# A Distributed Cloud based Video Storage System with Privacy Protection

Kang Il Choi, Jung Hee Lee, Bhum Cheol Lee

*Network Computing Convergence Lab.*, ETRI, Daejeon, Korea

**forerunner@etri.re.kr, jhlee@etri.re.kr, bclee@etri.re.kr**

***Abstract*— In this paper, we present a novel method to protect privacy information for the Cloud based Video Storage System (CVSS), which not only distribute the CVSS geographically, but also use different privacy protection key algorithm for different CVSS to encode/decode the actual video data itself stored in the storage with the subscriber key for the privacy protection so that the system even under the hacking of the CVSS systems, still provide the privacy protection of the video data. We present how this system stores the video stream data transferred from the network connected camera such as IP CCTV. As the system receives the video stream, it masks the privacy related part, such as facial information or car plate number and so on, of the video stream data with a scrambling key and it also encrypts the scrambled video stream data with an encryption key. In this paper, we also present how the system retrieves the privacy information protected video image requested by either the network control centre or end users. When the network control centre or end user requests the networked video, it retrieves the corresponding video image from the video storage first. Then, it decrypts the image with the decryption key and unscrambles the decrypted image with the unscrambling key. Then it transfers the network video back to the network control center or to the end-user. We present the architecture of the distributed CVSS with the privacy protection for the Cloud based Network Function Virtualization System. We also provide flowchart for receive/transmit operation of the DCVSS. Finally, we present a POC implementation of the distributed CVSS in the Cloud based Network Function Virtualization System.**

***Keyword*—** Cloud Video Storage System, Privacy Protection

## I. INTRODUCTION

In general, components of a video data storage system, a camera, a monitor, a video recording device, are connected to each other over a closed network to monitor the facility such as a predetermined building or convenience facility.

In this case, a user agent is present in a user device to provide video data to the user device. Accordingly, a camera, a server, and the user device control the camera through mutual interface communication.

Also, video data photographed from the camera is recorded in a storage device within the server and is also transferred to a viewer of the user device.

The above system is generally configured as a closed network among the camera, the server, and the user device for controlling the camera and storing the video data.

In the closed network, the user agent operating in the user device obtains state information of the camera by transmitting a command to the camera through the server, and the camera transfers current state information to the user agent through the server.

A camera server provides interface communication between the user agent and the camera. Also, the camera server enables a user to store an image through the user agent or enables the server to execute a command, such as displaying the image on the viewer in lieu of the user.

When the user desires the image to be displayed on the viewer of the user device, the image transferred to the server is transferred to the user device.

When the user desires to store the image in the storage device, the image transferred to the server is stored in the storage device within the server.

However, a camera monitoring system connected using the closed network has constraints in extensibility. In addition, when the user is not directly connected to the closed network, it is difficult to provide a function capable of controlling the camera through a general network (for example, the Internet) or at least viewing or storing an image.

In this environment, providing the privacy protection is one of the social issues because of several hacking accident ends up with huge privacy information leaking. There are several different approaches to cope with this privacy protection for the video data storage system. However, almost all approaches focus on the IP camera side to provide secure transmit of the video data collected by the IP camera [3-12].

In this paper, we propose a novel privacy protection approach in the video data storage server side, which encoding/decoding the actual video data itself stored in the storage with the subscriber key for the privacy protection so that the system even under the hacking of the CVSS system, still provide the privacy protection of the video data.

The paper is structured as follows. Section II describes an overview of the Cloud based Video Storage System (CVSS) which supports Privacy Protection. We also describe the operation of the CVSS with flowcharts so that how the system

Manuscript received January 29, 2016. This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (B0101-15-233, Smart Networking Core Technology Development)

Kang Il Choi is with the Electronics Telecommunication Research Institute, Daejeon, South Korea (phone: +82-42-860-1704; mobile: +82-10-3861-7758; fax: +82-42-860-5213; e-mail: forerunner@etri.re.kr).

Jung Hee Lee is with the Electronics Telecommunication Research Institute, Daejeon, South Korea (e-mail: jhlee@etri.re.kr).

