Asian Journal of Information Technology 14 (3): 84-91, 2015
ISSN: 1682-3915

Predator-Prey Model for Infectious Virtual Machines in IaaS Cloud Environment Based on Lakota-Volterra Equation

[1]S.B. Dash, [2]H. Saini, [1]T.C. Panda and [3]A. Mishra
[1]Department of Information Technology,
Orissa Engineering College, 752050 Bhubaneswar, India
[2]Department of Computer Science and Engineering,
Jaypee University of Information Technology, 173234 Solan, India
[3]Department of Mathematics, CUT&M, 761211 Paralakhemundi, India

Abstract: Infrastructure as a Service (IaaS) is an innovative and one of the significantly achieved developments in the cloud computing environment. Providing security to the cloud virtual machines and users' data are the greatest challenge of information system. So, understanding the risks of the security and privacy in the cloud and developing efficient and effective solutions for it is really a difficult task. This manuscript describes about the mathematical ontology and a new model based on the Lakota-Volterra equation known as Predator-Prey Model which predicts the trustworthiness of the IaaS virtual platform. The proposed research would minimize the threats to the virtual machines in the cloud environment irrespective of the user's applications and security policy. It will basically ensure the degree of the security of virtual machines in a cloud environment which helps the cloud service providers to take the quick decisions and about the up gradation of the counter attack measurements.

Key words: Cloud virtualization security, Lakota-Volterra equation, Predator-Prey Model, measurement, challenge, mathematical ontology

INTRODUCTION

Cloud computing is a distributed computing environment that provides a virtualized environment to the cloud users for accessing and exchanging their applications and data through internet. According to National Institute of Standards and Technology (NIST), one of the most accepted definition of cloud computing is "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". 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" (Hamdaqa and Tahvildari, 2012; Moreno-Vozmediano *et al*., 2013; Zissis and Lekkas, 2012). The cloud service provider provides the services to the registered cloud users on payment basic across the glove. The cloud services are basically categorized as SaaS, PaaS and IaaS. The services are available to the users depending on cloud deployment and the SLA (Service Level Agreements) between the service providers and the cloud users (Dash *et al*., 2014a, b; Prasad *et al*., 2013; Aymerich *et al*., 2008). 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 dynamically to build up the ad hoc systems. A Virtual Machine (VM) is a dedicate software environment which runs operating systems and applications in the guest machine to help users application execution (Dash *et al*., 2014a; Saini *et al*., 2013; Li *et al*., 2010). So, VMs are logical machines having almost the same architecture as a real host machine, running an operating system in it. The architecture of Virtual Machine (VM) system is shown in Fig. 1. According to the cloud architecture, multiple Virtual Machines (VMs) share the same physical machine.

In the present manuscript, it is achieved by the help of Predator-Prey Model (Mell, 2012; Moghadam, 2013; Ashktorab and Taghizadeh, 2012; Jing and Jian-Jun, 2010;

Corresponding Author: S.B. Dash, Department of Information Technology, Orissa Engineering College, 752050 Bhubaneswar, India

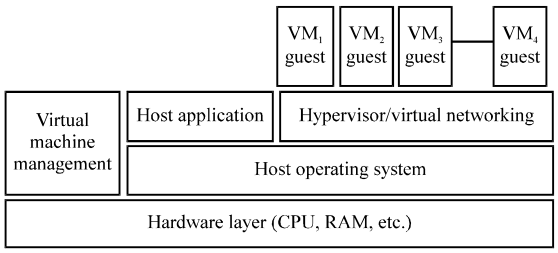

Fig. 1: The architecture of Virtual Machine (VM)

Shaikh and Haider, 2011). A small predator population in the midst of plentiful prey eventually outgrows its food source which eventually contracts by being eaten, the two populations cycling through boom and bust, 90 degrees out of phase with each other.

