IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. III (Jul.-Aug. 2017), PP 73-76
www.iosrjournals.org

Model of Cloud Computing Platform as a Service to VR/AR Military Cyber Simulation Operation Problem

*Jungho Kang [1]
[1](Department of Computer Science, Korea Military Academy, Republic of Korea)
Corresponding Author: Jungho Kang

Abstract : *Recently, This paper we propose the placement of Cloud Computing to solve considering the effective range of rifles and suggest the algorithm to delete the program when VR/AR Military Cyber Simulation Operation Problem. we analyze various problems that arise when using AR (Augmented Reality) technology for military Simulation Operations and suggest ways to improve them. In order to solve cyber attacks and threats (physical attacks, technical attacks) that may arise when VR/AR is applied in the military, and to solve all the problems such as limitations of 'scalability, we will examine how cloud computing is applied to the US Army and how to apply 'cloud computing' to our military.*

Keywords: *Virtual Reality, Augmented Reality, Cloud Computing, Cyber Warfare, Scalability, Security*

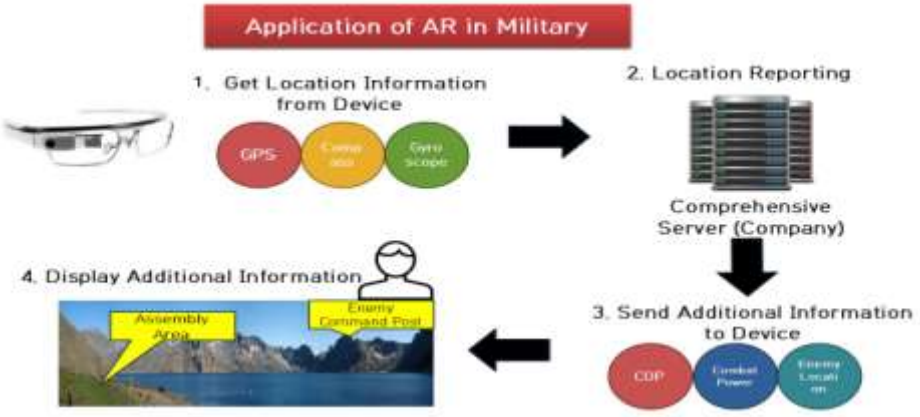
Date of Submission: 15-07-2017 Date of acceptance: 26-07-2017

I. Introduction

Korea and other countries around the globe have taken interest in the "4th Industrial Revolution" nowadays. The 4th Industrial Revolution is a period accomplished by the harmony of manufacturing industry and ICT. The core of the revolution includes Artificial Intelligence, Robot Automation, Internet Of Things, Nano Technology etc. Among these concepts, Augmented Reality is the main axis of the 4th Industrial Revolution. VR/AR is growing and expanding along with the development of 5G LTE, and studies of this technique is in progress mainly by Japan and US from the latter half of 1990s. Augmented Reality is a technique that puts virtual images upon real world. GPS, gravity sensor, gyrosensor inside a device send information to a server, them the server analyzes the information drawing a 3D image that comes under the position of the device. Subsequently, the server sends the 3D image and additional information to the device, plating real world with them. VR/AR makes data processing and data exchange easy for users. Therefore, applying VR/AR in medical care, media, national defense, construction, manufacturing process would bring magnificent results.

Much research has been done beforehand on how to manipulate and develop VR/AR technology. However, studies on security problems of VR/AR are yet insufficient. Because users gain VR/AR information by calling them from the server, security problem and scalability problem are inevitable. For example, if 3D images from VR/AR technology in manufacturing process or national defense are leaked, it can be a national disaster. Furthermore, corporation whose IT infrastructure is poor but is about to enter the overseas market, soldiers who perform their duties overseas, or the headquarters that move frequently because of a war have to constantly install a server every time they move, which causes budget problem and energy problem. Thus, this study will show the development of VR/AR technology to come and how VR/AR will conduct the server to guarantee security and scalability when military cyber Simulation Operations are performed.

