

A CP Intrusion Detection Strategy on Cloud Computing

Yizhang Guan, Jianghong Bao

School of Mathematics Science, South China University of Technology, Guangzhou, China

e-mail: yzhguan@scut.edu.cn, yzhguan@scut.edu.cn

Abstract—Cloud Computing is a general concept of the computing service which is reliance on the Internet for satisfying the computing needs of the users. The providers and the users of the service will be benefit for the new organization pattern. In this paper, we propose a framework for the construction of a CP intrusion detection system in E-Government. The idea can help people construct a flexible security system based on a well organized strategy and statistical model.

Index Terms—Cloud Computing; E-Government; Intrusion Detection

I. INTRODUCTION

In last century, we can say, people need the computers. For recent years, we must say people need the internet for communication. But for these years, we have to say, people need service more than the mass data from internet. The service can be explained as some computing function. As the development of the technology and hardware, we can imagine that it is possible to get rid of the great mass of the spending for fixed assets, such as expensive networks server and software. Just a web browser can help us complete our common business applications online from the provider on internet. That is the scene the cloud computing providers describe to us.

We can call it win-win solution for both users and providers. But it brings us more serious problems as well. As we know, many problems, such as privacy, intrusion detection, are so serious in the net world. We do not find a sure way to improve the system at present. Once Cloud Computing is applied in practical, that means, the service providers are in charge of all our core hardware and computing process, the users will worry about who will supervise the providers and control their behavior. Some engineers think there nothing to do but just trust the providers as before. The other most important problem is intrusion detection system.

The current intrusion detection systems are complicated but far from complete. At first, the researchers were weighed down with a great variety of the attacks. In order to keep up with the attacks development which change quickly, the researchers have advanced to fixed battle lines and positional warfare. Some security systems have been built up. At the present time, we depend on these secure systems largely, but we find the networks are not safe enough yet. The networks

administrators often find themselves trap in a dilemma between the running performance and security. They have to change the security strategy after a period of time because of a new attack technology. In Cloud Computing, the status is more serious. In this paper, we propose a framework for the construction of an intrusion detection system. The idea can help us construct a flexible security system based on a well organized strategy and statistical model.

II. CLOUD COMPUTING

Let us begin with Cloud Computing. I believe the idea has explodes to discussion at the beginning. IT magnates describe the future of the usage and imagine the benefit from the service. In fact, some of them have build up the centre. And Engineers devote to compare the possible technology of Cloud Computing with the grid computing. They don't seem to be as exciting as the magnates, because they do not find any new technology compared by grid computing. The attitude of the software managers is not clear yet. But some of them have led the new development edition of the corresponding software to the direction. However, they deal with concrete matters relating to work.



Figure 1. Users in Cloud Computing

It is possible to get rid of the great mass of the spending for fixed assets, such as expensive networks server and software. Just a web browser can help us complete our common business applications online from the provider on internet. That is the scene the cloud computing providers describe to us. We can call it win-win solution for both users and providers.

The researchers always depict internet as cloud before in their diagrams. So, as the idea turns out, it is nothing surprising. Since we pay constant attention to the capacity

Sponsors: Famous Brand Specialty for Information Management and Information System of Ministry of Education (N9050040); SRP (Student Research Plan) in South China University of Technology (Y1080270).

of Cloud Computing which will support our business work in the future, we prefer to lay the hardware “on” the cloud.

There many problems in the development of Cloud Computing. It is out of questions. In fact, one of them, such as privacy, is so serious in the net world. We do not find a sure way to improve the system at present. Once Cloud Computing is applied in practical, that means, the service providers are in charge all our core hardware and computing process, the users will worry about who will supervise the providers and control their behavior. Some engineers think there nothing to do but just trust the providers as before.

III. E-GOVERNMENT IN CLOUD COMPUTING

A. E-Government and Privacy

We have to face with many problems before we can enjoy the technology of Cloud Computing. After all, the privacy of the users is a difficult one. If researchers can not propose an improved system, the technology of Cloud Computing is limit to advance. Of course, we can turn around. That means we can push it away in some fields. For example, we can ignore it in E-Government.

