Design of Mobile-based Security Agent for Contents Networking in Mixed Reality

Donghyun Kim[1], Jaehyun Lim[2], Seoksoo Kim[3*]
[1,2]Student, Multimedia, Hannam University
[3*]Professor, Multimedia, Hannam University

융합현실에서 콘텐츠 네트워킹을 위한 모바일 기반 보안 중계 설계

김동현[1], 임재현[2], 김석수[3*]
[1,2]한남대학교 멀티미디어학과 학생, [3]한남대학교 멀티미디어학과 교수

Abstract Due to the development of ICT technology, convergence reality contents are utilized as technology for providing services in various industrial fields by visualizing various information such as sensor information and shared information in a service platform showing only simple three-dimensional contents. Research is underway to reduce the weight of applications by transmitting the resources of the object to be enhanced to the network as the information and the contents to be provided increase. In order to provide resources through the network, servers for processing various information such as pattern information, content information, and sensor information must be constructed in a cloud environment. However, in order to authenticate data transmitted and received in real-time in a cloud environment, there is a problem in that the processing is delayed and a delay phenomenon occurs in the rendering process and QoS is lowered. In this paper, we propose a system to distribute cloud server which provides augmented contents of convergent reality service that provides various contents such as sensor information and three - dimensional model, and shorten the processing time of reliable data through distributed relay between servers Respectively.

Key Words : Mixed Reality, Contents, Security Agent, Mobile Networking, Rendering

요 약 ICT 기술의 발전으로 인하여 융합현실 콘텐츠는 단순한 3차원 콘텐츠만을 보여주는 서비스 플랫폼에서 센서 정보, 공유 정보등 다양한 정보 등을 가시화하여 제공함으로서 다양한 산업분야에서 서비스 제공을 위한 기술로서 활용되어지고 있다. 제공되는 정보와 콘텐츠가 증가함에 따라 증강되는 오브젝트의 리소스를 네트워크로 전송하여 어플리케이션을 경량화하는 연구들이 진행되고 있다. 네트워크를 통해 리소스를 제공하기 위해서는 패턴 정보, 콘텐츠 정보, 센서 정보 등 다양한 정보들을 처리하기 위한 서버들이 클라우드 환경에서 구축되어야 한다. 그러나 클라우드 환경에서 실시간으로 송수신되는 데이터를 인증하기 위해서는 그 처리과정이 길기 때문에 랜더링 과정에서 딜레이 현상이 발생하여 QoS가 떨어지는 문제가 있다. 따라서 본 연구에서는 센서 정보, 3차원 모델 등 다양한 콘텐츠를 제공해주는 융합현실 서비스의 증강 콘텐츠를 제공해주는 클라우드 서버를 분산하고 분산된 서버간 중계를 통하여 신뢰된 데이터를 처리하는 시간을 단축하기 위한 시스템을 설계하였다.

주제어 : 융합현실, 콘텐츠, 보안 중계, 모바일 네트워크, 랜더링

*This paper has been supported by the 2018 Hannam University Research Fund.
*Corresponding Author : Seoksoo Kim(sskim@hnu.kr)
Received February 12, 2019 Revised March 6, 2019
Accepted March 20, 2019 Published March 28, 2019

1. Introduction

Due to the development of display devices, augmented reality service using hologram is commercialized, and research on mixed reality combining augmented reality with virtual reality has become active.

In case of augmented reality, the contents are simply enhanced to provide virtual information and objects using only the information of the user. However, in the case of HMD (Head Mounted Display) using a holographic output display such as a holographic lens, And outputs the processed data. In order to output virtual data, it is required to be transformed into an output image by matching a virtual object in a virtual space. There are a number of things that you need to know about, such as: To solve this problem, the system structure is changing in such a way that resources are provided through a network and only rendering is processed by a built-in processor.

However, in the case of mixed reality, it is not necessary to synthesize and provide only virtual information, but receive information about the reality and information of the user from the sensor, the mobile terminal, and be independently processed.

For this purpose, a mobile agent for providing information from various servers such as a server for collecting sensor information, a server for transforming and transmitting a 3D model resource for rendering, and a server for providing a moving image stream should be configured.

For this, a mobile-based security agent consists of a system that relays the multiple agents so that they can communicate spontaneously without human interaction [1].

