Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT GROUP KEY DISTRIBUTION SCHEME IN NVR

[1] GUN-WOOK CHOI, [2] YONG-WOON HWANG, [3] IM-YEONG LEE
[1,2,3] Department of Computer Science and Engineering, Soonchunhyang University, South Korea
E-mail: [1]choigu@sch.ac.kr, [2]hyw0123@sch.ac.kr, [3]imylee@sch.ac.kr

ABSTRACT

NVR is a network video surveillance system that can be used in the Internet environment. Through the system, the user can acquire image information remotely and use it for various purposes. However, when cameras connected to the network or not connected to the network are connected to the Internet, security problems such as unauthorized access and leakage of image information occur. Therefore, this paper can solve various threats effectively by encrypting image information generated in IP CCTV through symmetric key group key management.

Keywords: *IP CCTV, Group Key Management, Authentication, NVR*

1. INTRODUCTION

This Network Video Recorder (NVR) is installed at important sites that need to be monitored in complex cities and major buildings, and can be used for prevention and post-war measures against various kinds of risks such as crime, fire, and traffic accidents[1]. Recently, Internet-based network video surveillance system has attracted attention and individuals have become popular enough to purchase IP CCTV (Internet Protocol Closed Circuit Television) to check their personal space anytime and anywhere on the Internet[2]. IP CCTV includes the concept of closed-circuit television (CCTV) and consists of cameras, transmission devices, amplifiers, and control system. As the use of IP CCTV is increased, the crime rate is increased especially through the surveillance equipment, and the arrest rate of the criminal is increased, contributing greatly to creating an environment where citizens can live with peace of mind. However, the cameras that were connected to the closed network were connected to the Internet, which is a public channel[3]. Illegal access to image data transmitted through a public network to take data or control the camera can be used for various crimes. Also, the damage of privacy infringement such as exposing the identity to the leaked image data is becoming a big social problem[4].

In this paper, we propose an efficient group key management system using symmetric key in NVR. IP CCTV with a specific location or purpose can be grouped together to distribute a session key to encrypt video data, and only a user with access to the group can access the video data. In addition, when a new IP CCTV joins in a group or when an old IP CCTV is excluded from a group, it can cope with Forward / Backward threats by re-forming the group and redistributing the new key. This paper introduces related works in Chapter 2, and discusses security requirements in Chapter 3. Chapter 4 introduces the proposed schemes, Chapter 5 analyzes the proposed schemes, and concludes with the final Chapter 6 conclusions.

2. RELATED WORKS

2.1 NVR

Conventional DVR (Digital Video Recorder) video surveillance system is a system that monitors and connects analog cameras using coaxial cable. Due to the use of coaxial cable, DVR systems have been difficult to control and manage remotely because of cost increase due to distance, low recording quality, high cost efficiency, and a few cameras connected to a closed network. Recently, we have been using NVR (Network video recorder) to replace this[5]. A dedicated server for video recording, monitoring, event management, playback, etc. of a camera or video server installed on the network, and receives and stores digital images through an IP camera. Theoretically, there is no limitation on the number of IP cameras and it is possible to perform monitoring in a plurality of management layers[6]. In addition, easy installation and management is possible, remote monitoring can be performed in wide area, and the system can be constructed at low cost with efficiency. Recently, NVR system has been used in each home to build a security system[7].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2 Group Key Management

NVR can configure several IPCCTV in the network and can receive video data remotely. Due to the nature of IP CCTV, video data is transmitted through an open network, so image data encryption is an essential element for image data leakage and user privacy protection[8]. In order to provide this efficiently and safely, the group key management technique can safely protect the image data. The group key management scheme is a technique of using a group key to locally group nearby nodes or nodes having a specific purpose or feature, and to maintain group security. The method used in this paper is a type in which a leader of a group IP CCTV performs a mutual authentication process with a key management server on behalf of a group based on a cluster structure. [9]. After that, the key management server sends the group key to be used in the group to the leader of the IP CCTV, and the leader distributes the group key again to the group members. In addition, if a new IP CCTV joins the group or old IP CCTV leaves, the group can be re-formed to reissue the group key, thereby coping with threats such as data leakage that may occur by using old keys[10].

3. SECURITY REQUIREMENT

In this chapter, we propose an efficient group key management system using symmetric key in NVR. In order to safely distribute the group key after forming a group of several IP CCTVs according to a specific purpose, the group leader and the key management server must be able to access image data efficiently by mutual authentication using each other. In addition, it is necessary to prevent re-transmission attack by reusing session data and disguising as a legitimate user, and it should not be possible to communicate using a key that is used when re-grouping.

· **Mutual Authentication:** The group leader and the key management server should be able to securely distribute group keys after verifying that they are legitimate entities through mutual authentication. By providing mutual authentication, an attacker can not intercept data as a legitimate object and prevent data leakage.

· **Replay Attack:** To provide secure service, mutual authentication and distribution of group keys must be provided. In the process of providing authentication and key distribution, an attacker can intercept the message and resend the already communicated content to disguise it as a legitimate entity. To prevent this, even if the contents of the communication are randomized and the message is retransmitted, it should not be authenticated as a legitimate entity.

· **Key Refresh:** When a specific event occurs or a certain period passes, a new key must be generated and operated. It is possible to increase the safety by replacing the key when the group circle changes while using the group key of the same group.

· **Authentication / Integrity:** The recipient must be able to decrypt the message only after authentication of the encrypted data has been verified after passing the authentication. By using the message after identifying the legitimate object, a malicious attacker should be able to send a message so that the key can not be exchanged.