The details of this model are worth exploring. The prey is assumed to enjoy an unlimited food supply and will grow at a rate proportional to its population, less a rate at which it gets eaten. The rate at which it gets eaten is assumed proportional to both its own population and the predators' population. The predator dies at a rate proportional to its population, unless it is fed in which case we add a growth rate proportional to both its population and the population of prey.

The Predator-Prey Model can be understood by considering the growth of rabbits in the present of foxes in the jungle. If there is an infinite food supply, the rabbits would live happily and experience exponential growth. On the other hand, if the foxes were left with no prey to eat, they would die faster than they could produce and would experience exponential population decline. A similar analogy to the Predator-Prey Model can be used to predict the growth of a malicious attack in the cloud based networks

CLOUD VIRTULAZATION COMPONENTS

Hypervisor layer: Hypervisor is the abstraction layer that provides the necessary resource to share hardware resources between the virtual machines. Hypervisor layers have two main models: para virtualization such as Xen and Hyper-V and the other model is full virtualization such as VMW are. Often these two models trade-off a level of isolation to increase the sharing of resources among VMs (Li *et al*., 2010).

vSwitch or virtual network layer: This layer is responsible for multiplexing traffic between virtual NIC (Network Interface Card) and physical NIC (Network Interface Card). The vSwitch also controls the VM traffic of a single host that does not touch the physical NIC of the host and vSwitch manages the customer trust zone. The virtual network also acts like a physical switch in non-virtualized environments (Li *et al*., 2010; Mansukhani and Zia, 2012).

Virtual machines: VM's is a software layer that emulates the real physical machine, these VMs run under the control of hypervisor layer that further virtualizes and emulates the hardware resources and returns the same to the virtual machines (Li *et al*., 2010).

SECURITY ISSUES IN CLOUD VIRTUAL MACHINE

The security issues in cloud computing environment are greatest challenge of information system. Understanding the risks of the security and privacy in the cloud and developing efficient and effective solutions for it is really a difficult task. Confidentiality, integrity, reliability and availability are widely used terminology for security issues in cloud computing environment means that the user's data in the cloud should remain confidential and protected from unauthorized access (Grobauer *et al*., 2011). So, the implementation of the cloud computing architecture must be ensured about the security of its resource nodes. Some of the security issues occur in cloud computing are listed here (Dash *et al*., 2014b; Tianfield, 2011; Xu and Yan, 2012; Grobauer *et al*., 2011; Takabi *et al*., 2010; Xiao and Xiao, 2013; Mell, 2012).

Cloud security: This includes organizational and technical issues related to keeping cloud services at an acceptable level of security by ensuring the computing resources (virtual machines) available and usable by its authentic users. Security threats to cloud infrastructure would affect multiple users even if only one site is attacked (Takabi *et al*., 2010). These risks can be overcome by using encrypted file systems, security applications, data loss software and buying security hardware.

Privacy in cloud: Privacy is the process of making sure that the user's data remains private, confidential and restricted from unauthorized users. Due to data virtualization the users data may be stored in various virtual data centres rather than in the local computers. So, the unauthorized users may access the private information of the authorized users. Data authentication is one of the most popular options of security before putting the sensitive data into cloud (Takabi *et al*., 2010).

Data integrity and reliability: In cloud computing, anyone from any location can access the data. Cloud does not differentiate between common data and sensitive data. So, an important aspect of cloud services is availability of user's data with reliability. It is necessary for the cloud service provider to ensure the integrity by making their system capable to check over the cloud data from any unauthorized access.

Performance and bandwidth cost: The major issues that can affect performance in cloud based environment is due to the unethical transaction-oriented and data access applications. So, the users who are at a long distance from cloud providers may experience high latency and delay, this is due to the availability bandwidth in the network. Bandwidth cost may be low for smaller internet-based applications which are not data intensive but could significantly, grow for data-intensive applications. The service providers instead of saving money on hardware, they should spend more for the bandwidth. This can deliver intensive and complex application over the network.

