JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

Mathematical models can be used in cloud computing frameworks

Ashwani Sethi[1], Vishal Kumar[2]
[1,2]Guru Kashi University, Talwandi Sabo

Abstract

Increasing levels of financial and professional information is being stored on the cloud, which has generated questions about the safety of the environment. In order to prevent security threats from entering the systems, it is necessary to identify where they originate. Even when it comes to cloud security, it's critical to consider how resources are managed and profit margin generated. Analysis strategies, including but not limited to: security threat, resource allocation and companies with higher model, are required to solve these challenges. This achieves the basic necessity of diverse showing strategies, for example, though not constrained; security danger as well as income raises models. This specific overview report will attempt to investigate security threats and chance mitigation in distributed computing. It gives send off of exactly the manner in which viral hit can attack the virtual gadgets on the cloud, investigates the greatest security hazards as well as countermeasures by supplying the viral danger showing within virtual gadgets as well as chance alleviation.

Keywords: cloud computing frameworks, Security threat model, Analysis strategies.

1 Introduction

There are still a variety of options available that can be applied to data in real time in a modern computing context. A complete technique of computer processing is deemed to have been delivered at the larger scale [1] when the mathematical calculations used to execute the procedures are combined. System load can be determined by calculating how likely each component is to be used, based on its statistical models. An increasing number of businesses and academics have benefited from a rise in distributed computing revenue over the past decade. The following three help models, four sending models, and five qualities capture the essence of distributed computing:

- In addition, there are three service models to choose from: IaaS, PaaS, and SaaS
- There are four types of cloud deployment: public, private, community, and hybrid
- Bread network access, Resource pool, fast elasticity, and measured service are the five features discussed above.

These three issues will be addressed in this paper. As a starting step, this specific study presents a single structure for distributed computing as a science and invention as well as an architectural framework, industry and administration framework. We choose distributed computing analytics for the third and second issues because it covers a wide variety of distributed computing topics by incorporating numerical arrangements and intuitively suspecting. Techniques for that paper will focus on distributed computing, clever investigation, and business understanding and engineering know-how.

2 CONCEPT OF CLOUD COMPUTING

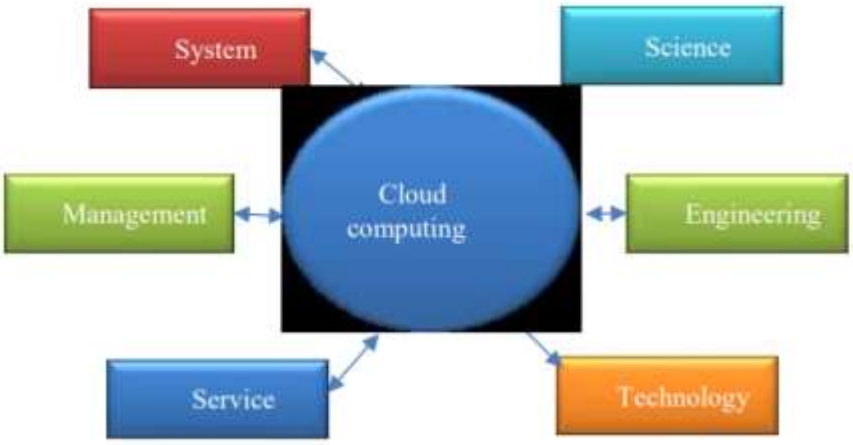
In so many areas of unmatched data expansion, distributed computing frameworks have become the norm. Mists are a common method used by businesses to communicate their logical and operational applications. They don't have to spend money on building and maintaining their own server farms. However, operators of dispersed

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

computing data centres can reduce the total cost of IT foundation ownership by helping a wider range of clients combine registration assets and accumulating frameworks. Cloud data centre owners can further reduce expenses by utilising good focused assets for booking, tonne adjustment, parcel directing reconciliation, and the board of a few regionally divergent information community fragments.

For determining and improving the quality of distributed computing or data frameworks based on mists, the development of numerical models is crucial. The working approach of distributed computing (CC) is characterised by a high degree of stress, as are the main components of CC:

- flow of requests for computing resources (CR) issue
- consumers' accidental use of the required CR as well as their existence in the system;
- inadvertently dissatisfied with the time and the deletion CC's infrastructure
- For example, the CC's response time is a critical temporal characteristic that must be made available to a certain group of clients.
- Requirement for optimum PR use in light of customers' purchased results of calculations and operating conditions, based on price of time delay;
- For optimal use by both operators and clients, an adjustment in the working method of the CC must be implemented as soon as possible.



