International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.2, No.5, October 2013, pp. 337~346
ISSN: 2089-3337

Prediction of Trustworthiness in the Cloud Computing Environment using Predator-Prey Model

S.B.Dash*, H.Saini **, T.C.Panda*, A.Mishra***
* Department of Information Technology, Orissa Engineering College, Bhubaneswar-752050
** Department of Computer Science & engineering, Jaypee University of Information Technology, Solan-173234
***Department of Mathematics, CUT&M, Paralakhemundi-761211

Article Info

Article history:

Received Aug 18th, 2013
Revised Sep 20th, 2013
Accepted Oct 10th, 2013

Keyword:

Predator-Prey Model
Malicious objects
Trustworthiness
Cloud Computing

ABSTRACT

In recent years cloud computing is one of the significantly achieved development in the IT industry. Most of the companies are running their applications in the cloud due to the rapid advancement in communication network. Cloud computing is a distributed computing environment that enables the users to access and exchange their resources (applications and data) remotely and provides services to use the remote hardware and software within a network, without the knowledge of technological infrastructure. It gives a platform to use the application in the form of services which is more scalable, reliable, high performance and relatively low cost as compared to other distributed computing infrastructures. Therefore, the cloud computing is a greatest challenge of information system, but the main challenge in the cloud computing is the data security and protection to the users. Therefore, the implementation of the cloud computing architecture must be ensured about the security of its resource nodes. This manuscript describes about a new model based on the Lakota-volterra equation known as Predator-Prey Model which predicts the trustworthiness of the cloud. It will basically ensure the degree of the security of resource nodes in a cloud environment which helps to take the decisions about the upgrade of the counter attack measurements.

Corresponding Author:

Second Author,
Departement of Computer Science & Engineering,
Jaypee University of Information Technology,
Waknaghat, Solan-173234.
Email: hemraj1977@yahoo.co.in, hemraj.saini@juit.ac.in

1. INTRODUCTION

Understanding the risks of the security and privacy in the cloud computing environment [1, 2, 3] and developing efficient and effective solutions for it is really a difficult task. Confidentiality, integrity 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. But attackers/ hackers are often breaking the security barriers and use network node or network traffic to access the confidential data [4, 5, 6]. They use various types of attacks to exploit vulnerabilities in the network. Therefore, it is important to predict and detect the malicious activities.

Cloud-based network as depicted in figure-1 is one of the most popular networks in the present society. It requires an Internet connection and work over any physical infrastructure with numbers of computer nodes. In simple words cloud computing can be defined as a distributed computing environment that enables the users to access and exchange their resources (applications and data) remotely and provides services to use the remote hardware and software within a network without the knowledge of technological infrastructure[7, 8].

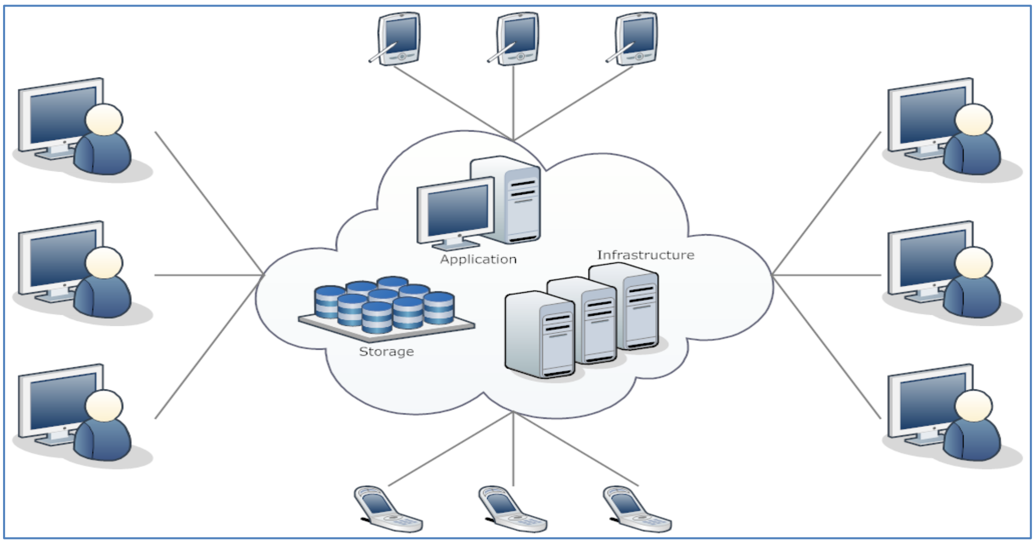

Figure 1. Cloud environment.