II. Possible Cyber Attacks when Applying VR/AR in Military



[Fig. 1] Application of VR/AR in Military

2.1 What is Augmented Reality?

Augmented Reality is a technology that overlaps real world images or backgrounds with three-dimensional virtual images. Mobile device gains current location related information at first, then the device sends the information to the server. Data relevant to the information is stored in the server rooms, so the server can respond to the device by sending the data that corresponds to the information received. At last, corresponding data is displayed on the device overlapping the real world image[1].

Augmented Reality can be achieved by two separate methods. One is Object Recognition System and the other is Location Based System. Object Recognition System is a way to offer information through interaction in respect of a particular object, irrespective of its location. Location Based Sysetm is a way which can be driven by three pieces of information: geographic/location data, electronic compass, and gravitational sensor.

2.2 Physical Attacks

There are cyber attacks and cyber defense in the form of cyber warfare. Cyber attacks include hacking and physical destruction, and cyber defense has information protection and physical encryption[2]. We have to consider physical destruction, the use of VR and VR/AR in cyber attacks, and the hacking of VR, VR/AR's company (server room).

Physical destruction in the cyber attack is not a cyber attack by infiltrating into a technical part, but a cyber attack by destruction in the hardware part which contains the source of the information. The attack technique of physical destruction is not preferable because it is too dangerous and the probability of success is low and there are many limitations in maintaining the covertness which is one of the core of cyber warfare. However, if a physical destruction attack is performed through VR/AR technology, it can maintain the covertness, increase the probability of success and reduce the risk. Combining the high infiltration capabilities of combatants such as elite agents or special forces performing special missions with VR/AR technology, you will be able to execute very high level attacks. Entering the enemy server room by attaching the VR/AR applied wearable device to infiltrating agent, they send what they see in the act through VR/AR in real time and the server tells how to destroy the enemy server without any trace. In addition, if these infiltration Simulation Operations are continuously simulated through VR/AR, and trainings are carried out repeatedly, the individual competence of each agent will increase, so that the dangerous form of cyber attack technique of physical destruction will become less dangerous than before and the probability of success will also increase.

Possible Cyber Attacks when Applying VR/AR in Military	
Physical Attacks	Technical Attacks
・ It is possible to know the exact information about the hardware part which is the target of the physical attack, so it can be destroyed without any trace ・ Simulation can increase the probability of success	・ Direct technical hacking of server (company) is possible ・ Attack using log of the server with information of location, compass, and gravity sensor of mobile device is possible

[Table 1] Possible Cyber Attacks when Applying VR/AR in Military

2.3 Technical Attacks

If the enemy has VR/AR technology to conduct cyber attacks, hacking on the enemy's server can bring good results. The opponent integrates position information, compass sensor, and gravity sensor information from the VR mobile device to transmit three-dimensional images to the display of the device. In this case, the location information of all mobile devices will be recorded in the log of the server room, and the statistical data of where the enemy's VR was used frequently will also be stored. You can also obtain a lot of information stored in the company directly through hacking.

III. Application of Cloud Computing

3.1 What is Cloud Computing?

Cloud computing means accessing remotely hosted data or services using a minimal number of computer devices. The cloud computing model provides a shared pool of configurable resources that can be quickly provided and distributed through minimal administrative effort or interaction with service providers, enabling access to the network anytime, anywhere. To summarize, five representative characteristics of cloud computing are

① on-demand self service
② broad network access
③ resource pooling
④ fast elasticity

⑤ measured service

In other words, users use software, storage, network, and other computing resources as needed, and pays a certain fee accordingly. Cloud computing has three types of services (IaaS, PaaS, and SaaS), each of which has a range of management and control according to the services provided, and the military is currently targeting the provision of IaaS cloud services. Currently, the Department of Defense is planning and promoting cloud computing in a pilot phase in 2012, and the adoption of cloud saves 80% of physical space and saves about 40% of energy consumption [3].