Bhum Chul Lee is with the Electronics Telecommunication Research Institute, Daejeon, South Korea (e-mail: bclee@etri.re.kr).

supports the privacy protection for the CVSS. In Section III, we describe the architecture of the distributed CVSS (DCVSS) with the Privacy Protection for the Cloud based Network Function Virtualization System. We also describe the operation of the DCVSS with flowcharts so that how the system supports the privacy protection for the DCVSS. Finally, In Section IV, we describe the POC implementation of the DCVSS with the Privacy Protection in the Cloud based Network Function Virtualization System.

## II. CLOUD BASED VIDEO STORAGE SYSTEM

Fig. 1 is a control block diagram illustrating a control configuration of a Cloud based Video Storage System (CVSS) [1,2].

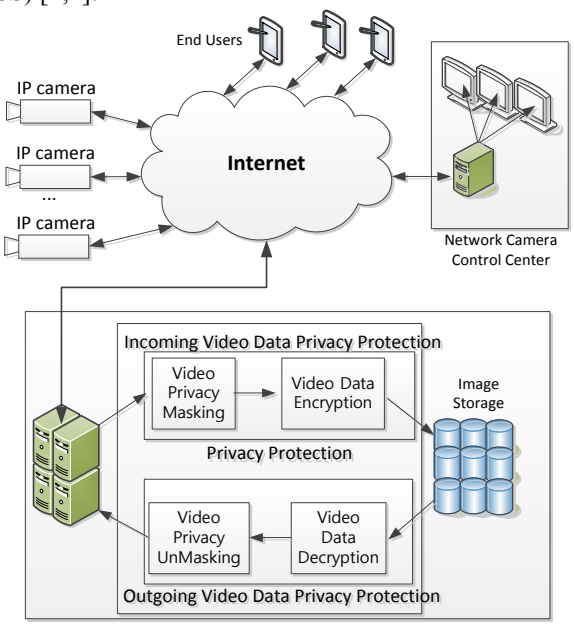


**Fig. 1 Cloud Based Video Storage System**

In Fig. 1, the CVSS system consists of an "Incoming Video Data Privacy Protection (IVDPP)", an "Outgoing Video Data Privacy Protection (OVDPP)" block and Image Storage. The IVDPP block creates a protected image by applying a privacy protection algorithm to an original image received in the IVDPP block. The IVDPP block stores the protected image into the Image Storage. The OVDPP block retrieves a protected image from the Image Storage and creates the original image by applying a privacy release algorithm to the protected image.

In Fig. 1, the CVSS may be included in a device capable of photographing an image, for example, an imaging device such as a network camera, a mobile communication terminal, and a closed-circuit television (CCTV), or may be stored in a storage server, for example, a network server and a cloud configured to store an image photographed by the imaging device.

In Fig. 1, in the incoming direction, the IVDPP block includes "Video Privacy Masking (VPM)" block and "Video Data Encryption (VDE)" block.

In Fig. 1, the VPM block detects the privacy image from the original image which is received from the remote video capturing system. The VPM block detects the privacy image based on at least one of the edge information of the original image, shape information, color analysis information, and learning information about a previous privacy image.

In Fig. 1, the VPM block obtains the edge information by analyzing the original image and detects a boundary between a face and a portion excluding the face using the edge information.

It determines whether the face is present within the original image by comparing the results of analyzing the original image and shape information about a facial shape. Also, the VPM block compares the color analysis information with unique color distribution information of the face and thus, may more accurately detect the face.

Additionally, the VPM block detects a facial area using learning information about the previous privacy image, including an Adaboost learning scheme.

In Fig. 1, the VPM block performs masking by scrambling the privacy image detected by the VPM block to a privacy protection image using a set of scrambling keys. The VPM block scrambles the privacy protection image to be expressed using a predetermined color and a predetermined figure.

In Fig. 1, the VDE block creates a protected image in which the privacy protection image input from the VPM block and the general image is encrypted using an encryption key.

In Fig. 1, the VDE block may increase security about the privacy protection image by encrypting the privacy protection image and the general image. Then, the VDE block transfers the protected image to the image storage.

The image storage block may assign a unique number capable of recognizing the protected image input from the VDE block and thereby stores the protected image.

The image storage transfers the protected image to the OVDPP block in response to a control command of the Network Camera Control Center or the End Users.

In Fig. 1, the OVDPP block operates relatively inversely to the IVDPP block. In Fig. 1, in the outgoing direction, the OVDPP block includes a Video Data Decryption (VDD) block and a Video Privacy Unmasking (VPU) block.

