Using Visualization Technology to Detect and Prevent Attacks in Cloud Computing

Tom Terry Jr. and Huiming Yu
Department of Computer Science
College of Engineering
North Carolina A&T State University
Greensboro, NC, USA

Abstract - Cloud computing is a newly emerged technology that provides a flexible and scalable information infrastructure to users. It also attracts hackers to attack cloud computing systems. Enhancing cloud computing security has become very urgent and important. In this paper we discuss the characteristics of cloud computing, various threats, visualization and visual analytical technologies, and propose a Cloud Computing Security Visualization Prototype System (CCSVPS) that will use visual analytical and visualization technologies to analyze cloud computing traffic information, display traffic data in multiple views and multi-levels, and make rapid and correct decisions for actions. We will use CCSVPS to detect and prevent Indirect Denial of Service as one of experiments.

Keywords *– cloud computing, visualization, security*

I. INTRODUCTION

Cloud computing is a newly merged technology that provide a flexible and scalable information infrastructure to guests. It is transforming the way people use the internet and how servers provide services to customers. It provides various infrastructures that allow users to support their businesses, store data, and use various services, without investing in new infrastructure, training new personnel, or licensing new software. The cloud infrastructure provides services in a distributed environment, while sharing resources and the storage of data in a data center. These services are divided into several categories such as Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). The major advantage of cloud computing is that it provides dynamic, on-demand infrastructure at a favorable cost [1, 2].

Visualization is an increasingly effective technology to help researchers and administrators to capture network traffic packets, understand network traffic and captured data. Visualization technology encompasses the interpretation, analysis, representation and communication of views and network traffic information. It takes advantage of strong human pattern recognition skills through visual representations that can often make patterns and anomalies evident to the user. By interactive visual interface visual analytics helps users and administrators analyze large quantity of data and make rapid and accurate decisions [3, 4, 5, 6].

In order to keep cloud computing systems secure and stable we can use visualization and visual analytics technologies to monitor the cloud computing traffic, interact with the system in real-time, to detect abnormal behaviors, and to proactively respond to the various attacks. In this paper we propose a Cloud Computing Security Visualization Prototype System. In section II cloud computing security related issues will be presented. In section III our current research will be discussed. In section IV future work will be discussed.

II. CLOUD COMPUTING SECURITY

Cloud computing consists of guest and provider sides. In figure 1 the guest side is the enterprise portion and the provider side is the service provider portion. There are various threats on both sides.

A. Guest and Provider Sides

The guest side is the end user who signs up with the company to use the cloud. The guest side of a cloud is what the client has access to when he/she creates an account. It is the interface that clients see after they enter their credentials and have the ability to use the services provided by the cloud. The guest side provides the end user with the ability to choose cloud services and environment such as operating system and applications they will use in the cloud. The guest side may consist of different users, laptops, tablets, cell phones, various computers and enterprise centers. The provider side of a cloud in figure 1 is the service provider which consists of application servers, service platforms, runtime environments and data centers. One example of application server is WebSphere Application Server that is a Java EE, EJB supported technology-based application platform. Build, deploy and manage robust, agile and reusable SOA business applications and services of all types while reducing application infrastructure costs. There are three or more datacenters provided in case of an emergency so guests will always have access to their information on the cloud. It is the responsibility of the provider to manage those resources. There are multiple service platforms that perform management, engineering, inventory and repair functions for service providers and their networks. These support services are used when data in the datacenter might become corrupted. They provide support to get the datacenter up and running again so the customer will have access to their data [7].