3.2 Case Studies of Cloud Computing Application in the US Army

In the case of the US Army, there are many troops deployed. Therefore, it should be able to collect information of millions of devices from the field quickly and at any time, send it to the base, analyze it, send it back to the people in battle, and prevent the threat in front of it. The Army introduces a tactical advanced cloud node coupled with advanced analysis tools as part of Distributed Common Ground System (DCGS), a software that transmits allied and enemy positions every hour. Brigadier commanders in particular deal with massive data. But they do not have the bandwidth to move this data all at once. Thus, the only way to respond to this problem on the battlefield is tactical cloud computing. Already in 2011, cloud computing nodes have been deployed at the Bagram airfield in Afghanistan, and the Army headquarters is receiving real-time information via DCGS. In addition, DCGS, originally developed for the integration of information from the army, the navy and the air force, introduced a cloud computing node, which enabled a container size of 6m height providing 1,800 cores of processing capacity and meaningful answers.

The US Army's engineering center, Communications-Electronics Research, Development and Engineering Center (CERDEC), also introduced cloud computing nodes. As a result, the next generation of cloud nodes have been minimized to a toaster size and mounted in armed vehicles or UAVs. When storing or transmitting vast amounts of information gathered by troops on actual battlefields, they are no longer blocked by connection problems or bandwidth problems. Especially, it is possible to process it at the site where information is gathered[5].

3.3 Security Assurance by Cloud Computing

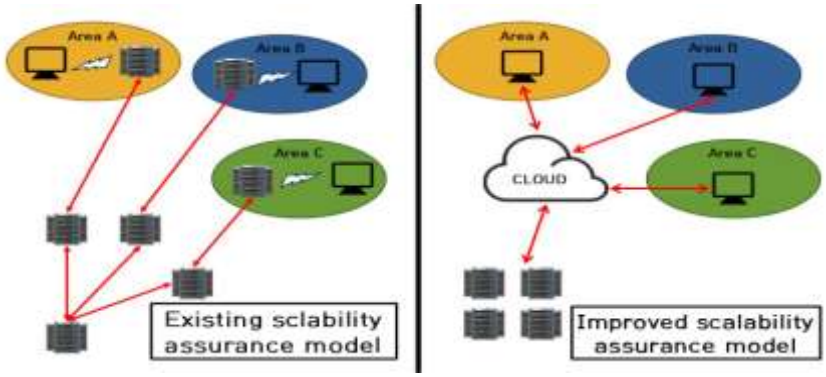
In an existing computing environment, all information within the military is stored in the computer of the unit or stored on each server. In this environment, the military must live with constant cyber threat. In addition, servers are scattered all over the country, making it difficult to manage them in an integrated manner, resulting in security vulnerabilities. However, when the environment is transferred from the existing environment to the cloud computing environment, it is possible to improve the mobility using the wired and wireless network, which is the strength of cloud computing, and at the same time ensure high security by intensive security management of the data center. Unlike traditional computing environments, in a cloud computing environment, administrators in the data center can monitor the performance of cloud service users, test vulnerabilities in the system, and immediately change new threats or vulnerabilities when they are found. In addition, if work involves military secrets or military data from cloud storage, then user authentication technology and access control can be used to ensure greater security than existing computing environments.

