International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.107-114
http://dx.doi.org/10.14257/ijsia.2014.8.2.11

Concept Design and Case Studies of Testbed based on Cloud Computing for Security Research

ByungRae Cha[1], SuJeong Sim[2] and JongWon Kim[3]

[1,3]*School of Information and Communications, GIST, Korea*
[2]*Dept. of Computer Engineering, National Chonnam Univ., Korea*
brcha@nm.gist.ac.kr, sjsimox@hanmail.net, jongwon@gist.ac.kr

Abstract

Recently, there has been increasing researches on computing environment caused by changes in computing paradigm of security aspects with respect to big data issues and eco-system of cloud computing. Because the cloud computing is operated on a variety of devices, there is a demand for the security aspects corresponding to various cloud computing devices. In this sense, this paper is proposed the concept design of a testbed for security research and described the cases studies of cyber-quarantine and cyber-criminal investigation using SRTB (Security Research TestBed based on cloud computing) for various computing application.

Keywords: *Cloud Computing, Testbed, Security Research, Multi-tenancy, Virtualization, Resource Management*

1. Introduction

Recently there has been increasing researches on computing environment caused by changes in computing paradigm of security aspects in relation to cloud computing. Big data issues and eco-system of cloud computing are operated on a variety of devices which are required for the security aspects corresponding to various cloud computing devices. However, there are multiple difficulties in establishing the actual computing environment for security verification and performing a security test based on the clouds computing environment in terms of time and cost. In order to resolve these problems, we propose the pilot research in association with a testbed for cloud computing-based security research using virtualization and multi-tenancy. In addition, we describe 2 case study scenarios of cyber-quarantine and cyber-criminal investigation for Security Research TestBed based on cloud computing (SRTB) for various computing application. This paper is organized as follows. In Section 2, we described the related work for testbed research and project in domestic and aboard. In Section 3, the SRTB is defined. In section 4, explanation on the functions and experiment life cycle of SRTB is presented. Section 5 describes 2 case study scenarios of SRTB for application. Finally, the conclusion and future work is presented in Section 6.

2. Related Work

In accordance with the changes of computing paradigm, the studies of global scale Testbed are activated. We briefly describe the domestic and international testbed studies.

The GENI (Global Environment for Network Innovations) [1] in USA is a unique virtual laboratory for at-scale networking experimentation where the brightest minds unite to envision and create new possibilities of future internets. The GENI mission is to open the way for transformative research at the frontiers of network science and engineering and inspire

ISSN: 1738-9976 IJSIA

and accelerate the potential for groundbreaking innovations of significant socio-economic impact. Figure 1 shows the GENI resource map of live map showing ProtoGENI and PlanetLab.