SECURITY THREATS IN CLOUD VIRTUAL MACHINE

A threat is define as an external force by which the nodes existing in one state transfers into other. A node in the cloud environment stores the data and information and gives the user a virtualized platform to use the application in the form of services. There are significant numbers of attacks or intrusions occurs in the cloud based applications. Some well known attacks are listed below (Dash *et al*., 2014b; Che *et al*., 2011; Hyde, 2009; Moghadam, 2013; Ashktorab and Taghizadeh, 2012; Jing and Jian-Jun, 2010).

SQL injection attack: An SQL injection is a computer attack mostly affects to SaaS Model in which malicious code is embedded with a poorly-designed application, executes unauthorized SQL commands by taking advantage of insecure interface connected through internet (Takabi *et al*., 2010). SQL injection attacks are used to access information from databases which is protected from public access. SQL injection attacks are avoided by ensuring systems having strong input validation.

Abuse and nefarious use of cloud computing: In this threat, the hackers take the advantages of shortcomings in the authentic registration process associated with cloud. After the successful registration, the cloud service providers offer SaaS, IaaS and PaaS services to the users. But hackers may be able to conduct susceptible activities like Spamming and Phishing. This threat exists in all the three layers of the service models.

Net sniffers: Net sniffer is a type SaaS Service Model threat in which the attackers use to gain access through applications which can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted. Then, data can be publicly available and read by any one.

Session hijacking: Session hijacking is a security attack on a user session over a protected network. When a user logs into a website, a session is created on that web server for that user, this session contains all user's information being used by the server so the username and password is not required at every page request. So, hackers having adequate knowledge can exploits a valid computer session and gains access to a user's session identifiers through HTTP. The web server uses a unique identifier (session identifier) to authenticate the users for the session. The hackers by using session hijacking attack unethically gets the user's session identifier and then gain the illegal access to the user data. The most common session hijacking attacks are session prediction, session side jacking, session fixation, cross site scripting and available in SaaS and PaaS.

Man in the middle attack: Another type of session hijacking is known as a man in the middle attack. Where, the attacker uses a sniffer to observe the communication between devices and collect the data that is transmitted. In this the attackers make independent connections with the victim's computer and making them believe that they are connected directly to each other over a private connection. But in fact the entire session is controlled by the attackers. This is a threat to SaaS.

Denial of services: A Denial of services is a attack in the SaaS layer that attempts to make the network resource and services actually assigned to the authorized users virtually unavailable. As it acts as an interrupt or suspend of services for authorized users temporarily or indefinitely.

User to root attacks: In this type of attack, an intruder seizes the account and password information of an authorized user and he can acquire limitless access to the whole system. Buffer overflows are used for establish

console connection for authorized processes. This type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity and the information is captured by intruders from this overflowed data. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines.

Flooding attacks: Flooding is a Denial of service attack that is designed to increase network conjunctions by flooding it with huge amount of traffic. Flooding attacks occur when a network or service becomes so weighed with packets contains data. It attacks a server or host with connections that cannot be completed and finally fills the host memory buffer with unused and redundant data. Once the buffer is full no further connections can be made. So, the result is a denial of service. It is available in PaaS and IaaS layer of cloud service model.

Privacy breach: Since, data from various users and business organizations available together in a cloud environment, so breaching in cloud environment will attack the data of the authorized users. Hence, the unauthorized users can access the private data of the cloud users and do some susceptible activities with the data. This will affect mostly the SaaS users (Shaikh and Haider, 2011; Sato *et al*., 2010; Vouk, 2008).

Out of these number of security threats some are vulnerable to IaaS. Sometimes it may affect to the cloud Virtual Machines (VM). So, a prediction model can help the cloud service providers to monitor the virtualized environment.

THE PREDICTION MODEL

An attack is an external force by which the Virtual Machines (VM) existing in one category transfers into other category. The vulnerable virtual machines are the VM those can be exploited by the malicious attacks. Some are non-vulnerable VM that are not exploited by the malicious attacks. The attacked VM are vulnerable machines on which attacks are carried out but still they cannot help in propagation of infection. The infectious VMs are the infected VM and help in propagation of infection. And some are non-infectious VM are recovered from the infectious category and having no infection (Aymerich *et al*., 2008).

