ISA-based model for risk detection in Cloud Computing environment

Amal BENFATEH*
Department of Physics;
Telecommunication & computer Network Team;
Samlalia Science faculty;
Cadi Ayyad University
Marrakech, Marocco

F. GHARNATI
Department of Physics;
Telecommunication & computer Network Team;
Samlalia Science faculty;
Cadi Ayyad University
Marrakech, Marocco

T. AGOUTI
Computer Science Departement
Telecommunication & computer Network Team;
Samlalia Science faculty;
Cadi Ayyad University
Marrakech, Marocco

Abstruct—Cloud computing is the result of the evolution and the adoption of existing technologies and paradigms. Because of its accessibility via internet, that makes it subject to a large variety of attacks. In present paper, we focus on risk assessment by using an intelligent software agent to develop an immune system of cloud.

Key-Words: -Cloud computing; risk assessment; intelligent software agent; intrusion detection

1 INTRODUCTION:

Today's organizations are a target of information security attacks. More we use e-service, more we are in penetration danger. Attacks could be due to a human or software treat… maybe it is difficult to discover the kind of attacks but we know it would lead to harm our data or our system, or worst, lose a large amount of money; that's why organizations spend millions of dollars on security of technical equipments such as firewalls, intrusion detection systems, encrypting systems, anti-virus tools to protect their systems against threats. Nevertheless, there is always a cleaver intruder that succeeds in sneaking or exploits unknown vulnerability. Therefore, organizations need to manage their information security risks to protect their assets and thus their business values.

Regarding to CSI/FBI survey 2007, 13% of companies which are participated in the survey have no idea that how much they spent for security in last year. The 48% of them suppose that they should invest just 1% of IT budget for security awareness but just 39% are using ROI (Return on Investment) to ensure how much is enough to spend on security. The 46% of companies have obviously found at least one security incident in the past 12 months but only 29% of them have security risk management techniques in progress. What is the most challenge for these companies?

The answer is simple. They don't know about what they have, and what they need. They want to know which asset or technology has a security risk and for which one, they have enough security control to protect. [1]

On the other hand, risk management is usually human activity that includes assessing task and developing security strategy… the important part of the risk management is identifying treats and vulnerabilities by taking into account all past incidents and their impacts on system. To manage this challenge we propose exploit advantages and benefits of software agents to automate this important activity.

2 CLOUD COMPUTING ENVIRONMENT:

2.1 Cloud characteristics :

The National Institute of Standards and Technology's definition of cloud computing identifies five essential characteristics: [2]

- On-demand self-service: give the customer the possibility to provision power of computing as needed without any human interaction.
- Large network access: make the cloud available from any type of network using any client platform.
- Resource pooling: cloud uses a multi-tenant model to serve multiple consumers. The resources have to be pooled to maximize the number of consumers.
- Measured service: cloud systems must monitor resources usage appropriate to the type of service. This can be done by using a metering capability.
- Rapid elasticity: capabilities can be elastically provisioned and released, in some cases automatically,