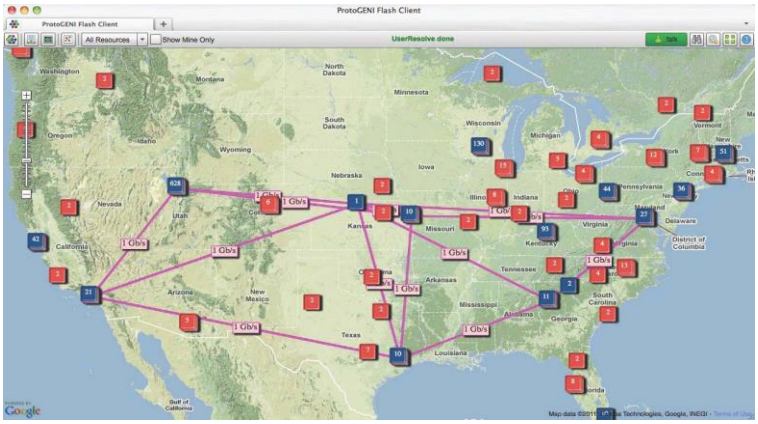


Figure 1. GENI Resource Map

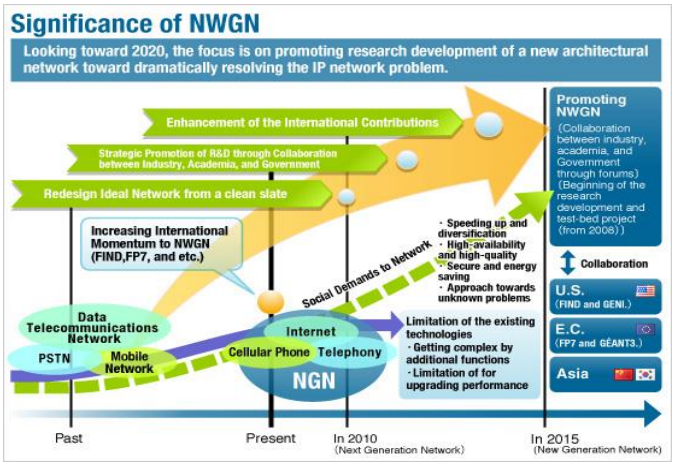


Figure 2. Significance of NWGN

Within FP7, the European Commission has facilitated the creation of European expert groups around the theme FIRE (Future Internet Research and Experimentation) [2-4]. FIRE has two related dimensions: on one hand, promoting experimentally-driven long-term, visionary research on new paradigms and networking concepts and architectures for the future Internet; on the other hand, building a large-scale experimentation facility supporting both medium- and long-term research on networks and services by gradually federating existing and new testbeds for emerging or future Internet technologies. By addressing future challenges for the Internet such as mobility, scalability, security and privacy, this new experimentally-driven approach is challenging the mainstream perceptions for future Internet development.

The NWGN (NeW-Generation Network) [5, 6] is based on new design concepts looking further beyond the next-generation network (NGN) and the Internet. In short, it aims to fundamentally solve difficult issues and limits in an improved and extended Internet, by a clean slate approach designing unconstrained by existing technologies as shown in Figure 2.

The FIF (Future Internet Forum) Testbed Working Group [7] in Korea pursues open discussion and practical exploration on construction, operation, and experimentation of Future Internet testbeds with industry, university, and research laboratory partners. The activities of the FIF Testbed Working Group focus on envisioning Future Internet testbeds, practical construction, operation, and experimentation of testbeds, and sharing state-of-the-art technologies on Future Internet testbeds.

3. Definition of SRTB

SRTB (Security Research TestBed based on cloud computing) refers to a test-bed for cloud-based security research. It can give an actual security test by building up an actual network using network simulation of NS (Network Simulator) [8]. SRTB consists of resource management, virtualization, multi-tenancy, template tools, and monitoring tools. Cloud resources are controlled by the resource management. The cloud resources are also virtualized by the virtualization. Multiple security researches are simultaneously supported by multi-tenancy. The template tools provide a variety of template functions with relation to VM, computing, and networking. The monitoring tools are monitoring the relative target to connection with the template tools.

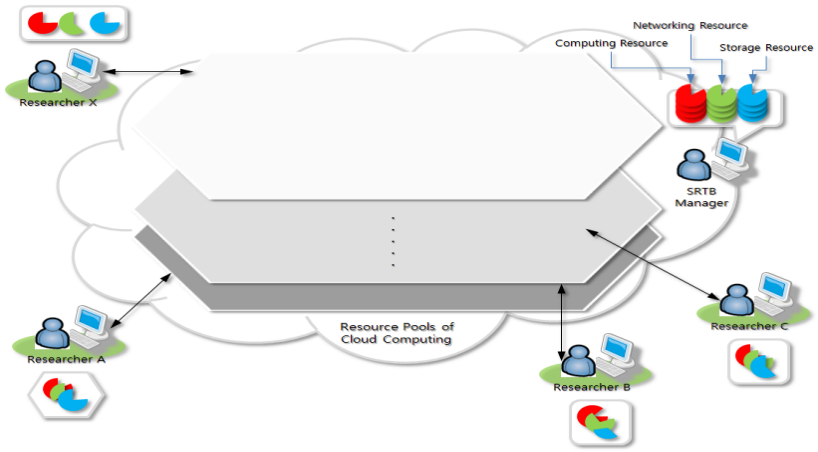


Figure 3. Multi-tenancy Function of SRTB

In the aspects of resource management of SRTB, the cloud resources can be divided into physical, logical, and composite resources. In the accessing resources for security researchers, their authentication procedure and an access control policy for the assigned resources are given. The virtualization of SRTB greatly supports computing, storage, and network virtualization. Multi-tenancy of SRTB means the use of one S/W by several users. SRTB in multi-tenancy environment makes a resource pool and provides one service based on it. All security researchers share this service as shown in Figure 3.