Cloud computing can be implemented by the concepts of public clouds, private clouds, and hybrid clouds. The data in the cloud nodes is stored based on the cloud deployment models i.e. public clouds, private clouds and hybrid clouds and cloud service models shown in figure-2 such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [9, 10, 11].

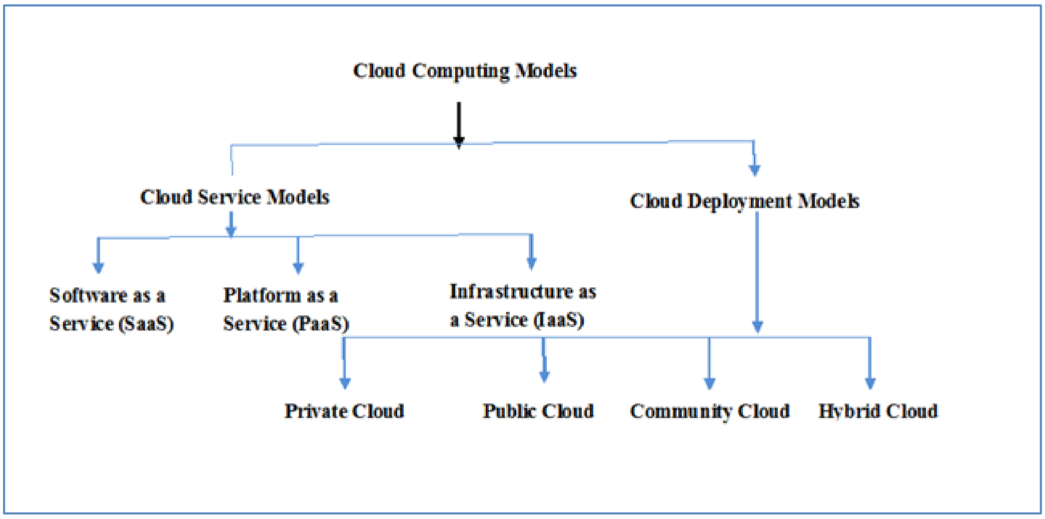

Figure 2. cloud computing models.

A node in the cloud environment stores the data and information and gives the user a platform to use the application in the form of services. Therefore, there is a significant possibility of intrusions or attacks to occur in the cloud based applications.

An attack is define as an external force by which the nodes existing in one state transfers into other. Based on the attacks in the cloud environment the nodes are classified in different types.Vulnerable/exposed nodes are the nodes those can be exploited by the malicious attacks. Some vulnerable nodes on which attacks are carried out but still they cannot help in propagation of infection are called attacked nodes. Some of them are the infected nodes and help in propagation of infection known as infectious nodes which is the most hazardous category [12, 13, 14]. The recovered nodes from the infectious category and having no infections are called as non-infectious nodes. Therefore, it is better to predict infectious nodes in the network. It can be predicted from the attack history or from the vulnerability analysis of the network which requires a considerable efforts and use of resources. The trustworthiness in a cloud based network is a concept that encompasses not only security but also safety, survivability of its nodes and other properties that guarantee a network will behave as expected. In a network no of infectious nodes will be minimized then the network is worthy and being trusted [15]. Therefore, a prediction method can help to fix the suspected domain to check the infectious nodes. In the present manuscript it is achieved by the help of Predator-Prey Model [16, 17]. 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 [18, 19, 20, 21, 22].

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.

In the current manuscript there are three more sections to explore the complete Predator- Prey model in the cloud as section-II: Terminology used, Section-III: Model, Section-IV: Modeling of dynamics of single population i.e. Exposed Computer Nodes (ECN) in cloud, Section-V: Modeling of dynamics of both populations i.e. Exposed Computer Nodes (ECN)and Infectious Computer Nodes, Section-VI: Explanatory points of the proposed model, Section-VI: Some Numerical Simulations and Section VII: Conclusion.

