International Journal of Advanced Research in Engineering Technology & Science ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-11 Issue-2 February-2024 www.ijarets.org

STOCHASTIC MODELING FOR CLOUD PERFORMANCE ANALYSIS: A MATHEMATICAL APPROACH

Subodh Kumar
Research Scholar, Glocal School of Science
The Glocal University, Mirzapure Pole , Saharanpur (U.P).

Dr. Uma Shanker
Research Supervisor, Glocal School of Science
The Glocal University Mirzapure Pole , Saharanpur(U.P).

Abstract:

When comparing the response of the slowest node to that of the fastest node in a cloud infrastructure, mathematical models aid in illustrating the best possible performance attainment. One useful and important method for comprehending interdependencies in cloud computing is the analysis of mathematical models. It is especially useful for determining ideal values and forecasting equilibrium behavior. To achieve the efficacy of optimal utility, mathematical models are thus employed for future deployment, software updates, and resource allocation. In this research, we examine various security risks and suggest a stochastic mathematical model for traversal costs when assigning tasks to various Virtual Machines (VMs) using dispatchers. Ubuntu and the mathematical model are used to allocate jobs.

Index Terms **- Stochastic mathematical model, VM, dispatcher, service request monitor**

I. INTRODUCTION

Cloud computing has tremendous advantages which offers on demand service by the usage of computer resources that are pulled with the distant data centre and it can be controlled by the provider of cloud services which include networking capabilities, development tools, data storage, virtual and physical servers and programs with the monthly subscription fee billed base on the consumption by the user. The exponential rise of linked devices, including smartphones, smart cards, and other gadgets, is the main driver of cloud computing. It can be used to divide large computer jobs into a great number of smaller ones, which can then be handled in a parallel manner at a huge scale.

A stochastic model depicts an environment where uncertainty exists. It serves as a model for a process that has some level of randomness. The word stochastic originates from the Greek term “Stokhazesthai”, which means to aim or speculate. Dan certainty in the fact of existence in the real world is the stochastic model for representation of anything. The deterministic model on the other hand, predicts the outcomes with complete confidence. It includes a set of equations which are precisely described. The stochastic models are the most likely model for the yield of various outcomes in each time after the performance.

A family of random variables known as a stochastic process is one in which the parameter is chosen at random from an index set. Let's use the index set "time" as an example. The random variables are designated by the letters X_t for a continuous process and X_n for a discontinuous process. One of the most used index sets is "Time," and another is vectors, denoted by the symbol "Xu,v" where u,v is the position.

We offer a mathematical model of market-oriented cloud in this paper. The market-oriented cloud computing architecture suggests the existence of three key agents, namely the "Virtual Machine (VM) Monitor," "Dispatcher," and "Service Request Monitor," which together direct the service request examiner and controller as to whether to accept a job or not, and if accepted, how to carry out the job effectively and efficiently.

This research presents the mathematical model of the cloud and the traversal cost of the dispatcher's job assignment to various VMs. As a result, this paper does not address the roles of VM Monitor and Service Request Monitor. Here, we've concentrated solely on the dispatcher's role, which uses an ant colony system to distribute

workloads to available VMs. We have proposed a mathematical model to address this. This paper is organised as follows: Section 2 find out the research gap by analysing the research work already conducted by various researchers. The methodology used in this research is presented in section 3. Section 4 consists of results and analysis followed by conclusion in section 5.

II. LITERATURE REVIEW

This section gives background information about who has conducted similar research, what that research has or has not revealed, and how the most recent study adds to the discussion of constructing and developing mathematical models for cloud computing performance and applications of cloud computing using mathematical model.

Shahdi-Pashaki et al.,[1] refers to the process of setting up virtual machines and servers to do the necessary computations. In order to address the resource management issue in CC, this research proposes a novel strategy based on Group Technology (GT), a powerful methodology for managing resources in cellular manufacturing systems. In order to integrate the VMs, servers, and tasks in the best possible way while concurrently controlling a number of crucial variables, such as task migrations, server load fluctuations, and the number of VMs, a mathematical model was designed. This LINGO 9 programme is used to solve a number of tiny problems to check the viability of our suggested model.

Pinto et al., [2] concludes that Fog computing is one example of a distributed modern processing architecture that can reduce latency, increase scalability, and improve efficiency. Two of these changes include a cloud-fog computing infrastructure for large-scale operation and search procedures and a mathematical model to evaluate the architectures of distribution-based UAVs. Analysis has been done on the advantages of fog computing over conventional cloud computing.