Mobile agents that interworking between systems have reference data for recognizing the situation because they can be affected by data transmission during mutual interaction. I do not know how to do this, but I do not know how to do it. At this time, the core of mobile agent technology is to reduce network traffic and shorten network latency[2].

However, APs (Access Points) are changed flexibly according to the dynamic movement of the user, and the movement of the agents is frequent, which causes an important security problem. In this paper, we propose a solution to solve the problem of mobile security agent which provides a real-time system[3],

In this paper, we design a convergent real-time system that transmits data from a server and a mobile agent providing various information, and monitor the profiling of an attack that behaves abnormally, so that data can be more efficiently compared with a method using an existing cloud service We have designed a security relay system that provides contents of convergence reality service to protect.

To do this, we predefine mobile agents, active functions, and customizable security policies, and then identify attacks based on scenarios.

2. Related Works

In the cloud computing, the expansion of the mobile agent that is interwork ed to interact with each mobile agent must be resilient. This requires virtualization of resources.

However, cloud computing security follows the notion of cloud computing, and it needs to maintain confidentiality, integrity, and availability and the security of the associated cloud systems. To do this, we need to make sure that there are two problems with access to the cool- do.

To solve this problem, researches on integrity cloud computing storage have been conducted[4,5].

Cloud security risk assessment[6] has been published to standardize these studies, and most of the integrity monitoring and intrusion detection solutions are cloud computing.

File system-based integrity tools and intrusion detection systems such as Tripwire [7] and AIDE [8] allow malicious attackers to distribute malicious code through a virtual machine to attack a user's system.

Due to these problems, mobile security agents [9] have been able to develop applications in distributed systems, and various security agents have been designed using distributed systems [10,11].

However, agent systems generally do not meet all the needs of the overall operation and need to develop additional functions for security and fault tolerance of agents and mobile hosts.

Especially, in the case of mobile agents based on fusion realities with frequent dynamic physical movements, it is necessary to take into account the data connection delay time as the AP providing data is changed. In addition, And the processing process to perform the processing of the mobile security agent. Therefore, it is necessary to design an additional mobile security agent.

Therefore, in this paper, we design a mobile security agent that improves the host and security fault tolerance in the mobile security agent system using the distributed system in accordance with the network rendering of the hologram device and the mixed reality service.

3. MR Contents Cloud Server

In a cloud computing architecture, a central server for sending and receiving data between mobile agents must be statically deployed and a method for processing data transmitted from each mobile agent host terminal. Especially, when the real terminal is recognized by the host terminal, it is necessary to check the mobile agent linked with the middle server to check the interworking data based on the unique ID of the pattern of the recognized object.

An important feature of this cloud computing environment is the need for economical network access points that take into account reliability, infrastructure determinism, location independence, flexibility, resiliency and substantiality.

In this paper, we design the cloud architecture as shown in Fig. 1 to enable communication based on multi access point to receive data from data storage and sensor node, because servers configuring the cloud have different processing areas for each server.

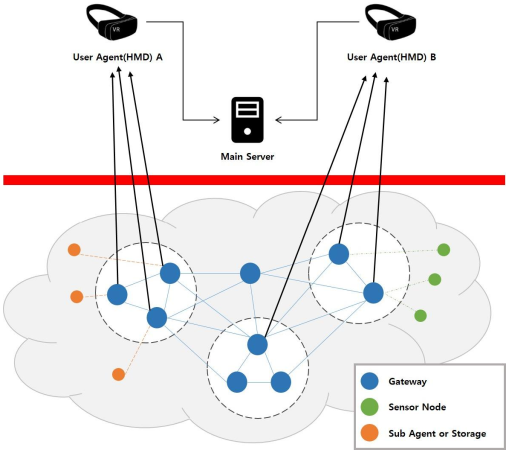

Fig. 1. Cloud Server Networking

A typical cloud architecture is designed to communicate multiple cloud components to each other through an application programming interface and to provide end users with a variety of services to end-users. Software as a Service (SaaS), Platform as a Service (PaaS), and IaaS Infrastructure as a Service) and provides infrastructure resources, application platforms and software as a service to customers[12].

Each service delivery model places different levels of security requirements in the cloud environment.

