Honeypot Service based on Cloud against DDoS to support VoIP Service

Byungrae Cha, Sujeong Shim
GenoTech Inc., GwangJu,
Korea
brcha@nm.gist.ac.kr,sjsimox@hanmail.net

ABSTRACT: *Computing is facing another revolution. This time it is called 'Cloud Computing' and involves accessing software applications, data storage and processing power over the Internet. In this paper, we describe the multistage anomaly detection scheme to DDoS attacks in cloud computing resource of future internet. This scheme is composed by 3 stages. Monitoring stage performs misuse detection by rules of attack patterns to well-known DDoS attacks. Lightweight anomaly detection stage could classified volume data into large volume data and small volume data, and applied Bayesian methods. And focused Anomaly detection stage is performed to detect new DDoS attacks by unsupervised learning algorithm.*

Keywords: Honeypot, Cloud Computing, DDoS, VoIP

Received: 19 November 2014, Revised 24 December 2014, Accepted 4 January 2015

1. Introduction

Computing is facing another revolution. This time it is called 'Cloud Computing' and involves accessing software applications, data storage and processing power over the Internet. Gaining access to computing resources online may not initially seem that radical a proposition. However, Cloud Computing is already starting to turn the software industry upside down. After all, once people start running programs over the Internet they will have no need to purchase and install them on their own computers. Companies will also not be required to purchase and maintain so much hardware and software if it can simply be rented online. The growth of Cloud Computing therefore threatens the survival of many software vendors and corporate data centers. [1] Information Technology Laboratory of NIST [2] has defined Cloud Computing in 2009. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model *promotes* availability and is composed of five essential characteristics, three service models, and four deployment models. The documents of many research institutions (ENISA, CSA, SUN, etc) on cloud computing are always referred to a DDoS attacks item warningly. DDoS attacks pose a major threat to the availability of interest services. A DDoS attacker can greatly reduce the quality of a target internet service or even can completely break the network connectivity of a server generally to achieve resource overloading; a DDoS attacker will first compromise a large number of hosts and subsequently instruct this compromised host to attack the service by exhausting a target resource. And cloud systems of SMEs will be the main target for hackers. Recently Amazon's cloud services were stopped by a TCP Syn-flood attack during short interval time. In this situation, Security tool market in cloud computing environment is formed newly. DDoS attack and response have been extended from previous research. Jelena and Peter have classified DDoS attack and defense by mechanisms and Sumit has classified DDoS attack by techniques as professional.

2. Related Work

2.1 Ddos Attack

In March 2009, VeriSign commissioned Forrester Consulting to conduct a study on distributed denial of services (DDoS) threats and protection. This survey included 400 respondents from the US and Europe and was designed to provide quantitative data regarding today's DDoS threats and companies' defense strategies against these threats. [3]

