A SECURITY MODEL FOR CLOUD COMPUTING BASED ON AUTONOMOUS BIOLOGICAL AGENTS

Fatemeh Arabalidousti[1] and Touraj Banirostam [2]

[1,2] Department of Computer Engineering, Islamic Azad University, Central Tehran Branch ,Tehran, Iran

ABSTRACT

Besides many advantages which cloud computing creates, there are different concerns such as security. In this paper, the conceptual model based on Biological Immune System (BIS) will be proposed in order to create security in cloud computing. BIS has several features such as distributed computing, self organizing, self-learning that are considered in distributed environments like clouds. In proposed model, five groups of autonomous agents are used. The structure of agents is based on Biological Agents (BA) that have memory and could use previous experiments. Agents have the ability to learn and interact with each other. Each agent has different functions. Their designs are based on B and T lymphocyte. This model is designed at two levels. In the first level, roles, relationship and activities of each agent are described and their components such as modules, programs and functions are shown in the second level. By using these intelligent autonomous agents, attacks can be identified and intrusion can be prevented. The proposed model is based on collaboration of the agents and doesn't need centralized management.

KEYWORDS

Biological Agents, Biological Immune System, Cloud Computing, Security.

1. INTRODUCTION

Cloud computing is a new technology based on distributed processing, parallel computing and grid computing, which has been developed recently and is one of the attractive topics in the field of information technology [1]. Set of resources are provided by many computers and are allocated to users as needed. Thus, all applied programs can obtain calculation capacity, storage space and a variety of software services according to their need [2].

Cloud computing provide advantages such as high scalability, remote data storage, reduction of cost by sharing computing and storage resources [3]. Nevertheless, it faces different challenges. Security is one of the key challenges. Acceptance of cloud computing services requires solving the security problems [1]. Therefore, many attempts are made to create a safe environment because the increase of interaction in cloud increased security concerns. To overcome the security problems in cloud computing, using new methods like Autonomous Computing and BIS (BIS) provides new approaches to overcome this issue. Immune system is an autonomous system of which components interact with each other without a central system. The system is able to identify insiders and outsiders and to learn and interact with the operating concept [3]. The BIS is an autonomous system in which all control and security operations are done without the intervention of the central system. Therefore, BIS, a new method to overcome the security challenges in cloud computing can be proposed.

In the next section, related works about security of cloud computing and method of using agents are given. The BIS will be described in section 3. In section 4, the proposed model will be introduced. Designing of agents will be explained in section 5 and finally conclusions will be presented.

2. RELATED WORKS

Since the security is very importance in the cloud, different methods have been presented in this section. First, methods of increasing the security of the cloud are presented. Then, works performed for modeling of BIS are described. One of the methods of establishing security of cloud is collaborative intrusion detection. This proposed system is a kind of DIDS which supports partner IDS idea in cloud environment. Each IDS notifies other IDSs that attack or suspicious event has occurred. They exchange all of IDS alerts and verify them [4]. A new intrusion detection model for cloud is AdjointVM. AdjointVM is an IDS that is composed of both explicit and implicit parts. In explicit part, traditional IDS can be used to monitor applied programs of user level. This part includes strong analysis laws and package focus on a specific data event of the host. In implicit part, each protected virtual machine (VM) is added to a VM which uses virtualization technology for monitoring statuses of the protected VM core and uses explicit and implicitly IDS for protecting integrity [5].

What was mentioned above was related to detection methods introduced in the cloud. Now agent-based methods for BIS modeling are reviewed. An approach to an intrusion prevention system (IPS) which is inspired by the Danger model of immunology is proposed. This novel approach used a multi immune agent system that implements a non-linear classification method to identify the abnormality behavior of network system [6]. Agent-based artificial immune system (ABAIS) is applied to intrusion detection systems (IDS). A multiagent-based IDS (ABIDS) inspired by the danger theory of human immune system is proposed [7]. Banirostam had modeled the BIS with using Biological Agent (BA) based on Capra Cognitive Framework [8]. Montealegre introduced an Agent-based artificial immune system model for the detection of faults in a distributed satellite [9].