SaaS is a rapidly emerging service delivery model that meets the requirements of enterprise IT services that can access applications from a variety of client devices via the thin client interface over the Internet. This model runs a multi-tenant application that uses a single instance to process multiple clients across multiple organizations to minimize risk [13].

IaaS provides a variety of ways of delivering products remotely to an entire computer infrastructure such as virtual machines, storage devices, servers, applications, and virtualized environments. This enables consumers to provision storage, operating systems, processing, applications, and other related resources and distribute and execute them under their own control. Cloud providers do not have to worry about building and managing the infrastructure provided by cloud administrators like Nimsoft or Rightscale[14].

PaaS provides a unified environment for consumers to build and control applications and define application hosting environment configurations without having to manage or control the underlying cloud infrastructure including networks, servers, operating systems, storage and resources. In PaaS, everything else is abstracted from the consumer through the services that the cloud provider provides remotely.

Cloud computing is considered one of the most promising technologies in computing today. There are four deployment models identified for the cloud architecture solutions described below.

In this paper, we use PaaS module instead of SaaS model because we need to build a cloud environment for security between each mobile agent or servers constituting a cloud based on a central server that manages existing mixed reality.

In addition, the configured server consists of the server layer as shown in Fig 2. It follows a cloud configuration with high portability and diverse data and applications [15].

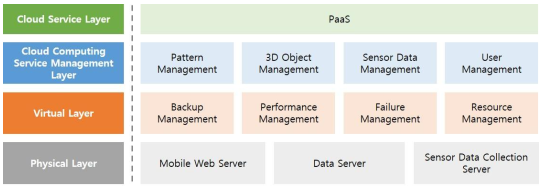

Fig. 2. Cloud Server Layer

4. Mobile-based Security Agent

Framework for dynamic security services and policies. For this, active activation-based activation policy is needed. This policy requires a detailed and detailed dynamic control of the action and verifies whether each subject is authorized to call data.

The framework for verifying the right to invoke data supports a variety of authentication protocols depending on the distributed functions in the centralized essence control list. In addition, once used for validation, the host that is used once removes the access right by using the revocation schema and adds it to the illegal access control list so that the malicious attacker can not use the access right of the used host.

In the case of the monitoring framework proposed in this paper, by using the process of recognition measurement used in the above function authority confirmation framework, the host having the access authority and the agent or the host having the access authority when accessing the dynamic access pointer And the agents that are not in the identified list are added to the list of threat agents and the priority of blocking is applied to confirm the calling authority.

This requires new basic line support to monitor the internal system structure and runtime behavior.

The monitoring proposed in this paper classifies data structure according to the security policy statement and designates it as a framework to check the upper level access control list, label and rule by performing low level set and mapping, To compare a class with a form with an arbitrary accessor control type, define the main platform and the sub-platform separately as shown in Fig 3.

The reason for using mobile-based security agents in a mobile computing environment is that it is easy to remove the flow of raw data from the network, and when a large amount of data is stored on a remote host, the data is processed not in the network but in the area This is because data processing is distributed and processing according to complicated security policy can be performed at the same time.

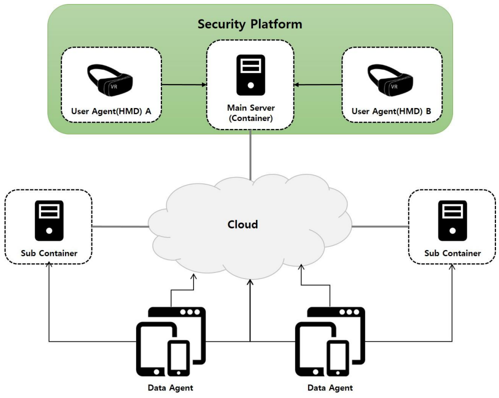

Fig. 3. Cloud Security Framework

Therefore, the end-user agent, that is, the dynamic agent, establishes a trust relationship with the main server and the security platform, and subagents that perform functions of the cloud computing service management layer such as data processing, resource provisioning, It is designed to reduce the security risk in data transmission by allowing access to the platform only to the main server.

For this, the mobile security agent must solve the problem about the network latency. Existing mobile security agents encapsulate protocols and use code that has the code to implement the protocol necessary for each host to properly encode and interpret data when it is exchanged in a distributed system.