Zhang et al., [3] concludes that, The Internet of Things (IoT) as it currently exists leverages cloud platform data access storing techniques, but the hash algorithm has flaws in the areas of ineffective data processing and low fault tolerance. A thorough analysis of numerous trade-offs in algorithmic optimization and a variety of hardware alternative designs are required for the development of successful integrated vision techniques. Because of this, finding design areas with the optimum performance trade-offs is challenging for developers.[4] The right mix is a growing trend with the advent of autonomous devices and cloud technologies. Therefore, this study presents design and invention of automated mechanical devices based on the D-T fuzzy control system taking into account the IoT.[5]

The literature studied reveals that most of the research explains about the types of security threats, load balancing in general and single objective in cloud computing with mathematical model. This study introduces the stochastic mathematical model.

III. METHODOLOGY USED

Experimental Setup

The Ubuntu 10.04 Server edition has been used to set up a private cloud that comprises of two servers, Server A and Server B.

Server B controls the nodes, whereas Server A controls the cloud, cluster, warehouse, and storage. We set up Machine A with a Core2duoX6800 processor, 2GB of DDR 2 RAM, and an 80 GB hard drive. A AMD PhenomeII X4 965 processor, 4 GB of DDR3 RAM, and a 250 GB hard drive power Machine B. Through a quick local area network, the nodes interact with one another. This paper presents the outcomes of local accessing several web services that are active on the web servers. The aforementioned cloud environment has been the subject of experiments. We used the subsequent commands to run the web services on Machine A:

If [!-~/.$euca/mkey.priv$]; $then$

mkdir -p -m 700~/. $euca$

touch~/.$euca/mykey.priv$

chmod 0600~/.$euca/mykey.priv$

euca- add- keypair mykey> $\sim/.euca > \sim/.euca/mykey$

If

First, we presumptively believe that VM 1 is the point of attack and is infected with malware. Any virtual computer or physical system on the cloud is impacted by resource sharing. Once the physical computer is impacted, it's possible that VMs 2, 3, and so on will also be impacted, and so on until the entire cloud is impacted. Here, we employ the Las Vegas Randomized Algorithm (LVRA), which guarantees that, "if there is a solution at all, you will always obtain one." The challenge is to successfully simulate the initial attack.

Second, we employ stochastic modelling to calculate the likelihood of events contained in a forecast in order to foresee possible outcomes. Historical information, such as previous market results, typically places restrictions on the random variables. Last but not the least, we need to understand the scenario in which users are vying for resources with varying financial capabilities. We assume that when users propose their bids for requests for cloud resources, they all do so simultaneously and are solely aware of their own offers. Later, the resources are distributed according to the proportions of the bids.

The chance of risk loss C(x), risk occurrence p(x) and occurrence of potential states of risk environment is unpredictable due to characteristics of cloud computing service itself. Therefore, taking into account the unpredictability of risks, this research seeks to quantify the cloud computing risk using the information entropy method. Information relates to the decrease of uncertainty in human cognition. Shannon, the creator of the theory, developed the idea of information entropy and used it to define the amount of information present in a system quantitatively describe the degree of uncertainty information.

In contrast to the conventional analysis of cloud computing risk, this research includes security in cloud computing for attribution at three levels as shown in Fig. 1. Cross analysis of cloud computing risk at different angles and levels.

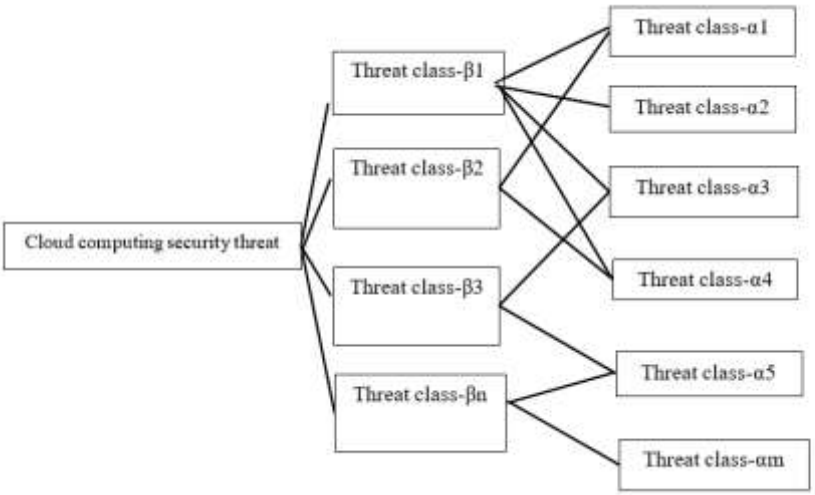

Fig. 1 Security threats in cloud computing

The three levels represent:

The purpose of this paper's research is the target layer.

