Indian Journal of Science and Technology, Vol 9(34), DOI: 10.17485/ijst/2016/v9i34/100185, September 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

# Mathematical Ontology for Infectious Virtual Machines in IaaS Cloud Environment

**S. B. Dash[1], H. Saini[2], T. C. Panda[3] and A. Mishra[4]**

[1]CUTM, Paralakhemundi, R.Sitapur - 761211, Odisha, India; dash_satyabrata@yahoo.co.in
[2]Department of Computer Science and Technology, Jaypee University of Information Technology, Waknaghat, Solan - 173234, Himachal Pradesh, India; hemraj1977@yahoo.co.in
[3]Department of Mathematics, Ravenshaw University, Revenshaw College Campus, College Square, Cuttack - 753003, Odisha, India; tc_panda@yahoo.com
[4]Department of Mathematics, CUTM, Paralakhemundi, R.Sitapur - 761211, Odisha, India; registrar@cutm.ac.in

## Abstract

**Background/Objectives**: Cloud virtualization is a creative and one of the altogether accomplished improvements in the current figuring environment. It provides a virtualized environment based on Service Level Agreement (SLA) to cloud. **Methods/Statistical Analysis**: Infrastructures of Physical machines are rapidly replacing by Virtual machines (VMs) for their abilities to emulate hardware environments, share hardware resources, and utilization of a variety of operating systems. Accordingly, giving security to the cloud virtual machines and clients' information is one of the essential difficulties to data frameworks. This manuscript describes about the mathematical ontology based upon the attacked VMs and infectious VMs which predicts the trustworthiness of the IaaS virtual platform. **Findings:** The proposed work will diminish the dangers to the VMs in the cloud surrounding independent of the client's security and applications approach. **Application/ Improvements:** It will fundamentally guarantee the level of the security of VMs in a cloud situation which assists the cloud administration suppliers to take the fast choices and about the up-degree of the counter assault estimations.

**Keywords:** Cloud Computing, Cloud Virtualization Security, Mathematical Ontology, Predator-Prey Model, SLA

## 1. Introduction to Cloud Virtualization

Distributed computing gives a virtualized situation to the cloud clients for getting to and trading their applications and information through the web. As per National Institute of Standards and Technology (NIST) "Distributed computing is a model for empowering omnipresent, helpful, on-interest system access to a mutual pool of configurable figuring assets that can be quickly provisioned and discharged with insignificant administration exertion or administration supplier communication[1]". European Community for Software and Software Services (ECSS) defines "cloud computing as the delivery of computational resources from a location other than your current one[1-4]". The cloud administration supplier gives the administrations to the enlisted cloud clients on pay per use essential over the glove. The administrations accessible to the clients are arranged as PaaS, SaaS and IaaS. The administrations are accessible to the clients relying upon cloud sending and the SLA (administration level assentions) between the administration providers (CSP) and the cloud clients[4-6]. IaaS is the most popular service model that deals with the infrastructure and storage requirements in cloud environment. The services which are available in terms of infrastructure and storage are virtualized. Virtualization is the process which splits, allocates, and resizes the resources vigorously to erect the ad-hoc systems. A Virtual Machine (VM) is a dedicate software environment which runs applications and operating systems in the guest machine to help users application execution[7-9]. So, VMs are logical machines having almost the same architecture as a real host machine, running an operating system in it. The architecture of the virtual

*Author for correspondence

machine (VM) system is shown in Figure-1. According to the cloud architecture, several virtual machines (VMs) share the same physical machine.

## 2. Cloud Virtualization Components

*Hypervisor Layer* – Hypervisor is the abstraction layer that gives the important asset to share equipment assets between the virtual machines. Hypervisor layers have two fundamental models: Para virtualization, for example, Xen and Hyper – V and the other model is full virtualization, for example- VMWare. Frequently, these two models exchange off a level of seclusion to expand the sharing of assets among VMs[8-9].

