Journal of Theoretical and Applied Information Technology
15th September 2019. Vol.97. No 17

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

A STUDY ON VIDEO DATA ACCESS CONTROL TECHNOLOGY USING CP-ABPRE SCHEMES IN CCTV ENVIRONMENT

YONG-WOON HWANG [1] , IM-YEONG LEE[2]

[1,2] Department of Computer Science and Engineering, Soonchunhyang University, South Korea

E-mail: [1]hyw0123@sch.ac.kr, [2]imylee@sch.ac.kr

ABSTRACT

Recently, CCTV has been advancing with the development of IoT technology and intelligence converging with CCTV, as opposed to recording only videos as in the past. Currently, it is used in various fields. Therefore, there are various security threats in the advanced CCTV environment. For example the attacker can acquire the information of the user captured on the CCTV by acquiring the transmitted video data. Also it is possible to disturb the integrity of the video data by leaking or manipulating it to the outside. Additionally, if an attacker hacks a server that manages multiple CCTV videos, many CCTVs can be affected by the attacker's actions. In this paper, to solve the security threat CCTV, video data is encrypted and managed on the server using the CP-ABE method of attribute-based encryption so that only authorized users can access the video data. In addition, if a person with different attributes wants to access the video data, the video data can be accessed safely by re-encrypting the video data using proxy re-encryption techniques based on the attributes of the accessor.

Keywords: *CCTV, Attributes Based Encryption, Proxy re-encryption, Access Control*

1. INTRODUCTION

Closed circuit television (CCTV) is advancing with by the development of Internet of Things (IoT) technology and intelligence and converging with CCTV, as opposed to recording only video as in the past. with closed circuit television. Nowadays, it is widely used in everyday life. CCTV is used to monitor traffic situations and public places such as kindergartens and parks in real time, to observe the scene in case of an accident, to check the evidence at a site, and to use it as a means of crime prevention. However, as shown in Figure 1, there are various security threats in CCTV environments as used in various fields. In particular, the security of the section where the CCTV video is sent to the server is weak [1]. In this way, the attacker can acquire the transmitted video data, obtain the information of the user taken by the CCTV, and manipulate it to cause serious damage to society. Also, when a server that manages video of multiple cameras is hacked by an attacker, many CCTVs can be affected by an attacker. In order to solve these security threats, various security technologies such as video data encryption and secure tunnel configuration exist. However, when encrypting video data using symmetric keys, the key distribution problem between CCTV and server users should be considered separately. When the video data is encrypted using the public key, the server decrypts the encrypted video data, encrypts it with the other party's public key, and transmits the encrypted data. At this time, the server has a problem that can view the video data. To solve this problem, this paper proposes access control technology that enables authorized users in CCTV environments to safely access video data by applying Ciphertext-policy at Attribute-Based Encryption (CP-ABE) and proxy re-encryption (CP-ABRE) encryption. Until recently, techniques applying CP-ABE in various environments such as Cloud computing, Mobile, IoT have been studied. However, among the proposed

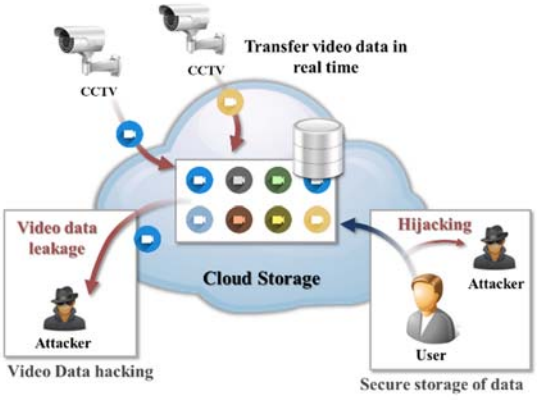

Figure 1: Security Threats in CCTV Environments

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

studies, there are schemes that are vulnerable to camouflage attacks and inefficient schemes in which all keys and ciphertexts are updated at the time of user withdrawal. If instead CP-ABE and CP-ABPRE are applied to the CCTV environment, the following can be satisfied. First, the video data is encrypted with the attribute-based encryption and managed by the server, so that the user can access the video data when the attribute of the user satisfies the attribute of the access policy specified in the encrypted video data. Second, when another user having a different attribute that does not correspond to the access policy attribute specified in the video data accesses the video data, the manager requests a new access policy the data owner. The administrator then re-encrypts the encrypted video data based on the new access policy. This allows additional authenticated users, in addition to users who have existing access to video data, to securely access the video data.