THE PREYDATOR-PREY MODEL

The Predator-Prey Model can be understood by considering the growth of rabbits in the present of foxes in the jungle. If there is an infinite food supply, the rabbits would live happily and experience exponential growth. On the other hand, if the foxes were left with no prey to eat, they would die faster than they could produce and would experience exponential population decline. A similar analogy to the Predator-Prey Model can be used to predict the growth of a malicious attack in the cloud based networks (Chapman *et al*., 2011; Gorman *et al*., 2004; Cull, 1981; Murray, 1989; Wu and Wang, 2011).

Initially, in the virtual machines there are very few infections and hence recovery rate will be less. Gradually, the infections increased and hence the recovery rate will be increased. After some time an equilibrium state will be achieved in between recovery rate and infections by malicious attacks in the cloud network.

In the present scenario, prey is Exposed Virtual Machines (EVM) in cloud and predator is Infectious Virtual Machines (IVM) in cloud. Hence, in the text the Predator-Prey Model states that:

- EVM rises to a constant number of amounts per unit of time as new nodes are added to the network. In other words, there are no other factors limiting EVM population growth apart from predation
- Each IVM infects a constant proportion of the EVM population per unit of time. In other words, doubling the EVM population will double the number infected per IVM, regardless of how big the EVM population is
- IVM reproduction is directly proportional to EVM consumed; another way of expressing this is that a certain number of EVM consumed results in new IVMs
- A constant proportion of the IVM population dies per unit of time. In other words, the IVM death rate (approaching to non-recoverable state) is independent of the recoverable process as there are other means like hardware failure or power failure (Cull, 1981; Murray, 1989; Wu and Wang, 2011)

Above mentioned situation (Fig. 2) (Saini *et al*., 2013) can be better represented by Lokta-Volterra equations also known as the Predator-Prey equations. They evolve in time according to the following pair of equations:

$$\frac{dP}{dt} = P(\alpha - \beta N_0) \quad (1)$$

$$\frac{dN_0}{dt} = -N_0(\gamma - \delta P) \quad (2)$$

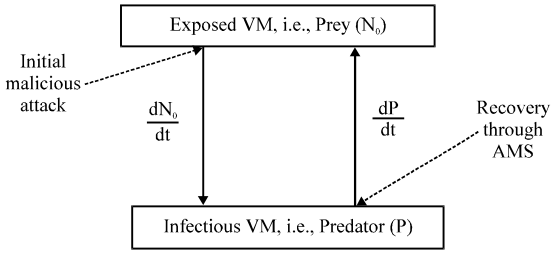

Fig. 2: Predator-Prey Model for cloud based network

Where:

N_0 = The number of number of prey, i.e., exposed VM in cloud to the malicious attacks
P = The number of some predator, i.e., infected VM in cloud which are ready to spread the infection to other healthy VM
dP/dt = The growth rate of the infected VM
dN_0/dt = The growth rate of the exposed VM
α = A coefficient of intraspecific competition
β = Per-capita rate of predation of the predator
γ = Death rate of predator
δ = The product of the per-capita rate of predation and the rate of conversing exposed VM into infectious VM

Equation 1 and 2 can also be written as follows:

$$\frac{dP}{dt} = -\left(\frac{1-N_0}{\mu_2}\right)P \quad (3)$$

$$\frac{dN_0}{dt} = -\left(\frac{1-P}{\mu_1}\right)N_0 \quad (4)$$

In Eq. 4, the extra minus sign distinguishes the predators from the prey. Note if P is zero, then:

$$\frac{dN_0}{dt} = -N_0 \quad (5)$$

and the predators are in trouble. But, if N_0 ever become zero then:

$$\frac{dP}{dt} = P \quad (6)$$

and the prey population grows exponentially.