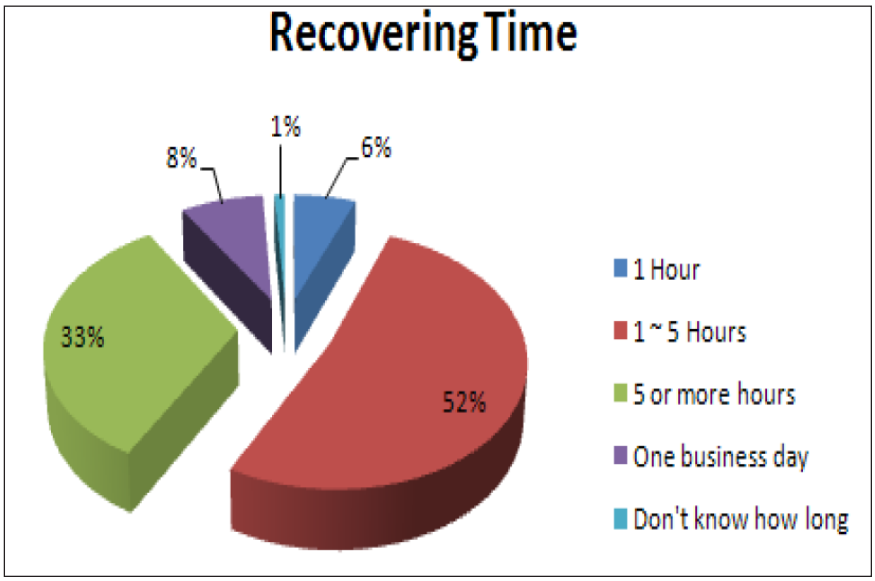

Figure 1. Recovering time from a DDoS attack

A total of 124 survey respondents said their organizations experienced one or more DDoS attacks that disrupted their services. For those 124 IT decision-makers, recovering from the effects of the attack was a non-trivial undertaking: 64 reported that it took them between 1 and 5 hours to restore their services, while 41 said the recovery process took between 5 and 8 hours. A smaller percentage,10 respondents, indicated that it took more than one business day to fully restore their services as shown in Figure 1. The notorious July 4 attacks, which were orchestrated by a custom bot, included SYN, PING, and GET floods. These attacks on U.S. and South Korean networks targeted more than 47 government and private institutions.

Although the magnitude of the attacks was fairly low (averaging 39 megabytes per second),2 more than 200,000 bots were employed, greatly amplifying the impact and reach of the attacks. Besides this type of direct flood attack, in which a high volume of spoofed packets is sent directly to the victim(s), attackers are increasingly using reflection flood attacks. In reflection flood attacks, attackers use recursive DNS servers to bounce attacks to their victims, and in the process amplify the attack and make it more difficult to track down the attack source. While many organizations are increasingly concerned about the DDoS threat, few organizations have specific DDoS protection mechanisms in place. Those that do address DDoS often rely on approaches that lack the capacity and agility to mitigate attacks rapidly and preferably before they reach the network. Despite popular belief, the following measures, when implemented within most organizations, are insufficient to mitigate today's diverse, large-scale attacks: Over-provisioning of bandwidth, Firewalls, IDS, IPS, Routers, Black hole routing, and Reliance on ISP mitigation.[4]

2.2 Threat Models In Cloud Computing

In this section, we model threats on cloud computing environment as shown in Table 1. The resources of cloud computing are facing the new target of attackers or resources for attack.

We briefly describe the DDoS attacks of threat model 1 in cloud computing as shown in Figure 2. The members of Cloud Computing in DDoS attacks are composed of Normal Cloud User, Cloud Manager, Malicious User, and External Monitor. And the Cloud system is classified into target cloud system and Zombie PC or Leased Resources. The Eucalyptus cloud system is classified into Cloud Controller, Cluster Controllers, and Node Controllers.Figure 2 (A) is the targets of DDoS attack in cloud computing environment: Cloud Controller or Cluster Controller. The major target of DDoS attacks in the Cloud system will be Cloud Controller.

Targets / Attacker	Cloud System	External Legacy System
Malicious Cloud User	-	Threat 2
External Attacker	Threat 1	-

Table 1. Threat models in cloud computing

The Cloud Controller is the gateway to provide all the services in cloud system. Cluster Controller is always hidden to support computing resources behind Cloud Controller Although the Cloud Controller is exposed to external to provide services. The minor target will be Cluster Controllers. The ripple effect of Cluster Controller by DDoS attack is smaller than Cloud Controller, but it has a significant impact on cloud system performance.