3. BIOLOGICAL IMMUNE SYSTEM

The immune system plays an important role in defending body against various threats to health, such as pathogens, cancer cells or modified-self proteins. The immune response is traditionally divided into innate and adaptive immune responses [10]. Lymphocytes as the primary immune cells are divided into two major groups: B cells and T cells. A simple definition of B lymphocytes is a population of cells that express clonally diverse cell surface immunoglobulin (Ig) receptors recognizing specific antigenic epitopes [11]. On occasion, however, a B cell does make a catch. When a B cell's receptors bind to its cognate antigen, that B cell is triggered to double in size and divide into two daughter cells – a process immunologists call proliferation. Both daughter cells then double in size and divide to produce a total of four cells, and so forth. Each cycle of cell growth and division takes about 12 hours to complete, and this period of proliferation usually lasts about a week. At the end of this time, a "clone" of roughly 20 000 identical B cells will have been produced, all of which have receptors on their surface that can recognize the same antigen. Now there are enough to mount a real defense [12]. Once a virus gets into a cell, antibodies can't get to it, so the virus is safe to make thousands of copies of itself. Mother Nature recognized this problem, and to deal with it, she invented the famous "killer T cell," another member of the adaptive immune system team. Like B cells, T cells are produced in the bone marrow, and on their surface they display antibody-like molecules called T cell receptors (TCRs) [12]. When a T cell's receptors bind to their cognate antigen, the T cell proliferates to build up a clone of T cells with

the same specificity. This proliferation stage takes about a week to complete, so like the antibody response, the T cell response is slow and specific[12].
After entry of pathogenic bacteria or a virus to the body, the cells such as dendritic cells and macrophages send signals associated with external factors to T Helper. After receiving the signal, T-Helper cells send orders to T-Killer and B cell and the T-Killer cell directly attacks the cells contaminated with virus or cancerous cells while B-cell releases the related antibodies to pathogenic bacteria [12]. Activation of special types of B-cell and T-Killer cells depending on the intruder antigen type. If the intruder antigen was pathogenic bacteria, B lymphocytes would be activated and autopoiesis, but if it was a virus or defective cell, T lymphocytes would be activated and autopoiesis [12]. APC-cell, antigen presenter cells, is a set of different types of cells that are able to identify and process antigen. These cells presented their findings to another cell and persuaded them to start an immune response against pathogens.

4. PROPOSED MODEL

According to the independent operation of the BIS elements, this system can be used to design secure systems in the cloud. The use of BIS has two reasons: Firstly, the immune system is a self-organized and distributed system to protect the body against attack of pathogens. Secondly, current techniques used in increasing security in cloud computing don't address some of the challenges. Requirement for this system is an existence of independent elements in the cloud. In this model, an intrusion detection system based on multi-agent architecture is designed. Agents are mobile in the model and derived from architecture of immune cells. These agents are divided into 5 categories: Presenter, T-Helper, T-Memory, B and T-Killer. Each of these agents is designed based on autonomous computing architecture. Autonomic computing tries to develop the communication infrastructure and overcome the complexity with approach of tasks assignment to the elements available in the system.

Autonomous agents should be able to identify and restore defective components, and also protect themselves. They are aware of the internal and external environment and communicate with each other and share their knowledge. The proposed model is shown in Figure 1.

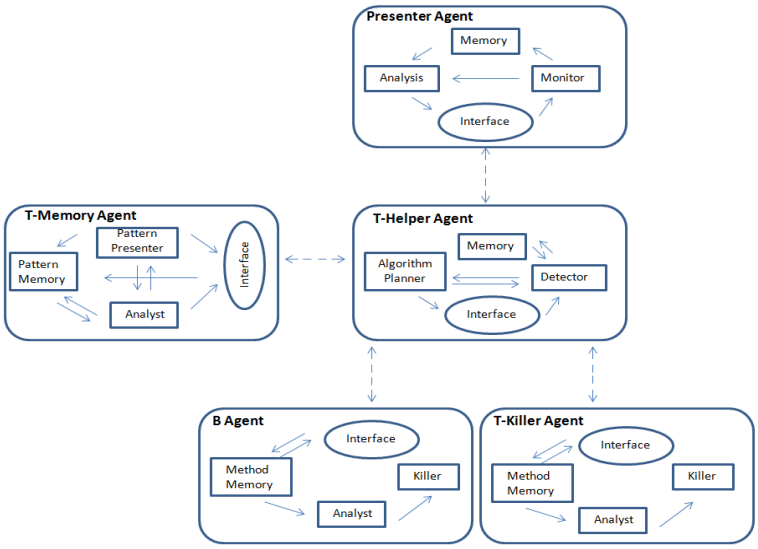

Figure 1. The proposed model

These agents are able to learn, monitor the environment, discover outsider and finally kill them. System is going to be robust over the time and the knowledge will be increased. These agents are

deployed in the data centre of cloud and when one of them is removed from the system, another agent will be replaced quickly.