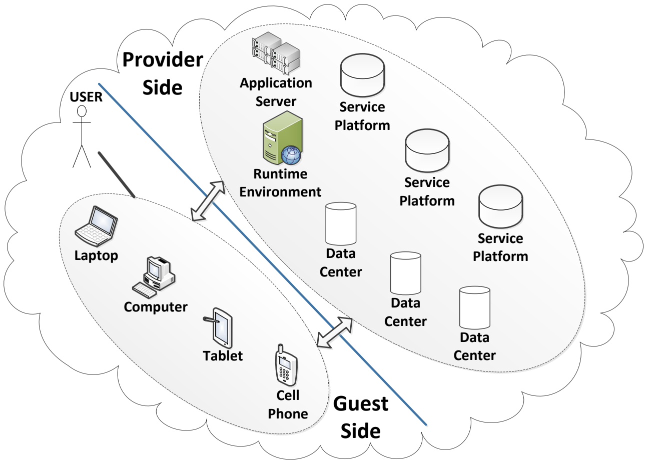

Figure 1. Guest and Provider Sides of Cloud Computing

B. Cloud Computing Threats

Cloud computing offers numerous advantages. It also brings various threats, risks and privacy issues to users. These attacks such as social engineering attack, XML signature wrapping attack, malware injection, data manipulation, account hijacking, traffic flooding, and wireless local area network attack pose a great risk to cloud computing systems. There have been many instances where companies have fallen victims to cloud computing being hacked [7, 8, 9]. We categorized cloud computing threats into external threats, guest to guest threats and cloud to guest threats as shown in figure 2.

External threats include computer and network attacks that can occur by using Internet. These threats can be SQL injection, Cross-site scripting, Denial of Service, Indirect Denial of Service, network sniffing, etc. Indirect Denial of Service is an example that occurs in cloud computing. An Indirect Denial of Service attack is a big threat to cloud computing. A guest to guest threat is where a user of the cloud system attempts to attack another user on the cloud for malicious purposes. Guest to guest threats involves a user on the same cloud performing a malevolent attack against another user by sending a file that may contain a virus of some sort. The examples are cloud malware injection, insecure or incomplete data deletion, Mis-configuration, etc. Cloud to guest threats could be the most malicious type of attack that can occur in the cloud infrastructure. A cloud with malicious software encapsulated within a virtual machine could bring down different virtual machines, making the cloud unstable. Trojan horse is an example.

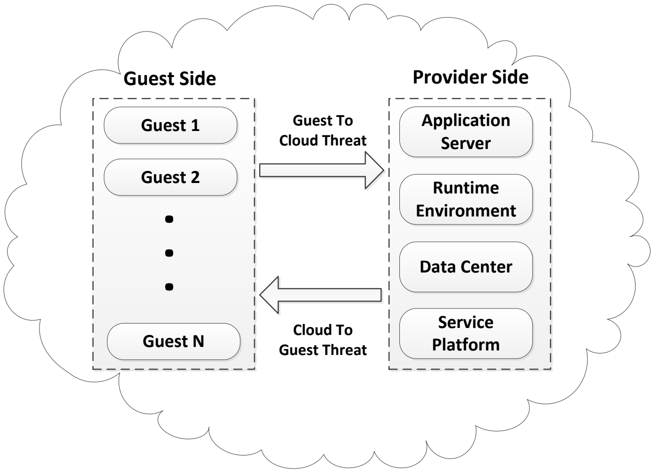

Figure 2. Threats in Cloud Computing

III. CURRENT RESEARCH

We propose a Cloud Computing Security Visualization Prototype System (CCSVPS) that will use visual analytical and visualization technologies to analyze cloud computing traffic information, display traffic data in multiple views and multi-levels, and make rapid and correct decisions for actions. We will develop visual analytical algorithms, and a smart visualization module to help users and administrators monitor cloud computing traffic, analyze collected large quantity data and make decision.

A. Indirect Denial of Service attack

Denial of Service (DoS) is a serious attack that can be categorized as two types; stopping a service and resource exhaustion. Stopping a service is the crashing of a system or network. In most cases it requires intervention from an administrator to reboot or power off the system for the system to get back online. The second type involves flooding the system or network with so much information that the system cannot respond. One of the more severe types of attacks would be a SYN flood, which is simply a type of Denial of Service.