3 CALCULUS OF CLOUD COMPUTING

Using numerical arrangements and natural suspicion, this segment presents distributed computing analytics, which addresses a wide range of distributed computing topics.

How you can know resources in cloud computing?

To describe distributed computing, PC framework assets are used while NIST use computing assets that include IT assets. In other words, in a distributed computing environment, the assets should occasionally be PC framework, figure, or even IT assets. Is it true that PC framework, processing, and IT assets are all the same? No, in terms of numbers,

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

IT $\subseteq$ ICT $\subseteq$ computing.

That is,

IT resources $\subseteq$ ICT resources $\subseteq$ computing resources

Some PC framework assets may be IT assets or ICT assets at other times. It's a portion of calculating assets in this way. The preceding numerical analysis suggests that IT assets are fairly confined in semantics, whereas ICT is substantially more broad and registration assets are extremely standard and might be used as distributed computing assets.

A new enquiry is sparked by the examination that was previously indicated. Distributed computing has a number of advantages. In any case, we know that the assets include computer framework assets, capacity assets, processing assets, ICT assets, IT assets, and so on. Reviewing the fundamentals of this particular subject

Question 1: Is it possible to classify all of these cloud computing resources as "big data"? If so, we have a solution.

Information technology resources, also known as ICT resources, computing resources, and large amounts of data Cloud computing's strategic resources, then, are big data. Cloud computing's resources and services are built on a foundation of big data.

How to understand types of cloud?

Private and public clouds can be mixed together in the Hybrid Cloud, as can private and public IT resources.

$$\text{Hybrid cloud} = \text{public cloud} + \text{private cloud}$$

$$\text{Hybrid cloud} = \text{public cloud} \vee \text{private cloud} \vee \text{community cloud}$$

How to understand cloud services

IaaS, PaaS, and SaaS are all forms of infrastructure as a service.

There are three tiers to these services. As a result, the connections between them can be described as

IaaS $\oplus$PaaS < IaaS $\oplus$ SaaS. Am I right?

Cloud Analytics = Big data Analytics + Cloud Computing

Big data analytics is mathematically represented by Wu, Buyya, and Ramamohana (2016).

$$\text{Big data Analytics} = \text{Machine learning} + \text{Cloud Computing} \quad (1)$$

Artificial intelligence, of which machine learning is a component, is referred to as $\subseteq$ machine intelligence. Then we'll be able to host a party.

$$\text{Big data Analytics} = \text{artificial intelligence} + \text{Cloud Computing} \quad (2)$$

Based on,

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

$$\text{Big Data analytics} = \text{Big data} + \text{Big data analysis} + \text{Big DW} + \text{Big DM} + \text{Big SM} + \text{Big ML} + \text{Big Visualization}$$

Data warehouse, data mining, statistical modelling, and machine learning are all examples of DW. Then we have

$$\text{Cloud Analytics} = \text{Big data} + \text{Big data analysis} + \text{Big DW} + \text{Big DM} + \text{Big SM} + \text{Big ML} + \text{Big Visualization} + \text{Cloud Computing} \quad (3)$$

In light of this, it may be concluded that the aforementioned finding is more inclusive than (1) or (2).

4 PURPOSE OF THE STUDY

The purpose of this survey study is to provide concrete information on how to construct mathematical models on the cloud based on the models presented in this survey:

1. Model of security protection

2. model of profit-maximizing revenue

We believe that VM 1 (virtual machine one) is in fact the inventory of assault and the conduit for the transmission of diseases. Because of the sharing of resources, any virtual machine on the cloud can be referred to as a "real" physical device. It is possible that VM 2 and VM 3 and so on may also be affected, and the process continues until the entire cloud is genuinely afflicted. Las Vegas Randomized Algorithm (LVRA) is what we use now, and it promises to always discover a solution as long as there is some sort of response. There is a lot of discussion on how to replay the initial strike correctly.