2. TERMINOLOGY USED

x=Number of Exposed Nodes in cloud i.e. prey

y=Number of Infectious Computer Nodes in cloud i.e. predator

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 exposed computer nodes into infectious computer nodes

$\mu_1 = \gamma/\delta$

$\mu_2 = \alpha/\beta$

dx/dt=Growth rate of infectious computer nodes in cloud i.e. Prey

dy/dt =Growth rate of exposed computer nodes in cloud i.e. Predator

3. MODEL

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [23, 24, 25, 26]. The discussion can be made in several sub-chapters.

a. Initially, very few infections and hence recovery rate will be less.

b. Gradually, the infections increased and hence the recovery rate will be increased.

c. After some time an equilibrium state will be achieved in between recovery rate and infections by Malicious attacks in the cloud network.

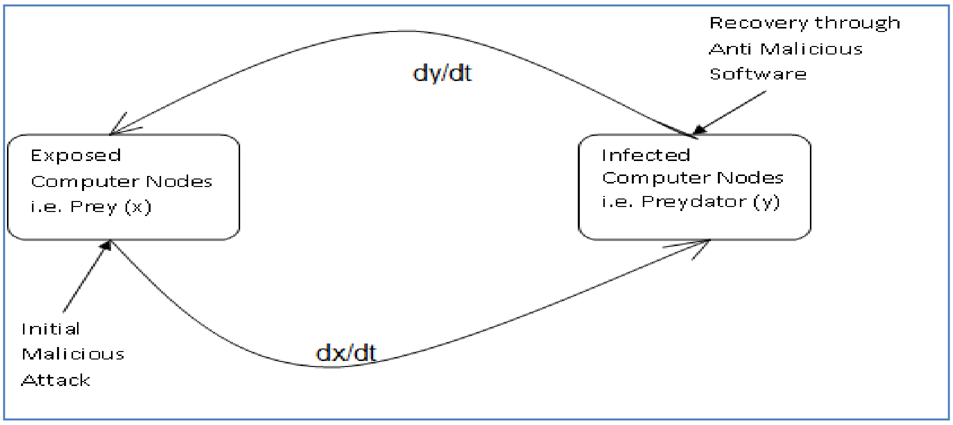

Figure 3. Preydator-Prey Model for cloud based Network

In the present scenario prey is Exposed Computer Nodes (ECN) in cloud and Predator is Infectious Computer Nodes (ICN) in cloud. Hence, in the text the Predator-Prey model states that-

- ECN 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 ECN population growth apart from predation.
- Each ICN infects a constant proportion of the ECN population per unit of time; In other words, doubling the ECN population will double the number infected per ICN, regardless of how big the ECN population is.
- ICN reproduction is directly proportional to ECN consumed; another way of expressing this is that a certain number of ECN consumed results in new ICNs.
- A constant proportion of the ICN population dies per unit of time. In other words, the ICN death rate (approaching to non-recoverable state) is independent of the recoverable process as there are other means like hardware failure or power failure.

Above mentioned situation (Figure-3) 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-

$dx/dt=x(\alpha-\beta y)$ (1)

$dy/dt=-y(\gamma-\delta x)$ (2)

Where,

- x is the number of number of Prey i.e. exposed computer nodes in cloud to the malicious attacks.
- y is the number of some Predator i.e. infected computer nodes in cloud which are ready to spread the infection to other healthy computer node.
- dx/dt and dy/dt represents the growth rate of the two populations i.e. infected computer nodes and exposed computer nodes respectively.
- α is a coefficient of intraspecific competition.
- β is per-capita rate of predation of the predator.
- γ is death rate of predator.
- and δ is the product of the per-capita rate of predation and the rate of conversing exposed computer nodes into infectious computer nodes

Equation-1 and equation-2 can also be written as follows-

$dx/dt=(1-y/\mu\_2)x$ (3)

$dy/dt=-(1-x/\mu\_1)y$ (4)

In equation-4 the extra minus sign distinguishes the predators from the prey. Note if x is zero, then

$dy/dt=-y$ (5)

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

$dx/dt=x$ (6)

and the prey population grows exponentially.