Risk class layer: The various classes of cloud computing risk are expressed using the notation i, i = 1, 2,..., n;

Risk factor layer:

Cloud computing is influenced by several cloud computing risks are expressed using the notation j, j = 1, 2,...,m;

The intricate cross linkages between the risk class layer and the risk factor layer in this risk characteristics hierarchy set it apart from the typical research hierarchies and can better capture the unpredictable nature of cloud computing risk.

$$p(\beta i, \alpha j) = \frac{1}{\sum_{j=1}^{k} p(\alpha j)} p(\alpha j) \quad (1)$$

Then incorporate it into the formula for information entropy, as given below.

$C(\beta i) = \sum_{\alpha=1}^{n} p(\beta i, \alpha j) C(\alpha j)$ (2)

Proposed threat detection design

Assume that the virus has already infected at least one VM and has spread to others. Each VM can be infected by viruses due to the dynamic resource sharing across VMs, which eventually infects the entire cloud. We employ the Las Vegas Randomized Algorithm (LVRA) in our model, which guarantees that, if a solution exists at all, you will always receive it. The challenge is to successfully simulate the initial attack.

We employ random Fibonacci sequences in this model. The examples below illustrate this:

Due to this:

$L_n = \frac{1}{\gamma}(a_{n-1} + a_{n+1})$ (3)

$L_0 = 2;\ L_1 = 1$ (4)

In the beginning, no node is affected; later, node 1 is affected.

$a_0 = 0$, $a_1 = 1$ (5)

are the initial pair of seeds.

L_n is the maximum number of nodes that could be impacted.

Considering * above, we presume that all VMs communicate with one another and that is the random Fibonacci sequence.

IV. RESULTS AND ANALYSIS

4.1 Performance analysis of cloud

The Method of Measuring and Evaluating Using Information Entropy. The degree of risk uncertainty, the degree of risk loss, and the frequency of risk threats will all be carefully measured and assessed in this paper after the risk assessment system has been established.

Step 1: Create Tables 1 and 2 for the assessment table, and give the P(j) and C(j) of risk factors in the third layer weights based on the opinions of 15 subject-matter experts.

Assuming that P(x, y) and C(x, y), where x represents risk factors and y represents the weight level, respectively, are the experts' assessments of the distributions of risk frequencies and risk losses. P(j) and C(j) calculations are thus represented by the following formula:

$P(\alpha_j)$ = 0.2, 0.4, 0.6, 0.8 and 1 (4.1)

P(x,1), p(x,2), p(x,3) (4.2)

C(j)= 0.2, 0.4,0.6, 0.8, 1and c(x,1), c(x,2), c(x,5) (4.3)

The distribution of C(j) and P(j) of expert opinions; the greater the expert opinions' dispersion, the greater the uncertainty of the evaluation outcomes. Conversely, the higher the certainty of the assessment results, the more concentrated the expert assessments are. Accordingly, the assessment weight of each risk factor can be expressed using the following formula:

(1 X5 j=1 p_{ij} log5 j) (1 X5 j=1 c_{ij} log5 j) V (j) = 2 r (4.4)

The value of V(j) represents the contribution it makes to risk assessment; the larger the value, the more significant the contribution.

Step 2: Using Equation (1) get the weight of entropy coefficient P(i,j);

Step 3: Using Equations (2) and (3) and the P(i,j), determine the risk level of uncertainty H(i) and risk losses level C(i).

Step 4: Determine the steady-state probability for each risk class P(i) = (P(1),P(2),..., P(6)) using the Markov

chain method.

First, build the transfer matrix between each risk class using the cloud computing security risk assessment system presented in Fig. 5.1 along with the frequency P (j) of each risk factor:

$$Q = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{36} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{26} \end{bmatrix} \quad (5.5)$$

The diagonal elements P (ii) in the matrix stand for the likelihood that a risk class I event occurred on its own, while the elements P (ij) stand for the likelihood that a risk class I and j event occurred simultaneously. The value of these diagonal elements depends on the characteristics of each risk class.