Stochastic, on the other hand, is exhibiting how to work out the likelihood of results inside a gauge in order to predict what conditions would look like under different circumstances. Verifiable subtleties, such as prior market results, are usually required to justify conflicting elements.

5 RESULTS AND DISCUSSION

A. Security threat model

1. The top security threats in cloud computing

Security threats that target specific frameworks can be found in distributed computing, but so can more general threats. Maltreatment and depraved use of distributed computing, shaky points of interaction and Ape's, new gamble profile, pernicious insiders, Shared innovation issues, information misfortune or perhaps record and spillage or perhaps administration commandeering are just a few of the many issues that could arise.

2. Risk Mitigation

STRIDE has identified a set of countermeasure strategies for each category of threat it has assessed. Spoofing customer identity, manipulating data, information leakage, denial of elevation and the administration of honor are all part of the Step condensing. In the table below, you'll find a summary of these findings. The best defense depends on the specific attack:

Table 1: STRIDE Threats and Countermeasures

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

Threat	Countermeasures
Spoofing user identity	Use strongauthentication. Do not store secrets (for example, passwords) inplaintext. Do not pass credentials in plaintext over thewire. Protect authentication cookies with Secure Sockets Layer(SSL). Use data hashing andsigning. Use digitalsignatures.
Tampering with data	Use strongauthorization. Use tamper-resistant protocols across communicationlinks. Secure communication links with protocols that provide message integrity. Create secure audittrails.
Repudiation	Use digitalsignatures. Use strongauthorization
Information disclosure	Use strongencryption. Secure communication links with protocols that providemessage
Denial of service	Validate and filterinput.
Elevation of privilege	Follow the principle of least privilege and use least privileged service accountstorun processesandaccessresources.

3. Viral attack in Virtual Machine (VMs)

Infections attack the body of a man cell in a similar way to how virtual computers are attacked on the cloud. Data that may be breached and the entire phone system could be wiped out if a virtual device is disconnected from the physical device. In any case, the virtual printer's security isn't up to par with expectations. Infections will be able to spread their attacks from one virtual machine to the next because of the strong sharing of resources from a large server or even among the virtual machines themselves. The image below illustrates how a viral hit can appear at any point in the cloud and attack the various virtual machines therein.

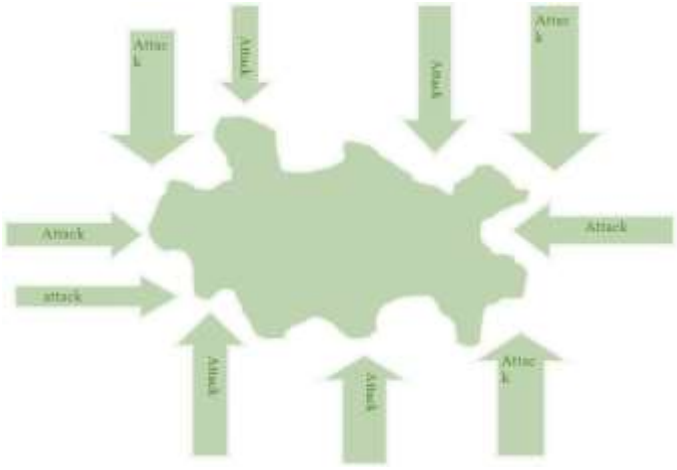


Figure 2: Viral attack VMs on the cloud

There are a number of possible attacks against virtual machines (VMs) in the cloud depicted in Figure 2 below. These assaults progress one small step at a time until the entire object is affected by the assault. When viral hits are disseminated in their entirety, cloud users run the risk of losing their data. Throughout this research, we offer a viral model cycle that can fend off such a large number of attacks. When a virtual machine (VM) is targeted, it is possible that the next virtual machine (VM) will be targeted as well, and so on.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