· **Forward / Backward Secrecy:** When the group is re-formed due to the change of the group circle, it should not be used for group communication by using the existing key. A group of malicious attackers can join a group and eavesdrop on a message when forming a group with a previously used key.

4. PROPOSED SCHEMES

In this chapter, we propose a mutual authentication and group key management system using symmetric key in NVR. Figure 1 is a all scenario of the proposed schemes. The proposed scheme proposes two different schemes of key distribution in the group member 's join and leave step. The proposed schemes consists of group key distribution step, group join step, and group leve step. The system parameters used in the communication are as follows.

ID_* - Identifier of $*$

r_* - $*$ Generated random value

$G1$ - Group 1

KMS – Key management server

$GLIC_{G1}$ – IP CCTV Leader in Group 1

IC_{G1} – IP CCTV members in Group 1

NIC_{G1} –New IP CCTV in Group 1

OIC_{G1} – Old IP CCTV in Group 1

$h()$- One-way hash function

Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

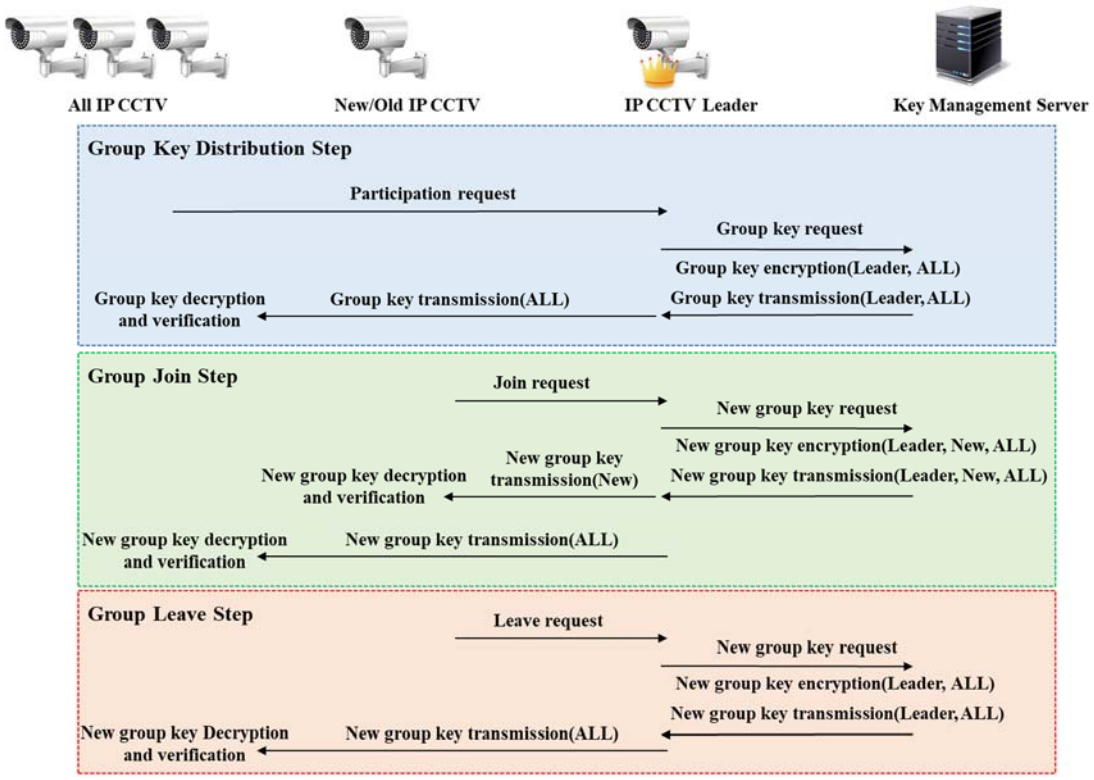

Fig. 1 : Flow of the Proposed Scheme

$E_*()$ - Decryption with $*$

$D_*()$ - Decryption with $*$

$GK1$ - Shared key between IP CCTV Leader and KMS

GSK_{G1} - Group session key of group G1

MAC_* - * Message authentication code

$EGSK$ - Encrypted group key

$AuthM$ - Authentication message M

4.1 Proposed Scheme 1

Proposed scheme 1 is a method in which KMS manages regeneration of keys in the process of joining and leaving group members. This scheme consists of a group key distribution step, a join step, and a leave step.

4.1.1 Group key distribution phase

It is the step where the leader of the group forms a group and the group key is distributed from KMS.

Step 1. The group members create a message $M_{IC_{G1_x}}$ using identifier ID_{G1}, $ID_{IC_{G1_x}}$, and random value $r_{IC_{G1_x}}$ to construct a group, add a symmetric key $K_{IC_{G1_x}}$ to the message $M_{IC_{G1_x}}$, generate a hashed $MAC_{IC_{G1_x}}$, and send it to the group leader IPCCTV $GLIC_{G1}$ do. The formula for this is as follows.

$$M_{IC_{G1\_x}} = (ID_{G1} \parallel ID_{IC_{G1\_x}} \parallel r_{IC_{G1\_x}})$$

$$MAC_{IC_{G1\_x}} = h(ID_{G1} \parallel ID_{IC_{G1_x}} \parallel r_{IC_{G1\_x}} \parallel K_{IC_{G1\_x}})$$

Step 2. $GLIC_{G1}$ generates MAC_{G1} by using group members' messages and collects MAC_{G1} of group members to generate $AuthM_{G1}$. Next, r_{G1} is encrypted using the group leader key Er_{G1}. Finally, $AuthM_{G1}$ and Er_{G1} are sent to the Key Management Server KMS. The formula for this is as follows.