It is obvious that people working in E-Government do not involve privacy trouble. The group company is the same.

B. E-Government in Cloud Computing

It is obvious that people working in E-Government do not involve privacy trouble. But, how the technology helps the development of the E-Government? Let us illustrate the question with the E-Government in China.

The E-Government in China is underdeveloped or you can think it disparate development. The local governments build up their E-Government dispersedly. The development and the quality of network maintenance largely depend on the investment from local government. As the relationship of the neighbor provinces become closer and closer, we realize the inconvenience it brings to us. In order to improve the system, we pay attention to set up the “bridges” between the governments’ databases as below.

It is absolute to be uneconomical. If we take the idea of Cloud Computing, we can improve the system for all local service. How we can do it? Let us explain it specifically. The government should build up a data centre on Cloud Computing for the whole country, and make E-Government to centralization. It can bring us:

- The government will be up to be in charge of all the important information.
- The government affords the large part of the investment for the data centre.
- The local government is up to be in charge of the update for the local database.
- The local government can access the other local database easily.

- The local governments afford a small part of the investment for the hardware and management.

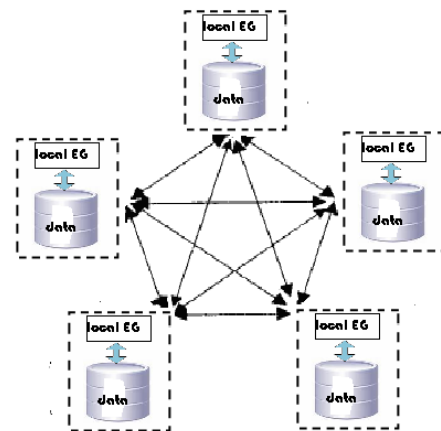


Figure 2. Relationship between local government networks

Above all, the economic power is not the most important one as before with the technology.

IV. CONSTRUCTION OF INTRUSION DETECTION SYSTEM

In the first section, we discuss on the intrusion detection system at present. The researchers were weighed down with a great variety of the attacks from the battle. And in order to keep up with the technology of attacks which change quickly, the researchers have advanced to fixed battle lines and positional warfare. The strategy seems so passive. The researchers consider a new strategy or rules become more active.

There are two way to improve the system. Both of them refer to the idea of Cloud Computing. One is to introduce the idea to the security system. The other is to make the strategy based on the statistical model for the security system on Cloud Computing. We focus on the last one.

We propose a framework for the construction of an intrusion detection system. The idea can help us construct a flexible security system based on a well organized strategy and statistical model.

A. The given sample space

The researchers have advanced to fixed battle lines and positional warfare, in order to keep up with the change of the attack technology, and integration the functions to stronger the security system.

Many researchers agree, as the attacks happen, the behavior of the networks must be changed. That is to say, the features of networks can be extracted as some random variables. Limit the value range for the given networks. In fact, if the network without attacks, the random variables is limit the value range in an interval, which is defined as the networks are without attacks. Once some characters of the networks vary, that means, some attacks are occurring, the value range should be out of the intervals. If we can

realize the change in time, we succeed in intrusion detection.

B. Divide the sample space

Many researchers select some kinds of attacks as their object of study, and give the solution to detect intrusion. We call it “fixed battle lines” and “positional warfare”. It is undoubtedly logical that to integrate the function in security system to stronger the capability. But the problem is, whether the integration is efficient or not. Doing experiments is one of important methods, but it is expensive too. The economical one is to use trace data for simulation. In fact, these two methods can tell us whether the sample is efficient or not after the operation, but it can not help us how to choose the setting. In this paper, we prefer qualitative analysis method to construct a security system. That is, we propose a more reasonable strategy to organize the system, before the experiment.

The idea is as follows. Take all attacks as the sample space, Ω , although we do not know them exactly. We try to divide the space, since it is difficult to deal with all the intrusion through a single strategy. If we divide the space completely, we shall discover more efficient method as the number of the sub-set is smaller. We hope it satisfy with: The decomposition of a set into a family of mutually exclusive sets. If such sets are available, each sample, ω , in Ω , only belongs to one sub-set, called event in probability theory. Thus, when we focus on the events to construct an intrusion detection algorithm, the work become more efficient than before.

