applied sciences

MDPI

Article

Machine Learning Evaluation of the Requirement Engineering Process Models for Cloud Computing and Security Issues

Muhammad Asgher Nadeem and Scott Uk-Jin Lee *

Department of Computer Science and Engineering, Hanyang University, Ansan 15588, Korea; nadeem@hanyang.ac.kr

* Correspondence: scottlee@hanyang.ac.kr

Received: 26 July 2020; Accepted: 20 August 2020; Published: 24 August 2020

Abstract: In the requirement engineering phase, the team members work to get the user requirements, comprehend them and specify them for the next process. There are many models for the requirement engineering phase. There is a need to select the best Requirement Engineering model, and integrate it with cloud computing, that can give the best response to the users and software developers and avoid mistakes in the requirement engineering phase. In this study, these models are integrated with the cloud computing domain, and we report on the security considerations of all the selected models. Four requirement engineering process models are selected for this study: the Linear approach, the Macaulay Linear approach, and the Iterative and Spiral models. The focus of this study is to check the security aspects being introduced by the cloud platform and assess the feasibility of these models for the popular cloud environment SaaS. For the classification of the security aspects that affect the performance of these model, a framework is proposed, and we check the results regarding selected security parameters and RE models. By classifying the selected RE models for security aspects based on deep learning techniques, we determine that the Loucopoulos and Karakostas iterative requirements engineering process model performs better than all the other models.

Keywords: requirement engineering models; security of RE model; classification of requirement engineering models

1. Introduction

1.1. Requirement Engineering Models

Requirement engineering (RE), as the initial phase of software engineering, is used for the definition of the customer's requirement, documenting them, and efficiently maintaining them throughout the project. To achieve these objectives, the team members carry out requirement elicitation, specification, verification and validation. The management of team members, cost and time are the mandatory factors for this phase. There are many hurdles in the gathering of requirements, which lead to many difficulties in the other phases of development. For this study, four requirement engineering models were selected, which are integrable with cloud computing, and we investigated their security measures. The requirement engineering models are as follows:

1.1.1. Linear Process Requirements Engineering Model by Kotonya and Sommerville

The requirement engineering model given by Kotonya and Sommerville suggests an abstract linear RE process model. It comprehends the activity repetition involved in the requirements elicitation, negotiation, analysis, documentation and validation. Their model shows that many stages are interconnected and dependent upon each other.

1.1.2. Macaulay Linear Requirements Engineering Process Model

This is the pure linear RE process model given by Macaulay. It is the solution of the linear RE process model of Kotonya and Sommerville, which involves the overlapping of the tasks. It eliminates the overlapping of activities. The major stages of this model are specified as understanding of the concept, analysis of the problem, performance of a feasibility study, requirement analysis and modeling, and at the end, the documentation of the process. The presenter of this model shows that the most important things in their model are the positive relationship between customer and supplier, and the prevailing condition and present situations of the environment.

1.1.3. Loucopoulos and Karakostas Iterative Requirements Engineering Process Model

Loucopoulos and Karakostas gave a cyclic approach to the completion of the requirement engineering phases. This model is based on iterative development. They focus on the idea that the different phases of requirement engineering are iteratively connected, such that the elicitation, specification and validation of the requirements given by the customer can be better achieved in an iterative matter.

1.1.4. Spiral Model for Requirements Engineering Process

The spiral model for requirements engineering is presented by Kotonya and Sommerville. It works on the basic software engineering model, which is a spiral, however, it is a spiral process development practice for the requirement engineering phase, and not for software development. Each spiral in this model comprises four major activities, such as requirements elicitation, requirements analysis and negotiation, requirements documentation and requirements validation. The main development objective of the spiral model is to avoid all the possible situations that compromise the quality of the project and can affect in the estimated increase in the cost of the project.

1.2. Cloud Computing

Many cloud service providers, including Microsoft, Amazon, Google, Salesforce.com and Go Grid, operate by means of virtualization skills, and combine them with self-service facilities for their computing requirements using the Internet. For the service providers, ensuring that the customers' applications and their concerned information is protected is difficult. Nowadays, enterprises need an expansion in their infrastructure; however, the major risk is the maintenance of the security of their data and underlying applications. Organizations and other users are worried about the ways security and reliability can be retained in the cloud computing environment. The major concern of many corporations is the secure transfer of their requests, and most direct their data towards the community and mutual cloud. To minimize these security-related anxieties, the cloud provider needs to guarantee that the customers have a secure environment and other security policies, including service-level agreements. The technology of cloud computing is enabling the provision of various applications, IT infrastructures and other services, which can be accessible from remote places.