In cloud computing all servers work in a service specific manner with internal communication among them. When a server is overloaded or has reached the threshold, it transfers some of its jobs to a similar service-specific server to offload tasks. If a hacker successfully attacks one server and causes the denial-of-service, the victim server will transfer upcoming tasks to other servers in order to offload jobs. Thus, the same thing will occur on other servers and the hacker is successful in engaging the whole cloud system by just interrupting the usual processing of one server, in essence flooding the cloud.

An Indirect Denial of Service attack occurs when a DOS attack denies more services than the hacker intended. It is a big threat to cloud computing. Indirect Denial of Service works unintentionally because a hacker intends to deny the service of a specific aspect of a cloud but affects other aspects. Suppose a hacker wanted to stop users from logging into the cloud by sending false requests to slow down the network and increase the workload on the server. The hacker indirectly denies the service of users who also want to log out of the cloud and of users who want to upload or download from the cloud. The impacts depend on the level of sophistication of the cloud system. The cloud computing system notices the lack of availability, and may try to 'evacuate' the affected service instances to other servers. It results in additional workload for those other servers, and thus the flooding attack passes to another service type, and spreads throughout the whole computing cloud [7, 10].

B. Cloud Computing Security Visualization Prototype System

Based on the characteristics of cloud computing we propose a Cloud Computing Security Visualization Prototype System (CCSVPS) that will use visual analytical and visualization technologies to analyze cloud computing traffic information, display traffic data, and make rapid and correct decisions for actions. We will use CCSVPS to detect and prevent Indirect Denial of Service attacks as one of the experiments. The Cloud Computing Security Visualization Prototype System consists of four major parts. The first part is a user friendly interface that allows users to interact with cloud computing systems in real-time [11]. The second part is a traffic capturer that can capture cloud computing traffic data according to administrator's requirements. The third part is a set of visual analytical algorithms that provide function to filter out unnecessary captured data, analyze data, discover the malicious packets, prevent and react to attacks. The fourth part is a smart visualization module that helps users monitor cloud computing traffic and understand captured data.

- **Visual Analytical Algorithms**

A large quantity of cloud computing traffic data will be collected and saved in a database. In order to allow a user/system to synthesize cloud computing information, to derive insight from a large quantity of complicated, ambiguous and conflicting data, to detect and discover unexpected network behaviors, and to combine with administrator's knowledge to provide assessment and communicate assessment effectively for actions several algorithms have been and will be developed. The first algorithm is a filter algorithm that will filter out unnecessary data according to administrator setting. The second algorithm is an analytical reasoning algorithm that integrates the neural network technique and analytical reasoning process to analyze a large quantity of traffic data, to discover correlations of data, to provide assessment and communicate assessment effectively for actions. This algorithm checks some parameters of incoming IP packets to provide analyzed information. The third algorithm is preventing algorithm. Based on the results of algorithm 2 and input of administrators this algorithm will make rapid and correct decision for actions.

Our research is focusing on Indirect Denial of Service attacks right now. Once an Indirect Denial of Service attack is detected the third algorithm will stop to spread over cloud computing. Once a server is overloaded the preventing algorithm will check current situation, compare with normal cases, and then decide it is an attack or normal overloaded work. If it is an Indirect Denial of Service attack it will keep the victim server from transferring upcoming jobs to other servers. These algorithms will run on the hypervisor of the provider side.

- **A Smart Visualization Module**

A smart visualization module will be designed and implemented to display complicated data on the screen in an easy to view, easy to understand fashion. This module will take advantage of advanced visualization techniques to display filtered network data in 2D, 3D and 4D formats according to a user's needs.

Multivariate data visualization techniques will be used because it provides the functions to help users investigate certain activities or anomalous behavior in greater detail. Multivariate data visualization techniques can be classified as projection based where only subset of the variables is visualized. Projection based requires some ordering or prioritization of the dimensions. Multiple projection views can be linked and made highly interactive. Multi-dimensional data are mapped onto 2D plots, plotting n-dimensional points as polyline segments through the N axes. Parallel coordinates will be used in this module. We will brush the large of amount of data by focusing on certain subset of data and making drill down/roll up operation very efficient.