The technology of attacks is emerging. So the sample space is unknown. We consider a decomposition method in statistical theory, though the idea is not direct and fixed.

1) Gobar CPID

Suppose that we have attained a series of characteristic indexes for flow rate by principal component analysis, \mathbf{X}_i . \mathbf{X}_i act as a \mathbf{p} dimension vector and $\mathbf{p} > 1$. The intrusion detection can be described as a change-point detection problem as below.

$$\mathbf{X}_i \sim \begin{cases} N_p(\mu_0, \Sigma_0) & i \leq \tau \\ N_p(\mu_1, \Sigma_1) & i > \tau \end{cases} \quad (1)$$

where τ is the position of change-points(attacks), mean values, μ_0 and μ_1 , covariance Σ_0 and Σ_1 , τ , all of these are unknown. Both Σ_0 and Σ_1 are nonsingular.

We can assume that for the interval is short enough. It means that there is only one change-point or none in an interval.

Note that

$$\bar{\mathbf{X}}_{0,k} = \frac{1}{k} \sum_{i=1}^k \mathbf{X}_i \quad (2)$$

$$\bar{\mathbf{X}}_{0,k} = \frac{1}{k} \sum_{i=1}^k \mathbf{X}_i \quad (3)$$

and

$$\mathbf{W}_k = \left[\sum_{i=1}^k (\mathbf{X}_i - \bar{\mathbf{X}}_{0,k})(\mathbf{X}_i - \bar{\mathbf{X}}_{0,k})' + \sum_{i=k+1}^n (\mathbf{X}_i - \bar{\mathbf{X}}_{k,n})(\mathbf{X}_i - \bar{\mathbf{X}}_{k,n})' \right] / (n-2) \quad (4)$$

($n > \mathbf{p} + 1$ for nonsingular)

We consider the mean firstly. Note that

$$\mathbf{Y}_k = \left[\frac{k(n-k)}{n} \right]^{\frac{1}{2}} (\bar{\mathbf{X}}_{0,k} - \bar{\mathbf{X}}_{k,n}) \quad (5)$$

\mathbf{Y}_k denote the deviate before and after the change. k is the position of the change. The test statistic is Hotelling- \mathbf{T}^2 .

$$\mathbf{T}_k^2 = \mathbf{Y}_k' \mathbf{W}_k^{-1} \mathbf{Y}_k, (k = 1, 2, \dots, n-1), \quad (6)$$

Then, the sum of the deviate is

$$\mathbf{T}_f^2 = \max \mathbf{T}_k^2, (k = 1, 2, \dots, n-1). \quad (7)$$

Consider the co-variance probability problem for the change of mean value as below:

$$\mathbf{H}_0 : \Sigma_0 = \Sigma_1 \quad (8)$$

Then, the test statistic is

$$\mathbf{G}^* = -2 \log(\Lambda) = \sum (n_i - 1) \log \frac{|\hat{\Sigma}_i|}{|\hat{\Sigma}_{pooled}|} \quad (9)$$

If both the expected value and variance has changed, the null hypothesis is

$$\mathbf{H}_0 : \mu_0 = \mu_1, \Sigma_0 = \Sigma_1 \quad (10)$$

The null hypothesis can be separated as two hypothesis as

$$\mathbf{H}_{0,1} : \mu_0 = \mu_1 | \Sigma_0 = \Sigma_1 \quad (11)$$

$$\alpha v \delta \mathbf{H}_{0,2} : \Sigma_0 = \Sigma_1 \quad (12)$$

The ML statistic become as

$$\Lambda = \frac{|\hat{\Sigma}_0|^{\frac{k}{2}} \times |\hat{\Sigma}_1|^{\frac{n-k}{2}}}{|\hat{\Sigma}|^{\frac{n}{2}}} \quad (13)$$

where $\hat{\Sigma}$ is the predict statistic of Σ .