The greatest advantage of multi-tenancy is economy of scale. If SRTB is used, researchers do not need to make new individual system for security research and can minimize IT investment. Also, as only one system is managed, the management cost can be reduced. When errors are found, all researchers can have the same benefits by one correction and use simultaneously by one upgrade. The template tools of SRTB provide a template for the system constructed for assigned resources (*i.e.*, computing, storage, and networking). The monitoring tools of SRTB provide a variety of tools to monitor the system produced in the template tools as shown in Figure 4.

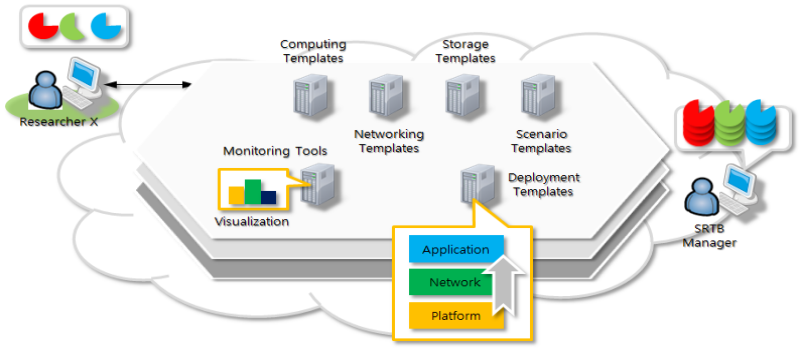


Figure 4. Template, Deployment and Monitoring Tools of SRTB

4. Functions & Experiment Life Cycle of SRTB

4.1. Functions of SRTB

The functions of SRTB include resource management, VM preliminary and tolerance, script, emulator, template, deployment, and monitoring functions. Resource management functions of SRTB include management of physical, logical, and synthetic resources which are assigned to a researcher and a SRTB administrator. Function of a VM preliminary and tolerance provides additional resources to the assigned resources for flexibility. In order to solve the system operation problems, a tolerance function are offered with respect to giving emergency state to VM operation. Functions of script and emulator provide the emulator function of NS and help researchers describe a scenario using a NS script. It sets a network by analyzing a NS script code and fitting script code objects to the NS script driven and described in VM. The templates and deployments support the convenient operation and fasten deployment of testbed environment construction as shown in Figure 4. And monitoring tools offer monitoring, logging, auditing, analysis, and visualization functions.

4.2. Experiment Life Cycle of SRTB

Figure 5 presents the research experiment life cycle of SRTB using various components as shown in Figure 4. The experiment life cycle of SRTB is composed by 4 steps. Firstly, to conduct security research and test in SRTB, the utilization of resources should be assigned by the SRTB administrator. Secondly, the assigned resources are designed, deployed and composited by researcher or pre-descripted templates. Researcher constructs VM, OS, storage, and network using the provided template and the composed templates. It also constructs a virtual network using the constructed system. In addition, researcher constructs a variety of monitoring tools based on the constructed system and networking for monitoring and inspection of the assigned resources. The security researchers make a security research scenario by the NS or shell script using the constructed system, networking, and monitoring tools on SRTB. Thirdly, the experiment scenarios are operated, monitored, and analyzed. The security researchers operate the security research scenarios using the NS or shell script. When the security research scenario is operated, the results of monitoring and inspection by monitoring tools are produced in many different forms. The results are analyzed by the statistical techniques and data mining methods. The visualization of results is also reported in GUI environment. Lastly, when the security research scenario and analysis are completed, the assigned resources are withdrawn to the SRTB administrator. And the produced results by the

security research scenario are stored in researcher's private storage or shared storage by researcher groups.