4. MODELLING OF DYNAMICS OF SINGLE POPULATION I.E. EXPOSED COMPUTER NODES (ECN)IN CLOUD.

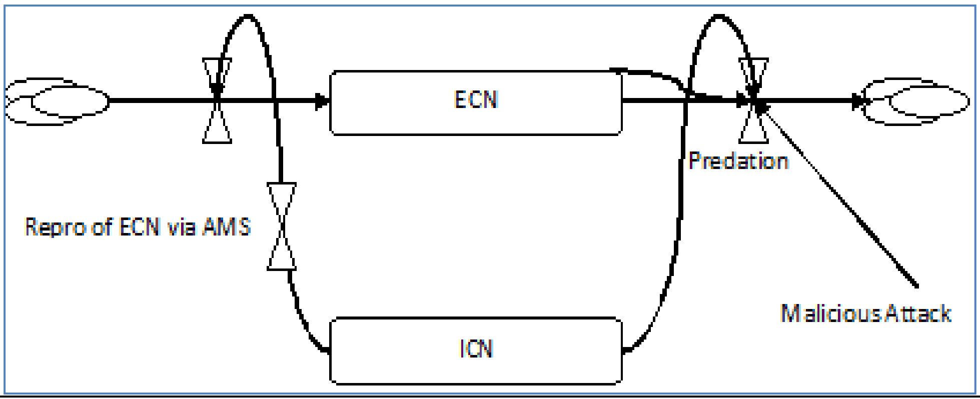

Figure 4. Model diagram of dynamics of single population i.e. ECN

In a cloud based network ECN can be reproduced by adding new nodes and the ICN can be recovered by the help of Anti Malicious Software (AMS). Another aspect is here the predation which affects the ECN populations as shown in figure-4. In this situation the exposed computer nodes grow exponentially as shown in figure-5.