$$MAC_{G1} = MAC_{IC_{G1_1}} \oplus MAC_{IC_{G1_2}} \cdots MAC_{IC_{G1_x}} \oplus r_{G1}$$

$$AuthM_{G1} = (M_{IC_{G1_1}} \parallel M_{IC_{G1_2}} \cdots M_{IC_{G1_x}} \parallel MAC_{G1}).$$

$$Er_{G1} = E_{GK1}(r_{G1}).$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

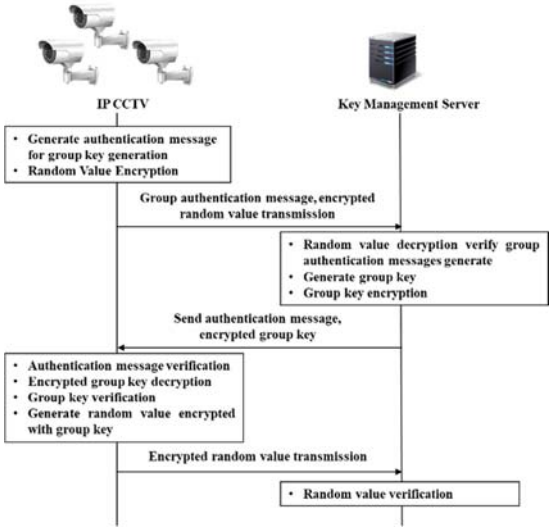

Fig. 2 : Group Key Distribution Phase

Step 3. The KMS decrypts the erg to obtain the random value r_{G1}` Then, a message $M_{IC_{G1_x}}$ sent from IPCCTV and a symmetric key $K_{G1_x}$ are combined to generate a $MAC_{IC_{G1_x}}$`. MAC_{G1}` is generated and compared with the received MAC_{G1}.

$$r_{G1}` = D_{GK1}(Er_{G1})$$

Step 4. The KMS generates the group session key GSK_{G1} by hashing the random value r_{G1} of the MAC_{ICM} and the and the random value r_{G1} of the server. The formula for this is as follows.

$$GSK_{G1} = h(MAC_{G1} \| r_{G1} \| r_{ICM})$$

$$MAC_{ICM} = h(ID_{ICM} \| r_{ICM} \| r_{G1})$$

GSK_{G1} encrypts each IPCCTV symmetric key to generate $EGSK_{IC_{G1_x}}$. Then, the MAC_{ICM} is enerated by hashing the identifier ID_{ICM} of the server, the random value r_{ICM} of the server, and the random value r_{G1} of the group. The formula for this is as follows.

$$EGSK_{IC_{G1_x}} = E_{K_{IC_{G1_x}}}(GSK_{G1})$$

$$MAC_{ICM} = h(ID_{ICM} \| r_{ICM} \| r_{G1})$$

Finally, $Auth_{ICM} = (r_{ICM} \| MAC_{ICM})$ is generated using random value r_{ICM} and MAC_{ICM}, and then $Auth_{ICM}$ and $EGSK_{IC_{G1_x}}$ are transmitted to the $GLIC_{G1}$.

Step 5. The $GLIC_{G1}$ generates MAC_{ICM}` by hashing the identifier $ID_{ICM}$ of the $KMS$, the random value $r_{ICM}$`, and the random value r_{G1}.

$$MAC_{ICM}` = h(ID_{ICM} \| `r_{ICM} \| r_{G1})$$

After that, it compares the MAC_{ICM}` value received from the KMS and confirms that they are the same. If the values are the same, the $GLIC_{G1}$ delivers $EGSK_{IC_{G1_x}}$ to the IC_{G1_x} belonging to the group. Each IC_{G1_x} belonging to the group can decrypt and obtain GSK_{G1}.

$$GSK_{G1} = D_{K_{IC_{G1_x}}}(EGSK_{IC_{G1_x}})$$

Step 6. IC_x generates hash of group ID_{G1}, $ID_{IC_{G1_x}}$ $ID_{IC_{G1_x}}$, and GSK_{G1}, generates $ACK_{IC_{G1_x}}$, and sends it to the $GLIC_{G1}$.

Step 7. The $GLIC_{G1}$ generates an $ACK_{IC_{G1_x}}$ by hashing ID_{G1}, $ID_{IC_{G1_x}}$, and GSK_{G1}, and sends it to the $GLIC_{G1}$. The $GLIC_{G1}$ generates an ACK_{G1} using the received $ACK_{IC_{G1_x}}$ and transmits it to the KMS. The formula for this is as follows.

$$ACK_{IC_{G1_x}} = h(ID_{G1} \| ID_{IC_{G1_x}} \| GSK_{G1})$$

$$ACK_{G1} = ACK_{IC_{G1_1}} \oplus ACK_{IC_{G1_2}} \cdots ACK_{IC_{G1_x}} \oplus r_{ICM}$$

Step 8. The KMS generates an ACK_{G1}` and generates a random value $r_{ICM}$ from the received $ACK_{G1}$. Compares the received $r_{ICM}$ with the previously generated `r_{ICM} to verify that the key is distributed correctly.

$$ACK_{G1}` = ACK_{IC_{G1\_1}} \oplus ACK_{IC_{G1\_2}} \cdots ACK_{IC_{G1\_x}} \oplus r_{ICM}$$

4.1.2 Join phase

The process of new IP CCTV joining the group.

Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

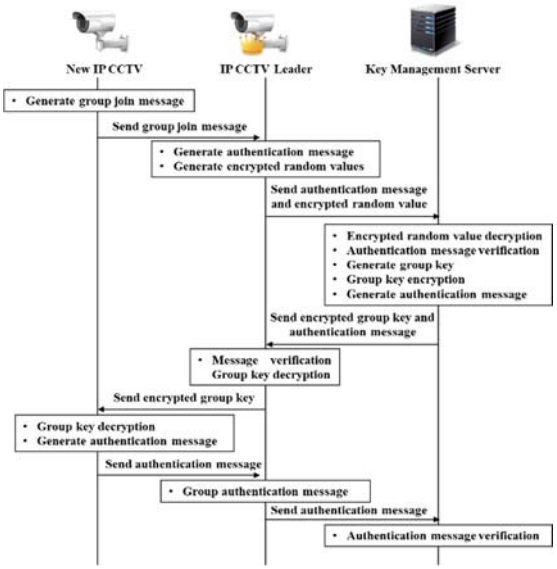

Fig. 3 : Join Phase of Proposed Scheme 1

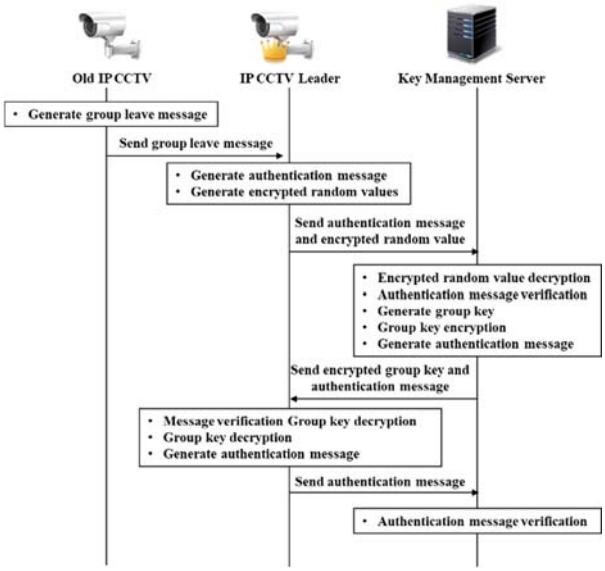

Fig. 4 : Leave Phase of Proposed Scheme 1

Step 1. The new IPCCTV NIC_{G1} generates $MAC_{IC_{G1_{new}}}$ by hashing the ID_{G1}, $ID_{IC_{G1_{new}}}$, random value $r_{IC_{G1_{new}}}$ and symmetric key $K_{IC_{G1_{new}}}$ to join the group. Then, a message $M_{IC_{G1_{new}}}$ is generated using the ID_{G1}, the $ID_{IC_{G1_{new}}}$, the random value $r_{IC_{G1_{new}}}$, and the join request message $join\_request$. The formula for this is as follows.

$$MAC_{IC_{G1\_new}} = h(ID_{G1} \parallel ID_{IC_{G1_{new}}} \parallel r_{IC_{G1\_new}} \parallel K_{IC_{G1\_new}})$$

$$M_{IC_{G1\_new}} = (ID_{G1} \parallel ID_{IC_{G1_{new}}} \parallel r_{IC_{G1_{new}}} \parallel join\_request)$$

Step 2. Send $MAC_{IC_{G1_{new}}}$ and message $M_{IC_{G1_{new}}}$ to the $GLIC_{G1}$. The $GLIC_{G1}$ generates MAC_{G1} and $AuthM_{G1}$ using the received value and encrypts the random value r_{G1} using the group leader key Er_{G1}. Finally, $AuthM_{G1}$ and Er_{G1} are sent to the key management server. The formula for this is as follows.

$$MAC_{G1} = MAC_{IC_{G1_{new}}} \oplus r_{G1}$$

$$AuthM_{G1} = (M_{IC_{G1_{new}}} \parallel MAC_{G1})$$

$$Er_{G1} = E_{GK1}(r_{G1})$$

Next, A key verification step is the same at step 3 in 4.1.1(group key distribution phase).

4.1.3 Leave phase

At the group leave step, the old IP CCTV is leave to the group, and the existing group is the process of distributing the new group key for safety.

Step 1. The old IP CCTV OIC_{G1} generates $MAC_{IC_{G1_{old}}}$ by hashing the ID_{G1}, $ID_{IC_{old}}$, random value $r_{IC_{G1_{old}}}$ and symmetric key $K_{IC_{G1_{old}}}$ to join the group. Then, a message $M_{IC_{G1_{old}}}$ is generated using the ID_{G1}, the $ID_{IC_{old}}$, the random value $r_{IC_{G1_{old}}}$, and the leave request message $leave\_request$.

$$MAC_{IC_{G1\_old}} = h(ID_{G1} \parallel ID_{IC_{G1_{old}}} \parallel r_{IC_{G1\_old}} \parallel K_{IC_{G1\_old}})$$

$$M_{IC_{G1\_old}} = (ID_{G1} \parallel ID_{IC_{G1_{old}}} \parallel r_{IC_{G1_{old}}} \parallel leave\_request)$$

Step 2. Send $MAC_{IC_{G1_{old}}}$ and message $M_{IC_{G1_{old}}}$ to the $GLIC_{G1}$. The $GLIC_{G1}$ generates MAC_{G1} and $AuthM_{G1}$ using the received value and encrypts the random value r_{G1} using the group leader key Er_{G1}. Finally, $AuthM_{G1}$ and Er_{G1} are sent to the key management server. The formula for this is as follows.

$$MAC_{G1} = MAC_{IC_{G1_{old}}} \oplus r_{G1}$$

$$AuthM_{G1} = (M_{IC_{G1_{old}}} \parallel MAC_{G1})$$

$$Er_{G1} = E_{GK1}(r_{G1})$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Next, A key verification step is the same at step 3 in 4.1.1(group key distribution phase).