MODELLING OF DYNAMICS OF SINGLE POPULATION I.E. EXPOSED VIRTUAL MACHINES (EVM) IN CLOUD

In a cloud based network EVM can be reproduced by adding new nodes and the IVM can be recovered by the help of Anti Malicious Software (AMS). Another aspect is here the predation which affects the EVM populations as shown in Fig. 3. In this situation, the exposed virtual machines grow exponentially as shown in Fig. 4 (Saini *et al*., 2013).

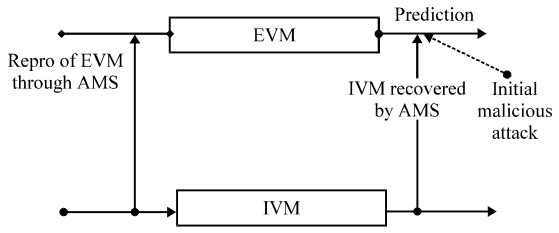

Fig. 3: Model diagram of dynamics of single population, i.e., EVM

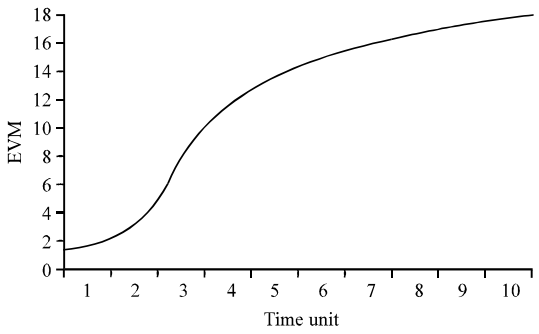

Fig. 4: EVM grows exponentially

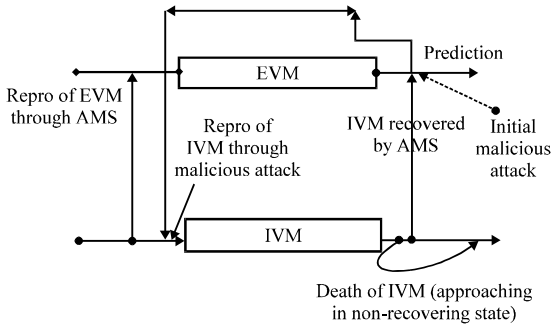

Fig. 5: Model diagram of dynamics of both populations, i.e., EVM and IVM

MODELING OF DYNAMICS OF BOTH POPULATIONS I.E. EXPOSED VIRTUAL MACHINES (EVM) IN CLOUD AND INFECTIOUS VIRTUAL MACHINES (IVM)

This reflects the assumption that the IVM reproduction is proportional to rate of predation on the EVM as depicted by Fig. 5 (Saini *et al*., 2013). In this case,

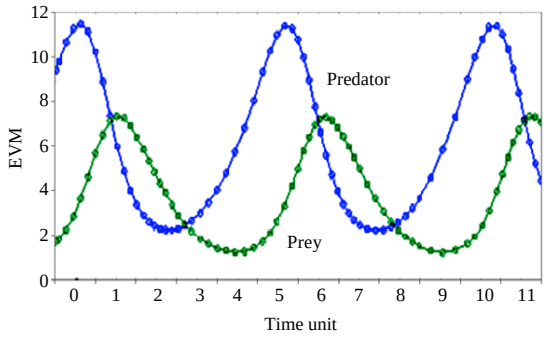

Fig. 6: EVM population crashing as the IVM population increases followed by a crash in the IVM population (Saini *et al*., 2013)

the EVM and the IVM compartments cycle with the EVM population crashing as the IVM population increases, followed by a crash in the IVM population as shown in Fig. 6.