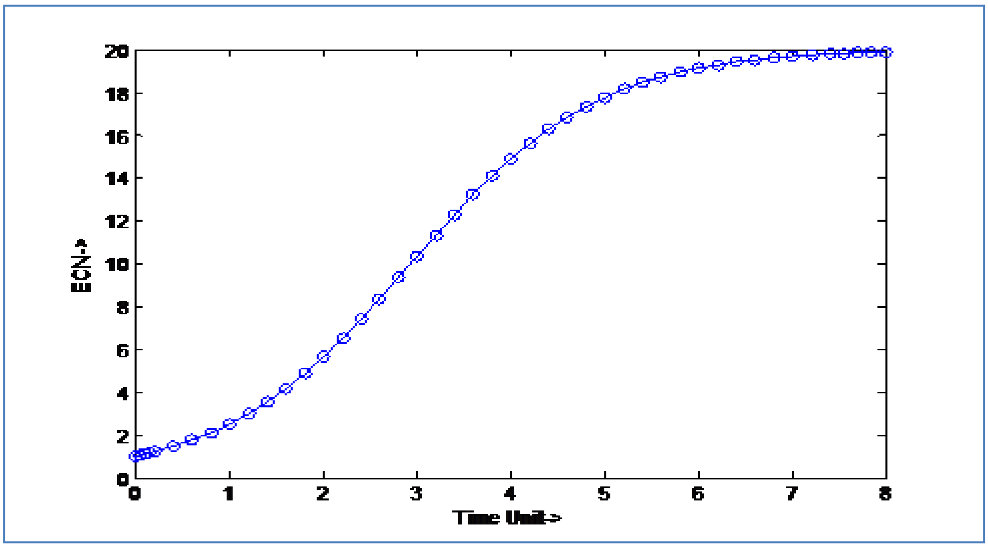

Figure 5. ECN grows exponentially

5. MODELING OF DYNAMICS OF BOTH POPULATIONS I.E. EXPOSED COMPUTER NODES (ECN) IN CLOUD AND INFECTIOUS COMPUTER NODES

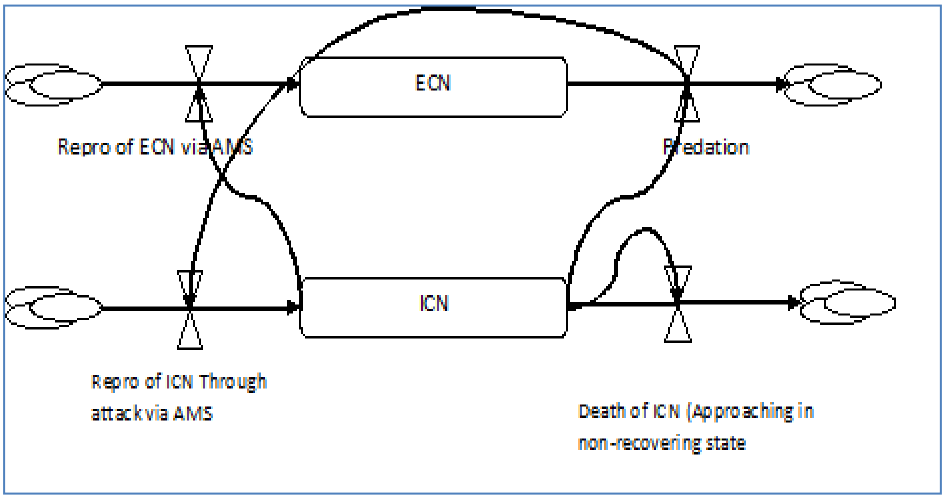
ECN
Repro of ECN via AMS
Predation
ICN
Repro of ICN Through attack via AMS
Death of ICN (Approaching in non-recovering state

Figure 6. Model diagram of dynamics of both populations i.e. ECN and ICN

This reflects the assumption that the ICN reproduction is proportional to rate of predation on the ECN as depicted by figure-6. In this case the ECN and the ICN compartments cycle, with the ECN population crashing as the ICN population increases, followed by a crash in the ICN population as shown by figure-7.

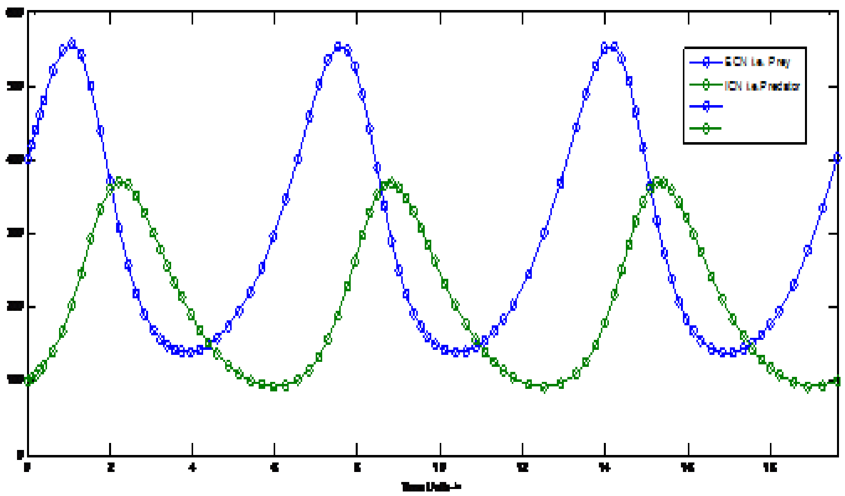

Figure 7. ECN population crashing as the ICN population increases, followed by a crash in the ICN population

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. 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:

$$dx/dt = 0.2x - 0.0025xy$$
$$dy/dt = -0.1y + 0.002xy$$

where x and y are the populations of exposed computer nodes and infectious computer nodes 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 computer nodes and exposed computer nodes. An AMS recovers some fraction of malicious attacks (per unit time) is used to control the infection. This system is modelled by the equations:

$$dx/dt = ax - bxy - ex$$
$$dy/dt = -cy + dxy - fy$$

Where, e and f are the respective rates at which the infectious nodes recovered by AMS and Exposed nodes 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.$(c + f/d, a - e/b)$.

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 computer nodes will increase whilst the equilibrium stock of predators i.e. infectious computer nodes 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 computer nodes by the statements that the equilibrium number of exposed computer nodes will decrease whilst equilibrium number of infectious computer nodes remains unchanged in the cloud (since f = 0).

7. NUMERICAL SIMULATIONS

Let exposed computer nodes (prey) and infectious computer nodes (predator) are there in the cloud based networks. If the initial conditions are 80 exposed computer nodes and 40 infectious computer nodes at some instances, one can plot the progression of the two types of nodes over time as shown in figure-8. The choice of time interval is arbitrary.