3.4 Scalability Assurance by Cloud Computing

The Korean Ministry of National Defense began piloting cloud computing in 2012, and the US Department of Defense (DOD) was already envisioning the application of the cloud before that. The first reason for the rapid transition from traditional server to cloud computing is to save money. Michael Dell, IT giant, said, "The federal government spends approximately $76 billion to support its widely dispersed information technology assets. Up to 30 percent of that spending could be saved by further reducing IT overhead, consolidating data centers, eliminating redundant networks and standardizing applications[4]." The problem with military networks in particular is that there are many unnecessary expenditure fields. In the United States, spending is on the rise because management standards for security, hardware, and software licenses are all different among military units around the world. Korea is no exception. It is not possible to properly integrate the information of each army in the Joint Chiefs of Staff in Gyeryongdae, Daejon, even if there is a small mistake because army, navy and air force use different C4I(command, control, communication, computer and intelligence) system. Cloud computing can reduce defense costs by consolidating the management of information assets of different units and reducing the number of IT personnel required for maintenance. In addition, high scalability can be ensured by using cloud service. Because of the various networking standards and policies between garrisons, temporary camps, and forward deployed units, every time they move, they must erase the computer before connecting to the network. Then, every time a user connects to the network, they must have different login information and an email account. However, having cloud service can fix this problem by managing personal information in the cloud server. The problem of scalability of existing computing does not simply end with the inconvenience of creating a new account when the computer is deleted. In the case of the US Army deploying troops across the globe, it also appears in the ARFORGEN (Army for Generation) process, a way to efficiently create trained troops and hand over to combat commanders. When a unit is training in the field for the next deployment in accordance with the ARFORGEN process, the computer used by the unit can not connect to the network in the garrison unless there is a special

reset. Eventually, the Army Battle Command System (ABCS) used at this time is active during training, but left unused for months without training. This leads to the loss of important information[5].

From the perspective of scalability, it can be said that it is difficult to maintain a military network anymore with existing computing methods, which require users to change their authentication and lose important information each time. Cloud computing is inevitable at this point, especially when augmented reality, premised on high scalability, is about to be used in training and practice [3],[9].



[Fig. 2] Comparison of Scalability Assurance Model

IV. Conclusion

The concept of cloud computing first appeared in the Compaq (American computer company) internal document in 1996, but the military is introducing it in 2012 and is expected to be commercialized soon. As with the cloud, the VR/AR will be introduced soon and will be used in the defense sector in the future. However, applying this thoughtlessly without a thorough review of the many security issues is exactly the same as leaving a serious threat to national security.

When working with VR/AR technology, cloud computing can solve both scalability problems and security issues which saves money and energy. We should try to implement the VR/AR technology on the IaaS based and Hybrid model cloud by benchmarking the precedents of US military and ensure the security and scalability of the VR/AR technology.

References

Journal Papers:

[1] Kim Hyo Koon, Son Young Joo, Kim Myung Seok, Lee Seon Jim (2017). The Present and Future of "AR (Augmented Reality) versus VR (Virtual Reality) versus MR (Mixed Reality)". *Defense & Technology, (455)*, 76-87.
[2] Ho-Kyun Park (2013). Types and Information Security Technology on Cyber Warfare. *The Korea Contenta Association Review, 11(4)*, 41-44
[3] Worl-Su Jang, Jumh-Younh Choi, Jong-in Lim (2012). A Study on adopting cloud computing in the military. *Journal of the Korea Institute of Information Security & Cryptoloogy, 22(3)*, 645-654.
[4] Kyoung-a Shin, Sang-jim Lee (2012). Information Securtiy Management System on Cloud Computing Service. *Journal of the Korea Institute of Information Security & Cryptology, 22(1)*, 155-167.
[5] Wylie Wong (2013) , The Army Brings the Cloud to the Battlefield, July, Summer 2013 Issue .

Theses:

[6] Major Dallas A. Powell, jr., *The Military Applications of Cloud Computing Technologies*, pp 11, Jan, (2013).
[7] Huiuk Lee, "Who hacked into our hearts",Hangyeorae21(2014).
[8] Lawrence Pingree, Ruggerro Contu, Eric Ahlm, 'context Aware Security and Intelligence Sharing Concepts Merge to Create Intelligence-Aware Security Controls'. Gartner Group, March, (2014).
[9] Kyoung-a Shin, Sang-jim Lee (2012). Information Securtiy Management System on Cloud Computing Service. Journal of the Korea Institute of Information Security & Cryptology, 22(1), 155-167.

JungHo Kang . "Model of Cloud Computing Platform ac a Service to VR/AR Military Cyber Simulation Operation Problem." IOSR Journal of Computer Engineering (IOSR-JCE) 19.4 (2017): 73-76.