However, in order for the protocol to implement new security requirements or improve efficiency, the new protocol requires frequent upgrades because the system must be upgraded periodically to update the code.

Due to this problem, the mobile-based security agent must make the remote host move to establish the channel based on the proprietary protocol. However, because of this, the mobile security agent needs to access autonomously and asynchronously, so it has to rely on expensive network connection. However, it occurs frequently according to the recognition of the reality object, which is the data connection in the fusion reality. Since the number of patterns is often checked for detection, there is a problem in that the resource efficiency of the connection is lowered.

In order to solve this problem, the mobile agent includes tasks and transmits them to the network. In order to provide the data, the connected agents are distributed independent of the existing processes and operate asynchronously.

Unlike existing hosts, a mobile agent can dynamically respond to a situation or an event in which a malicious attack occurs. Therefore, the fault tolerance is high and a distributed system can be easily constructed.

Mobile service provisioning is a function that is performed after users are registered in the mobile cloud architecture. When a user requests a service through the security agent framework, the security agent framework relays the request to the sensor networking or the surrounding network connection network[16].

The security agent framework, which knows the service execution details and the user's service profile, continues to call this service.

As mentioned earlier, the security agent framework periodically removes the schema for the service profile once used and dynamically associates with the illegal access list, so if there is a limited version of the user service profile, the appropriate service parameter is requested for that profile manager . The security agent framework obtains the additional information needed by the service invocation, service parameters, and service-providing network entities and sends service invocation requests to the service invoking entity.

If the user is running a service on the user's device, it is assumed that the service is running on the user's device, as long as the local notifies the network of its function. Because the mobile device can accommodate the execution of a security agent, the security agent framework is passed to the user's device.

When the user service is requested, the security agent sends the request to the central server. In the central server, after receiving the additional service information from the agent, the service agent sends the service call to the entity providing the service.

The profile agent for the cloud service provider creates a service agent. Service Agents deliver service results to the security agent framework, which processes service results.

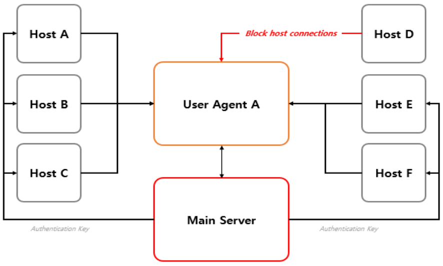

Fig. 4. Trust between Host and Agent

As shown in Fig 4, a host that is authenticated by the main server receives data and resources from the user agent but blocks the connection if the host is unauthenticated.

In the fusion real world, various contents such as sensing data, connection between mobile devices, and other agents can be requested to be served by other devices. Therefore, various approaches for starting and displaying the platform to the end user are required We designed this.

As shown in Fig 5, if you want to access a fixed centralized server, you should look at the schema of the device you are accessing and provide a call to enable various accesses. The agent server then runs its own terminal to provide a call to the agent responsible for service management and provisioning to ensure that it is an authorized user. If the terminal of the provided agent is a mobile device, it is designed to take this into consideration because it uses a flexible terminal.

If a response to a malicious remote host is found, it filters the subsequent traffic on the remote host to monitor the service load on the approach to a sustainable level, and adds a schema that blocks spoofed packets or maliciously marked hosts to the list.

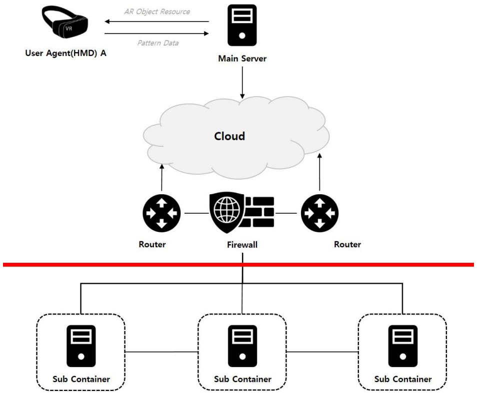

Fig. 5. Security Test-bed

If the service load goes above the threshold, it blocks the attacker who generates the most service load. This action minimizes disadvantages to legitimate remote hosts and takes necessary steps to prevent the network from being overloaded. Detection time, false positive rate, and false negative rate are considered to evaluate the intrusion detection system.