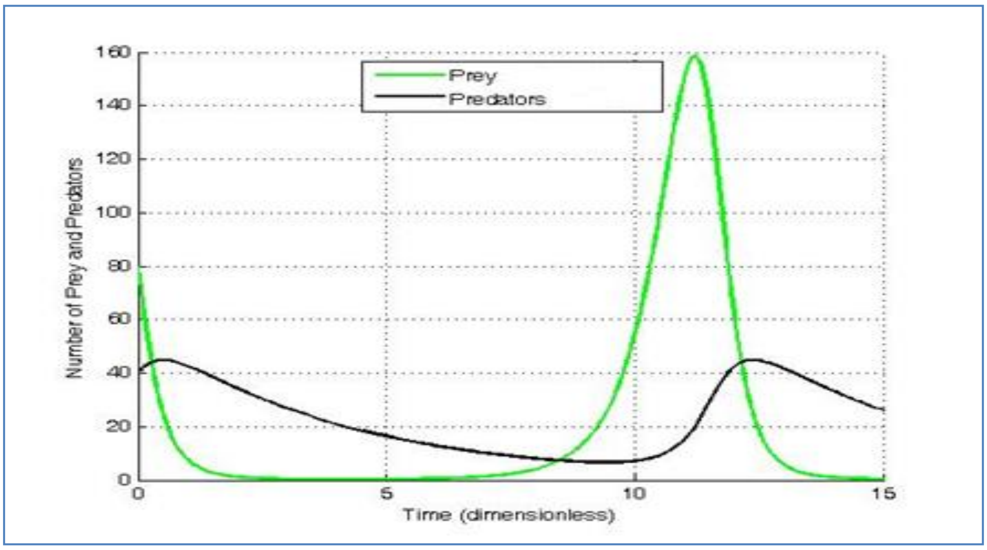

Figure 8. Exposed computer nodes and Infectious computer nodes with respect to time, where, initially 80 Exposed computer nodes and 40 Infectious computer nodes in the computer network.

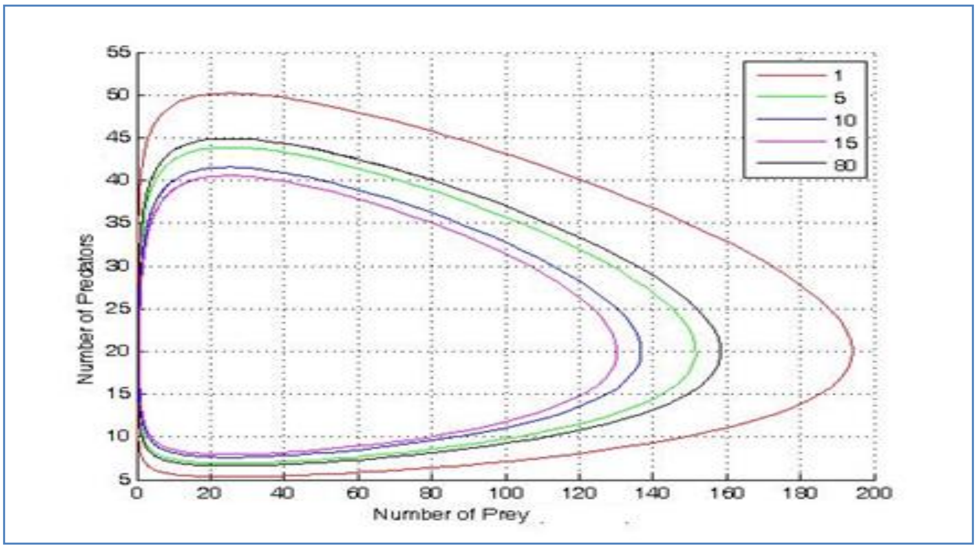

Figure 9. The oscillatory nature of the population of the two types of the compute nodes in the cloud.

One can also plot a solution which corresponds to the oscillatory nature of the population of the two types of the compute nodes as depicted in figure-9. 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.