In Fig. 1, the VDD block decrypts the privacy protection image and the general image from the protected image using a decryption key when the protected image is input from the image storage. Here, the decryption key may be identical to the encryption key, or may be another key capable of performing decryption and corresponding to the encryption key.

In Fig. 1, the VPU block detects the privacy protection image from the privacy protection image and the general image decrypted by the VDD block. The VPU block detects, from the privacy protection image and the general image, the privacy protection image that is expressed using at least one of the predetermined color and the predetermined figure.

The VPU block detects the privacy protection image based on at least one of the edge information of the original image including the privacy protection image and the general image, shape information, color analysis information, and learning information about a previous privacy image. In addition, the VPU block detects the privacy protection image as an image expressed using at least one of the predetermined colors and the predetermined figure of the privacy protection image.

In Fig. 1, the VDD block unscrambles the privacy protection image detected by the VPU block to the privacy image using an unscrambling key. The unscrambling key may be identical to the scrambling key, or may be another key corresponding to the scrambling key.

In response to a control command of the Network Camera Control Center or the End Users, the VDS block transmits the

original image including the privacy image and the general image, or may transfer the original image to the Network Camera Control Center or the End Users.

### *A. Receive Operation of the CVSS*

Fig. 2 is a flowchart illustrating a receive operation method of a Cloud Based Video Storage System (CVSS).

In Fig. 2, the CVSS determines whether a privacy image is detected from an original image when the original image is input, and scrambles the privacy image to a privacy protection image using a scrambling key when the privacy image is detected.

The original image may include at least one of the privacy image including user information, for example, at least one of facial information, license plate information, and privacy information, and a general image excluding the privacy image. Specifically describing, the CVSS determines whether the privacy image is detected from the original image when the original image is input.

In Fig. 2, the CVSS detects the private image based on at least one of the edge information of the original image, shape information, color analysis information, and learning information about a previous privacy image.

In Fig.2, the CVSS obtains the edge information by analyzing the original image M1, may detect a boundary between a face and a portion excluding the face using the edge information, and may determine whether the face is present within the original image by comparing a result of analyzing the original image and shape information about a facial shape.

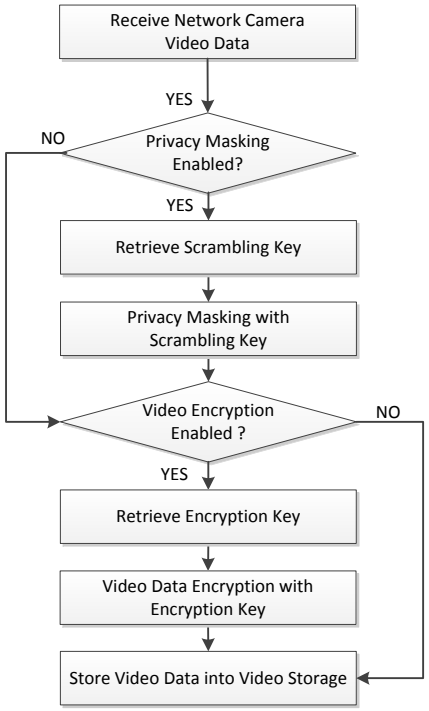


**Fig. 2 Receive Operation of the Cloud based Video Storage System**

Also, the CVSS compares the color analysis information with unique color distribution information of the face and thus, may more accurately detect the face. Additionally, the CVSS may detect a facial area using learning information about the previous privacy image, including an Adaboost learning scheme.

When the privacy image is detected, the CVSS performs masking by scrambling the detected privacy image to the privacy protection image using a set of scrambling key.

After this operation, the CVSS creates a protected image in which the privacy protection image and the general image are encrypted using an encryption key, and transfers the protected image to the image storage.

When the privacy image is not detected from the original image, the CVSS performs encryption operation on the original image.

### *B. Transmit Operation of the CVSS*

Fig. 3 is a flowchart illustrating an operation method of a CVSS when an image is output from the CVSS.

In Fig. 3, when an image request signal requesting an original image is input, the CVSS receives a protected image stored in the image storage, and the CVSS decrypts the protected image to an original image including a privacy protection image and a general image using a decryption key and detects the privacy protection image.