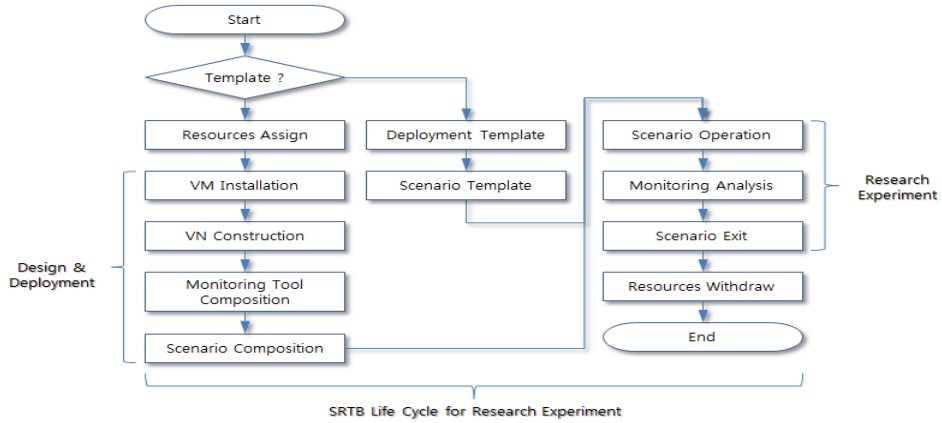
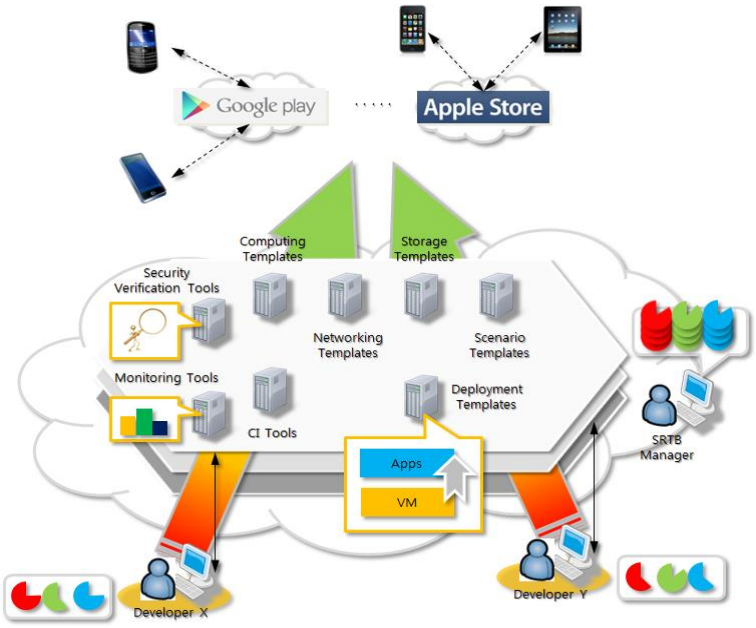


Figure 5. Experiment Life Cycle of SRTB

5. Scenario of SRTB

5.1. Case Study 1: SRTB for Cyber-Quarantine

As shown in Figure 6, it is possible to provide the test environment of mobile and computing application development by virtualization and multi-tenancy functions of SRTB. Specially, CI (Continuous Integration) tools managed the developed source code and development environment parameters. And developed source codes are verified and tested by the security verification tools.