EXPLANATORY POINTS

The Lotka-Volterra Model for cyber attacks and defense consists of a system of linked differential equations that cannot be separated from each other and that cannot be solved in closed form (Saini *et al*., 2013). Nevertheless, there are a few things those can help to understand the model as follows:

Explanatory point 1: A Lotka-Volterra Predator-Prey Model is described by:

$$\frac{dP}{dt} = 0.2P-0.0025P.N_0$$

$$\frac{dN_0}{dt} = 0.1N_0+0.002P.N_0$$

where, P and N_0 are the populations of exposed VM and infectious VM in the cloud environment, respectively at time t. In this scenario, the equilibrium points of the system can be located and classified by the point (0, 0) as the saddle point with the point (50, 80) as centre.

Explanatory point 2: Assume that populations of infectious VM and exposed VM. An AMS recovers some fraction of malicious attacks (per unit time) is used to control the infection. This system is modelled by the equations:

$$\frac{dP}{dt} = a.P-b.P.N_0-e.P$$

$$\frac{dN_0}{dt} = -c.N_0+d.P.N_0-f.N_0$$

where, e and f are the respective rates at which the infectious VM recovered by AMS and exposed VM decreased due to external reasons like data crashed and be in non-recoverable state. In the mentioned scenario, the non-zero equilibrium point in the first quadrant, i.e. (c+f/d, a-e).

Explanatory point 3: Under the harvesting conditions (i.e., values of e and f) f>0 and 0<e<a the equilibrium stock of prey, i.e., exposed VM will increase whilst the equilibrium stock of predators, i.e., infectious VM will decreases.

Explanatory point 4: It can be shown that the average level of each population over one cycle equals its equilibrium value. The effect of the use of an anti malicious software which recovers the predators, i.e., the infectious VM by the statements that the equilibrium number of exposed VM will decrease whilst equilibrium number of infectious VM remains unchanged in the cloud (since f = 0).

NUMERICAL SIMULATIONS

Let exposed virtual machine (prey) and infectious virtual machine (predator) are there in the cloud based networks. If the initial conditions are 80 exposed VM and 40 infectious VM at some instances, one can plot the progression of the two types of VM over time as shown in Fig. 7. The choice of time interval is arbitrary.

One can also plot a solution which corresponds to the oscillatory nature of the population of the two types of the VM as depicted in Fig. 8. This solution is in a state of dynamic equilibrium. At any given time in this phase plane, the system is in a limit cycle and lies somewhere on the inside of these elliptical solutions. There is no particular requirement on the system to begin within a limit cycle and thus in a stable solution but it will always reach one eventually (Wu and Wang, 2011; Batiha *et al*., 2007; Elliott, 2010; Ouedraogo *et al*., 2002).

These graphs clearly illustrate that in each cycle, the population of exposed VM is reduced to extremely low numbers yet recovers (while the population of infectious VM remains sizeable at the lowest density of exposed VM). So, the numbers of non-infectious VM in the cloud will increase.

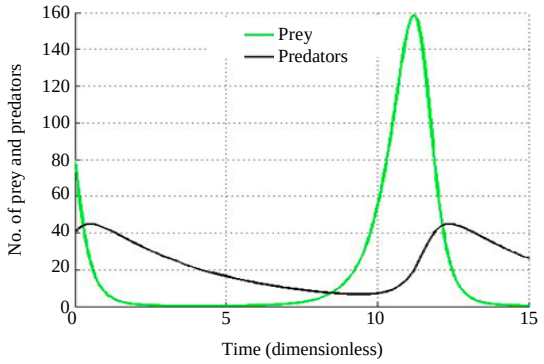

Fig. 7: Exposed VM and infectious VM with respect to time where, initially 80 exposed VM and 40 infectious VM in cloud network (Saini *et al*., 2013)

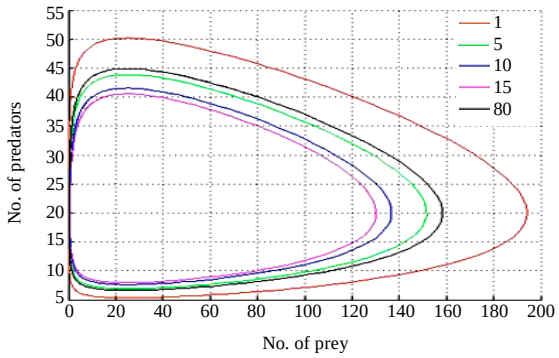

Fig. 8: The oscillatory nature of the population of the two types of VM in the cloud (Saini *et al*., 2013)