In this paper, the proposed scheme can be used in a 2nd generation digital CCTV environment, not all CCTVs. For example, it may be used as evidence for CCTV in the police interrogation room used for criminal investigations, and the reason is that only authorized users can acquire video data.

2. RELATED WORKS

This chapter discusses attribute-based encryption and proxy re-encryption that are the basis of data access control techniques.

2.1 Bilinear Map

Bilinear mapping has been proposed as a tool to attack elliptic curve cryptosystems in the past, but it is used recently as a cryptographic tool for information security[2]. A bilinear map is a function that satisfies the following properties:$G_1 X G_1 \rightarrow G_2$.

• Bilinear**:** For any *P,Q,R, e (P, Q +R)=e(P,Q)·e(P,R)* and *e(P+Q,R)=e(P,R)·e(Q,R)* are established.

• Non-degenerate: For all pairs P , Q of G_1, (P ,Q)≠0.

• Computable: For any P , Q , there must be an efficient algorithm that can compute e (P ,Q).

2.2 Attribute-based Encryption

In 2005, Sahai et al. proposed an extension of the concept of identity based encryption (IBE). It is a method of performing encryption and decryption

Figure 2: CP-ABE scheme

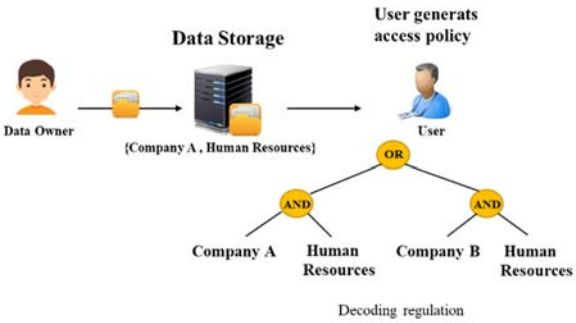

Figure 3: KP-ABE scheme

based on a set of attributes(address area, job) of each entity and an access policy for accessing a given set of attributes or not. There are two types of attribute-based encryption: CP-ABE and KP-ABE. When a CP-ABE generates a ciphertext, the sender specifies the access policy and sends it to the receiver, and the receiver decrypts the ciphertext based on its attribute set [2, 3]. If the recipient who wants to access the video data has attributes [Company A], [Human Resources], [Team Leader] as shown in Figure 2, the sender generates an access policy with the attribute [Company A, Human Resources Department], When encrypted, only recipients who satisfy the access policy can decrypt the ciphertext. KP-ABE is a decryptable set of attributes that encrypts the sender and generates and decrypts the key according to the access policy that the recipient is based on, as shown in Figure 3. Decryption is possible if the decryptable attribute set satisfies the attribute [Company A, Human Resources Department] in the access policy based on the attribute set of the recipient, with the ciphertext encrypted with [Company A, Human Resources Department]. The difference between the two schemes is that the access policy is generated by the data owner or is generated by the user. In this paper, the CP-ABE technique is used to control users to access stored video data.

2.2.1 Satisfying an Access Policy

In this scheme, we consider an access policy consisting of AND gates between positive and negative attributes. The set of all attributes is