4.2 Proposed Scheme 2

Proposed scheme 2 is a method in which a new IP CCTV is allocated a new group key in order to join the group in the group join step. This is how IP CCTV Leader redistributes the new group key again.

4.2.1 Group key distribution phase

It is the step where the leader of the group forms a group and the group key is distributed from KMS. The method of receiving the key is the same as the proposed scheme 4.1.1.

4.2.2 Join phase

The process of new IP CCTV joining the group.

Step 1. The procedure that the new IP CCTV generate MAC, random number and symmetric key is the same, at step 1 in 4.1.2(join phase).

Step 2. Send $MAC_{IC_{G1_{new}}}$ and $M_{IC_{G1_{new}}}$ to the IP CCTV leader $GLIC_{G1}$. $GLIC_{G1}$ generates a new group key through GSK_{G1}^{new} generates authentication message MAC_{G1} and $AuthM_{G1}$ encrypts random value Er_{G1} and sends $AuthM_{G1}$ and Er_{G1} to KMS. The formula for this is as follows.

$$GSK_{G1}^{new} = h(GSK_{G1} \parallel r_{G1} \parallel MAC_{IC_{G1_{new}}})$$

$$MAC_{G1} = MAC_{IC_{G1_{new}}} \oplus r_{G1}$$

$$AuthM_{G1} = (M_{IC_{G1_{new}}} \parallel MAC_{G1})$$

$$Er_{G1} = E_{k_{G1}}(r_{G1})$$

Step 3. KMS generates MAC_{G1} through $MAC_{IC_{G1_{new}}}$` and $MAC_{G1}$` operation and verifies $verify\ MAC_{G1} = `MAC_{G1}$ to confirm that it is a legitimate object. The formula for this is as follows.

$$MAC_{IC_{G1_{new}}}` = h\,(M_{IC_{G1_{new}}} \parallel K_{G1_{new}})$$

$$MAC_{G1}` = MAC_{IC_{G1_{new}}}` \oplus r_{G1}`$$

Step 4. The KMS generates a new group key GSK_{G1}^{new} encrypts the group key $EGSK_{IC_{new}}$ to be transmitted to the new IP CCTV, generates an authentication message

$Auth_{ICM}$, and transmits $Auth_{ICM}$ and $EGSK_{IC_{G1_{new}}}$ to the $GLIC_{G1}$. The formula for this is as follows.

$$GSK_{G1}^{new} = h(GSK_{G1} \parallel r_{G1} \parallel MAC_{IC_{G1_{new}}}),$$

$$EGSK_{IC_{new}} = E_{K_{IC_{G1_{new}}}}(GSK_{G1}^{new} \parallel MAC_{IC_{G1_{new}}})$$

$$Auth_{ICM} = h(ID_{ICM} \parallel GSK_{G1}^{new} \parallel r_{G1})$$

Step 5. The $GLIC_{G1}$ generates and verifies the $`Auth_{ICM}$ message to $verify\ Auth_{ICM} = `Auth_{ICM}$ that the KMS generated the group key correctly.

$$`Auth_{ICM} = h(ID_{ICM} \parallel GSK_{G1}^{new} \parallel r_{G1})$$

Step 6. The NIC_{G1} can decrypt the $EGSK_{IC_{new}}$ to obtain the group key.

$$D_{K_{IC_{G1_{new}}}}(EGSK_{IC_{new}}) = (GSK_{G1}^{new} \parallel MAC_{IC_{G1_{new}}})$$

Step 7. $GLIC_{G1}$ generates the information $Engk_{GSK}$ and the authentication message $Hngk_{GSK}$ which group members can regenerate the group key, and sends it to the group member. The formula for this is as follows.

$$Engk_{GSK} = E_{k_{GSK}}(r_{G1} \parallel MAC_{IC_{G1_{new}}})$$

$$Hngk_{GSK} = h(GSK_{G1}^{new} \parallel GSK_{G1} \parallel ID_{G1})$$

Step 8. The group members decrypt the group key generation message $Engk_{GSK}$ to obtain the group key GSK_{G1}^{new}`, and generate and $verify\ Hngk = Hngk`$ the authentication message $Hngk`$. The formula for this is as follows.

$$D_{k_{GSK}}(Engk_{GSK}) = (r_{G1} \parallel MAC_{IC_{G1_{new}}})$$

$$GSK_{G1}^{new}` = h(GSK_{G1} \parallel r_{G1} \parallel MAC_{IC_{G1_{new}}})$$

$$`Hngk = h(`GSK_{G1}^{new} \parallel GSK_{G1} \parallel ID_{G1})$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