5. Comparison

We have implemented agents and traffic spoofing tools to evaluate detection and identification capabilities. A single remote host can overload a mobile node through a DoS attack, as shown in Fig 6. This shows the attacker's detection time. In most cases, a single attacker will be identified within 20 seconds of the start of a service attack.

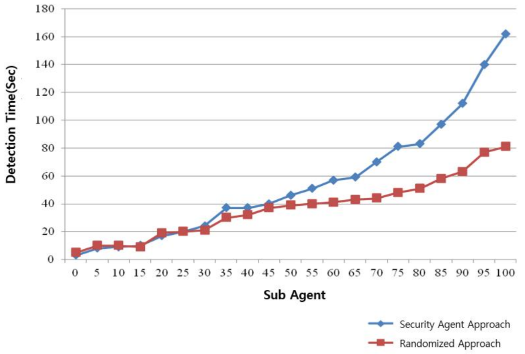

Fig. 6. Detection Time

It also evaluates mobile-based security frameworks using detection algorithms for attack defense. Because of the low false positive rate as shown in Fig 7 obtained from 100 experimental cases.

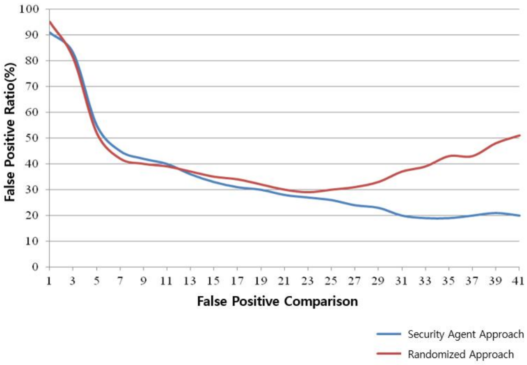

Fig. 7. False Positive Comparison

we plotted the trend of the curve on the plot. Fig. 8 also shows a graph of the upper sound level.

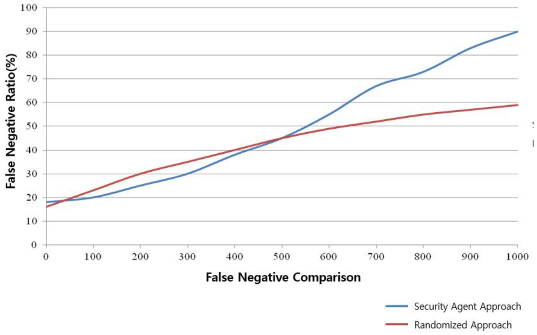

Fig. 8 False Negative Comparison

6. Conclusion

Cloud computing is a new and promising paradigm for delivering IT utilities as computing utilities. Because the cloud is designed to serve external users, providers must share resources and capabilities. Cloud computing increases the potential risk to security threats and privacy breaches, especially when the cloud is based on the Internet, rather than the organization's own internal network. The cloud computing model expands computer resources as needed and provides many of the benefits of running an existing cluster system. As mobile devices become more widespread, security issues arise in the cloud computing environments. In particular, it is expected that the number, severity, and sophistication of these threats will increase as more security issues such as DoS attacks increase malicious users and more sophisticated between mobile devices.

Mobile-based security agents in the cloud computing are useful because of their ability to communicate with mobile security agents. However, an attacker performing a malicious attack such as a DoS attack can take advantage of it.

In this paper, user agents with dynamic structure share data by transmitting data from authorized agents from main server of security platform.

In addition, a server that manages and processes three-dimensional models, pattern ID detection, sensor data, and the like is constructed in the same manner as existing cloud computing, and data is processed to transmit enhancement data in real time through the network.

Also, in this paper, we propose a mobile-based security framework for service provisioning against DoS attacks. We have a wide range of commercial applications for cloud computing. From a security perspective, many inexperienced risks and challenges have been introduced from relocation to the cloud.

REFERENCES

[1] K. J. Lee & W. S. Jeong. (2011). An Analysis of the Economic Effects for the Immersive Media Industry. *The Journal of Korean Institute of Communications and Information Sciences, 36(7),* 795-805.

[2] S. Jonathan (1992). Defining virtual reality: Dimensions determining telepresence. *Journal of communication, 42(4),* 73-93.