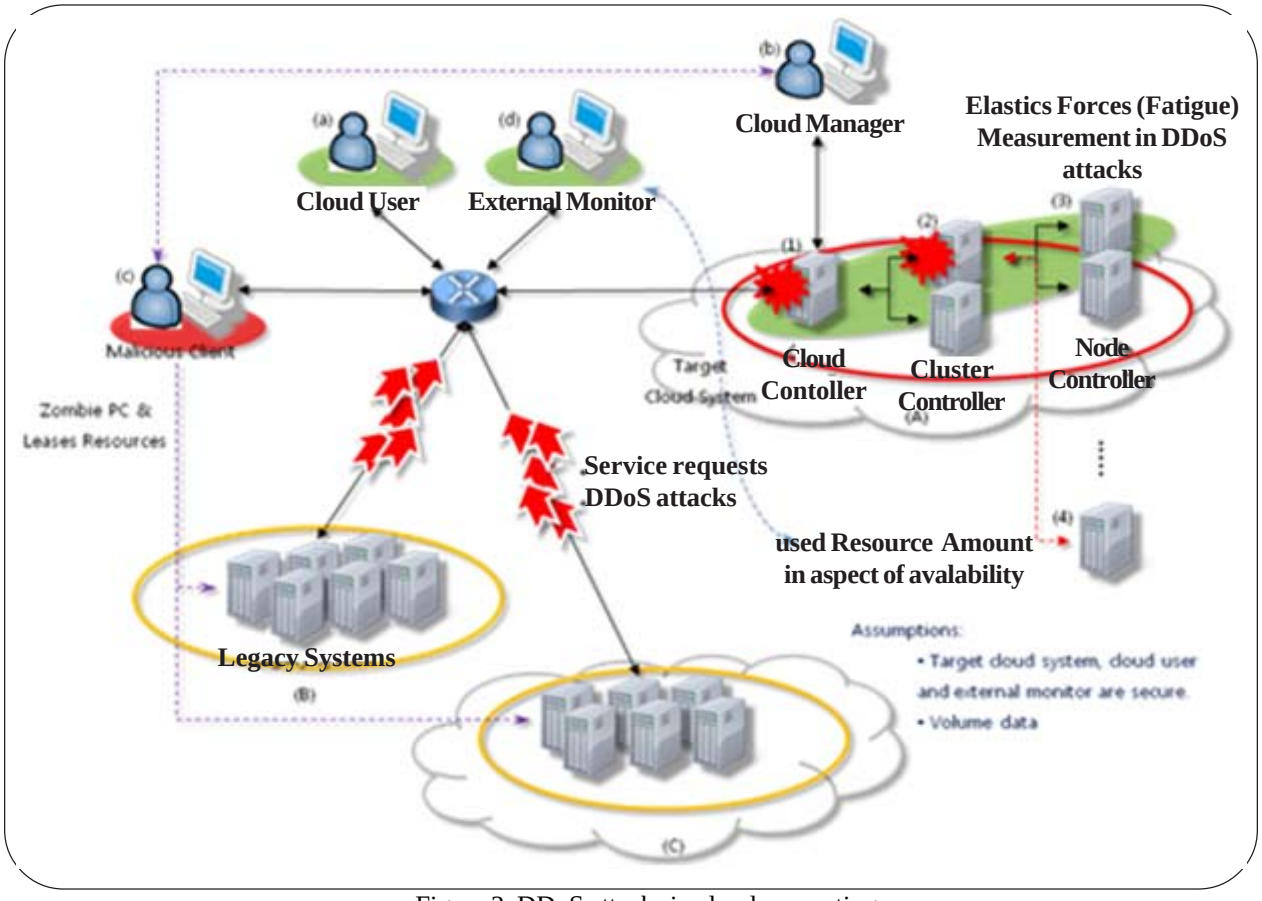

Figure 2. DDoS attacks in cloud computing

2.3 Multistage Anomaly Detection Of Ddos Attacks In Cloud Resource

We describe the multistage anomaly detection scheme to DDoS attacks in cloud computing environment as shown in Figure 3.

This scheme is composed by 3 stages: monitoring stage, lightweight anomaly detection stage, and focused anomaly detection stage. Monitoring stage performs misuse detection by rules of attack patterns to well-known DDoS attacks. Lightweight anomaly detection stage could classified volume data into large volume data for fine-grained data analysis and a small volume data for focused anomaly detection stage, and applied Bayesian methods to fine-grained data analysis. And focused anomaly detection stage is performed to detect new DDoS attacks in large volume data by unsupervised & semi-supervised learning algorithm.In monitoring stage, the misuse detection as pre-processing will detect the well-known DDoS attacks by rules for

volume data in cloud. Some DDoS attacks have distinct characteristics that can be easily captured with a small set of detection rules.