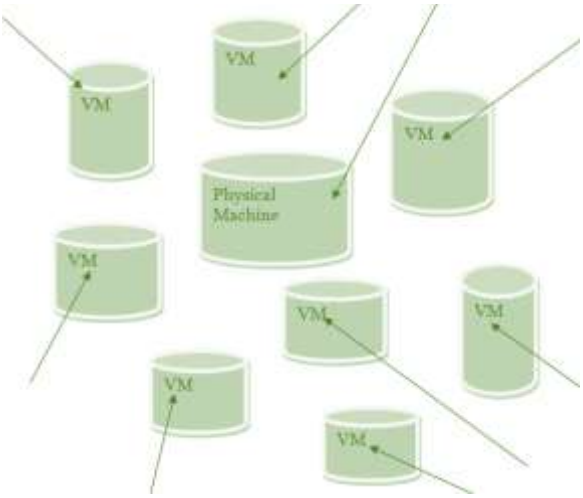


Figure 3: Viral attack on VMs in the cloud

4. Proposed Viral model system

I believe that at least one VM has been affected, and that additional VMs have been infected as well. Because of the high level of asset sharing across VMs, any one of them can become infected, which has an effect on the entire cloud. This model makes use of the Las Vegas Randomized Algorithm (LVRA), which claims that "you'll always find a solution, assuming there's a response.". In order to replicate the first strike, the cycle is working out exactly how to do so. We use random Fibonacci sequences in this model. Underneath, you may be able to prove this:

Given that:

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

$$L_0 = 2, L_1 = 1$$

Initially no nodes are affected " node 1" may be affected

$a_0 = 0, a_1 = 1$arethefirstpairofseeds. $L_n$is thepossiblenumberofnodes tobeaffected

Now, $a_n$is a solution (well-known) to the deterministic difference equation below:

$$a_{n+1} = a_{n+1} + a_n, n \leq 2$$

$$a_n = 0, a_1 = 1$$

from * above, we assume that All VMs talk to each and γ is the Random Fibonacci sequence.

5. The growth of threat attacks with respect to their percentage peryear

Since the 1960s, when they discovered the methods to avert this deluge of attacks, the grandeur of assaults has become increasingly apparent. People began referring to this time of year as "the cockerel's eggs" in the 1990s, as shown in the figure below. As long as there exist frameworks and people who understand them, more must be done to take advantage of these advancements. These attacks should be limited to a one percent or zero percent

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

level of severity, if at all, if they are to be taken seriously as a test for other cloud users and information society as a whole.

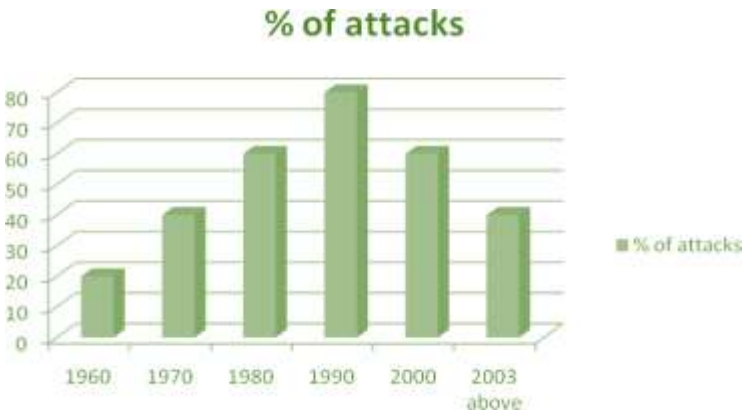


Figure 4: The percentage of threat attacks per year

B. Revenue Model

The stochastic and the appropriations of its for profit enhancement are depicted in this specific overview as two essential income boost models. When one or more variables in the model are unpredictable, this method of financial display is used. If you're trying to find out what conditions might seem like under different circumstances, then stochastic displaying is the best way to go. Past retail returns, for example, are often to blame for the inconsistencies that arise.

1. A stochastic revenue maximization

Formulations

It is possible to develop the pricing issue in this manner. It's currently working in the ca with x [0,C] area instances with capacity C. In order for it to generate income, it must change both the need (*) and (*) operations.

Note here basically tells how much time is remaining to purchase, as well as how quickly the timetable is running out. Non-expecting to cost approach p(s) is used by the supplier in order to increase the typical income with the full skyline. For example, the selection of dynamic circumstances in the ca whenever s [0, t] is given, we can denote programmer usage by X(s). When an opportunity arises, a need can be discovered.