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

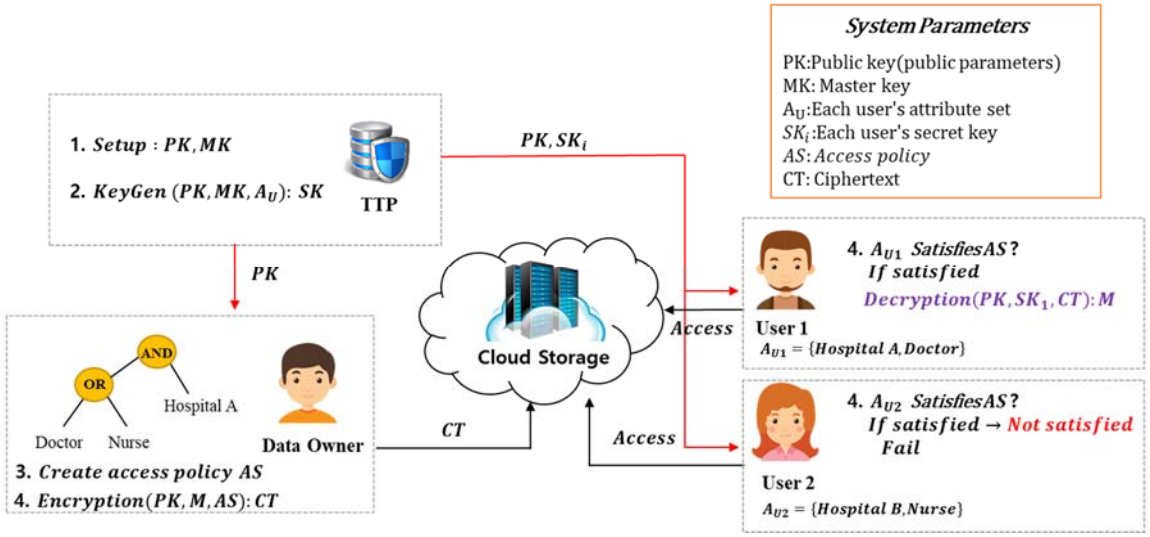

Figure 4: The CP-ABE model in a cloud environment

denoted by τ. The access policy is expressed as $\wedge\ (+\mathrm{d}_i, -\mathrm{d}_i)_{i\in\tau}$. Here, $+\mathrm{d}_i$ is a positive attribute that satisfies the access policy, and $-\mathrm{d}_i$ is a negative attribute that does not satisfy the access policy. Every user receives a secret key associated with the attribute set $S \subseteq \tau$ from the TTP. The user can decrypt the ciphers if the following conditions of the attribute are met [4, 5, 6]:

· If $+\mathrm{d}_i$ is satisfied with the AS, it is $i \in S$
· If $-\mathrm{d}_i$ is satisfied with the AS, it is $i \notin S$

Here, as is the access policy generated by the data owner.

2.2.2 Existing proposed CP-ABE Scheme

To date, much research has been done on data access techniques based on the CP-ABE scheme in the cloud environment. Figure 4 shows the CP-ABE access model in a cloud environment[7]. To put it simply, First, ttp generates the key and sends the key to the data owner and user. The data owner then generates an access policy based on the user's attributes and encrypts the data, and sends it to the cloud server. The user accesses the cloud and takes the encrypted data. If the attribute satisfies the access policy, decrypts the encrypted data.

However, existing schemes are vulnerable to various security threats and methods lacking efficiency. In particular the sekhar scheme [8] from 2012 and the Zhu scheme [9] from 2015, revoked users cause camoflage attacks that can access data with other user attributes. Therefore, the Xu scheme [10], Yagn scheme [11] from 2013, and Ramesh scheme [12] from 2016 apply attribute retraction to user withdrawal. However, the Xu scheme and the Yang scheme updating other users' keys and existing stored ciphertexts when the user leaves the system. In the Ramesh scheme the Attribute Authority (AA), has the inefficiency of constantly updating. In addition, the Xu schema and the Ramesh schema block access to the revoked user by removing the user ID, but do not remove the attribute, withdrawal the user attribute still in the server [6].

2.3 Attribute-based Proxy Re-encryption

The basic concept of Proxy En-encryption is to convert cryptographic statements that are encrypted with Alice's public keys when Alice and Bob communicate with each other so that the Proxy can transmit them and encode them into Bob's secret key. The proxy does not need to know the source of encrypted data or Alice's secret key because it can use the re-encryption key to re-encrypt cryptographic statements and convert cryptographic statements without the need to replicate existing ones. Figure 3 shows now this is applied in the CCTV environment.

By applying a proxy re-encryption technique to a attribute-based encryption, users (identified by attribute) can freely specify a proxy that re-encrypts cryptographic statements from one access policy to another. The attribute-based proxy re-encryption technique (AB-PRE) also has two schemes, CP-ABPRE and KP-ABPRE, we will apply CP-ABPRE techniques to propose user access control techniques.