For examples, attack symptoms of port scanning [5], backscatter [6, 7], and so on, Rule-based approaches have near-term appeal since they typically have low false-positive rates, even though their detection capabilities are limited to the set of attacks spanned by the rule-sets. As the name suggests the key constraint here is that the method not require significant processing so that it can be applied to a volume data.

Since the output of this stage triggers more detailed analysis in the third stage, false positives are less of a concern than false negatives. However, a false negative is a more serious. A false negative from the first stage will only cause more unnecessary work to be done in the second stage. Traffic anomalies on volume available between ingress interface and egress interface are often good indicators of flooding attacks.

Our approach involves the use of traffic time-series modeling to predict the expected future load on each customer facing interface. The large and small volume data are divided by traffic volume over network capability in time-axis. Fine-grained data analysis targets a large volume data, classifies by IP 6-tuple (srcaddr, dstaddr, protocol, srcport, dstport, flag), and makes small volume data.The Bayesian technique in second stage performs detailed analysis of DDoS attack candidate on network topology (source and destination) after fine-grained data analysis. Our specific scheme for the second stage involves the use of fine-grained data analysis of large volume data. Conceptually, fine-grained data analysis attempts to discover backscatter and scanning of DDoS attacks along source/destination IP and port numbers. Since the computational overhead with performing fine-grained data analysis is low, and the functionality provided is sufficient for investigating most known types of DDoS attacks we choose this approach. Our scheme is a combination of fine-gained data analysis and Bayesian technique-based approaches.

We can use distribution anomalies (backscatter and scanning) in fine-grained data analysis by Bayesian technique as triggers for further analysis. Even though our approach will reduce the search space for the third stage significantly, the scale of the problem is such that the computational overhead remains a concern. The other key requirements are accuracy, and the ability to detect useful DDoS attack candidates. Multi-dimensional (time-series and traffic space) clustering in small volume data using unsupervised learning algorithms provides another alternative for advanced coarse-grained data analysis. The basic theme of these approaches is to abstract the standard IP 6-tuple within multi-dimensional clustering techniques to report traffic patterns of interesting DDoS attack candidate. Typically, the complexity of the algorithm can be reduced by tuning the technique to report only interesting clusters, those that either have a large volume or those that have a significant deviation from an expected

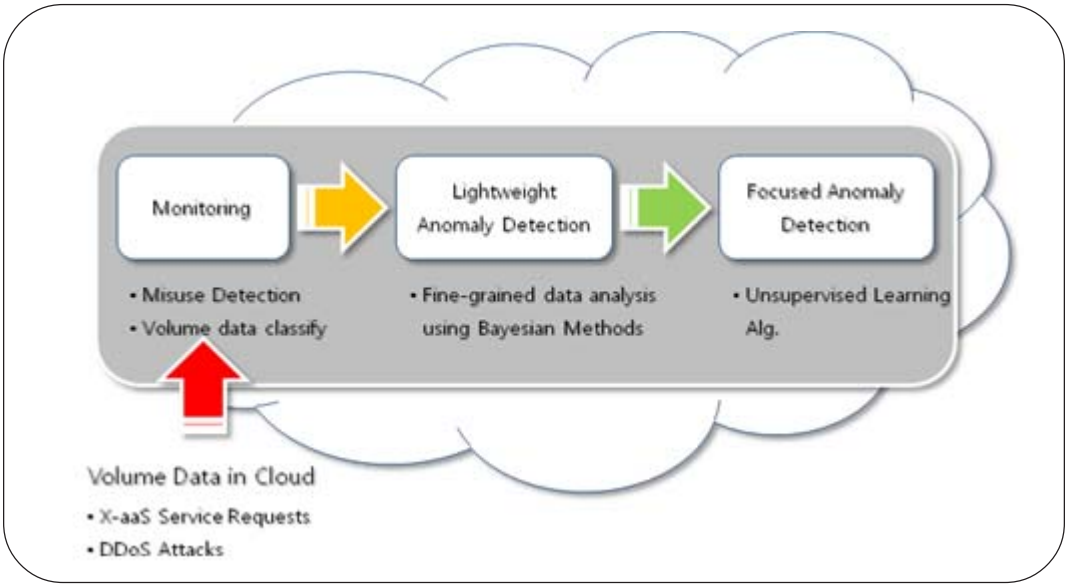

Figure 3. Multistage Anomaly Detection In Cloud Computing Resource

norm. Unsupervised learning algorithm in focused anomaly detection stage is used to detect significant deviations to identify hidden large volume anomalies of DDoS attack candidates.