Nowadays, the challenge in a multiple distributed cloud setting is cyber warfare. This is a multifaceted challenge for the client-server design. When the documents have been transferred to the cloud, security is the most significant consideration. The European Network Information Security Agency (ENISA) presented all the possible threats and available solutions in cloud computing. Lombardi L. and Pietro RD. [1] worked towards the controlling of intercommunication processes and the guarantee of high-level safety. The cloud network is much more vulnerable in the case of Address Resolution Protocol (ARP) spoofing, denial of service (DoS) or distributed denial of service (DDoS), domain name system (DNS), and internet protocol (IP) spoofing attacks [1]. The study presented cloud computing and its characteristics. The architecture of the cloud is much more complex than the security aspect and the secure working of the cloud environment. Security problems in the cloud

environment are triggered by its various characteristics. This study briefly showed the broad array of cloud computing aspects that have a high impact on the security of cloud computing.

There were growths of 70% in Advance Persistence Threat (APT) assaults [2], 68% in distrustful actions, and 56% in brute force attacks. APT attack is a linkage attack, in which an unapproved person gets access to a network and continues to work invisibly for a prolonged time. The International Data Center (IDC) is working on the study and analysis of the facts behind this. They are taking recommendations from companies' heads about what are the challenges that they are experiencing in the cloud. The survey's results demonstrate that security and privacy issues are the most pressing issue for 87% of customers [3].

Cloud computing has an infrastructure layer, a control layer and an application layer. In the context of cloud computing features, it is more simple and less error-prone to update policies of the network environment by using software or by taking advantage of programmability. Now, a security-specific program can be installed on the controller that alerts the system in the case of any intruder activity, and sophisticated network functions can be easily implemented with the help of a global view due to the centralization of the control.

The aim of this study is the selection and integration of the best RE model with cloud techniques for removing requirement-gathering hurdles and errors. There is the need for evolution in the security aspect introduced into cloud computing for given models. Four RE process models (the Linear and Macaulay Linear approach, and the Iterative and Spiral models) are selected for the evaluation of the security aspect of cloud computing. To check the security aspects affecting model performance, a framework is proposed for the selection of the best model. Supervised learning techniques are used and the performance is evaluated for different models.

2. Literature Review

The safety of cloud registering is overseen by strategy and the Service Level Agreement (SLA), which is the establishment of administration between client and supplier. Numerous scientists have examined and talked about the security concerns of distributed network. Fernandes D. et al. [3] recommended inclusive assessments of cloud safety issues, which included numerous key issues, such as dangers, powerlessness, and assaults, and they proposed scientific classifications for their gathering. Mazhar An. et al. [4] cleared up the security investigation focusing on correspondence, authority, design and legitimate perspectives. It gives an overview of the helplessness of Virtual Machine (VM) relocation, hypervisor, VM picture, and it discusses the security features. Flavio L. and Robert Di P. [5] introduced exhaustive data on the best foundation for the ensured cloud. Subashini and Kavitha [6] presented the safety issues of the service-modeled simulations in the cloud environment, and gave the solutions. Saripalli P. et al. [7] investigated the most significant confidentiality- and trust-based issues, examined the privacy, trust and security threats, and gave a solution for reliable and trustworthy cloud computing. The paper presents the security requests for better control, individual needs, and particular improved security practices.

The use of the Internet of Things and cloud computing provides a new opportunity for effective transportation. In the paper in [8], a novel multilayered cloud environment is proposed that uses a combination of both cloud computing and IoT. They presented a vehicular cloud service, using vehicular data mining for the analysis. They investigated how the cloud services could be designed and developed for effective vehicular data clouds operation. Their study contributes to the IoT environment by showing a novel software architecture for vehicular data clouds capable of integrating various elements into the infrastructure.

Yuhong L. et al. [9] plotted serious secrecy and security tests in cloud computing, characterized various current explanations, linked their strong points and limitations, and proposed future study directions. Zhaolong G. et al. [10] talked over the recent progresses in cloud computing, different security concerns and contests in cloud computing, and various related approaches and solutions. These solutions present a way to deal with these safety issues, and provide a relative investigation into

these methods. Zhifeng and Yang [11] gave an orderly survey of security issues with a trait-driven approach. The characteristics that were utilized include classification, accessibility, responsibility and protection preservability. For each property, a couple of issues were looked at for comparing protection arrangements. Ficco and Massimo [12] presented a modeling language which has a defined vocabulary for annotating Unified Model Language-based models with information related to avoiding cyber-attacks targeting applications and services arranged in combined clouds, and some stereotypes have been inherited from other models. This strategy is based on these logical steps:

- Required behaviors of the application are identified and modeled with Use Cases.
- Unwanted behaviors are defined as misuse cases.