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

8. CONCLUSION

Predator-Prey model for computing the proportion of the Exposed Computer Nodes (ECN) and Infectious Computer Nodes (ICN) to check the trustworthiness in the cloud based network is established. Our proposed model is to make the cloud computing architecture perfect and built a more comprehensive network. Two of the possible cases for the established model for modelling of dynamics of single population i.e. Exposed Computer Nodes (ECN) and modelling of dynamics of both populations i.e. Exposed Computer Nodes (ECN) and Infectious Computer Nodes (ICN) in the cloud are discussed. Various critical explanatory points are discussed with suitable examples and graphical presentations for better understanding about the model. As a result, it has been shown that the ECN and the ICN compartments cycle, with the ECN population crashing as the ICN population increases, followed by a crash in the ICN population. Further, as conclusion, the proposed work will help to find out the utility of a computer node and the impact of Anti Malicious Software with its efficiency in the cloud based network so as to increase the trustworthiness in the cloud environment.

REFERENCES

[1] Y. Jianfeng, C. Zhibin. *Cloud Computing Research and Security Issues*. *CISE* 2010. Dec, 2010.

[2] H.Sato,et al. *A Cloud Trust Model in a Security Aware Cloud*. *SAINT2010*, pp.121-124.

[3] Francesco M.A and Gianni F. *An approach to a cloud Computing network*.IEEE, August 2008, pp.-113-118.

[4] Xiaojun Yu, Qiaoyan Wen. *A view about cloud data security From data life cycle*. 978-1-4244-5392-4/10/ ©2010 IEEE.

[5] Mladen A. Vouch. *Cloud Computing Issues, Research and Implementations. Journal of Computing and Information Technology* - CIT 16, 2008, 4, 235–246.

[6] Xue Jing, Zhang Jian-jun2. *A Brief Survey on the Security Model of Cloud Computing. 978-0-7695-4110-5/10 © 2010 IEEE DOI 10.1109/DCABES*.2010.103.

[7] Engr: Farhan Bashir Shaikh, *Sajjad Haider.Security Threats in Cloud Computing*.978-1-908320-00-1/11@2011 *IEEE.*

[8] Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh. *A Novel Open Security Framework for Cloud Computing. International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.1, No.2, June 2012, pp. 45~52 ISSN: 2089-3337.

[9] Ashish Kumar. *World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER).* Vol.1, No.2, June 2012, pp. 53~58 ISSN: 2089-3337.

[10] M.Rajendra Prasad, R. Lakshman Naik, V.Bapuji. *Cloud Computing: Research Issues and Implications. International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.2, No.2, April 2013, pp. 134~140 ISSN: 2089-3337.

[11] Wenjuan FAN, Shanlin Yang, Jun Pei, He Luo. *Building trust into cloud . International Journal of Cloud Computing and Services Science (IJ-CLOSER*). Vol.1, No.3, August 2012, pp. 115~122 ISSN: 2089-3337.

[12] Hemraj Saini, Dinesh Saini. *Malicious Object dynamics in the presence of Anti Malicious Software.European Journal of Scientific Research*, [ISSN: 1450-216X], volume-18, Issue-3, pp.-491-499, (2007).

[13] Sylvain P. Leblanc, Andrew Partington, Ian Chapman, and Mélanie Bernier. *An overview of cyber attack and computer network operations simulation. In Proceedings of the 2011 Military Modeling & Simulation Symposium (MMS '11) (2011). Society for Computer Simulation International*, San Diego, CA, USA, 92-100.

[14] Hemraj Saini, T. C. Panda, Minaketan Panda. 2011. *Prediction of Malicious Objects in Computer Network and Defense. International Journal of Network Security & Its Applications (IJNSA),* Vol.3, No.6, pp.-161-171, 2011.

[15] Ian M. Chapman, Sylvain P. Leblanc, and Andrew Partington. *Taxonomy of cyber attacks and simulation of their effects. In Proceedings of the 2011 Military Modeling & Simulation Symposium (MMS '11) (2011). Society for Computer Simulation International*, San Diego, CA, USA, 73-80.

[16] Sean P. Gorman, Rajendra G. Kulkarni, Laurie A. Schintler, and Roger R. Stough. *A predator prey approach to the network structure of cyberspace. In Proceedings of the winter international synposium on Information and communication technologies* (WISICT '04) (2004). Trinity College Dublin 1-6.

[17] P. Cull. *Global stability for population models, Bull. Math. Biol*. 43 (1981) 47–58.