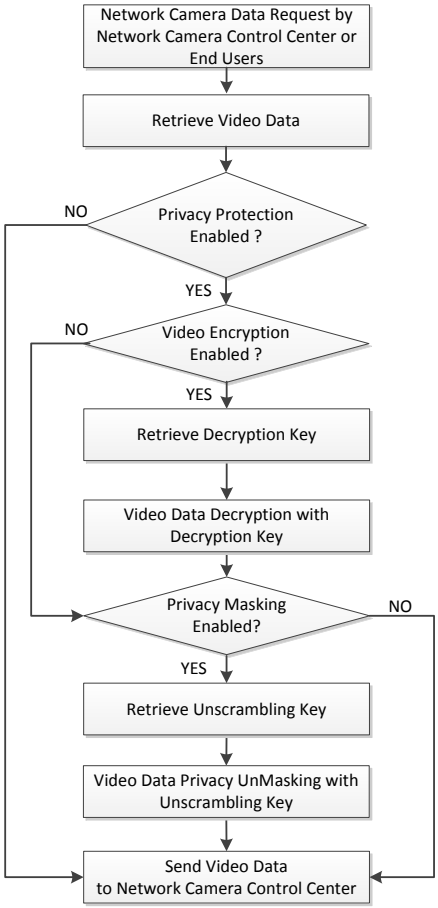


**Fig. 3 Transmit Operation of the Cloud based Video Storage System**

In response to a control command of the Network Camera Control Center or the End Users and the image request signal requesting the original image, the CVSS receives, from the image storage, the protected image to which a privacy protection algorithm corresponding to the original image is applied among images stored in the image storage.

Next, the CVSS decrypts the protected image to the original image which is including the privacy protection image and the general image using a set decryption key.

The CVSS detects, from the original image, the privacy protection image that is expressed using at least one of a predetermined color and a predetermined figure.

After this operation, the CVSS unscrambles the privacy protection image to the privacy image using an unscrambling key, and creates the original image including the privacy protection image and the general image.

The CVSS creates the privacy image by unscrambling, using the unscrambling key, the privacy protection image scrambled using a scrambling key.

Next, the CVSS creates the original image including the privacy protection image and the general image, and transfers the original image to the Network Camera Control Center or the End Users or a predetermined device having input the image request signal.

## III. Distributed Cloud based Video Storage System

Fig. 4 is an architecture diagram illustrating a distributed Cloud based Video Storage System (DCVSS).

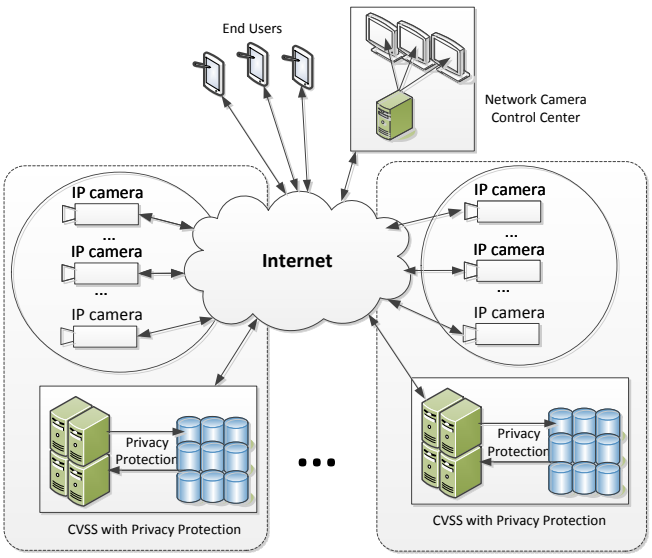


**Fig. 4 An architecture of the Distributed CVSS**

In Fig. 4, each individual DCVSS process the video images transmitted by a group of IP cameras, which is geographically close to the DCVSS, so that it can provide privacy protection for the video images generated by the group of the IP cameras.

In Fig.4, the Network Camera Control Center configure which DCVSS will handle which IP cameras in terms of the CVSS configuration and IP camera's configuration, which means the Network Camera Control Center knows who process the specific IP cameras video image and provide the privacy protection for the IP cameras.

When an end user request their own image, the network camera control center re-route the end-users request to the DCVSS who actually processed the image so that the DCVSS, who actually process the end user's IP camera, respond to the end-user's request.