Software security engineering requires the development of software to correct functioning in the case of malevolent attacks affecting them directly or indirectly. Semi-formal description models have attracted a lot of consideration in security engineering research, but there is still a long way to go before their final acceptance into the requirements engineering process in the environment of cloud computing. The solution discussed by Ficco is the first step in integrating security requirement specifications into the cloud computing environment. The synchronization among agents in a multi-agent system has received significant consideration because of its prospective applications in the cooperative control of autonomous vehicles, distributed sensor networks and flocking. The complement of state synchronization is output synchronization, which is done in heterogeneous networks. The network model is always imperfect due to time and communication delays [13]. A mix of two algorithms is used, leading to a novel algorithm which has the advantage of optimally tuned algorithmic parameters, while a data driven algorithm uses only input/output data from the process [14].

All the given approaches have security and communication hurdles, which lead towards a lower quality of requirement gathering and identification, and the given techniques are not checked for cloud computing platforms.

3. Methodology

In the market, there are many requirement engineering models being used and working efficiently with cloud computing models; as such, we have multiple choices for cloud computing models, as well as for requirement engineering. Whenever we are working with cloud computing, the major issue is the security concerns. For this paper, we worked on four different requirement engineering models.

Figure 1 shows the workflow for the classification of RE models that work with cloud computing, based upon selected security parameters using the deep learning approach. In this study, the supervised machine learning technique for implementing the cloud service model is used, and the cloud is taken as the software for the service model on which we perform our experiments. This involves taking the security parameters as input and implementing the machine learning technique for the classification. The classifier gives the results that govern us towards the targeted RE model, and takes us to the point of making a distinction among the four selected RE models.

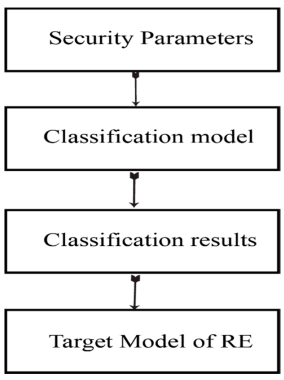


Figure 1. Workflow for the classification of Requirement Engineering models.

The process for this is diagrammatically explained in Figure 2.

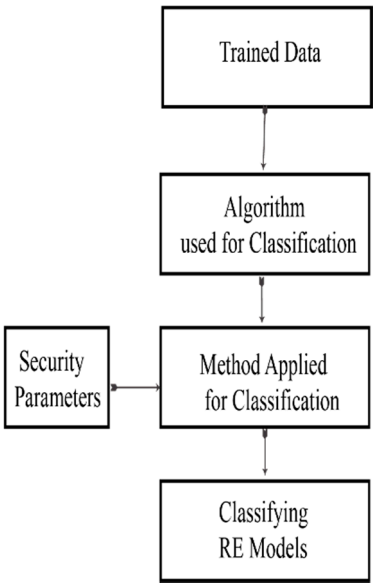


Figure 2. Flow Diagram for classification of RE model.

The method is divided into four steps.

1. The process starts with the importing of trained data as the input. It contains all the requirements of the RE models within the selected category.
2. The trained data is then applied to the training classification algorithm. This algorithm is used to classify the given data based on the directed method. There are many techniques available to perform the training of classification algorithms, i.e., convolutional neural network, the multilayer perceptron model, and others. Trained algorithms are used to select the best security parameter for classification of the best RE model.
3. We apply the security parameters to the selected classification method for the detection and prediction of different security concerns in the four selected RE models.
4. The results of this classification will help us to select the appropriate model in the user-specific environment, as well as determine the needs and expectations of the Software's performance. Classification factors of RE model are shown in Table 1.

Table 1. Classification factors of RE model.

Operation Factors of RE Model	**Security Working Efficiency Reliability**
Revision factor of RE model	Requirement's functional suitability Compatibility Ease of maintenance
Transition factor of RE model	Power of reuse Portability

3.1. Tag Distribution

The tag distribution and classification factors are shown in the Table 2, and the three selected security parameters are shown in Figure 3. The security parameters are selected based on the performance of our training algorithms. The selected security parameters of the given trained data are introduced as input into deep the learning approaches for the selection of RE models.

The selected security parameters are confidentiality, interoperability and integrity. Interoperability ensures the best generation and communication of information. Integrity introduces consistency, accuracy and completeness into security. Confidentiality provides the protection via authorization. Integrity and confidentiality breaches are the most common threats in security, and interoperability allows unrestrained communication in models.

Table 2. Tag distribution and classification factors.