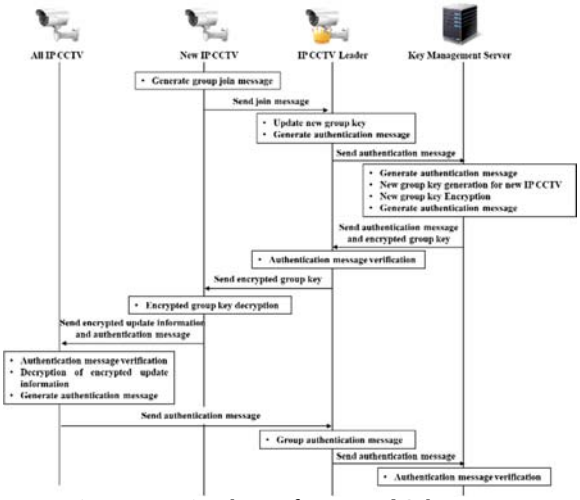

Figure 5 : Join Phase of Proposed Scheme 2

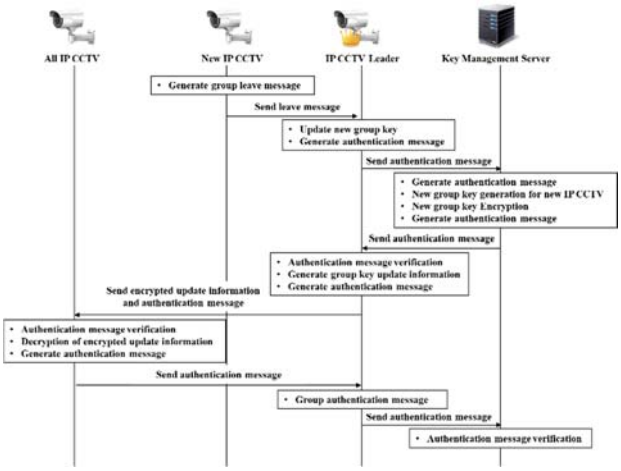

Figure 6 : Leave Phase of Proposed Scheme 2

Step 9. Group members generate an authentication message $ACK_{IC_{G1\_x}}$ and send it to the $GLIC_{G1}$.

$$ACK_{IC_{G1\_x}} = h(ID_{G1} \parallel ID_{IC_{G1_x}} \parallel GSK_{G1})$$

Step 10. The IP CCTV leader generates the ACK_{G1} of the group members as ACK_{G1} and sends it to KMS. The KMS $verify\ r_{G1} = `r_{G1}$ and the new group formation is completed.

$$ACK_{G1} = ACK_{IC_{G1_1}} \oplus ACK_{IC_{G1_2}} \cdots ACK_{IC_{G1_x}} \oplus r_{G1}$$

$$Er_{G1} = E_{k_{G1}}(r_{G1})$$

Step 3. KMS generates MAC_{G1} through $MAC_{IC_{G1_{old}}}$` and $MAC_{G1}$` operation and verifies $verify\ MAC_{G1} = `MAC_{G1}$ to confirm that it is a legitimate object.

$$`MAC_{IC_{G1_{old}}} = h\ (M_{IC_{G1_{old}}} \parallel K_{G1_{old}})$$

$$MAC_{G1}` = MAC_{IC_{G1_{old}}} `\oplus r_{G1}`$$

4.2.3 Leave phase

At the group leave step, the old IP CCTV is leave to the group, and the existing group is the process of distributing the new group key for safety.

Step 1. The procedure that the old IP CCTV generate MAC, random number and symmetric key is the same, at step 1 in 4.1.3(leave phase).

Step 2. Send $MAC_{IC_{G1_{old}}}$ and $M_{IC_{G1_{old}}}$ to the IP CCTV leader $GLIC_{G1}$. $GLIC_{G1}$ generates a new group key through GSK_{G1}^{new} generates authentication message MAC_{G1} and $AuthM_{G1}$ encrypts random value Er_{G1} and sends $AuthM_{G1}$ and Er_{G1} to KMS. The formula for this is as follows.

$$GSK_{G1}^{new} = h(GSK_{G1} \parallel r_{G1} \parallel MAC_{IC_{G1_{old}}})$$

$$MAC_{G1} = MAC_{IC_{G1_{old}}} \oplus r_{G1}$$

$$AuthM_{G1} = (M_{IC_{G1_{old}}} \parallel MAC_{G1})$$

Step 4. The KMS generates a new group key GSK_{G1}^{new} to be transmitted to the new IP CCTV, generates an authentication message $Auth_{ICM}$, and transmits $Auth_{ICM}$ and $EGSK_{IC_{G1_{new}}}$ to the $GLIC_{G1}$. The formula for this is as follows.

$$GSK_{G1}^{new} = h(GSK_{G1} \parallel r_{G1} \parallel MAC_{IC_{G1_{old}}})$$

$$Auth_{ICM} = h(ID_{ICM} \parallel GSK_{G1}^{new} \parallel r_{G1})$$

Step 5. The $GLIC_{G1}$ generates and verifies the $`Auth_{ICM}$ message to $verify\ Auth_{ICM} = `Auth_{ICM}$ that the KMS generated the group key correctly.

$$`Auth_{ICM} = h(ID_{ICM} \parallel GSK_{G1}^{new} \parallel r_{G1})$$

Step 6. The $GLIC_{G1}$ generates the information $Engk_{GSK}$ and the authentication message $Hngk_{GSK}$, which group members can regenerate the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

group key, and sends it to the group member. The formula for this is as follows.

$$Engk_{GSK} = E_{k_{GSK}}(r_{G1} \parallel MAC_{IC_{G1_{old}}})$$

$$Hngk_{GSK} = h(GSK_{G1}^{new} \parallel GSK_{G1} \parallel ID_{G1})$$

Step 7. The group members decrypt the group key generation message $Engk_{GSK}$ to obtain the group key $`GSK_{G1}^{new}$ and generate and $verify\ Hngk = `Hngk$ the authentication message $`Hngk = h(`GSK_{G1}^{new} \parallel GSK_{G1} \parallel ID_{G1})$. The formula for this is as follows.