CONCLUSION

This study describes about the mathematical ontology and a new model based on the Lakota-Volterra equation known as Predator-Prey Model which predicts the trustworthiness of the virtual machine system. It also describes the cloud virtualization technology, the components of cloud virtualization and the security issues and threats to cloud virtual machines. The Predator-Prey Model for computing the proportion of the Exposed Virtual Machines (EVM) and Infectious Virtual Machines (IVM) to check the trustworthiness in the cloud virtualization environment is established. Our proposed model is to make the cloud computing architecture perfect and built a more comprehensive network. The proposed research will help the cloud service providers to find out the utility of Virtual Machines (VM) and the impact of Anti Malicious Software (AMS) with its efficiency in the cloud environment so as to increase the trustworthiness.

NOMENCLATURE

N_0 = The initial no of VM that vulnerable to attack, i.e., the prey
N_A = The number of attacked VM in the cloud
P = The number of infectious VM actually searching, i.e., the predator
A = The coefficient of attack, i.e., N_A per P
K = The maximum number of attacks that can be made per P during the period N_0 are vulnerable
α = Coefficient of intraspecific competition
β = Per-capita rate of predation of the predator
γ = Death rate of predator
δ = The product of the per-capita rate of predation and the rate of conversing vulnerable VM into infectious VM
μ_1 = γ/δ
μ_2 = α/β
dP/dt = Growth rate of infectious VM in cloud, i.e., predator
dN_0/dt = Growth rate of vulnerable VM in cloud, i.e., prey

REFERENCES

Ashktorab, V. and S.R. Taghizadeh, 2012. Security threats and countermeasures in cloud computing. Int. J. Applic. Innov. Eng. Manage., 1: 234-245.

Aymerich, F.M., G. Fenu and S. Surcis, 2008. An approach to a cloud computing network. Proceedings of the 1st International Conference on the Applications of Digital Information and Web Technologies, August 4-6, 2008, Ostrava, Czech Republic, pp: 113-118.

Batiha, B., M.S.M. Noorani and I. Hashim, 2007. Variational iteration method for solving multispecies Lotka-Volterra equations. Comput. Math. Applic., 54: 903-909.

Chapman, I.M., S.P. Leblanc and A. Partington, 2011. Taxonomy of cyber attacks and simulation of their effects. Proceedings of the Military Modeling and Simulation Symposium, April 3-7, 2011, Boston, MA., USA., pp: 73-80.

Che, J., Y. Duan, T. Zhang and J. Fan, 2011. Study on the security models and strategies of cloud computing. Procedia Eng., 23: 586-593.

Cull, P., 1981. Global stability of population models. Bull. Math. Biol., 43: 47-58.

Dash, S.B., H. Saini, T.C. Panda and A. Mishra, 2014a. A theoretical aspect of cloud computing service models and its security issues: A paradigm. J. Eng. Res. Applic., 4: 248-254.

Dash, S.B., H. Saini, T.C. Panda and A. Mishra, 2014b. Service level agreement assurance in cloud computing: A trust issue. Int. J. Comput. Sci. Inform. Technol., 5: 2899-2906.

Elliott, C., 2010. Botnets: To what extent are they a threat to information security? Inform. Secur. Tech. Rep., 15: 79-103.

Gorman, S.P., R.G. Kulkarni, L.A. Schintler and R.R. Stough, 2004. A predator prey approach to the network structure of cyberspace. Proceedings of the Winter International Synposium on Information and Communication Technologies, January 5-8, 2004, Cancun, Mexico, pp: 1-6.

Grobauer, B., T. Walloschek and E. Stocker, 2011. Understanding cloud computing vulnerabilities. IEEE Secur. Privacy, 9: 50-57.