*VSwitch or Virtual Network Layer* – This layer is in charge of multiplexing activity between virtual NIC (system interface card) and physical NIC (system interface card). The vSwitch likewise controls the VM movement of a solitary host that does not touch the physical NIC of the host, and vSwitch deals with the client trust zone. The virtual system additionally acts like a physical switch in non-virtualized situations[8-10].

*Virtual Machines* – VM's is a software layer that copies the genuine physical machine, these VMs keep running under the control of hypervisor layer that further virtualizes and imitates the equipment assets and returns the same to the virtual machines[8,9].

## 3. Security Issues & Threats in Cloud Virtual Machine

Understanding the security danger and protection in the cloud surrounding and creating productive and viable solutions for it is truly a troublesome assignment for the cloud administration provider[8]. Honesty, secrecy, unwavering quality and accessibility of assets are generally utilized phrasing for security issues as a part of a distributed computing environment implies that the client's information in the cloud ought to stay private and shielded from unapproved access[4,7,8,14]. In this way, the usage of the distributed computing design must be guaranteed about the security of its asset hubs. A risk in the virtualized environment is an outside power by which the current cloud hubs in one state move into another. A hub in the cloud surrounding provisions the information and data and provides the client a virtualized stage to utilize the application as administrations. There are critical quantities of assaults or interruptions happen in the cloud based applications[8]. Some surely understood assaults are SQL Injection Attack, Net Sniffers, Abuse and Nefarious utilization of Cloud Computing, Session Hijacking, Man in the Middle Attack, Denial of Services, and User to Root Attacks. Out of these number of security dangers some are defenseless against IaaS. Once in a while it might influence to the cloud virtual machines (VM). So an expectation model can help the cloud administration suppliers to screen the virtualized environment.

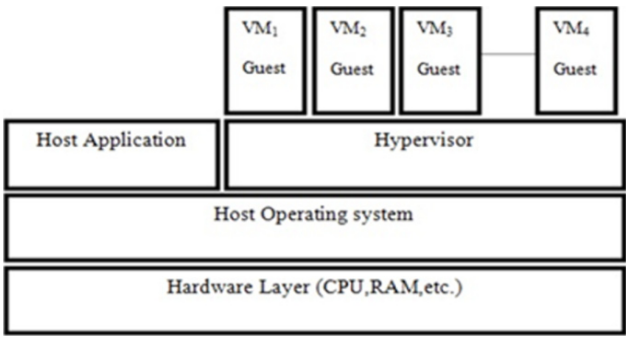



**Figure 1.** The architecture of virtual machine (VM)

## 4. Literature Review

In[15] proposed two scientific models to ponder the prey-predator framework in PC system. In the main model the creators sketched out the uninfected and contaminated hubs as prey and pernicious articles are predators. In the second sculpt vindictive articles shape the prey and against malevolent programming as the predator. Likewise, in[11] built up a stochastic model for transmission of malevolent items in the PC systems. In[12] introduced a scientific model alluded to the investigative worm proliferation (AAWP) model, which portrays the spread of worms that utilize irregular screening intriguing the idea of prey-predator epidemiological model. They contrasted the model and the weaver's test system and Epidemiological model talking the Red v2 worm and gave a quantitative investigation for observing, distinguishing and shielding against worm. PC infections and PC insusceptible frameworks are simply antecedents of an inevitable rich community of simulated network security life shapes that will live, bite the dust, coordinate and go after each other in the internet. In[13] creators examined a prey-predator framework, in which a few individuals from prey populaces and all predators are subjected to disease by parasites and determined conditions for

determination of all populaces. In[13] sketched out the intrusion of an inhabitant prey-predator or host parasites framework by another strain of parasites. It additionally contemplated the comparative phenomena.