5. DESIGN AGENTS

Five different agents are designed based on autonomic computing each having its own capabilities. Internal components and relations between them are shown in Figure 1. The function of each agent is described the following.

5.1. Presenter Agent

In this model, the role of this agent is antigen Presenter cell. This agent moves in the data center and monitors environment, recognizes normal functions of the units under its control and records them in its memory. When information gained via monitoring environment is reviewed and audited, if a defect occurs, Presenter agent sends the audit trail to T-Helper agent to receive a compliance pattern for eliminating the causes of the occurring defect. This agent has four modules which are listed below:

Interface: This module is responsible for communicating between modules of this agent and other agents.
Monitor: This module monitors the internal environment and is looking for anomaly conditions.
Memory: This module records the node's normal functions and maintains data obtained from Monitor.
Analysis: This module studies information obtained from the monitors interfaces and memory modules. In case of intrusion or security problems occurring in the system, it will request pattern.
Figure 2 shows the flowchart of the internal functions of this agent.

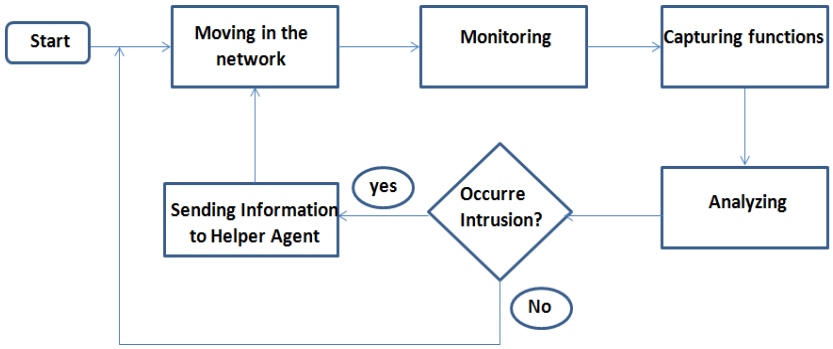

Figure 2. The flowchart of internal functions of Presenter agent.

5.2. *T- Helper Agent*

This agent that is shown in figure 3 plays role of T-Helper cell. When it receives pattern request from Presenter agent, it gives pattern to Memory agent. This request is because of intrusion occurring in the network. Intrusion can be divided into two categories: the first category is related to authorized users that intrude on unauthorized parts. The second category relates to activities occurring outside the network for intrusion into it. The first category of these activities is more dangerous than the latter. Since this intrusion is done by the users who have been authenticated in the system and can also do activities. For this purpose, different security policies for the two classes are established. T-Helper agent determines the type of intrusion after receiving the pattern

request. It sends this request to T memory agent and then transfers pattern to B or T Killer agent. When there is not a full compliance between them, T-Helper agent generates a new pattern selection algorithm based on its previous algorithms for selecting a pattern with the most compliance. This agent waits for receiving B and T-killer's feedback after sending the pattern. Then it stores the algorithm and feedback. The agent has the following modules:

Interface: This module is responsible for communicating between modules of this agent and other agents.
Detector: it recognizes the type of intrusion.
Algorithm Planner: This module designs a new selection algorithm when there is not a full compliance between the audit trail and patterns.
Memory: This module collects feedback related to selected algorithms and then gives to T-Memory agent.

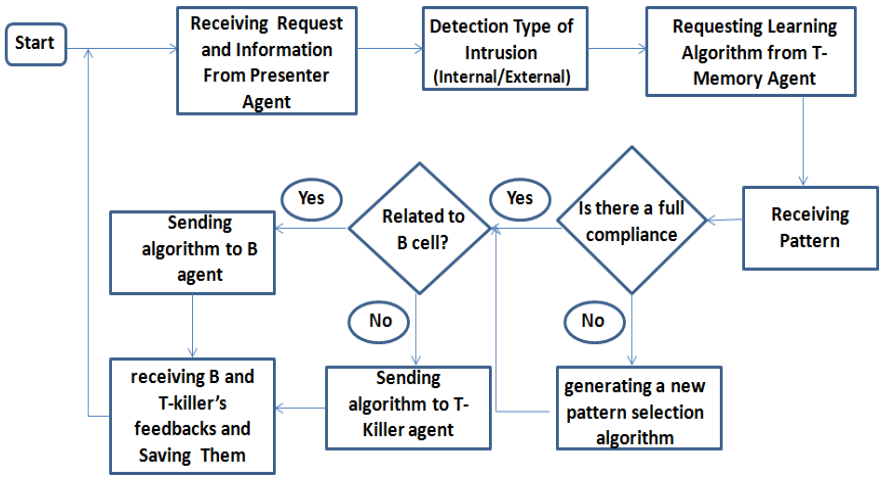

Figure 3. The flowchart of internal functions of T-Helper agent.