$dX(s) = 1$, and it is vanished at time s in the event that $dX(s) = -1$. If the number of active circumstances exceeds the capacity C at any time, the pricing policy will fail. As a starting point, the writer uses U to designate all possible pricing plans that meet s. (0)

$\int_0^S dX(m)[-x, C - x]$ (1)

$p(s)[0,1]1\ \forall s[0,t]$ (2)

Time in [0,s] is represented by m here. Imperative (1) refers to the limitation on one's abilities that was mentioned earlier. As long as there are still invalid costs, the contract can be completed as usual. Assuming u is a rate strategy, then With [0,t], the author denoted average yearly earnings by

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

$J_U(x,t) = E_u[\int_0^t p(s)X(s)ds], \forall t > 0$ (3)

Whent = 0, the estimated revenue for any utilization is zero at the very end of the horizon.

$J_U(x,0) = 0, \forall x \epsilon [0,C]$ (4)

Finding a pricing scheme that maximizes predicted profits over time is the provider's challenge.

[0, t], denoted by

$J*(x,t)$. Equivalently, $J*(x,t). = \sup_{u\in U} Ju(x,t)$ (5)

2. Stochastic System Model

Using the stochastic building model, we may look for situations when FCFS is overwhelmed by strong valuing. In addition, the model might be used to calculate the most severe reservation prices and limits in each case. The experts used a Markov chain-based approach to show what was happening.

The model was presented in three stages: first and foremost, the suppositions and a real-world model scenario were given. As a result, the various states and their depiction, as well as the assessment of their change probabilities, have been analyzed for the discrete division scenario.

Regardless, as the granularity of the model increases, so does the number of states. There is no limit to the express area if the divisions are reliable. To avoid this, in the third round, states met to pool states with highly comparable characteristics. In this way, the model depiction will be smoothed down, and the state area will be greatly reduced. This results in a model with a reduced number of states, and it also allows for the departure of steady conveyances. Moving from the second to the third stage in models with discrete dispersion simply shifts information from states to change probabilities. As a result, the findings from the two models are remarkably comparable. This could lead to the model's reputation being tarnished.

- A1: The arrival of a new job is determined by a stochastic process.
- A2: The process of terminating a job is stochastic.
- A3: There's a certain quantity of resources available for use.
- A4: random X with a recognized division/snowball division feature is the cost of the task.
- A5: Acceptance or rejection of a job is almost always instantaneous.
- A6: Tasks are only acknowledged when the price of theirs exceeds the relevant reserve selling price, regardless of whether a certain utilization level is met.

When there isn't enough probabilistic information available, the assets required for each assignment can be shown as irregularly adjustable with a perceived dispersion execution or, at the very least, using fluffy sets.

Using the following model circumstance, the paper's model creators were able to demonstrate their point more effectively. A constant asset need for each activity was a result of the founders' focus on the effects that varying rates had on income (twenty percent of the available limit). Work earnings have a discrete even distribution across time, ranging from 0.5 to 1.5. The capacity utilization (C0-C5) and the average income of each

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

undertaking are used to differentiate the states. The average annual salary for each occupation would be broken down into three categories: Underneath, this was discovered:

$$R(1: 0.5 <= r_{avg} <= 5/6, R2: 5/6 < r_{avg} <= 7/6, R3: 7/6 < r_{avg} <= 1.5).$$

2. Stochastic Model with discrete distribution

As a natural conclusion, the number of running assignments of type A and type B can be evaluated. This particular depiction would lead to a slew of ambiguous condition descriptions because of the wide range of earnings. A number of states with varied assignment mixes but equal usage and income will also be prompted by this. To circumvent this, states are given an elective significance. Both the ability used (or how many positions are filling in) and the all-out income of all currently operating roles can be viewed in every state of the model. This means that the documenting of the limit/income is a good way to recall a single state's values.

Regardless, the paradigm allows for a variety of states to be achieved. It is possible to obtain three different combinations of the condition 2/1.4, which provides both state 2 running position and total income of 1.4. Work and assignment blend 0.5, 2 positions 0.7, and work blend 0.9, each lead to the same result. When determining the likelihood of a migration, this state property should be taken into account. To make sure that the Markov property is genuinely met, the probability of a move should not be dependent on previous states. It's possible to classify the various changes that occur in each state using exactly the same three categories. There is a possibility that an assignment is started, completed, or not completed at all. Each event has a chance of occurring. The sum of all probability is determined by a single factor. To begin a brand-new position, an endogenously determined probability is used. Every projected spotless job with a certain salary has an equal chance of showing up. The chance of a task start divided by the number of available places gives us an idea of how likely it is that a specific activity will begin. Insofar as feasible, no new position can be recognized without much effort, and as a result, no state has a more obvious limit or transition to that which is not currently present. With the current situation, the possibility of a job start is actually added to the likelihood of no adjustment (as each additional work will be dismissed).