## 5. The Methodology

This proposed work will minimize the dangers to the virtual machines in the cloud environment independent of the client's security and applications approach[4,8]. It will essentially guarantee the level of the sanctuary of virtual machines in a cloud situation which assists the cloud administration suppliers to take the snappy choices regarding the up degree of the counter assault estimations[4]. An assault is an outer power by which the Virtual machine (VM) accessible in one class moves into another classification. The susceptible Virtual machines are the VM those can be misused by the vindictive assaults. Some are non-vulnerable VM that are not abused by the vindictive assaults[4,7,8]. The assaulted VM is vulnerable machines on which assaults are done, yet they can't help in the spread of contamination. The Infectious VMs are the tainted VM and help in the proliferation of infection. Furthermore, some are non-infection VM are recuperated from the irresistible classification and having no contamination[6]. Figure-2 outlined the communication between the exposed VM and Infectious VM.

### 5.1 Some Basic Terminologies

$N$ = The maximum number of Virtual machines (VM) that can be present per instance in the cloud environment based upon a single cloud service provider.

$N_S$ = The total number of non vulnerable VM (un-exposed VM)

$N_0$ = The underlying no of VM that susceptible against assault, i.e. the prey

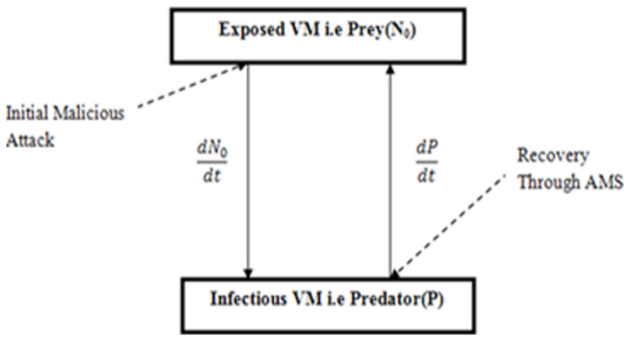



**Figure 2.** Predator-Prey Model for cloud based Network

$N_A$ = The number of assaulted VM in the cloud.

$P$ = The quantity of irresistible VM really seeking, i.e. the predator.

$A$ = The coefficient of threats, i.e. $N_A$ per P

$K$ = The greatest number of assaults that can be made per P amid the period $N_0$ is Vulnerable

$dP/dt$ = Growth rate of irresistible VM in cloud i.e. Predator

$dN_0/dt$ = Growth rate of irresistible VM in cloud i.e. Prey

### 5.2 The Mathematical Ontology

In general

- The maximum number of VM (N) present per in the cloud is a function of $N_S$ and $N_0$ so

$$N = f(N_S, N_0) \tag{1}$$

- The number of attacked VM is a function of $N_0$ and P so

$$N_A = f(N_0, P) \tag{2}$$

The equation-2 can be can be written as the partial differential equation of the from

$$\frac{\partial N_A}{\partial N_0} = f_1(N_{0,P}) \tag{3}$$

or

$$\frac{\partial N_A}{\partial P} = f_2(N_0, P) \tag{4}$$

But from the above two equation the equation-3 has more probability of getting the value of $N_0$ and P, as P is a part of $N_0$ virtual machines. If the predator P can generate a total PK number of attacks and $\frac{\partial N_A}{\partial N_0}$ diminishes gradually as $N_A$ approaches maximum[16,17]. Hence

$$\frac{\partial N_A}{\partial N_0} = PA(PK - N_A) \tag{5}$$

Where, A is the coefficient of threat i.e. $N_A$ per P. If the value of A is larger, then the value of $\frac{\partial A}{\partial P}$ will be larger. So it is very difficult for the Predator (P) to find the unattacked cloud VM. But if the value of P will increase than the value of $\frac{\partial A}{\partial P}$ must decrease in a inverse ratio to P due to the intra VM attack inside the cloud environment. The figure-3 appeared underneath is a case of intra VM assault where assault in VM1 mirrors to VM2 and VM3.