In Fig. 4, by distributing the DCVSS system geographically so that the DCVSS process the video images transmitted by a group of IP cameras which is geographically close to the DCVSS, we can provide the Quality of Service requirement from the end-user, such as low latency for the video image processing.

In Fig. 4, by applying separate privacy protection key algorithm (which arithmetically identical but generate different key output) per geographically separated DCVSS, we can also provide separation of privacy protection in case of hacking, so that hacking on the one DCVSS doesn't affect the other DCVSS.

### A. Receive Operation of the DCVSS

Fig. 5 is a flowchart illustrating a receive operation method of a DCVSS. In Fig. 5, if privacy protection and privacy masking is enabled, then the DCVSS retrieve both personal scrambling key and site dependent scrambling key. And the DCVSS do privacy masking the video data with combined (personal + site) scrambling key. If video encryption is enabled, the DCVSS retrieve both personal encryption key and site dependent encryption key. And the DCVSS encrypt the video data with combined (personal + site) encryption key.

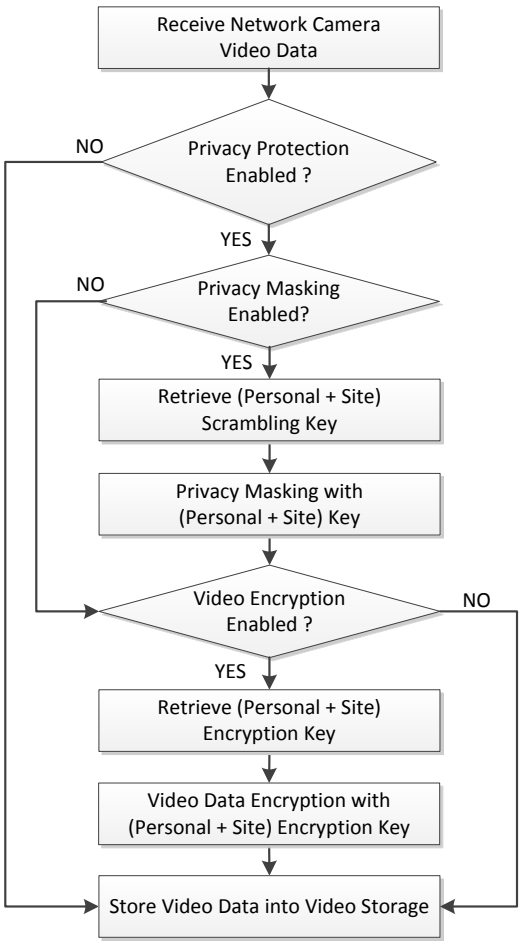


**Fig. 5 Receive Operation of the DCVSS**

### B. Transmit Operation of the DCVSS

Fig. 6 is a flowchart illustrating transmit operation method of a DCVSS. In Fig. 6, if privacy protection and video encryption is enabled, then the DCVSS retrieve both personal decryption key and site dependent decryption key. And the DCVSS decrypt the video data with combined (personal + site) decryption key. If privacy masking is enabled, the DCVSS retrieve both personal unscrambling key and site dependent unscrambling key. And the DCVSS unmasking the video data with combined (personal + site) unscrambling key.