2.4 Experiments Data of DDoS

The Information Systems Technology Group (IST) of MIT Lincoln Laboratory, under Defense Advanced Research Projects Agency (DARPA ITO) and Air Force Research Laboratory (AFRL/SNHS) sponsorship, has collected and distributed the first standard corpora for evaluation of computer network IDS [8].The DARPA datasets have included the many attacks with symptons of port scanning, backscatter, and so on, as shown in Figure 4.

2.5 Honeypot Security

A honeypot is a deception trap, designed to entice an attacker into attempting to compromise the information systems in an organization. The honeypot can serve as an early-warning and advanced security surveillance tool, minimizing the risks from attacks on IT systems and network. Honeypots can also analyze the ways in which attackers try to compromise an information system, providing valuable insight into potential system loopholes. Honeypots can be classified into two categories: low-interaction honeypots that are often used for production purpose, and high-interaction honeypots that are used for research purposes. Low-interaction honeypots works by emulating certain services and operating system and have limited interaction. The advantages of low-interaction honeypots are that they are simple and easy to deploy and maintain. High-interaction honeypots are more complex, as they involve real operating system and applications. By giving attackers real systems to interact with, no restrictions are imposed on attack behavior, and this allows administrators to capture extensive details about the full extent of an attacker's methods.

3. Honeypot Service Based on Cloud Against DDoS to Support VoIP Service

Recently, the mega trends in the ICT sector can be aggregated into the Cloud Computing, Big-data, and IoT (Internet of Things). The needs of security tools and information security framework to provide seamless services are emerging within this mega trends.

In this study, the proposed technology is the security tools and security strategies to provide seamless services for VoIP-as-a-Service in the private cloud infrastructure. As shown in Figure 5, to provide a seamless service of VoIP, the proposed technology using private cloud infrastructure and virtualization technique can mitigate attacker's power and decoy attackers to impede service.

3.1 Honeypot Security Service Based on Cloud

The proposed technology of honeypot security service based on cloud is listed techniques for the construction of the security strategy for supporting the VoIP service as follows:

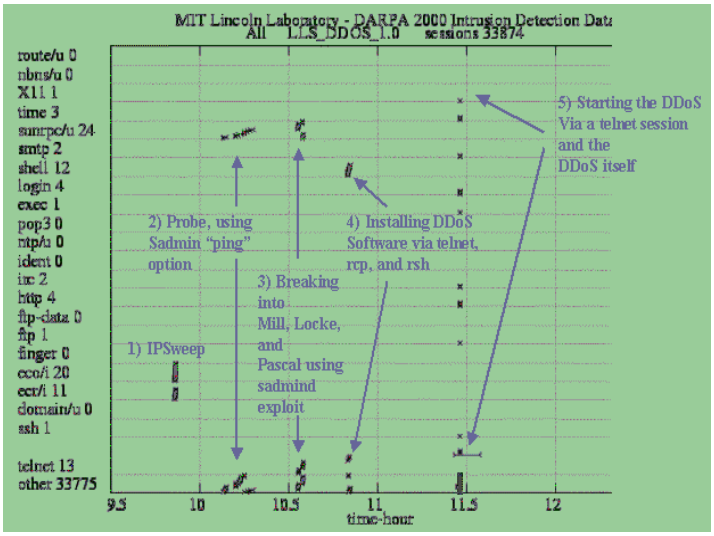

Figure 4. LLS DDoS 1.0 in MIT Lincoln Lab

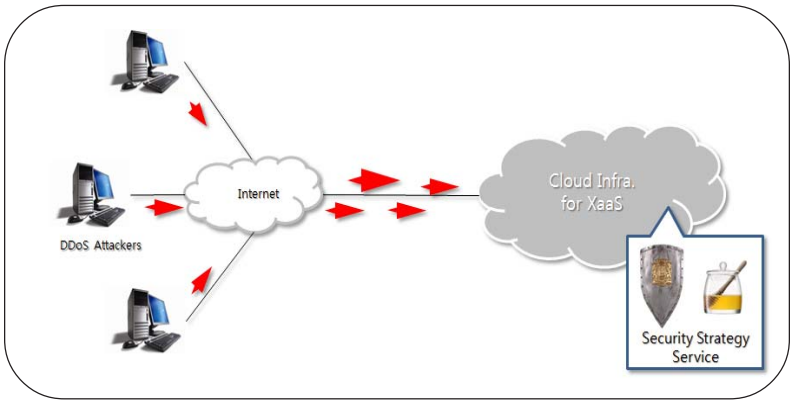

Figure 5. Concept diagram of Honeypot Security Servicebased on Cloud Computing

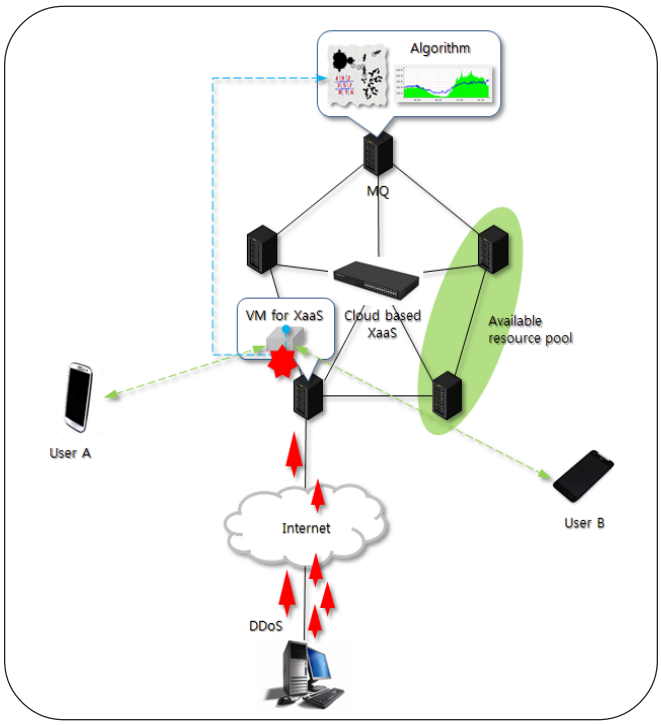

Figure 6. Security strategy service 1 of Honeypot based on Cloud infrastructure

Construction technique of open-source cloud computing infrastructure

Techniques of virtualization and real-time migration

Techniques of monitoring and MQ (message queue)

Security technique of Honeypot

The construction to support honeypot service is composed by the private cloud infrastructure, VoIP service, virtual machine, monitoring function, security strategy algorithm, MQ system, and users. Figure 2 presents the components of the proposed system and the state of DDoS attack.

3.2 Strategy of Honeypot Service against DDoS

The figures from Figure 6 to Figure 9 illustrate the proposed honeypot security function and security strategy service based on cloud infrastructure. Figure 6 presents the VoIP service on private cloud infrastructure and shows the state of DDoS volume traffic by attackers. In this situation, whenever the monitoring function on cloud infrastructure checked the network traffics and