Serial No.	Parameter	Description
1.	Security	The security is checked for confidentiality, integrity and availability in the cloud environment.
2.	Requirement's functional suitability	Functional suitability of the requirement is one of the essential aspects to consider for RE.
3.	Power of reuse	Can we reuse the design and another part of the product?
4.	Portability	Are the final software product and the components portable?
5.	Ease of maintenance	The ease of maintenance affects RE model selection.
6.	Compatibility	We have to choose an RE model based on compatibility background.
7.	Reliability	Reliability is the main concern for the developer and the clients.
8.	Working efficiency	The choice of suitable RE model also depends on the working efficiency of the model.
9.	Employability	You have to check the skills of your employees before selecting the RE model.
10.	Functional requirements	Functional requirements matter a lot for the working of software projects.
11.	Time requirement	Time is an important component for the selection of the RE model, as we always want to complete the project fast.
12.	Cost	The development cost should be considered in the model selection.
13.	Iteration	What number of iterations a model supports can affect the efficiency and performance of the RE models.
14.	No. of client–developer meetings	Client–developers meeting are very important for better software project development.

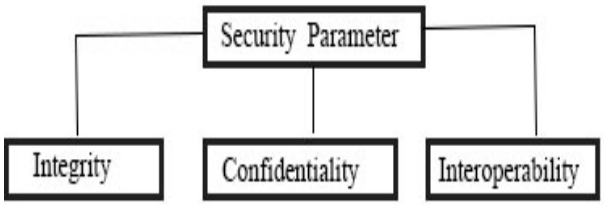


Figure 3. Selected security parameters.

The 14 different aspects for the choice of best RE model are shown in Table 2. We are using the aspects of Security, Requirement's functional suitability, Power of reuse, Portability, Ease of maintenance, Compatibility, Reliability, Working efficiency, Employability, Functional requirements, Time Requirement, Cost, Iterations, and No. of client–developer meetings in Tag Distribution.

3.2. Deep Learning Model for RE Model Classification

For deep learning, we used multiple layers of artificial neural networks for the learning practice. The working of neural networks along with deep learning is based on the working of the human brain.

In deep learning, we use multiple numbers of neurons; these neurons are the proceeding units for the model. These neurons are responsible for the RE model's classification and tag representation. The selected deep learning model shows an impressive performance as regards the security parameters and representing the interrelation of the cloud computing model (SaaS) with the RE model. In our study, we used the convolutional neural network model and the multilayer perceptron model. We find these two models of deep learning to be the most suitable choice for the study.

3.3. Multi-Layer Perceptron Model (MLP)

In the artificial neural network, the Multi-Layer Perceptron model works on the feed forward approach. It has multiple hidden layers working with one input and one output layer. Two hidden layers are used in our setup, as shown in Figure 4. This model works on the mapping principles that match the initial training datasets with the suitable targeted dataset, which counted as the output. The setup has a directed graph with multiple node layers connected with each other. We processed the elements of the layers by using a nonlinear activation function, but without applying this activation function to the input layer. The complete processing was done using the neurons, which are actually the nodes in the Multi-Layer Perceptron model. For the training of the model, we used back propagation, which is a widely used supervised learning technique. The used Multi-layer Perceptron model with one input and output layer and two hidden layers is shown in Figure 4.

The mathematical form of the Multi-Layer Perceptron Model is shown below:

$$MLP(x) = g\,(xW^1 + b^1)\,W^2 + b^2 \tag{1}$$

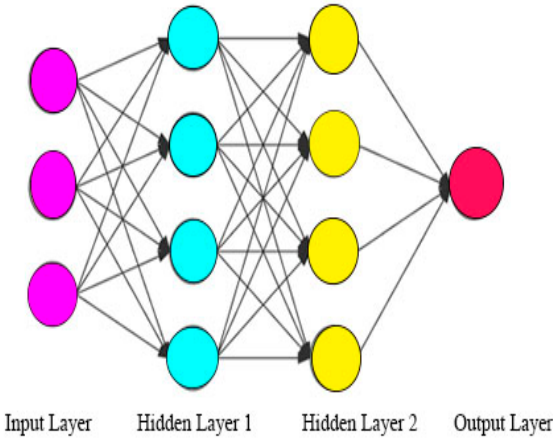


Figure 4. Multi-Layer Perceptron model.