So

$$\frac{\partial A}{\partial P} = -b\frac{A}{P} \tag{6}$$

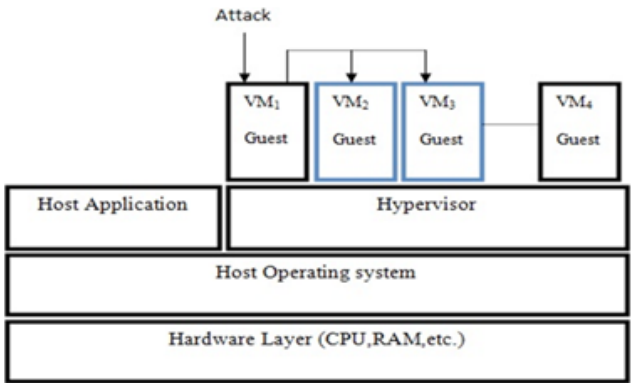



**Figure 3.** Intra Virtual machine attack

or

$$A = aP^{-b} \tag{7}$$

Where a and b are constant value.

Substituting the value of A from equation -7 in equation-5 we have

$$\frac{\partial N_A}{\partial N_0} = PaP^{-b}(PK - N_A) \tag{8}$$

$$\frac{\partial N_A}{PaP^{-b}(PK - N_A)} = \partial N_0$$

Or

$$\frac{\partial N_A}{(PK - N_A)} = \partial N_0 . PaP^{-b} \tag{9}$$

Now by integrating both side of equation-9

$$\int \frac{\partial N_A}{(PK - N_A)} = \int \partial N_0 . PaP^{-b}$$

Or

$$\int \frac{\partial N_A}{(PK - N_A)} = \int \partial N_0 . a . P^{(1-b)}$$

Or

$$\int a . P^{(1-b)} \partial N_0 = \int \frac{\partial N_A}{(PK - N_A)}$$

And finally therefore we have

$$a . P^{(1-b)} N_0 = -\ln\left(1 - \frac{N_A}{PK}\right) \tag{10}$$

$$\ln\left(1 - \frac{N_A}{PK}\right) = -a . P^{(1-b)} N_0$$

Or

$$1 - \frac{N_A}{PK} = e^{-a.P^{(1-b)}N_0}$$

So finally we obtained

$$N_A = PK(1 - e^{-a.N_0.P^{(1-b)}}) \tag{11}$$

So the number of attacked virtual Machines $N_A$ depends upon the value of $N_0$, P and K by taking value of a and b as constant values. Some assumptions for predator and prey are

- In the above equation – 11 the value of $N_A$ depends on P and $N_0$ with the value of K.
- The value of K can be variable subject to the value of $N_0$ and P or remain constant.
- If the value of K remain constant then depending on the value of a and b then the value of $N_A$, $N_0$, & P can be predicted easily.
- The number of attacked virtual machine $N_A$ should not be greater or exceed the vulnerable virtual machine $N_0$ i.e (Prey).
- The number of infections virtual machine P i.e. the predator should not exceed the number of $N_0$ and $N_A$.

Now to calculate P it is important to choose the value a, b. From the equation-11 as we observed for $N_A = Lim_{p\to\infty} f(N_0, P)$, and the values of a and b depending on the value of K.

If the value of a and b are

(a) a = 1 and b = 1 then $N_A \to \infty$

(b) a =2 and b = 2 then $N_A \to 2KN_0$

depart on the value of K.

(c) a > 2 and b > 2, then $N_A = 0$

In the above 3 cases, if the value of a and b are 1 and greater than 2 then it is very difficult to find the value of $N_0$, P. And If the value of a and b is 2 then

$$N_A = aKN_0 \tag{12}$$

So finally by putting the values for constant a=2 and b=2, the new value of $N_A$ is

$$N_A = PK(1 - e^{\frac{-2N_0}{P}}) \tag{13}$$

And by solving for $N_0$ from the above equation we get

$$N_0 = \frac{1}{2} P . Ln(PK - N_A) \tag{14}$$

So in a cloud based network EVM ($N_0$) can be reproduced by adding new nodes and the IVM(P) can be recovered by the help of Anti Malicious Software (7). Another aspect is here the predation which affects the EVM populations as shown in figure-4. In this situation the exposed virtual machines grow exponentially as shown in figure-5.