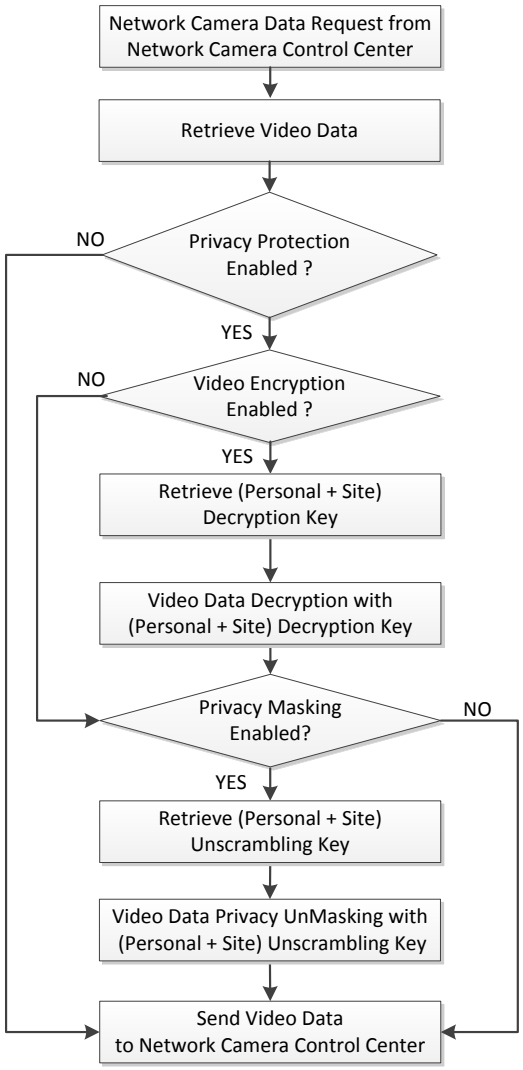


**Fig. 6 Transmit Operation of the Cloud based Video Storage System**

## IV. An POC Implementation of the Distributed CVSS in the Cloud Based Network Function Virtualization System

Fig. 7 is a POC implementation of the distributed Cloud based Video Storage System (DCVSS) in the Cloud based Network Function Virtualization System, which consist of a DCVSS Control Center, Daejeon DCVSS and Seoul CVSS.

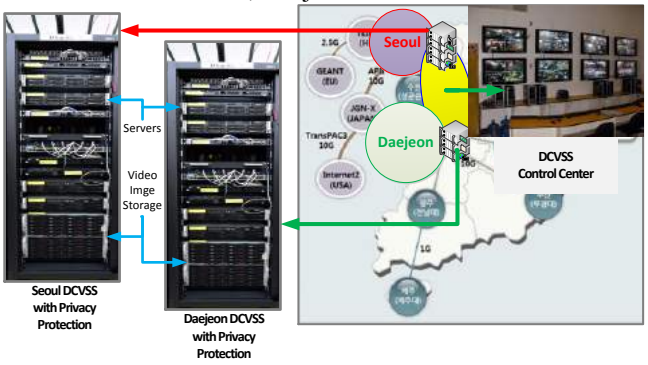


**Fig. 7 An implementation of the Distributed CVSS in the Cloud Network Function Virtualization System**

In Fig. 7, each DCVSS consists of Servers, which process the IP camera network image, Video Image Storage, which stores the IP camera network images, and Privacy Protection Module, which running on the Servers, encrypts and decrypts the IP camera images for privacy protection.

In Fig. 7, each DCVSS also apply separate key system for the privacy protection algorithms. End users from Daejeon areas access their video image through Daejeon DCVSS with privacy protection, and the End users from Seoul area access their video image through the Seoul CVSS.

In Fig. 7, there are two DCVSS system with privacy protection, Daejeon DCVSS, which provide privacy protection for the video images generated by the group of the IP cameras located in the Daejeon area, and Seoul DCVSS, which provide privacy protection for the Seoul areas

In Fig. 7, the DCVSS Control Center control the setup process for each DCVSS and configure each DCVSS so that each DCVSS not only process the video images from the group of IP cameras located geographically close to the DCVSS but also use different privacy protection key algorithm. The Daejeon DCVSS configured to process the group of IP cameras from the Daejeon area with privacy protection key algorithm A, and the Seoul DCVSS configured to process the group of IP cameras from the Seoul area with privacy protection key algorithm B. With this configuration, even the Daejeon DCVSS hacked so that the video image of it hacked, the video images in the Seoul DCVSS are safe and provide privacy protection because these two DCVSS use different privacy protection key algorithm.

## V. Conclusion

In this paper, we presented a novel method to protect privacy information for the Cloud based Video Storage System (CVSS), which encoding/decoding the actual video data itself stored in the storage with the subscriber key for the privacy protection so that the system even under the hacking of the CVSS system, still provide the privacy protection of the video data. On the top of this, by distributing the CVSS system geographically and by applying separate privacy protection key algorithm, we can prevent huge privacy information leaking and localize the privacy leaking. We presented how this system stores/retrieves the video stream data transferred from the network connected camera such as IP CCTV to/from the cloud based video storage system. In the paper, we presented the detailed procedures and algorithms for these processes. In this paper, we masked the privacy related part and encrypted the scrambled video with an encryption key so that we protected the privacy information of the networked video stream, which is stored in the cloud based video storage system. We presented the architecture of the distributed CVSS with the privacy protection for the Cloud based Network Function Virtualization System. We also provided flowchart for receive/transmit operation of the DCVSS. Finally, we presented the implementation of the distributed CVSS in the Cloud based Network Function Virtualization System