5.3. *T-Memory Agent*

This agent is similar to T-Memory cells. According to the request sent by Helper agent, this agent gets information from this and sends proposed pattern to it until its compliance with the obtained information is reviewed. This pattern includes the methods of eliminating intrusion activity. In figure 4, the internal functions of this agent are shown. This agent has four modules which are listed below:
Interface: This module is responsible for communicating between modules of this agent and other agents.
Pattern Presenter: this module presents pattern considering the obtained information.
Pattern Memory: This module will record the successful patterns.
Analyst: All decisions of T-Memory agent are taken by this module.

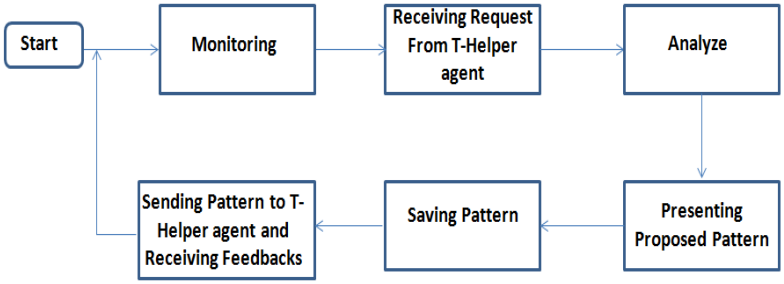

Figure 4. The flowchart of internal functions of T-Memory agent

5.4. *B Agent (BA)*

The agent plays the role of B cells. As mentioned, the activities of the network are divided into two parts: intrusion via users or non-user. The patterns related to users are transferred to this by Helper agent, and then it uses the patterns and prevents intrusion. This agent communicates with agent to use their correct methods. Then it disables access of offending user. Finally, if this method is successful, necessary feedbacks are sent to helper agent. Figure 5 shows the internal functions of this agent.

The agent has the following modules:

Interface: This module is responsible for communicating between modules of this agent and other agents.
Analyst: All decisions of B agent are taken by this module.
Killer: This module kills the main reason of intrusion.
Method Memory: this module records all of the correct procedures to eliminate intrusion.

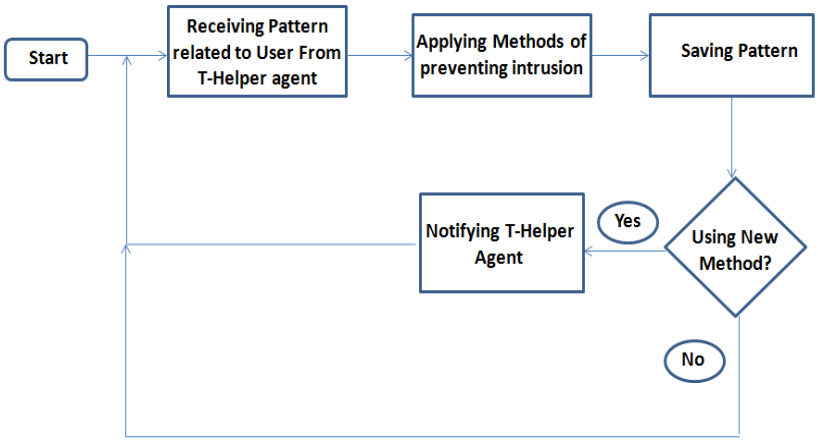

Figure 5. The flowchart of internal functions of B agent.

5.5. T-Killer Agent

Modules of this agent are similar to B agent. The difference between this agent and B is that T-killer agent prevents external intrusion. In figure 4, the internal functions of this agent are shown.

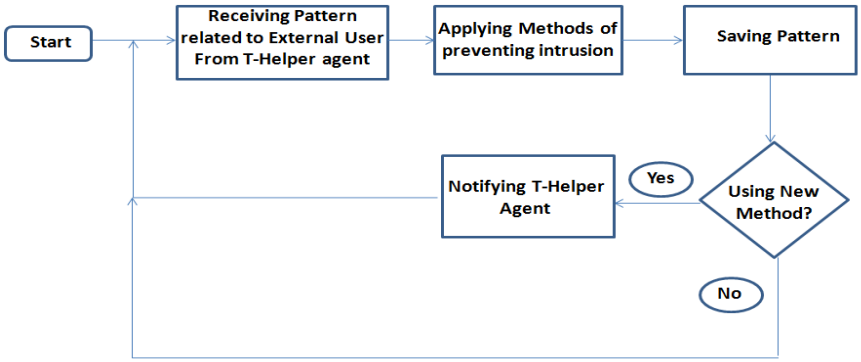

Figure 6. The flowchart of internal functions of T-Killer agent.