[18] J.D. Murray. *Mathematical Biology, Springer-Verlag, Berlin, Heidelberg*, New York (1989).

[19] Lifeng Wu and Yinao Wang. *Estimation the parameters of Lotka-Volterra model based on grey direct modelling method and its application. Expert Syst. Appl*. 38, 6 (2011), 6412-6416. DOI=10.1016/j.eswa.2010.09.013 http://dx.doi.org/10.1016/j.eswa.2010.09.013

[20] B. Batiha, M. S. M. Noorani, and I. Hashim. *Variational iteration method for solving multispecies Lotka-Volterra equations. Comput. Math.* Appl. 54, 7-8 (2007), 903-909. DOI=10.1016/j.camwa.2006.12.058 http://dx.doi.org/10.1016/j.camwa.2006.12.058.

[21] Claire Elliott. Botnets: *To what extent are they a threat to information security?. Inf. Secur. Tech*. Rep. 15, 3 (2010), 79-103. DOI=10.1016/j.istr.2010.11.003 http://dx.doi.org/10.1016/j.istr.2010.11.003

[22] Moussa Ouedraogo, Djamel Khadraoui, Haralambos Mouratidis, and Eric Dubois. *Appraisal and reporting of security assurance at operational systems level*. J. Syst. Softw. 85, 1 (2012), 193-208. DOI=10.1016/j.jss.2011.08.013 http://dx.doi.org/10.1016/j.jss. 2011.08.013

[23] Cayirci, Erdal, Ghergherehchi, Reyhaneh. *Modeling cyber attacks and their effects on decision process. Simulation Conference (WSC)*, Proceedings of the 2011 Winter (2012), 2627 – 2636. Digital Object Identifier : 10.1109/WSC.2011.6147970.

[24] Lindqvist, U. and E. Jonsson. *How to Systematically Classify Computer Security Intrusions. Proceeding of IEEE Symposium on Security and Privacy*, London, pp: 154 – 163 (1997).

[25] Tidwell, T., R. Larson, K. Fitch and J. Hale. 2001. *Modeling Internet Attacks. Proceedings of the IEEE Workshop on Information Assurance and Security*. Unites States Military Academy, West Point, NY.

[26] G. P. Schaffer. *Worms and Viruses and Botnets, Oh My!. Published By The IEEE Computer Society, IEEE Security & Privacy*, pp. 52-58 (2006).

BIOGRAPHY OF AUTHORS

Satyabrata Dash is a Ph.D research scholar at CUTM, Paralakhemundi. He has received M.Tech. degree in Computer Science Engineering from KIIT university Bhubaneswar in 2006.Presently he is working as an Assistant Professor(IT) in Orissa Engineering College, Bhubaneswar. He is having around 9 Yrs of teaching experience and published 6 research papers in international and national journals.

Hemraj Saini is a faculty member in the Department of Computer Science & Engineering, Jaypee University of Information Technology, Waknaghat, India -173234. He received his B.Tech. in CS&E from NIT Hamirpur (H.P.), M.Tech. degree in Information Technology from the Punjabi University Patiala, Punjab and PhD degree from Utkal University, Bhubaneswar in 1999, 2005 and 2012 respectively. His main professional interests are in Mathematical Modeling, Simulation, Cyber Defense, Network Security and Intelligent Techniques.

T. C. Panda is a Retd. Professor of Mathematics (Berhampur University, India), Founder Professor of Mathematics & Computer Sc. (Mizoram Central University, India) and currently associated as Principal with Orissa Engineering College, Bhubaneswar, Orissa, India-752050. He received his Masters from Banaras Hindu University in 1968 and Ph. D. from Berhampur University in 1975. His main interests are Fluid Dynamics, Air Pollution Modeling, Monsoon Dynamics, Numerical Weather Prediction, Meso-Scale Modeling, Remote Sensing Techniques, Numerical Solution of Partial Differential Equations and Cyber Defense.

Ashok Mishra has received Ph.D (Mathematics) from Berhampur University, Berhampur, in the year 2003 on the topic Study on Different Aspects of Two Phase Flow Phenomena. Presently he is working as Registrar CUTM, Paralakhemundi, Odisha, India. He is having around 17 years of experience in Teaching & Administration. He has published 21 research papers in international and national journals.