2) Local CPID

The idea of local CPID is based on the networking protocol. The CUSUM method can be used in such statistical algorithm. Some intrusion detection systems have illustrated a lot of practical trace data or simulation networks stream data on the test experience.

The main variables and formulas are given in [11].

3) Posterior CPID

The posterior CPID can be look as the back-stage management. The technology of the networks attacks becomes more and more complex. The statistical test can help us find the change points caused by attacks, but we often determine the source as soon and accurately as we expect. We want to make sure the causes by further analysis. So, the posterior CPID is considered as well.

The method can ignore the limit of the computing time and trace data storage. But it doesn't mean we can record the trace data as popular as possible. If we record the trace data for the main stream of the networks, it would pull down the service quickly.

For another hand, the method depends largely on the networks itself. That means, to attain a universal probability model in posterior CPID is difficult.

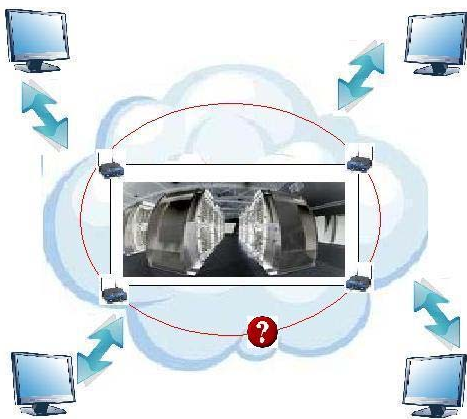


Figure 3. Relationship between local government networks (figure caption)

C. CPID in Cloud Computing

The information security system is more serious on Cloud Computing. In order to reduce the cost, we direct to the more efficient method to do the work.

The framework of the intrusion detection system includes global CPID, local CPID and posterior CPID.

V. FURTHER WORK

The idea, Cloud Computing, make us think over the technology in grid computing. If we want to take it in practical, we should find more efficient way to organized our system, including the security system. On the other hand, we need to find a way to do our experience. The trace data is rare and too little to Cloud Computing. A simulation system is necessary.

REFERENCES

- [1] M. Basseville, I. V. Nikiforov, "Detection of Abrupt Changes: Theory and Applications," Englewood Cliffs: Prentice-Hall, 1993.
- [2] O. Spatscheck, L. Peterson, "Defending Against Denial of Service Attacks in Scout," Proc. USENIX Symp. Operating Systems and Design Implementation, Feb.1999: pp. 59-72.
- [3] M. Csorgo, L. Horvath, "Limit Theorems in Change-Point Analysis." gbv.de, 1997.
- [4] J. Chen, A. K. Gupta, "Parametric statistical change point analysis," Birkhäuser, 2000.
- [5] Y. Z. Guan, Z. F. Hao, "The MDR Algorithm for Edge Detection on Change-point Theory," IEEE International Symposium on Intelligent Information Technology Application 2008, pp. 558-562
- [6] T. H. Kerr. "Decentralized filtering and redundancy management for multisensor navigation," IEEE Trans. Aerospace and Electronic systems, 1987, AES-23: pp. 83-119.
- [7] M. A. Sturza, "Navigation System Integrity Monitoring Using Redundant Measurements," Navigation, Woodland Hills, 1988.
- [8] J..Lemon, "Resisting SYN Flooding Dos Attacks with a SYN Cache," Proc. USENIX BSDCon Conf., Feb.2002.
- [9] C..Jin, H. Wang, K. G. Shin, "Hop-Count Filtering: An Effective Defense Against Spoofed Ddos Traffic," Proc. ACM Conf. Computer and Comm. Security[C], Oct.2003: pp. 30-41.
- [10] X. Wang, M. Reiter, "Defending Against Denial-of-Service Attacks with Puzzle Auctions," Proc. IEEE Symp. Security and Privacy, 2003: pp. 78.
- [11] H. Wang, D. Zhang, K. G. Shin, "Change-Point Monitoring for the Detection of DoS Attacks." IEEE Transactions on dependable and secure computing, 2004.
- [12] D. Yau, J. Lui, F. Liang, "Defending Against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles," IEEE/ACM Transactions on Networking, 2005, 13(1): pp. 29-42.