3.4. Convolutional Neural Network Model (CNN)

Convolutional neural networks are the form of neural network used for grid data processing. In this study, CNN is used as the second deep learning neural model. This also works via the feed forward approach. For CNN, we have many convolutional layers that work with the visual cortex and perform the functionality of the cells in the model. Pooling of the layers with the convolutional layer is done so as to minimize the number of features. In this step, we are reducing the parameters that are less significant in the framework. The use of the convolutional layer in the CNN eliminates the computational complexity of the model. We worked with one-dimension (1D) schemes for better classification results. The convolutional neural network model is shown in Figure 4. The mathematical form of the convolution neural network model is:

$$\mathrm{CNN}(x) = \partial\,(W \,.\, r_{vi}(x) + b) \tag{2}$$

3.5. Security Dimensions

1. Software security: Software security means that the software must continue to function under heavy attack of the malicious code. It is the main challenge as cloud computing is mainly used to provide Software-as-a-Service. If the software security fails then the clients will experience many implementation bugs and buffer overflow.
2. Infrastructure security: The greatest fundamental challenge experienced by the cloud providers is to prove that the physical and the virtual set-up of the cloud is trustable. Third-party verification is not enough to gain the trust of the corporate company owner and data managers that deal with the new business method. It is important for the business to receive verification that this cloud infrastructure is capable and trustworthy enough to manage all the corporate requests that the primary business is making.

3.6. Distinctive Zones of Security Issues

The distinctive zones of security issues in installed frameworks are as follows:

1. Virtual machine disconnection: This can prompt information spillage and cross-VMs assault, so the disengagement procedure ought to be arranged deliberately while conveying the virtual machine in the cloud framework [5].
2. Programmability: In a cloud domain, the business owner needs to utilize a programmable processor on each port. The key test of the applicability of this is to arrange a processor to execute parcel checking scripts over the selected cloud model. Numerous procedures are being organized to handle the utilization of a low level of reflection in order to accomplish high throughput execution [15].
3. Control of framework: Customer information is transmitted over the cloud nodes. Electronic access control system (EACS) arranges the validation framework and edge security by getting the help of Security Assertion Markup Language (SAML). This is a league convention, which contains confirmation accreditations. SAML is used to trade the data identified with subject or confirmation between the collaborating areas, and the demand and reaction is mapped in the Simple Object Access Convention (SOAP) depending on Extensible Markup Language (XML) [16].
4. SNMP Server: This is a straightforward system administration convention, which is intended to give a low-overhead component in order to gather the information from organized components.
5. User front end: A software engineer has to know the security aspects of the web-creating dialect, such as hypertext markup language (HTML)/cascading style sheets (CSS)/ personal homepage (PHP)/ java script (JS). Subhasini and Kavita [6] expressed that the seclusion hindrance can be broken via the escape clause or infusion veiled code. We assume that if an interloper has just traded off the database, there ought to be a legitimate front end control in order to avoid the mistake.
6. Framework: international business machine (IBM) characterized five practical security subsystems, which are review and consistence, get to control, stream control, personality administration and arrangement trustworthiness [17]. The structure has been planned in java and .net for confinement and asset bookkeeping, however they fizzled with string. The Multitasking Virtual Machine (MVM) gave a nonspecific Application Program Interface (API).
7. License: In the cloud, the real issue is the authorizing of the applications. This is an exceptionally complex issue, which the security researchers have still not discovered a legitimate arrangement for. The copying, selling, sharing or distribution of programming unlawfully is called programming theft. There are numerous conceivable assaults that could be made on this unapproved pilfered programming [18].
8. Service Availability: Technically, there is a huge number of approaches to accomplishing high accessibility in the cloud. Cloud administration has an operational model such as SaaS, PaaS or IaaS. In view of the prevailing security conditions of the cloud, the application and framework

levels need high accessibility and adaptability. Actually, there are some accessibility threats, such as DoS or Botnet DDoS [19]. Subhashini S. et al. [6] examined multi-level engineering to maintain the security as an aspect of the administrative structure.

9. Parallel application: Parallel application enhanced the execution of the framework while executing numerous applications in parallel. There is, though, an issue of common confirmation among them, and because of this weakness, some threats are conceivable. Because of high non-uniform information conveyance, the parallel calculation is agitated by disastrous effects that affect the load balance [20].

In cloud computing, one major security threat is the inability to know where the data and resources are physically placed. The control, maintenance and security policies are also hidden from the clients, which creates a barrier between the client and the service providers. Companies are participating in designing an intelligent business information system by cooperating with other social networking companies, and selling the clients' preferences and interests for the sake of money, thus violating laws. Clients are unaware of who is controlling the encryption/decryption keys, which mechanism they are using, and other details. To ensure the protection to the users, the cloud providers need to keep the clients up-to-date with all the application improvements and the latest security measures. In the context of ensuring the auditability of the records and the maintenance of security, the dynamic nature of virtual machines will make records management easy.

4. Results

Supervised learning techniques with a deep learning model, such as CNN and MLP, are widely used for classification purposes. We have used the Aurora 2 dataset with multiple files required for the training of data, and classified it in MATLABr2018b. There are many reasons for the selection of Aurora 2. It is a publicly available dataset and provides the best identification and recognition results when used with the CNN. It also provides parameter flexibility that performs better in selected models.