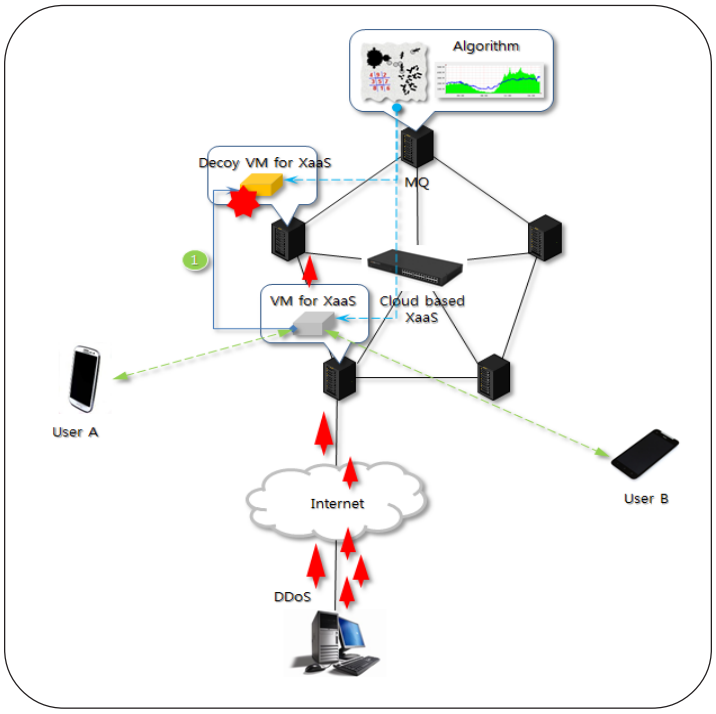

Figure 7. Security strategy service 2 of Honeypot based on Cloud infrastructure

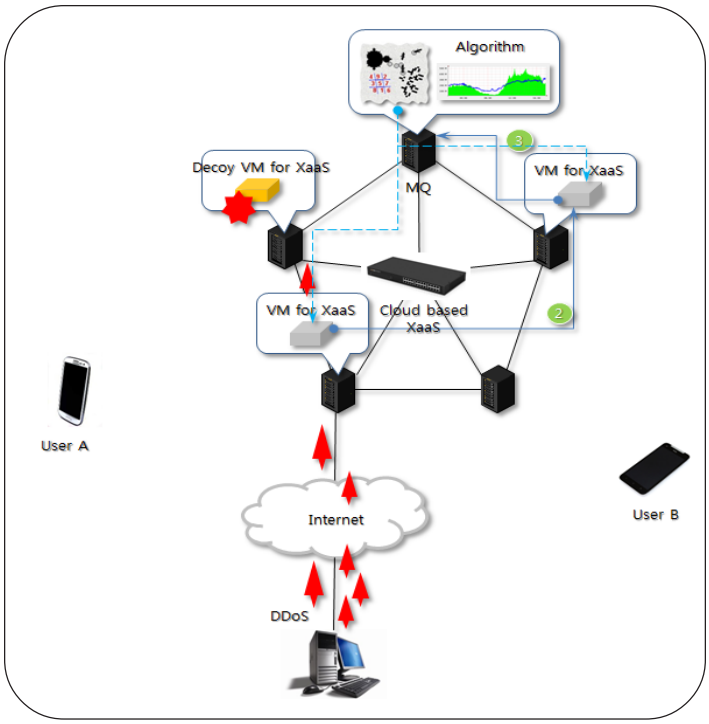

Figure 8. Security strategy service 3 of Honeypot based on Cloud infrastructure

available state of VoIP service. The virtual machine on private cloud infrastructure supports the VoIP service by requests of external users and attackers. The VoIP service that the attacker's target is the place to be in volume traffic congestion.

By monitoring function of cloud computing, the virtual machine supporting VoIP service is made the volume requests for session, and detected the approaching the limited state, and the many processes will be waited the resources to support service

with the volume network traffics. It's deadlock or bottleneck state. The monitoring function notifies the alarms of virtual machine state to the security strategy algorithm according to approach the threshold values of assigned computing power and network traffics.

Figure 7 illustrates the generation process of honeypot virtual machine by copying virtual machine of VoIP service. The level of copying virtual machine determines the low-interaction honeypot or high-interaction honeypot. In Figure 7, 1, the security strategy algorithm determines optimal network location to decoy attackers and assigns the resources to generate honeypot virtual machine using information among network location of attackers and available cloud resource pools of computing, storage, and networking. And the security strategy algorithm makes a detour or isolations, and entices to honeypots service.

In figure 8, the original VoIP virtual machine moves new network location, and prepares setting process to support seamless VoIP service using the private cloud resources(refer Figure 8, 2). Lastly, the original virtual machine that moved new network location for VoIP service notifies the completed message to the security strategy algorithm as shown in Figure 8.