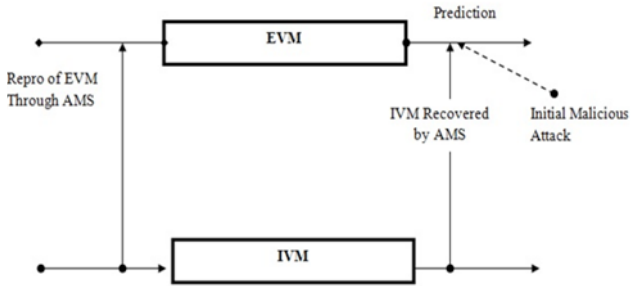



**Figure 4.** Model diagram of dynamics of single population i.e. EVM

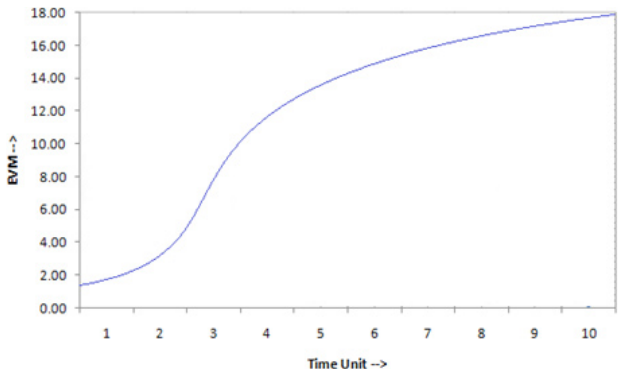



**Figure 5.** EVM grows exponentially

And by putting the new value of $N_0$ in $N_A$ in previous equation we have

$$N_A = PK - P^2K^2 + PK.N_A$$

Consequently

$$P^2K^2 - PK.N_A - PK + N_A = 0$$

$$P^2K^2 - PK(N_A + 1) + N_A = 0 \qquad (15)$$

Now the above equation is in the form of a quadratic equation, so we have to solve for the value of P.
And by solving for P we get

$$P = \left(\frac{N_A+1}{2K}\right) \pm \left(\frac{N_A-1}{2K}\right) \qquad (16)$$

Where P has two values $\frac{N_A}{K}$ and $\frac{1}{K}$

Hence the final acceptable value of P is $\frac{N_A}{K}$ as $N_A = f(N_0, P)$

This mirrors the suspicion that the IVM generation is corresponding to rate of predation on the EVM. For this situation the EVM and the IVM compartments cycle, with the EVM populace slamming as the IVM populace increments, trailed by an accident in the IVM populace as appeared by figure-6.

The values of P according to the value of K and $N_A$ are given in Table-1.

The value of K is the maximum numbers of threats that can be made per P during the period $N_0$ are susceptible. If the no of attacks per P will increase it is very difficult for the cloud service providers to detect the defect in the virtual machine based upon the behavior and predict the rate of infection in the cloud as shown in figure-7. This gives the values of P according to the values of K and $N_A$.