The results are derived using the methodology of the research. The training data is imported into the system. The given trained data is applied as input to the deep learning approaches. The cloud service model is implemented using supervised learning techniques. All experiments are performed using SAAS with cloud. The trained algorithms are tested with different deep learning approaches. Classification based on the security parameter is performed to select the best RE model among the selected models. Confidentiality, integrity and interoperability are the selected security parameters. The selected parameter is provided as input to the deep learning approaches for classification of the best RE model. The results of all deep learning techniques are ranked with regard to RE models for cloud based on security parameter. The best RE model is selected on the basis of the ranked results generated by different classification techniques. All the models are selected based on different aspects for the choice of the best RE model and classifications factors, as shown in Tables 1 and 2.

The evaluation of the results is presented using the most popular evaluation measure available on the market.

As we have to classify the requirement engineering models for the performance and security parameters, we classify and predict the performance using Accuracy, F-value and Recall.

$$\text{Precision (\%)} = \text{True Positive}/(\text{True Positive} + \text{False Positive}) \quad (3)$$

$$\text{Recall (\%)} = \text{True Positive}/(\text{False Negative} + \text{True Positive}) \quad (4)$$

$$\text{F - measure (\%)} = (2 * \text{Recall} * \text{Precision})/\text{Recall} + \text{Precision} \quad (5)$$

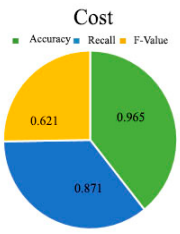
Classification results for the four requirement engineering models selected for security and performance evaluation are shown in Table 3.

Table 3. Classification results of selected 4 requirement engineering models.

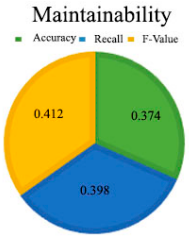
Requirement Engineering Models	Accuracy	F-value	Recall
MLRE	0.745	0.658	0.689
LKIRE	0.945	0.845	0.810
LPRE	0.784	0.678	0.578
SMRE	0.987	0.457	0.745

MLRE—Macaulay Linear Requirements Engineering Process Model, LKIRE—Loucopoulos and Karakostas Iterative Requirements Engineering Process Model, LPRE—Linear Process Requirements Engineering Model by Kotonya and Sommerville, SMRE—Spiral Model for Requirements Engineering Process.

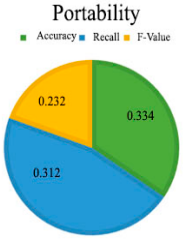
The formulas for the Accuracy, Recall and F-value have been applied to cost, maintainability, portability, reliability, reusability, time and security. Figure 5 shows pie graphs, with the yellow color representing F-value, green for the Accuracy and blue for Recall.



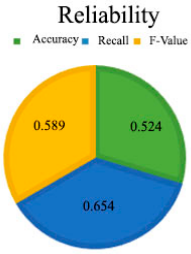
(**a**) Accuracy, Recall and F-value results of Cost



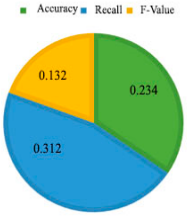
(**b**) Accuracy, Recall and F-value results of Maintainability



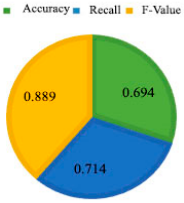
(**c**) Accuracy, Recall and F-value results of Portability



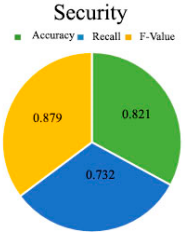
(**d**) Accuracy, Recall and F-value results of Reliability



(**e**) Accuracy, Recall and F-value results of Reusability



(**f**) Accuracy, Recall and F-value results of Time



(**g**) Accuracy, Recall and F-value results of security

Figure 5. Recall and F-value results of selected parameters.

4.1. Security Recommendation and Discussion

In this section, three planes are proposed: security design, where the cloud security is related and the dependence on each plane. The three planes are the presentation plane, cloud-benefit center plane and framework plane. All the associations that want to utilize cloud computing for their designed application are required to survey and possibly alter their product improvement method. Many business organizations are worried about moving their applications to the cloud to minimize cost. It helps to increase their productivity and application plane security, and counter the difficulties of the cloud environment. As such, an appropriate security system ought to be implemented. There are numerous application plane dangers in the field of control. In the public cloud engineering domain, the information moves among the business, and guarantees secrecy and respectability. The middleware devices display massive vulnerabilities, for example, vulnerabilities in network, links and end node devices inside the access layer of the cloud. The dangers of the vulnerabilities are grouped depending on what they influence: information privacy, accessibility or trustworthiness. To manage the difficulties, attacks and dangers, we have to consider the redesigning of the cloud architecture. The adaptability and versatility of this computing framework can offer critical advantages to the business firms.