## References

[1] Kang Il Choi, Jung Hee Lee and Bhum Cheol Lee, "Cloud based Video Storage System with Privacy Protection", *ICACT2015, 2015, pp. 448–451.*

[2] Kang Il Choi, Bhum Cheol Lee, Seung Woo Lee, Young Ho Park, Jung Hee Lee and Sang Min Lee, "Image processing apparatus and operation method thereof", *US20150055775 A1, Aug 20,2013*

[3] DJ Neal and Syed Shawon Rahman, "VIDEO SURVEILLANCE IN THE CLOUD?", *International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012*
[4] Yong-Hua Xiong, Shao-Yun Wan, Yong He and Dan Su, "Design and Implementation of a Prototype Cloud Video Surveillance System", *Journal of Advanced Computational Intelligence and Intelligent Informatics, Vol.18, No.1 pp. 40-47, 2014*
[5] Biao Song, Yuan Tian and Bingyin Zhou, "Design and evaluation of remote video surveillance system on private cloud", *2014 4th International Symposium on Biometrics and Security Technologies, 26 August 2014*
[6] Chia-Feng Lin, Shyan-Ming Yuan, Muh-Chyi Leu and Ching-Tsorng Tsai, "A framework for scalable cloud video recorder system in surveillance environment", *IEEE 9th International Conference on Ubiquitous Intelligence and Computing and IEEE 9th International Conference on Autonomic and Trusted Computing, UIC-ATC 2012, Article number 6332062, Pages 655-660*
[7] Räty, T.D., "Survey on contemporary remote surveillance systems for public safety", *IEEE Transactions on Systems, Man and Cybernetics, art. no. 5422679, pp. 493-515*
[8] Kim, I.S., Choi, H.S., Yi, K.M., Choi, J.Y., Kong, S.G., "Intelligent visual surveillance - A survey", *International Journal of Control, Automation and Systems, 8 (5), pp. 926-939*
[9] Zhao, Z., Cui, X., Zhang, H., "Cloud storage technology in video surveillance", *Advanced Materials Research 2012, 532-533, pp. 1334-1338*
[10] Rodríguez-Silva, D.A., Adkinson-Orellana, L., González-Castaño, F.J., Armiño-Franco, I., González-Martínez, D., "Video surveillance based on cloud storage", *2012 IEEE 5th International Conference on Cloud Computing, CLOUD 2012, art. no. 6253615, pp. 991-992.*
[11] Hossain, M.S., Hassan, M.M., Qurishi, M.A., Alghamdi, A., "Resource allocation for service composition in cloud-based video surveillance platform", *Proceedings of the 2012 IEEE International Conference on Multimedia and Expo Workshops, ICMEW 2012, art. no. 6266418, pp. 408-412*
[12] Pearson, S., "Taking account of privacy when designing cloud computing services", *2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011, art. no. 6014715, pp. 245-249*

**Kang Il Choi** received B.S. degree in Computer Science from KAIST, Korea and M.S. degree in Computer Science from Sogang University in 1992 and 1994, respectively. He is currently senior researcher of Electronics and Telecommunications Research Institute (ETRI), Korea. His research interests are Multicore Parallel Processing, Distributed Cloud Data Center, Data Plane Acceleration Technology and Network Virtualization.

**Jung Hee Lee** received B.E. and M.S. in Electronic Engineering at Kyungpok National University in 1984 and 1991, respectively. She is currently principal researcher of Electronics and Telecommunications Research Institute (ETRI), Korea. Her research interests are Flow based Network Processor, Multicore Parallel Processing, High Speed Parallel Switching and Network Virtualization.

**Bhum Cheol Lee** received M.S. and Ph.D. degree in Electric Engineering from Yonsei University, Korea in 1983 and 1997, respectively. He is currently Manager of Networking Computing Convergence Lab. in Electronics and Telecommunications Research Institute (ETRI), Korea. His research interests are Smart Network, Parallel Flow Processing and Network Virtualization.