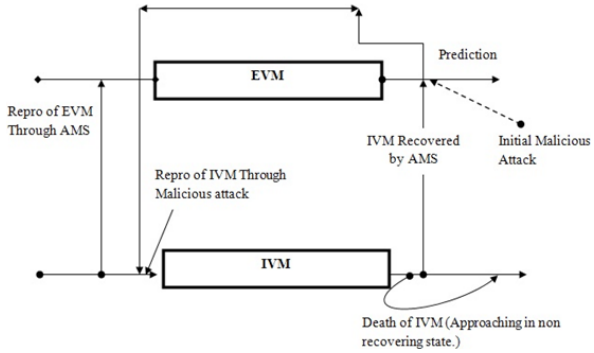


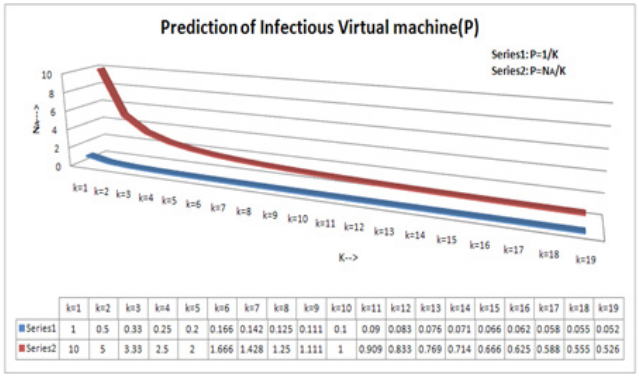

**Figure 6.** Model diagram of dynamics of both populations i.e. EVM($N_0$) and IVM(P)

**Table 1.** Prediction of P with K and $N_A$

| S.No | K | P=1/K | P=$N_AN_A$/K |
|---|---|---|---|
| VM1 | 1 | 1 | 10 |
| VM 2 | 2 | 0.5 | 5 |
| VM 3 | 3 | 0.33 | 3.33 |
| VM 4 | 4 | 0.25 | 2.5 |
| VM 5 | 5 | 0.2 | 2 |
| VM 6 | 6 | 0.166 | 1.666 |
| VM 7 | 7 | 0.142 | 1.428 |
| VM 8 | 8 | 0.125 | 1.25 |
| VM 9 | 9 | 0.111 | 1.111 |
| VM 10 | 10 | 0.1 | 1 |
| VM 11 | 11 | 0.09 | 0.909 |
| VM 12 | 12 | 0.0833 | 0.833 |
| VM 13 | 13 | 0.076 | 0.769 |
| VM 14 | 14 | 0.071 | 0.714 |
| VM 15 | 15 | 0.0666 | 0.666 |
| VM 16 | 16 | 0.0625 | 0.625 |
| VM 17 | 17 | 0.058 | 0.588 |
| VM 18 | 18 | 0.055 | 0.555 |
| VM 19 | 19 | 0.0526 | 0.526 |
| VM 20 | 20 | 0.05 | 0.5 |

**Table 2.** Values for listed parameters

| S. NO | Parameters | Explanation of equations | Equations |
|---|---|---|---|
| | A | The coefficient of attack i.e. $N_A$ per P | $A = aP^{-b}$ |
| | $N_0$ | Initial no of cloud VM vulnerable to attack i.e. the prey | $N_0 = \frac{1}{2} P.Ln(PK - N_A)$ |
| | $N_A$ | The number of attacked VM in the cloud | $N_A = PK - P^2K^2 + PK.N_A$ |
| | P | The number of infectious cloud VM actually searching i.e. the predator | $P = \frac{N_A}{K}$ |
| | $\frac{\partial P}{\partial N_0}$ | The rate of change of P with respect to $N_0$ | $\frac{\partial P}{\partial N_0} = \frac{KP - N_A}{\ln(KP - N_A)(KP - N_A) + KP}$ |




| | k=1 | k=2 | k=3 | k=4 | k=5 | k=6 | k=7 | k=8 | k=9 | k=10 | k=11 | k=12 | k=13 | k=14 | k=15 | k=16 | k=17 | k=18 | k=19 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Series1 | 1 | 0.5 | 0.33 | 0.25 | 0.2 | 0.166 | 0.142 | 0.125 | 0.111 | 0.1 | 0.09 | 0.083 | 0.076 | 0.071 | 0.066 | 0.062 | 0.058 | 0.055 | 0.052 |
| Series2 | 10 | 5 | 3.33 | 2.5 | 2 | 1.666 | 1.428 | 1.25 | 1.111 | 1 | 0.909 | 0.833 | 0.769 | 0.714 | 0.666 | 0.625 | 0.588 | 0.555 | 0.526 |

**Figure 7.** Prediction of P with K and $N_A$

If the value K is less then it is easier for the cloud service suppliers to detect the infection in the cloud. So it is important to minimize the value of K and $N_A$ as much as possible, to reduce the number of infectious virtual machines in the cloud as it is a trustworthy practice for cloud providers[18,19]. Therefore, the deployment of the cloud computing architecture must be guarantee about the security of its Virtual machines (VM).

So, the solution to the equations gives the values for listed parameters as shown in Table-2.