4.2. Application Planes

This layer is the plane that specifically conveys the outsourced programming to the customer. Clients do not have to pay money for the installation of the required software, they just need to pay the rent for its use. The security issues for this plane are end-to-end.

Data security is also one of the concerns of the application plane. A generic security platform is needed inside the cloud to get high visibility and end-to-end control over data. The complex administrative and security related issues are minimized by MacAfee and Intel with the introduction of end device visibility. Moreover, in the application plane, the organizational data is stored at the data centers of SaaS. Additionally, the cloud providers focus on the high availability, and they make backups and data replications across multiple sites. The vendors of Amazon, Google App and Elastic Compute Cloud (EC2) integrate the cryptographic algorithms for login access with Secure Shell (SSH). This can possibly avoid the malicious access and vulnerability issues that are caused by unauthorized access to the security model.

4.3. Administration Middleware Plane

From the database servers, PC programming gives administrations access to requested programs. Middleware can be described as stick programming that makes it simpler for the product to engineer and accomplish correspondence in a cloud domain. Client and administration verification is confirmed by the login procedure. Legitimate prerequisites and controls make another connection between the data of the association and the outsider, which depicts how the data should be taken care of and put away by the cloud suppliers.

For middleware trust and administration validity, numerous methodologies had been proposed. All methods give the administration trust in the cloud conditions; still, very little consideration has been given to deciding the validity of trust criticisms. The connecting device is validated by providing a user interface for the connection. Hence the security of the conventions is important for anchoring the Middleware plane.

4.4. Foundation Plane

Cloud foundation equipment can organize the parts and capacity framework. The cloud framework can deal with the PC capacities, for example, execution, transfer speed and capacity. In this part, we deal with the fundamental security issues in the framework plane, like bit freedom, arrangement of administration, cloud validation, interfacing convention and standard, gadget dependability and machine accessibility/validation. In the document framework plane, document blocking, I/O support

administration and pathname indexes are handled. A protected and productive cloud validation process and client reflection ought to be given in the foundation plane. Every single virtual machine cooperating for the verification process and machine accessibility administration is publicly accessible.

5. Discussion

Cloud specialist organizations are applying many safety efforts and are covering the security credits as per the request of the multitenant clients. The administrations of cloud providers are building their modules as per the foundations required. This implies that the difficulties emerging from the improvement of distributed computing can be handled by establishing a sound lawful body to secure and protect information.

Virtualization requires extra considerations for powerful and far-reaching systems in light of the fact that Virtual Machine Manager (VMMs) are a vast and complex framework. VMMs ought to separate the running parts so as to accomplish great effectiveness and throughput, by characterizing the virtualized arrangement. Finally, the security arrangement and proposed safety component for sheltering all the remaining parts focuses on the preferred standpoint for client and suppliers. The effectiveness, cost overhead and time administration are additionally presented. The results of this study showed that Loucopoulos and Karakostas' iterative requirements engineering process model is better for the security dimension, compared to the other models that are arranged according to the classification results, such as the Spiral Model, the Linear model and lastly the Macaulay Linear requirements engineering process model. Frequent changes in requirements necessitate the modification of parameters, which may disturb the functionality. Variation in security parameters for different systems, and the rapid increase in parameter size and different features may affect the performance.

6. Conclusions

Cloud-oriented RE model development is a novel idea that offers numerous advantages, for example, a stockpiling limit, cost diminishment and adaptability. Many software engineering projects are being designed and developed on the cloud platform, and they give better results than are required. For all the software engineering projects, the initial phase is the requirement engineering. There are different models for the requirements engineering; some of them are iterative and many of them focus on linear structure. Requirement engineering models are better integrated with cloud computing for the satisfaction of customer requirements. Cloud computing offers many new possibilities in multilateral project development to improve Software Development Life Cycle (SDLC) process. In this study, different RE models are classified in relation to cloud computing (SaaS model) via security aspects, and on the basis of these results the best performing model is classified.