$$D_{k_{GSK}}(Engk_{GSK}) = (r_{G1} \parallel MAC_{IC_{G1_{old}}})$$

$$`GSK_{G1}^{new} = h(GSK_{G1} \parallel r_{G1} \parallel MAC_{IC_{G1_{old}}})$$

$$`Hngk = h(`GSK_{G1}^{new} \parallel GSK_{G1} \parallel ID_{G1})$$

Step 8. Group members generate an authentication message $ACK_{IC_{G1_x}}$ and send it to the $GLIC_{G1}$.

$$ACK_{IC_{G1_x}} = h(ID_{G1} \parallel ID_{IC_{G1_x}} \parallel GSK_{G1})$$

Step 9. The $GLIC_{G1}$ generates the ACK_{G1} of the group members as ACK_{G1} and sends it to KMS. The KMS $verify\ r_{G1} = `r_{G1}$ and the new group formation is completed.

$$ACK_{G1} = ACK_{IC_{G1_1}} \oplus ACK_{IC_{G1_2}} \cdots ACK_{IC_{G1_x}} \oplus r_{G1}$$

5. ANALYSIS OF PROPOSED SCHEMES

In this chapter, we propose an efficient group key management system using symmetric key in NVR. We investigate the satisfaction of the security requirements introduced in Chapter 3 and compare the computational demands of proposed scheme 1 and 2 by analyzing the computation amount.

5.1 Mutual Authentication

The group leader and the key management server must be able to securely distribute group keys after verifying that they are legitimate entities through mutual authentication. In the proposed scheme, an authentication message is sent to each other through the authentication message $AuthM_{G1} = (M_{IC_{G1\_old}} \parallel MAC_{G1})$ and $Auth_{ICM} = h(ID_{ICM} \parallel GSK_{G1}^{new} \parallel r_{G1})$ So that the key can be securely distributed.

5.2 Replay Attack

To resist a replay attack, it must not be able to authenticate against legitimate entities by re-transmitting already communicated content and distributing mutual authentication and group keys. In the proposed scheme, it is possible to prevent a retransmission attack on a message by using a random number to generate a new message every session through a random value $r_{IC_{G1_{new}}}, r_{G1}$.

5.3 Key Refresh

Key Refresh should be generated when a specific event occurs or after a certain period of time. In this proposed scheme, when IP CCTV is added or removed from a group, a new key is reissued to provide a key refresh because the previously used key cannot be used. $MAC_{G1} = MAC_{IC_{G1_{new}}} \oplus r_{G1}$.

5.4 Authentication/Integrity

Authentication / Integrity allows the recipient to decrypt the message only after authentication of the data has been verified after authentication. In the proposed scheme $MAC_{G1} = MAC_{IC_{G1_{new}}} \oplus r_{G1}$, Authentication / Integrity is authenticated through the MAC value in the authentication key $AuthM_{G1} = (M_{IC_{G1_{new}}} \parallel MAC_{G1})$ and the signature value is verified through the Auth value and received encrypted data.

5.5 Forward/Backward secrecy

Due to the change of the existing group circle, it should not be used for group communication by using the existing key when the group is reformed. In the proposed scheme, when a new IP CCTV joins or leaves the existing group key GSK_{G1}, GSK_{G1} is newly updated by KMS or IP CCTV Leader, so that it can not communicate using a previously used key. Therefore, forward / backward secrecy can be provided.

5.6 Computational analysis

In this chapter, we analyze the computation volume by grouping IP CCTV groups into an efficient group key management system using symmetric keys in NVR. Comparing and analyzing the computational demands of proposed scheme 1 and 2, it compares the efficiency of the situation. In the case of the proposed scheme 1, KMS is a scheme of refreshing the group keys necessary for the join and leave step. This allows each IP CCTV and KMS to allocate a certain amount of computation to each

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

other and distribute keys. However, if there is a large number of IP CCTVs in the group, the burden of KMS will increase. In case of Proposed scheme 2, IP CCTV Leader refreshes the group key necessary for the join and leave step. This allows each IP CCTV to distribute keys and distribute most of the operations. However, proposed scheme 2 may be more inefficient than Proposed scheme 1 if the computational demands of the group IP CCTV are increased and the KMS computation in the group is sufficient or the IP CCTV is small. Figure 7 and Table 1,2 shows how the computation requirements of proposed scheme 1 and proposed scheme 2 change according to the number of IP CCTVs in each group. The test was conducted using the AES encryption operation and the SHA256 hashing operation at about 120MHz operation speed. In case of proposed scheme 1, KMS distributes keys by performing a cryptographic operation in the process of joining a new IP CCTV group and newly renewing a group key to form a new group. This increases the computation on the KMS, and the larger the number of groups, the greater the overall amount of computation. However, as the number of group members is smaller, the computation amount is not high, and if the KMS has sufficient computation capability, the computation amount to be borne by the IP CCTV can be small and efficient. In the case of proposed scheme 2, IP CCTV joins the group and newly updates the group key to reduce the amount of computation of KMS and increase the computation amount of each IP CCTV slightly. So, you can use KMS which is lacking in computation ability or use it more efficiently if there are many group members of the group. In addition, the total amount of computation is smaller than that of the proposed scheme 1 as the number of group members increases through hash computation rather than encryption computation. However, if KMS has sufficient computing power and group members of the group are significantly fewer, the computation amount of IP CCTV is higher than that of proposed scheme 1, which may not be effective for wireless IP CCTV which requires lightweight environment or IP CCTV with low computation capability.