[3] E. Damiani, S. Vimercati, S. Paraboschi & P. Samarati (2000). Securing XML Documents. *Proceedings of the 2000 International Conference on Extending Database Technology(EDBT2000).*

[4] Wen, Quan, Yufei Wang & Peng Li. (2018). Two Zero-Watermark methods for XML documents. *Journal of Real-Time Image Processing, 14(1),* 183-192.

[5] J. L. Raheja, A. Chaudhary, K. Singal. (2011). Tracking of fingertips and centers of palm using kinect. *In Computational intelligence, modelling and simulation (CIMSiM),* 248-252.

[6] S. A. Kumar. (2017). Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications, 76(6),* 8881-8900.

[7] S. H. Kim. (2016). Realtime 3D Human Full-Body Convergence Motion Capture using a Kinect Sensor. *Journal of Digital Convergence, 14(1),* 189-194.

[8] K. W. Park & J. Y. Lee. (2015). A Morphology Technique-Based Boundary Detection in a Two-Dimensional QR Code. *Journal of Digital Convergence, 13(12),* 159-175.

[9] S. M. Jung, J. G. Song, D. J. Hwang, J. Y. Aan & S. S. Kim. (2010). A Study on Software-based Sensing

Technology for Multiple Object Control in AR Video. *Sensors, 10(11),* 9857-9871.

[10] J. U. Hou, D. G. Kim & H. K. Lee. (2017). Blind 3D Mesh Watermarking for 3D Printed Model by Analyzing Layering Artifact. *IEEE Transactions on Information Forensics and Security, 12(11),* 2712-2725.

[11] A. F. Tawfiq & J. Lu. (2017). Securing Financial XML Transactions Using Intelligent Fuzzy Classification Techniques: A Smart Fuzzy-Based Model for Financial XML Transactions Security Using XML Encryption. *Ontologies and Big Data Considerations for Effective Intelligence. IGI Globa*l, 2017, 214-326.

[12] K. Fatma. (2017). High Performance and Reliable Fault Detection Scheme for the Secure Hash Algorithm. *Indian Journal of Science and Technology* 10.19 (2017).

[13] S. R. Kokate & S. G. Salunke. (2017). Implementation of Intelligent Malware Detection System Using Post Processing Techniques. *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA).* (pp. 1-4).

[14] S. W Jeong, U. R Chio & I. G. Lee. (2018). Cyber KillChain Based Security Policy Utilizing Hash for Internet of Things. *Journal of Digital Convergence, 16(9),* 179-185.

[15] H. U. Kim, H. J. Kim, J. H. Kang & M. S. Jun. (2017). A Study on Analysis and Countermeasure of Security threat in NFC. *Journal of Digital Convergence, 14(12),* 183-191.

[16] K. H Ko. (2018). An Estimating Algorithm of Vehicle Collision Speed Through Images of Blackbox. *Journal of Digital Convergence, 16(9),* 173-178.

김 동 현 (Donghyun Kim) [정회원]

- 2012년 2월 : 한남대학교 멀티미디어 공학(공학사)
- 2014년 2월 : 한남대학교 멀티미디어 (공학석사)
- 현재 : 한남대학교 멀티미디어 박사 과정
- 관심분야 : 영상처리, 증강현실, 정보보호
- E-Mail : donghyunk1986@gmail.com

임 재 현 (Jaehyun Lim) [정회원]

- 2012년 2월 : 한남대학교 멀티미디어 공학(공학사)
- 2014년 2월 : 한남대학교 멀티미디어(공학석사)
- 현재 : 한남대학교 멀티미디어 박사 과정
- 관심분야 : 3D, 영상처리, 증강현실, 정보보호
- E-Mail : lim3d@hotmail.com

김 석 수 (Seoksoo Kim) [정회원]

- 1989년 2월 : 경남대학교 컴퓨터공학(공학사)
- 1991년 2월 : 성균관대학교 정보전산학과(공학석사)
- 2002년 2월 : 성균관대학교 컴퓨터공학(공학박사)
- 현재 : 한남대학교 멀티미디어학과 교수
- 관심분야 : 멀티미디어 통신, 멀티미디어 저작, 컴퓨터 네트워크, 정보보호
- E-Mail : sskim@hnu.kr