Table 1: Assessment of security threat risk factor frequency

S.NO	LEVEL	SPECIFICATIONS
1	Very Low	In minor cases frequency of the security threat risks is very less moreover it do not happen.
2	Low	In minor cases the risk factors of security threats occur at frequency at low level
3	Medium	In few cases the security risk factors occur in the frequency at medium level
4	High	In most of the cases, occurrence and frequency of the risk factors are high
5	Very High	In the actual situations occurrence and frequency of the risk factors of security threats are very high

Step 5: Define the level of security risk associated with cloud computing, and conduct an integrated risk analysis. The degree of risk uncertainty H(i), the degree of risk loss C(i), and the frequency of risk occurrence P(i) are the three components that make up the definition of cloud computing security risk grade. Table 2 provides the precise definitions. The following is the formula used to determine each risk class grade:

Table 2: Grade of security threat risks

GRADE	SPECIFICATIONS
0 ≤ 0.2	Impact of Risk is ignored, goal of the risk maintenance is very clear and has more impact on the cloud computing for the security threats.
0.2 ≤ 0.4	The goal of maintaining the risks is to clear in the services providing cloud computing and it is managed well.
0.4 ≤ 0.6	Operating the services of cloud computing has few impacts. Generally, risk level of security in cloud services need a routine for maintenance.
0.6 ≤ 0.8	The determination of cloud computing services is very difficult. When the threat occurs, it affects the normal process of operation in cloud computing services.
0.8 ≤ 1	The factors causing risks cannot be determined. When the threat occurs, it is very difficult to make a comeback in the clous services. The risks of security threat are catastrophic.

Table 3: Results of assessment of distribution

	Distribution of Assessments				
Factors of Risk	**0.2**	**0.4**	**0.6**	**0.8**	**1**
Insider kind of threat	0.0	0.28	0.61	0.14	0.0
Ability of the service providers	0.0	0.08	0.82	0.14	0.0
Compliance of Laws	0.29	0.74	0.0	0.1	0.0
Management of keys	0.0	0.21	0.68	0.14	0.0
Isolation of Data	0.0	0.14	0.54	0.34	0.0
Encryption of data	0.0	0.14	0.41	0.34	0.14
Destruction of data	0.08	0.81	0.14	0.0	0.0
Migration of data	0.08	0.74	0.21	0.0	0.0
Backup of data and recovery	0.22	0.82	0.0	0.0	0.0
Authentication of identity	0.0	0.29	0.62	0.14	0.0
Upgrade of software	0.0	0.0	0.54	0.29	0.22
Prevention of network	0.0	0.28	0.61	0.14	0.0
Control of Access	0.0	0.08	0.82	0.14	0.0
Data physical location	0.29	0.74	0.0	0.1	0.0
System environment	0.0	0.21	0.68	0.14	0.0
Operation errors	0.0	0.14	0.54	0.34	0.0
Network bandwidth	0.0	0.14	0.41	0.34	0.14
Equipment replacement	0.08	0.81	0.14	0.0	0.0

In addition, the majority of the literature hasn't developed a risk assessment system or performed a quantitative study of the degree of uncertainty and loss associated with each risk during the risk weighting process. These research findings frequently only include technical risk and do not consider other risk factors, making it impossible to provide an accurate comparison of all hazards across all levels and dimensions.

The aforementioned issues are the key research topics in this study and need to be resolved in the process of assessing the risk associated with cloud computing. Sorting out the risk variables is what this post will do first.

By using a Markov chain to simulate the actual cloud computing risk environment and building risk attribute hierarchies with cross relations based on the risk factors, the study will be able to quantify the uncertainties surrounding risk occurrences and losses and perform a quantitative risk analysis from a variety of perspectives.

Table 4: Results of security threat performance analysis

	β_1	β_2	β_3	β_4	β_5	β_6
H	0.952	0.988	0.994	0.992	0.995	0.977
C	0.632	0.584	0.484	0.490	0.572	0.582
P	0.104	0.193	0.178	0.216	0.094	0.211
L	0.382	0.472	0.429	0.466	0.387	0.490
Risk grade of security in cloud computing is L=0.461						

The following can be learned from the examination of the research findings:

1) The grade of overall cloud computing security risk is expressed by L = 0.461. This value shows that this company's cloud computing security falls within the general risk category, its cloud computing service has some risk, requires routine maintenance, and is at an acceptable level.