Author Contributions: Conceptualization, M.A.N. methodology, M.A.N. and S.U.-J.L.; investigation, S.U.-J.L.; resources, S.U.-J.L.; data curation, M.A.N.; writing—original draft preparation, M.A.N.; writing—review and editing, M.A.N.; visualization, M.A.N.; supervision, S.U.-J.L.; project administration, S.U.-J.L.; funding acquisition, S.U.-J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the research fund of Hanyang University (HY-2020-1700).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lombardi, F.; Pietro, R.D. Secure virtualization for cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1113–1122. [CrossRef]
2. Ussath, M.; Jaeger, D.; Cheng, F.; Meinel, C. Advanced persistent threats: Behind the scenes. In Proceedings of the 50th Annual Conference on Information Science and Systems (CISS), Princeton, NJ, USA, 16–18 March 2016; pp. 181–186.
3. Fernandes, D.A.B.; Soares, L.F.B.; Gomes, J.V.; Freire, M.M.; Inácio, P.R.N. Security issues in cloud environments: A survey. *Int. J. Inf. Secur.* **2014**, *13*, 113–170. [CrossRef]

4. Ali, M.; Khan, S.U.; Vasilakos, A.V. Security in cloud computing: Opportunities and challenges. *Inf. Sci.* **2015**, *305*, 357–383. [CrossRef]
5. Di Pietro, R.D.; Lombardi, F.; Signorini, M.A.T.T.E.O. Secure Management of Virtualized Resources. In *Security in the Private Cloud*; CRC Press: Boca Raton, FL, USA, 2016. [CrossRef]
6. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2011**, *34*, 1–11. [CrossRef]
7. Saripalli, P.; Walters, B. Quirc: A quantitative impact and risk assessment framework for cloud security. In Proceedings of the 3rd International Conference on Cloud Computing, Miami, FL, USA, 10 July 2010; pp. 280–288.
8. Wu, H.; Yan, G.; Xu, L.D. Developing vehicular data cloud services in the IoT environment. *IEEE Trans. Ind. Inf.* **2014**, *10*, 1587–1595. [CrossRef]
9. Liu, Y.; Sun, Y.L.; Ryoo, J.; Rizvi, S.; Vasilakos, A.V. A survey of security and privacy challenges in cloud computing: Solutions and future directions. *J. Comput. Sci. Eng.* **2015**, *9*, 119–133. [CrossRef]
10. Gou, Z.; Yamaguchi, S.; Gupta, B.B. Analysis of various security issues and challenges in cloud computing environment: A survey. In *Identity Theft: Breakthroughs in Research and Practice*; IGI Global (International Publisher of Science and Technology): Hershey, PA, USA, 2017; pp. 221–247.
11. Xiao, Z.; Xiao, Y. Security and privacy in cloud computing. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 843–859. [CrossRef]
12. Ficco, M.; Palmieri, F.; Castiglione, A. Modeling security requirements for cloud-based system development. *Concurr. Comput. Pract. Exp.* **2015**, *27*, 2107–2124. [CrossRef]
13. Zhang, M.; Saberi, A.; Stoorvogel, A.A. Semi-global state synchronization for multi-agent systems subject to actuator saturation and unknown nonuniform input delay. *Eur. J. Control* **2020**, *54*, 12–21. [CrossRef]
14. Roman, R.C.; Precup, R.E.; Bojan-Dragos, C.A.; Szedlak-Stinean, A.I. Combined model-free adaptive control with fuzzy component by virtual reference feedback tuning for tower crane systems. In Proceedings of the 7th International Conference on Information Technology and Quantitative Management (ITQM)–Information Technology and Quantitative Management Based on Artificial Intelligence, Granada, Spain, 3–6 November 2019; pp. 267–274.
15. Beloglazov, A. Energy-efficient management of virtual machines in data centers for cloud computing. Ph.D. Thesis, The University of Melbourne, Melbourne, Australia, 2013.
16. Chen, Y.; Li, X.; Chen, F. Overview and analysis of cloud computing research and application. In Proceedings of the 2011 International Conference on E-Business and E-Government (ICEE), Shanghai, China, 6–8 May 2011.
17. Xing, T.; Huang, D.; Xu, L.; Chung, C.J.; Khatkar, P. Snortflow: A openflow-based intrusion prevention system in cloud environment. In Proceedings of the 2nd GENI Research and Educational Experiment Workshop (GREE), Salt Lake City, UT, USA, 20–22 March 2013; pp. 89–92.
18. Joshi, B.; Vijayan, A.S.; Joshi, B.K. Securing cloud computing environment against DDoS attacks. In Proceedings of the 2012 International Conference on Computer Communication and Informatics, Coimbatore, India, 10–12 January 2012.
19. Kang, S.; Veeravalli, B.; Aung, K.M.M.; Jin, C. An efficient scheme to ensure data availability for a cloud service provider. In Proceedings of the IEEE International Conference on Big Data, Washington, DC, USA, 27–30 October 2014.
20. Pal, S.; Khatua, S.; Chaki, N.; Sanyal, S. A new trusted and collaborative agent based approach for ensuring cloud security. In Proceedings of the 2014 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 27–30 October 2014.