With the endogenously supplied probability, at each state, one of today's working positions closes. It's essential to know what kinds of jobs are actually being done in order to calculate the chance of a person moving from one state to another with a lower level of ability. The likelihood of a runner tying up is the same regardless of where they are on the field. In order to reach state 2/1.4, you will need to find three excellent mixtures. According to the positions of the three mixes stated, the result may be as follows: twice an errand with income 0.5, twice an assignment with income 0.7, and twice an assignment with income 0.90. With everything considered, there are six spots. If a task is completed, the probability that it will be one of the jobs with a 0.5 income is 2/6 (according to the given work end likelihood). There is therefore an endogenously given work end probability of 2/6 and a move likelihood from state "2/1.4" to state "1/0.9" (which is in fact: an end devour with income 0.5 closures). The possibilities of elective advancement have been correctly calculated. Probabilities of changing a state back to a previous one are provided. State 0 and overburden states are the only fundamental calculations, so far as feasible.

3. General Stochastic Model with state classes

State classes combine a number of states into a single group. The limit reached and the range of incomes earned define a class. Each state is given a specific amount of money and a specific amount of time in which to spend it. Rather to using the total income of each express, the typical income is a better measure since it allows for comparisons between different limit stages of income.

The total revenue is divided by the number of active jobs to arrive at the average revenue.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

4. Optimality Conditions

Stochastic strong programming condition (5) In order to figure it out, creators might think about the Hamilton Jacobi concerns of its, which are the constant time partner of the Bellman situation. Ponder the events that transpire over a short period of time (t). Because the appearance and takeoff techniques are both Poisson, the supplier observes one more model with probability f(p)t + o(t), one less event with likelihood g(p)t + o(t), and no change in the rest of the likelihood mass by selecting an expense p. p As stated in the Optimality Principle,

$$J^*(x,t) = \sup_p[px\delta t + 0(\delta t) = f(p)\delta t * J(x+1,,t-\delta t) + g(p)\delta t^* J(x-1,t-\delta t) + (1-(f(p)$$

$$J(x+1,t-\delta t) + g(p)\delta t * J(x-1,t-\delta t) + (1-(f(p)+g(p))\delta t)J*(x,t-\delta t)] \quad (6)$$

At this point in the process, it should be impossible to discern between the expected income during the time span t and the normal value of the ideal expected income from the extra time period t-t, which are truly the leftover terms of the ideal anticipated income J (x, t) (6). Taking the limit of t 0 as our starting point, we get:

$\partial J(x,t)/\partial t = \sup$[px +f (p)(J *(x+ 1, t) -J *(x, t)) -g(p)(J *(x, t) -J *(x -1, t)) (7)

Note that (7) holds just for $1 \le x \le C-1$. When x = zero, There will be no departure above t, which means that when x = C the provider must determine a cost of one in order to shut down the arrival technique as previously described, it is obliged to cost zero. Consequently, p(0, t) = 0 in their model, and p(C, t) = 1. The equations used by the authors were as follows:

$$J*(0,t) = f(0),\delta tJ(1,t-\delta t) + (1-f(0)\delta tJ*(0,t-\delta t) + 0(\delta t)$$

$J*(C,t) = g(1)\delta t * J(C-1,t-\delta t) + (1-g(1)\delta t)J*(C,t-\delta t) + C\delta t + o(\delta t))$, based on this, we can conclude that

$\partial J^*(0, t) / \partial t = f_{(0)} J^*(1, t) - J^*(0, t)$ (8)

$\partial J^*(C,t)/\partial t = C - g_{(1)}(J^*(C,t)-J^*(C-1,t))$ (9)

6 Conclusion

Among consumers and corporations, cloud computing is in high competition since it provides highly nonlinear modular strategic planning for reliable and provided services in a pay as you use model to the general public. A cloud resource consumer can request many cloud resources at the same time in the cloud computing model. There must be an essential to secure that all cloud services are made available to those who want them in a timely manner. Cloud computing facilitates a high degree of protection and utilization through the use of allocation of scarce resources. As a compensation-as-you-use model that is excessively open, distributed computing is in high demand since it provides powerful, adaptable asset designation for reliable and assured administrations. A cloud asset client can simultaneously request a determination of cloud assets in distributed computing. As a result, there must be a plan in which all of the assets mentioned by cloud asset clients are presented in a viable manner to fulfil their needs. In light of the fact that there is a large pool of cloud clients, asset allocations allow for more openness and security. Benefit and income growth are essential for cloud customers.