2) The values of L(6) = 0.6, L(2) = 0.492, and L(4) = 0.466 are greater than other risk grades for the entire system. These statistics show that the most significant risks to this company's cloud security are related to administration security, data security, and network security. These factors are crucial in determining the security of this e-commerce platform and should be given more consideration in risk management decisions. On the other hand, L(1) = 0.382 and L(5) = 0.387 indicate that this firm's operational and physical security is well-managed.

Based on the information entropy theory, risk uncertainty is studied quantitatively, the influence of subjective elements on the results is decreased, and a reference standard for risk management decisions is provided. This article creates a risk assessment hierarchy with cross relations and categorizes the cloud computing risk into six classifications in comparison to previous research methodologies. The research study fills in the gaps in the literature regarding the level of uncertainty associated with each risk by calculating the steady-state probability of each risk class in the stable cloud computing process when combined with the Markov chain. It also provides a definition of risk grade based on information entropy. To give a more thorough risk assessment system, the author will keep identifying and including new security risk aspects of cloud computing in the upcoming work while avoiding redundant variables.

Stochastic modelling for security threat

Two separate web services have been the subject of our testing. However, to show how well our method worked, we submitted numerous copies of the identical web services as distinct tasks. The jobs were started at various dates. That our proposed goal function steadily increases as stochastic demand gradually rises and offers more optimal value when the stochastic demand is between a moderate and maximum range as shown in Table 5. This comparative analysis is also represented in terms of bar chart in Fig. 2 for better visualization.

Table 5: Comparative analysis of security threats proposed vs existing models

Parameters	Existing models	Proposed stochastic model
Business security threat	68	79
Data security threat	72	84
Application security threat	75	91
Network security threat	56	71

Physical security threat	83	88
Administration security threat	85	89

V. CONCLUSION AND FUTURE SCOPE

In this paper, assumptions in stochastic system for computing predicted income, utilization, and rejection rate are considered. Jobs must start (and stop) according to a stochastic process. Moreover, it is necessary to understand the job price cumulative distribution function. These presumptions do not, however, limit applicability. The proposed stochastic mathematical model for cloud computing takes different types of factors including requirement for the service, workload in the environment of application, multi-server system configuration system, agreement of service level, customer satisfaction, QoS, low quality penalty and renting cost of space, cost for energy consumption as well as the profit margin of the service provider. For the future research, few suggestions are; including the mathematical model for cloud computing and its applications that include blockchain and smart contracts which have the potential to change the current structure of cloud computing markets by enabling the development of the fully decentralized cloud technologies which lowers the cost through generation of predictable results without the need of any intermediaries. The establishment of the decentralized solutions using cloud computing on full integration enables the majority of companies to comply with the kinds of cloud solutions to avoid hardships on ownership.

REFERENCES

[1] Shahdi-Pashaki, S., Teymourian, E., & Tavakkoli-Moghaddam, R. (2018). New approach based on group technology for the consolidation problem in cloud computing-mathematical model and genetic algorithm. Computational and Applied Mathematics, 37(1), 693-718.

[2] Pinto, M. F., Marcato, A. L., Melo, A. G., Honório, L. M., & Urdiales, C. (2019). A framework for analyzing fog-cloud computing cooperation applied to information processing of UAVs. Wireless Communications and Mobile Computing, 2019.

[3] Wang, M., & Zhang, Q. (2020). Optimized data storage algorithm of IoT based on cloud computing in distributed system. *Computer Communications*, *157*, 124-131.

[4] Sharma, D. K., Singh, B., Regin, R., Steffi, R., & Chakravarthi, M. K. (2021, March). Efficient Classification for Neural Machines Interpretations based on Mathematical models. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2015-2020). IEEE.

[5] Yao, J., & Wu, F. (2022). Cloud automatic mechanical equipment based on D–T fuzzy control and internet of things. International Journal of System Assurance Engineering and Management, 13(4), 1696-1704.

[6] Aslanpour, M. S., Gill, S. S., & Toosi, A. N. (2023). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. Internet of Things, 12, 100273.

[7] Miao, W., Min, G., Wu, Y., Huang, H., Zhao, Z., Wang, H., & Luo, C. (2019). Stochastic performance analysis of network function virtualization in future Internet. IEEE Journal on Selected Areas in Communications, 37(3), 613-626.