Figure 5 shows the model when CP-ABPRE is applied to the CCTV environment. CP-ABPRE re-encrypts ciphertext C into C' with a changed access policy by specifying a proxy that converts ciphertext C encrypted with AS from existing CP-ABE schemes into an access policy AS' that matches other

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

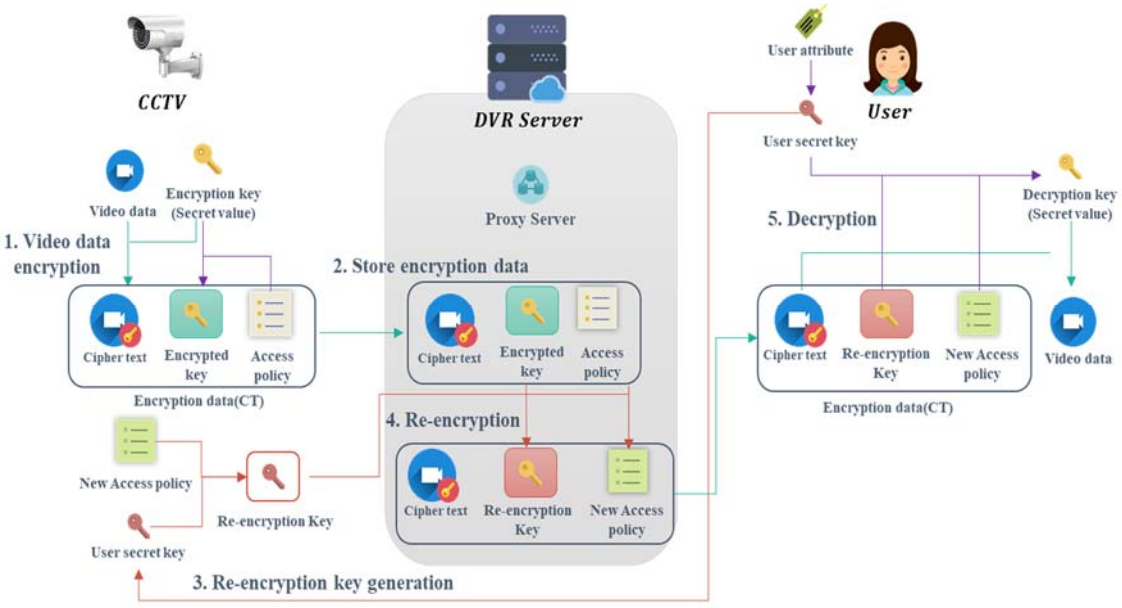

Figure 5: The CP-ABPRE model in CCTV environment

users' attributes [13]. This allows users with different attributes that are not satisfied with the nature of the access policy previously specified in ciphertext C to access the data using 'reencrypted C' through the changed approach policy. To date, various techniques of CP-ABPRE have been studied. This paper is also based on the Liang scheme[4] and is being studied to increase the efficiency of the computational complexity in case of ambiguity.

3. SECURITY REQUIREMENTS

In this chapter, we discuss security requirements that must be satisfied when applying attribute-based cryptography in a CCTV environment.

· **User collusion:** User collusion attacks can occur in a cloud environment using attribute-based cryptosystems, and users can infer secret key SK based on the attributes of others through collusion with each other. Therefore, when generating the secret key in the TTP, it is necessary to generate the secret key based on the attributes and a random function so that the secret key SK cannot be deduced from only the attributes of the user.

· **Camouflage attack:** In the CCTV environment, the attacker can attempt manipulate the acquired video data and attempt to attack the camouflage to show another screen at the same time. For this, encryption of video data should be applied. In the process of data transmission, video data should be encrypted and not be known. In addition, a user who is attribute revocation from the attribute-based crypto environment can access the server through the attributes of another user and can access the video data with the secret key SK that was previously held. Therefore, when a user who has left uses another user's attributes to access the server and attempt to check the video data, it should not be able to decode the video data, and an attribute cancellation technique is required for the user whose attribute has been revoked.

· **Access control for unauthorized users:** The video data stored in the server specifies the attributes of the user who can access the CCTV. Therefore, only the user who satisfies the access policy attributes specified in the encrypted video data should be able to decrypt the data. In addition, integrity and confidentiality of video data must be guaranteed.

4. PROPOSED SCHEMES

In this chapter, we propose a video data access control technique using attribute-based encryption in CCTV environments. The proposed scheme consists of two schemes: access control using attribute-based encryption and access to video data using attribute-based proxy re-encryption when adding a new user. The proposed schemes are secure against various security threats in the CCTV environment, such as replay attacks or camouflage attacks, in which the video data is encrypted with an attribute-based encryption. [Figure 6, 7] are usage scenario of the environment in which these proposed schemes are applied. Since the video recorded on CCTV in Figure 6 is encoded with the attributes of the special

Journal of Theoretical and Applied Information Technology
15th September 2019. Vol.97. No 17

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

and traffic departments of the A Police in area A, only users with the characteristics of the special and traffic departments of the A police station in area A can check the video data. In this case, if the criminal is a juvenile, the Youth department should also participate in the investigation and be given the authority to view the CCTV. However, because the Youth departments dose not have the right to decrypt video data from CCTV, they may also have the right to decrypt video data by converting department-specific access policy using attribute-based proxy re-encryption techniques as shown in Figure 7.