In order to simplify the graph and let the user see a clear picture we will collapses clusters of nodes that match well enough (over some threshold) into a single larger node. Clustering has been shown that is a useful and effective tool in process of discovering security events in unlabeled data, however not much has been done to use it in the process of characterizing such events [12]. In this module a user could have two choices. If the user prefers a connection between two separate nodes, he/she needs to automatically combine them into a single collapsed node. If the user wishes to view one or more of interconnections enough that a node or group of nodes falls below the threshold, then the collapsed node must be split. Once collapsed, the user uses the bottom layer to zoom inside the node to view the internal structure. The difficulties we face are developing an algorithm to collapse closely knit clusters of nodes, and decide the relationships between a collapsed node and other nodes for a detail view. We will study the Kohonen's self-organizing map algorithm and develop a mapping algorithm.

IV. FUTURE WORK

There are various threats to cloud computing systems. In order to protect cloud computing technologies of detection, prevention and responding various attacks must be developed. Based on characteristics of cloud computing we propose a Cloud Computing Security Visualization Prototype System (CCSVPS) that will use visual analytical and visualization technologies to analyze cloud computing traffic information, display traffic data in multiple views and multi-levels, and make rapid and correct decisions for actions.

Our current research focuses on detecting and preventing Indirect Denial of Service in cloud computing. In future we will implement the Smart Visualization Module and user interface, and use the CCSVPS to detect and prevent Indirect Denial of Service as one of experiments.

ACKNOWLEDGEMENT

This work was partially supported by National Science Foundation under the award numbers CNS-0909980, DUE-0830686 and DUE 1129136.

REFERENCES

[1] k. Decker, “What Joni Mitchell might say about cloud computing”, http://decker.com/blog/2010/05/what-joni-mitchell-might-say-about-cloud-computing/

[2] D. Jamil and H. Zaki, “Cloud computing security”, International Journal of Engineering Science and Technology, Vol. 3 No. 4, April 2011.

[3] L. Harrison and A. Lu, “The future of security visualization: lessons from network visualization”. IEEE Network, Vol. 26, Issue 6, 2012.

[4] X. Li, Q. Wang, L. Yang and X. Luo, “The research on network security visualization key technology”, Proceedings of 4th International Conference on Multimedia Information Networking and Security, 2012.

[5] X. Li, Q. Wang, L. Yang and X. Luo, “Network security situation awareness method based on visualization”, Proceedings of 3th International Conference on Multimedia Information Networking and Security, 2011.

[6] H. Yu, X. Dai, T. Baxliey, X. Yuan and T. Bassett, “A visualization analysis tool for DNS amplification attack”, Proceedings of the 3rd International Congress on Image and Signal Processing, October 2010.

[7] C. Barron, H. Yu and J. Zhan, “Cloud computing security case studies and research”, Proceedings of the 2013 International Conference of Parallel and Distributed Computing, July 2013.

[8] Cloud Security Alliance, “Top threats to cloud computing”, Cloud Security Alliance, March 2010.

[9] S. Qaisar and K. Khawaja, “Cloud computing: network/security threats and countermeasures”, Interdisplinary Journal of Contemporary Research In Business Volume 3, January 2012.

[10] M. Jensen, J. Schwenk, N. Gruschka and L. Iacono, “On technical security issues in cloud computing”, Proceedings of IEEE International Conference on Cloud Computing.

[11] H. Yu, L. Wang, J. Zhang and J. Barksdale, “Developing a secure geospatial visualization and collaboration system using software engineering technology”, International Journal of Computers and Applications, Vol. 28, Number 4, 2006.

[12] L. Portney, E. Eskin, and S. J. Stolfo. Intrusion Detection with Unlabeled Data Using Clustering. In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001), 2001.