REFERENCES: -

[1] Sun, Zhaohao. (2019). The Calculus of Cloud Computing. 10.13140/RG.2.2.13483.49446/1.

[2] Shyshkina, Mariya & Kohut, Uliana & Marienko, Maiia. (2018). The Systems of Computer Mathematics in the Cloud-Based Learning Environment of Educational Institutions.

[3] Szabó, Peter & Moucha, Václav & Ferencová, Miroslava. (2018). Cloud Computing and Numerical Mathematics. November 15 - 16, 2018, Grand Hotel Starý Smokovec, the High Tatras, Slovakia

[4] P.Singh, M.Dutta, N.Aggarwal,"A review of task scheduling based on meta-heuristics approach in cloud computing",Knowledge and Information Systems, vol. 52, nol.1, 2017. doi:10.1007/s10115-017-1044-2

[5] Sun, Z., & Wang, P. P. (2017). A Mathematical Foundation of Big Data. Journal of New Mathematics and Natural Computation, 13(2), 8-24.

[6] Mao, Yuxin & Bhuse, Vijay & Zhou, Zhongmei & Pichappan, Pit & Abdel-Aty, Mahmoud & Hayafuji, Yoshinori. (2014). Applied Mathematics and Algorithms for Cloud Computing and IoT. Mathematical Problems in Engineering. 2014. 1-2. 10.1155/2014/946860.

[7] Disha H. Parekh, R. Sridaran, (2013): An Analysis of Security Challenges in Cloud Computing. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013

[8] Bernd GroBauer, ToBias Walloschek, and elmar sTöcker Siemens: Understanding Cloud Computing Vulnerabilities.IEE Security and Privacy Vol#9 Issue 2,March 2011 pp 50-57, IEEE Educational Activities Department Piscataway, NJ, USA.

[9] Tim Pueschel, Fabian Putzke, Dirk Neumann(2012):Revenue Management for Cloud Providers- A Policy-based Approach under Stochastic Demand. " hicss, pp.1583-1592, 2012 45th Hawaii International Conference on System Sciences, 2012(ISBN: 978-0-7695-4525-7)

[10] Christian Delettre* – Karima Boudaoud – Michel Riveill(2011), Cloud Computing, Security and Data Concealment.16th IEEE Symposium on Computers and Communications (ISCC'11), pages 424-431, IEEE, Corfu, Greece, 28-30 June 201(ISBN: 978-1-4577-0681-3).

[11] Davide Tammaro†, Elias A. Doumith†, Sawsan Al Zahr†, Jean-Paul Smets‡, and Maurice Gagnaire(2011) , Dynamic Resource Allocation in Cloud Environment Under Time- variant Job Requests" cloudcom, pp.592-598, 2011 IEEE Third International Conference on Cloud Computing Technology and Science, 2011(ISBN: 978-0-7695-4622-3).

[12] Kalyani D Kadam, Sonia K Gajre and R L Paikrao. Article: Security issues in Cloud Computing. IJCA Proceedings on National Conference on Innovative Paradigms in Engineering and Technology (NCIPET 2012) ncipet(11):22-26, March 2012. Published by Foundation of Computer Science, New York, USA BibTeX

[13] Disha H. Parekh, R. Sridaran, (2013): An Analysis of Security Challenges in Cloud Computing. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013 .

[14] Wesam Dawoud , Ibrahim Takouna , Christoph Meinel (2010) , Infrastructure as a Service Security: Challenges and Solutions. Informatics and Systems (INFOS), 2010 The 7th International Conference on, 1-8

[15] Joel Weis and Jim Alves-Foss(2011): Securing Database-as-a-Service: Issues and Compromises(ISBN: 1540-7993). IEEE Security & Privacy, vol. 9, no. 6, pp. 49-55, November/December, 2011