The proposed scheme 1 consists of a phase of encrypting the CCTV registered video, a phase of accessing the user video data having the attributes,

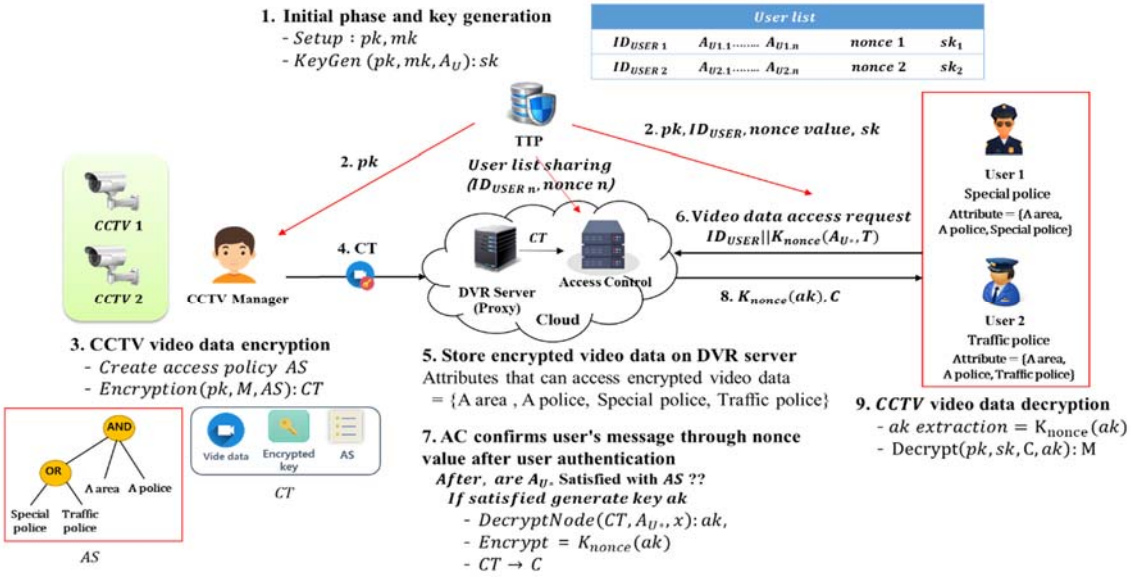

Figure 6: Scenario of the proposed scheme 1

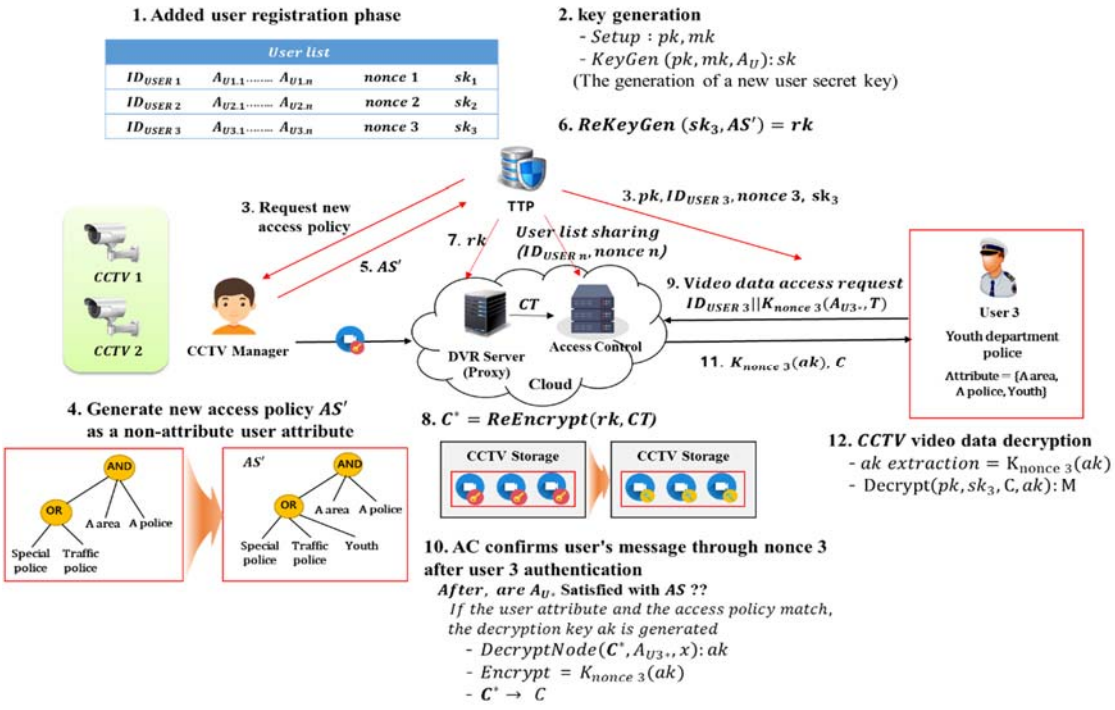

Figure 7: Scenario of the proposed scheme 2

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

and a phase of revocation the attribute upon the withdrawal of the user.

The proposed scheme 2 is based on the proposed scheme 1 and consists of different-attribute user access phase and attribute revocation phase when user withdraws.

The system parameters used in the proposed scheme are as follows.

· TTP: manages user attributes with trusted third party
· DVR Server: Video data storage server
· Access Control(AC) : User access control management server
· pk, mk: Public parameter, Master key.
· sk: user security key (decryption key).
· rk: Re-encryption key
· A_U, S: User attribute data, A set of attribute data
· AS, AS': Access policy, New access policy
· ak : Decryption key generated when the user attribute matches the AS
· $+\mathrm{d}_i, -\mathrm{d}_i$: Positive attribute data, Negative attribute data
· Nonce value: random value given to each user
· CT, C^*: Encrypted data, Re-encrypted data
· C: Attribute matching verified CT
· T: Timestamp

4.1 Initial phase

The proposed scheme 1 and 2 assumes the following.