Hamdaqa, M. and L. Tahvildari, 2012. Cloud Computing Uncovered: A Research Landscape. In: Advances in Computers, Volume 86, Hurson, A. and A. Memon (Eds.). Chapter 2, Academic Press, Oxford, UK., ISBN-13: 9780123965356, pp: 41-85.

Hyde, D., 2009. A survey on the security of virtual machines. http://www.cs.wustl.edu/~jain/cse571-09/ftp/vmsec.pdf.

Jing, X. and Z. Jian-Jun, 2010. A brief survey on the security model of cloud computing. Proceedings of the 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, August 10-12, 2010, Hong Kong, pp: 475 478.

Li, Y., W. Li and C. Jiang, 2010. A survey of virtual machine system: Current technology and future trends. Proceedings of the 3rd International Symposium on Electronic Commerce and Security, July 29-31, 2010, Guangzhou, China, pp: 332-336.

Mansukhani, B. and T.A. Zia, 2012. The security challenges and countermeasures of virtual cloud. Proceedings of the 10th Australian Information Security Management Conference, December 3-5, 2012, Perth, Western Australia, pp: 51-58.

Mell, P., 2012. What's special about cloud security? IT Prof., 14: 6-8.

Moghadam, S.S., 2013. A survey of virtualization security. Int. J. Scient. Eng. Res., 4: 1533-1536.

Moreno-Vozmediano, R., R.S. Montero and I.M. Llorente, 2013. Key challenges in cloud computing: Enabling the future internet of services. IEEE Internet Comput., 17: 18-25.

Murray, J.M., 1989. Mathematical Biology. 2nd Edn., Springer-Verlag, Berlin, Germany, ISBN-13: 9780387194608, Pages: 767.

Ouedraogo, M., D. Khadraoui, H. Mouratidis and E. Dubois, 2002. Appraisal and reporting of security assurance at operational systems level. J. Syst. Software, 85: 193-208.

Prasad, M.R., R.L. Naik and V. Bapuji, 2013. Cloud computing: Research issues and implications. Int. J. Cloud Comput. Serv. Sci., 2: 134-140.

Saini, H., S.B. Dash, T.C. Panda and A. Mishra, 2013. Prediction of trustworthiness in the cloud computing environment using predator-prey model. Int. J. Cloud Comput. Serv. Sci., 2: 336-344.

Sato, H., A. Kanai and S. Tanimoto, 2010. A cloud trust model in a security aware cloud. Proceedings of the 10th IEEE/IPSJ International Symposium on Applications and the Internet, July 19-23, 2010, Seoul, South Korea, pp: 121-124.

Shaikh, F.B. and S. Haider, 2011. Security threats in cloud computing. Proceedings of the International Conference on Internet Technology and Secured Transactions, December 11-14, 2011, Abu Dhabi, pp: 214-219.

Takabi, H., J.B. Joshi and G.J. Ahn, 2010. Security and privacy challenges in cloud computing environments. IEEE Secur. Privacy, 8: 24-31.

Tianfield, H., 2011. Cloud computing architectures. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, October 9-12, 2011, Anchorage, AK., USA., pp: 1394-1399.

Vouk, M.A., 2008. Cloud computing-issues, research and implementations. J. Comput. Inform. Technol., 16: 235-246.

Wu, L. and Y. Wang, 2011. Estimation the parameters of Lotka-Volterra model based on grey direct modelling method and its application. Expert Syst. Applic., 38: 6412-6416.

Xiao, Z. and Y. Xiao, 2013. Security and privacy in cloud computing. IEEE Commun. Surv. Tutorials, 15: 843-859.

Xu, X and J. Yan, 2012. Research on cloud computing security platform. Proceedings of the 4th International Conference on Computational and Information Sciences, August 17-19, 2012, Chongqing, China, pp: 799-802.

Zissis, D. and D. Lekkas, 2012. Addressing cloud computing security issues. Future Gener. Comput. Syst., 28: 583-592.