## 6. Conclusion and Future Work

This paper describes about the mathematical ontology based upon the attacked VMs and infectious VMs, which predicts the trustworthiness of the IaaS virtual platform. It also describes the cloud virtualization technology, the components of cloud virtualization and the security issues and threats to cloud VMs. The proposed work is to make the distributed computing design more immaculate which further be utilized to assembled a more secure and extensive systems. The work will assist the cloud administration suppliers to discover the convenience of VMs and the effect of Anti-Malicious Software (AMS) with its productivity in the cloud surroundings in order to expand the reliability. The mimicked results based upon the assaulted VMs and irresistible VMs will demonstrate the enhanced dependability in the cloud virtualization environment.

## 7. References

1. Hamdaqa M, Tahvildari L. Cloud Computing Uncovered: A Research Landscape. Advances in Computers. 2012; 86:41–85.
2. Moreno-Vozmediano R, S Montero R, M Llorente I. Key Challenges in Cloud Computing -Enabling the Future Internet of Services. IEEE Internet Computing. 2012; 17(4):18–25.
3. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. 2012; 28(3):583–92.
4. Dash SB, Saini H, Panda TC, Mishra A. Service Level Agreement Assurance in Cloud Computing: A Trust Issue. International Journal of Computer Science and Information Technologies. 2014; 5(3):2899–906.
5. Prasad MR, Naik RL, Bapuji V. Cloud Computing: Research Issues and Implications. International Journal of Cloud Computing and Services Science. 2013; 2(2):134–40.
6. Francesco MA, Gianni F. An approach to a cloud computing network. Czech Republic: Proceedings of First International Conference on the Applications of Digital Information and Web Technologies. 2008; p. 113–18.

7. Dash SB, Saini H, Panda TC, Mishra A. Prediction of Trustworthiness in the Cloud Computing Environment using Predator-Prey Model. International Journal of Cloud Computing and Services Science. 2013; 2(5):336–44.
8. Dash SB, Saini H, Panda TC, Mishra A. A Theoretical Aspect of Cloud Computing Service Models and Its Security Issues: A Paradigm. Journal of Engineering Research and Applications. 2014; 4(6):248–54.
9. Li Y, Li W, Jiang C. A Survey of Virtual Machine System: Current Technology and Future Trends. Guangzhou, China: Proceedings of Third International Symposium on Electronic Commerce and Security. 2010; p. 332–36.
10. Mansukhani B, Zia TA. The Security Challenges and Countermeasures of Virtual Cloud. Perth, Australia: Proceedings of the 10th Australian Information Security Management Conference. 2012; p. 51–8.
11. Saini H, Dinesh Saini D. VAIN: A Stochastic Model for Dynamics of Malicious Objects. ICFAI University Journal of Systems Management. 2008; 6(1):14–28.
12. Chen Z, Gao L, Kwiat K. Modeling the Spread of Active Worms. USA: Proceedings of INFOCOM: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. 2003; 3:1890–1900.
13. Hadeler KP, Freedman HI. Predator-prey populations with parasitic infection. Journal of Mathematical Biology. 1989; 27:609–31.
14. Tianfield H. Cloud Computing Architectures. USA: Proceedings of 2011 IEEE International Conference on Systems, Man, and Cybernetics. 2011; p. 1394–99.
15. Xiaoping X, Junhu Y. Research on Cloud Computing Security Platform. China: Proceedings of 2012 Fourth International Conference on Computational and Information Sciences. 2012; p.799–802.
16. Grobauer B, Siemens, Walloschek T, Stocker E. Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy. 2011; 9(2):50–7.
17. Takabi H, James BD, Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy. 2010; 8(6):24–31.
18. Mishra BK, Ansari GM. Predator-Prey Model for the attack of Malicious objects in computer network. Journal of Engineering and Applied Science. 2009; 4(3):215–20.
19. Xiao Z, Xiao Y. Security and Privacy in Cloud Computing. IEEE Communications Surveys & Tutorials. 2013; 15(2):843–59.