Figure 9 presents the transferring and updating (refer Figure 9) of VoIP service information by message queue system process. Thus, the users request the VoIP service. So, the original virtual machine supports the VoIP service to users (refer Figure 9).

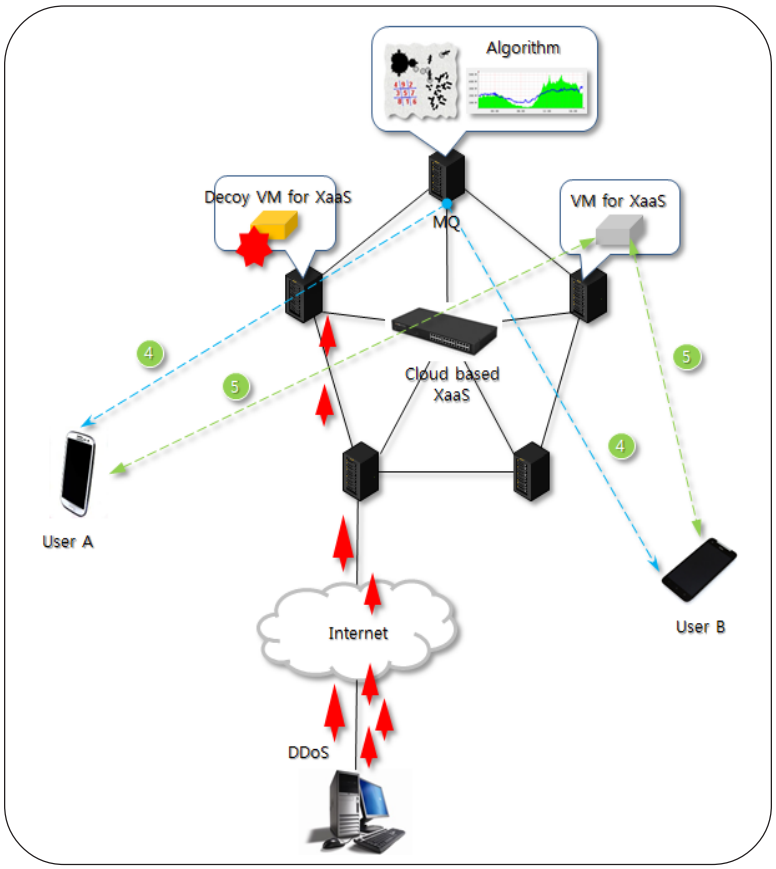

Figure 9. Security strategy service 4 of Honeypot based on Cloud infrastructure

4. Conclusions

Recently, the mega trends in the ICT sector can be aggregated into the Cloud Computing, Big-data, and IoT (Internet of Things). The needs of security tools and information security framework to provide seamless services are emerging within this mega trends. To provide a seamless service of VoIP, the proposed technology using private cloud infrastructure and virtualization technique can mitigate attacker's power and decoy attackers to impede service. We proposed the concept and basic design of honeypot security service and security strategy algorithm, and described simple process to support seamless VoIP service

using the private cloud resource and virtualization technique.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012R1A1A2041274). In addition, this research was also partially supported by the Ministry of Trade, Industry and Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) through the Promoting Regional specialized Industry.

References

[1] Christopher Barnatt. (2010). A Brief Guide to Cloud Computing, Robinson.

[2] Peter Mell., Tim Grance. (2009). The NIST Definition of Cloud Computing. Version 15, (October 7).

[3] Forrester Consulting. (2009). The Trends And Changing Landscape Of DDoS Threats And DDoS Protection, July 6.

[4] DDoS Mitigation: Best Practices for a Rapidly Changing Threat Landscape, VERSIGN

[5] http://en.wikipedia.org/wiki/Port_scanner

[6] http://en.wikipedia.org/wiki/Backscatter#Backscatter_on_the_internet

[7] Gyorgy J. Simon, Hui Xiong, Eric Eilertson,Vipin Kuma. (2006). Scan Detection: A Data Mining Approach, SIAM International Conference on Data Mining - SDM.

[8] DARPA Intrusion Detection Data Sets, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html