The agents of proposed model use a decentralized security mechanism to eliminate unknown security challenges and risks. In this model, it is not necessary to use and update security software. When a security incident occurs, the agents would be aware of the whole network and confront against it. However, the role of centralized node could not be eliminated or ignored, but according to the proposed model inspired by immune system, cloud computing will be more safe and agile. The robustness of network will not depend on the particular node and management of system will be decentralized.

The conceptual model inspired by BIS is presented. This model consists of a set of autonomous agents that can communicate with each other and increase their knowledge. Agents are able to learn. Over time, the knowledge of system will be increased and system will be reinforced. Agents are deployed in cloud data center and if one of them is removed, another agent will be replaced quickly. They continuously monitor environment, identify intrusion and eliminate them. Occurring intrusions are divided in two types: Users and non-users. Different methods are presented for each of these types. Presenter agent reviews the behavior of users and non-users in date center. Once the intrusion is identified, information is sent to Helper agent and this agent sends them to T-Memory agent until it receives function pattern. If there is not a full compliance, Helper agent will create algorithm and send it to B or T-killer agent. They eliminate intrusion according to the type of attack. In proposed model, the robustness of a system is not dependent on an especial node. Furthermore, the management of systems is decentralized.

6. CONCLUSION

In this paper, inspired by BIS and the autonomic computing, a conceptual model based on BAs with learning ability is proposed. The proposed model is composed of five different types based on B and T lymphocytes. This model is designed at different levels. In the first level, roles, relationship and activities of each agent are described and their components such as modules, programs and functions are shown in the second level. Also their interactions have been described. The main advantages of the proposed model are the use of BIS, decrease in the need for a central element, self-discovery and removal of defective, no need for updating, improvement of the knowledge and performance of the system through the time.

REFERENCES

[1] Xiaowei Yan, Xiaosong Zhang, Ting Chen, Hongtian Zhao, and Xiaoshan Li, (2011) "The Research and Design of Cloud Computing Security Framework", Advances in Computer, Communication, Control & Automation, LNEE 121, pp. 757–763. Springer.

[2] Jia Weihua, Sun Shibing, (2012) "Research on the Security Issues of Cloud Computing", Intelligence Computation and Evolutionary Computation, AISC 180, pp. 845–848. Springer,

[3] S. Pearson and G. Yee (eds.), (2013) "Privacy and Security for Cloud Computing", Computer Communications and Networks, Springer.
[4] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, (2010) "A Cooperative Intrusion Detection System Framework for Cloud Computing Network", International Conference on Parallel Processing Workshops, IEEE.
[5] Kong, Jinzhu, (2011) "AdjointVM, a new intrusion detection model for cloud computing", Elsevier.
[6] Muna, Elsadig, Abdullah Azween, and Brahim Belhaouari Samir, (2010) "Immune multi agent system for intrusion prevention and self healing system implement a non-linear classification", International Symposium in Information Technology IEEE, pp 1-6.
[7] Chung-Ming Ou, Yao-Tien Wang, Ou, C.R, (2011) "Intrusion detection systems adapted from agent-based artificial immune systems", IEEE international Conference, pp 115-122,
[8] T. Banirostam and M. N. Fesharaki, (2011) "Immune System Simulation with Biological Agent Based on Capra Cognitive Framework", 13th International Conference on Modelling and Simulation, IEEE UKSim 2011, Cambridge, UK, pp.122-127, DOI 10.1109/UKSIM.2011.32.
[9] Norma Montealegre, (2012)" Agent-based artificial immune system model for the detection of faults in a distributed satellite system", IEEE First AESS European Conference,pp 1-6.
[10] T. Fulop, C. Fortin, O. Lesur, G. Dupuis, J. R. Kotb, J. M. Lord and A. Larbi, (2012) "The Innate Immune System and Aging: What is the Contribution to Immunosenescence ?", Open Longevity Science 6: 121-132
[11] Tucker W, LeBien and Thomas F, Tedder, (2012) "B lymphocytes: how they develop and function", Bloodjournal : 1570-1580
[12] Lauren Sompayrac, (2003) "How Immune system works", Wiley-Blackwell.