Figire 6. Case Study 1 of SRTB for Cyber-Quarantine

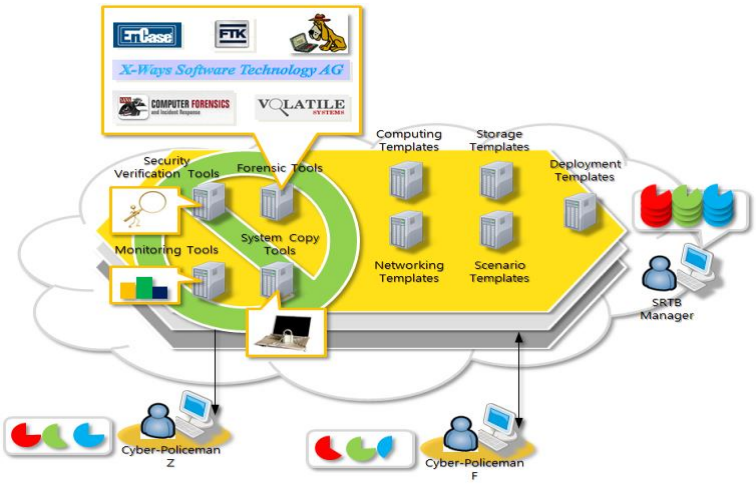


Figure 7. Case Study 2 of SRTB for Cyber-Criminal Investigation

5.2. Case Study 2: SRTB for Cyber-Criminal Investigation

The multi-tenancy function of SRTB provides many functions concurrently including digital forensic analysis tools (*i.e.*, EnCase [9], FTK [10], *etc.*,) for monitoring and implements computing and networking forensic. Results of forensic processing are analyzed, audited and reported, as shown in Figure 7.

6. Conclusion

This study is conducted pilot research to propose a security research testbed based on cloud computing and described 2 case study scenarios of cyber-quarantine and cyber-criminal investigation using SRTB. Further study is required to develop in order to a prototype to improve testbed environment and functions proposed in the pilot research.

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).

References

[1] GENI, http://www.geni.net.
[2] FIRE, http://www.ict-fire.eu/home.html
[3] A. Gavras, A. Karila, S. Fdida, M. May and M. Potts, "Future internet research and experimentation: the FIRE initiative", ACM SIGCOMM Computer Communication Review, vol. 37, no. 3, **(2007)** July, pp. 89-92.
[4] European Future Internet Portal, http://www.future-internet.eu/home/fisa-futureinternetsupportactions/future-internet-research-experimentation.html.
[5] NWGN, http://forum.nwgn.jp/english/about/.
[6] T. Aoyama, "New Generation Network (NWGN) Beyond NGN in Japan", http://fif.kr/documents/infocom2007_nwgn_TA.pdf, **(2007)** May 8.
[7] Testbed Working Group of Future Internet Forum, http://fif.kr/wg/testbed/wiki.php.
[8] NS, http://www.isi.edu/nsnam/ns/.
[9] ECASE, http://www.guidancesoftware.com/encaseforensic.htm.
[10] FTK, http://accessdata.com/products/digital-forensics/ftk.

Authors

ByungRae Cha is a research professor at school of Information and Communications, GIST, Korea. He received the Ph.D. degree in Computer Engineering from National Mokpo University in 2004 and the M.S. degree in Computer Engineering from Honam University in 1997. Prior to becoming a research professor at GIST, he has worked as a research professor in Department of Information and Communication Eng., Chosun University, and professor in Department of Computer Engineering, Honam University, Korea. His research interests include Computer Security of IDS and P2P, Neural Networks Learning, and Future Internet.

SuJeong Sim is finished Ph. D course and the M.S. degree in computer engineering from National Chonnam Univ. in 1999, and the B.S. degree in computer engineering from Honam Univ. in 1996. She has worked as a part time professor in Chonnam Univ., Chosun Univ. and Honam Univ. Her research interests include Information Retrieval, Data Mining, and Matching Language.

JongWon Kim received the B.S., M.S. and Ph.D. degrees from Seoul National University, Seoul, Korea, in 1987, 1989 and 1994, respectively, all in control and instrumentation engineering. In 1994-1999, he was with the Department of Electronics Engineering at the KongJu National University, KongJu, Korea, as an Assistant Professor. From 1997 to 2001, he was visiting the Signal and Image Processing Institute (SIPI) of Electrical Engineering - Systems Department at the University of Southern California, Los Angeles, CA. USA, where he has served as a Research Assistant Professor since Dec. 1998. From September 2001, he has joined as an Associate Prof. at the Department of Information & Communications, Gwangju Institute of Science and Technology (GIST, formerly known as K-JIST), Gwangju, Korea, where he is now serving as a Professor. He is focusing on networked media systems and protocols including multimedia signal processing and communications. Dr. Kim is a senior member of IEEE, a member of ACM, SPIE, KICS, IEEK, KIISE, and KIPS.