. 13–17, 2017.

[5] I. Shareeful, S. Fenz, E. Weippl, and H. Mouratidis, "A Risk Management Framework for Cloud Migration Decision Support," 2017.

[6] A. D. Kozlov and N. L. Noga, "Risk Management for Information Security of Corporate Information Systems Using Cloud Technology," *Elev. Int. Conf. "Management large-scale Syst. Dev. (MLSD*, pp. 1–5, 2018.

[7] N. Ahmad, Q. N. Naveed, and N. Hoda, "Strategy and procedures for Migration to the Cloud Computing," no. 1, p. 1, 2018.

[8] J. Martínez, M. Lorenzo, E. Sanchez, and R. Parra, "Computers & Education Cloud computing and education : A state-of-the-art survey," vol. 80, pp. 132–151, 2015.

[9] M. Shirzad and A. Hoseinpanah, "E-Learning Based on Cloud Computing," pp. 214–218, 2012.

[10] N. Pa, B. JNR, R. Nor, and M. Murad, "Risk Assessment of IT Governance : A Systematic Literature Review," vol. 71, no. 2, 2015.

[11] M. Nada, B. Youssef, B. Brahim, and R. Boubker, "Survey: Risk assessment models for cloud computing: evaluation criteria," vol. 1, pp. 3–7, 2017.

[12] R. P. Guide, "A Risk Practitioners Guide to ISO 31000 : 2018," 2018.

[13] E. Doherty, M. Carcary, and G. Conway, "Risk Management Considerations in Cloud Computing Adoption," no. August, 2012.

[14] D. Kearns, "Planning & Management Methods for Migration to a Cloud Environment Author :," no. 17, 2018.

[15] I. Kateeb and M. Almadallah, "Rate the challenges / issues of the cloud on- demand model," 2014.

[16] O. Jr, "Cloud Computing – Value Delivery by Balancing Benefits & Risks ISACA IT Governance Summit 2018," no. October, 2018.

[17] G. Wahlgren and S. Kowalski, "IT Security Risk Management Model for Cloud Computing : A Need for a New," 2013.

[18] V. H. Pardeshi, "Cloud Computing for Higher Education Institutes : Architecture , Strategy and Recommendations for Effective Adaptation," *Procedia Econ. Financ.*, vol. 11, no. 14, pp. 589–599, 2014.

[19] M. Mircea and A. I. Andreescu, "Using Cloud Computing in Higher Education : A Strategy to Improve Agility in the Current Financial Crisis," vol. 2011, 2011.

[20] R. M. Almajalid, "A Survey on the Adoption of Cloud Computing in Education Sector," pp. 1–12.

[21] R. Neware, "Cloud Computing Digital Forensic challenges," *2018 Second Int. Conf. Electron. Commun. Aerosp. Technol.*, no. Iceca, pp. 1090–1092, 2018.

[22] S. Chandel, T. Ni, and G. Yang, "Enterprise Cloud : its Growth & Security Challenges in," *2018 5th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/2018 4th IEEE Int. Conf. Edge Comput. Scalable Cloud*, pp. 144–152, 2018.

[23] F. Wildana, "Implementasi Cloud Computing di Beberapa Instansi," pp. 97–108, 2017.

[24] E. Cayirci, A. Garaga, A. S. De Oliveira, and Y. Roudier, "Open Access A risk assessment model for selecting cloud service providers," *J. Cloud Comput. Adv. Syst. Appl.*, pp. 1–12, 2016.

[25] E. Mostajeran, M. Nizam, M. Mydin, M. F. Khalid, B. I. Ismail, and R. Kandan, "Quantitative Risk Assessment of Container Based Cloud Platform," 2017.

[26] S. H. Albakri, B. Shanmugam, and G. N. Samy, "Security risk assessment framework for cloud computing environments," 2014.

[27] K. Djemame, "A Risk Assessment Framework for Cloud Computing," 2016.

[28] T. Bekefi, M. J. Epstein, and K. Yuthas, *Managing Opportunities and Risks By*. 2008.