6. CONCLUSIONS

Recently, as the use of network cameras increases for traffic situation monitoring and crime prevention, it is necessary to securely manage images with personal information and various situation information, control access to network cameras, and manage a large number of network cameras. In this paper, we propose an efficient group key management system using symmetric key cryptography in NVR. An IP CCTV reader representing a group of a specific purpose can perform a mutual authentication process with a key management server to allocate a group key and can not use an existing key when a group is reformed, And increased the safety of illegal access. However, there is a disadvantage that frequent communication is required for mutual authentication. Considering the computation power of IP CCTV, the computation amount is slightly higher using public key cryptosystem, but further research is needed to reduce the number of communication and to prevent frequent exposure of data for group key distribution to the communication path. IP CCTV has recently been experiencing frequent video data leakage accidents and needs constant attention so that it can respond to new threats.

Table 1 : Comparison of Proposed Scheme 1 Calculation Requirement

GROUP MEMBER	NEW IP CCTV	ALL IP CCTV	IP CCTV LEADER	CCTV KMS
CCTV 1	1E+2H	1E+3H	2E+3H	1E+3H
CCTV 30	1E+2H	30E+90H	2E+3H	1E+3H
CCTV 100	1E+2H	100E+300H	2E+3H	1E+3H

Table 2 : Comparison of Proposed Scheme 1 Calculation Requirement

GROUP MEMBER	NEW IP CCTV	ALL IP CCTV	IP CCTV LEADER	CCTV KMS
CCTV 1	1E+2H	1E+1H	2E	3E+2H
CCTV 30	1E+2H	30E+30H	2E	32E+2H
CCTV 100	1E+2H	100E+100H	2E	102E+2H

E – encryption
H – hash

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

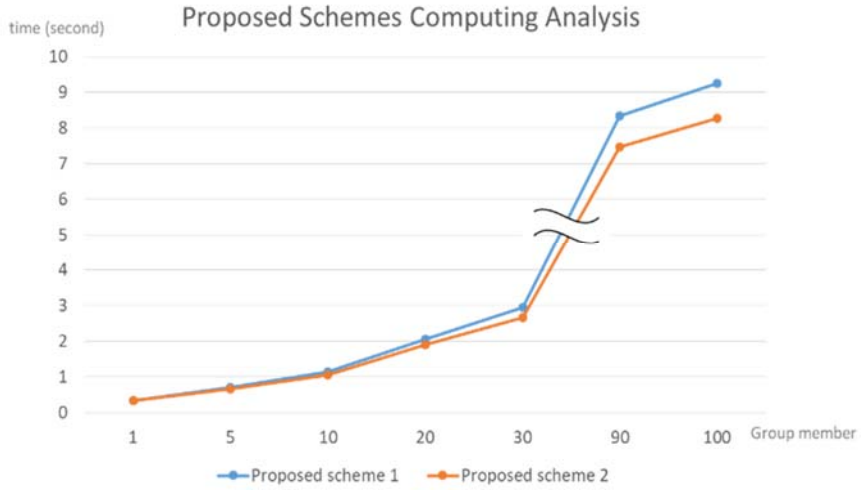

Figure 7: Comparison of proposed schemes calculation amount

ACKNOWLEDGMENTS: This research was supported by Barun ICT Research Center at Yonsei University.

REFERENCES:

[1] Lee, Kyungroul, et al. "An efficient key management solution for privacy masking, restoring and user authentication for video surveillance servers." Computer Standards & Interfaces 44: 137-143. (2016)

[2] Jiang, Rong, et al. "EAP-based group authentication and key agreement protocol for machine-type communications." International Journal of Distributed Sensor Networks 9.11: 304601. (2013)

[3] Lai, Chengzhe, et al. "LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks." Global Communications Conference (GLOBECOM), 2013 IEEE. IEEE, (2013)

[4] Lee, Kyungroul, Kangbin Yim, and Mohammad A. Mikki. "A secure framework of the surveillance video network integrating heterogeneous video formats and protocols." Computers & Mathematics with Applications 63.2: 525-535. (2012)

[5] Gu, Yi, et al. "Design and implementation of UPnP-based surveillance camera system for home security." Information Science and Applications (ICISA), 2013 International Conference on. IEEE, (2013)

[6] Tekeoglu, Ali, and Ali Saman Tosun. "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam." Computer Communication and Networks (ICCCN), 2015 24th International Conference on. IEEE, (2015)

[7] Costin, Andrei. "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations." Proceedings of the 6th International Workshop on Trustworthy Embedded Devices. ACM, (2016)

[8] Lai, Chengzhe, et al. "LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks." Global Communications Conference (GLOBECOM), 2013 IEEE. IEEE, (2013)

[9] Alezabi, Kamal Ali, et al. "On the authentication and re-authentication protocols in LTE-WLAN interworking architecture." Transactions on Emerging Telecommunications Technologies 28.4 (2017)

[10] Yang, Tingting, et al. "EAPSG: Efficient authentication protocol for secure group communications in maritime wideband communication networks." Peer-to-Peer Networking and Applications 8.2: 216-228. (2015)

[11] Choi, Gun-wook, et al. "A Study on Efficient Group Key Management Scheme in CCTV", KSII The 9th International Conference on Internet (ICONI), (2017)

[12] Choi, Gun-wook, et al. "Efficient Group Key Distribution Scheme in IP CCTV Environment", The 3rd International Workshop on Convergence Information Technology(IWCIT), (2017)