• Assume that video data is m, and CCTV encrypts video data in real time and transmits it to DVR Server. At this time, CCTV has enough performance to handle the computation.

• The user who wants to access the video data is a user registered in the existing TTP, and the AC performs user authentication through the registered user information.

• User list and attribute revocation list managed by TTP are shared with AC, and AC controls user access based on this.

4.2 Proposed Scheme 1

As shown in Figure 6, the proposed scheme 1 controls access to video data by using attribute-based encryption in the CCTV environment.

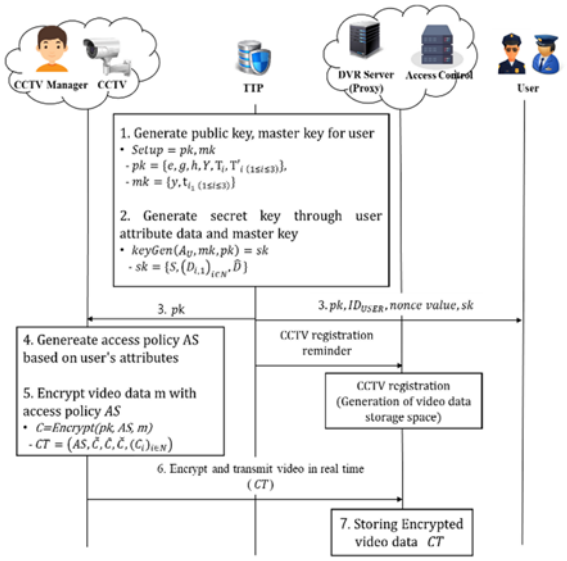

Figure 8: Initial phase and video data encryption phase

4.2.1 CCTV Video Encryption Phase

In this phase, the video data of the CCTV is encrypted using the attribute-based encryption. Only the user with the attribute of the designated access policy can access the video data[Figure 8]..

Step 1. When the CCTV sends a registration message to the TTP to request registration, the TTP generates a public parameter and a master key (pk, mk) after the CCTV registration.

· Setup steps: Generate pk, mk
  · $y, \mathrm{t}_i \in \mathrm{Z}_p (1 \le i \le 3)$
  · $g, h \in G$ at random
  · $\mathrm{Y} = \mathrm{e(g,h)}^y, \mathrm{T}_i = \mathrm{g}^{\mathrm{t}_i}, \mathrm{T}'_i = \mathrm{t}_i (1 \le i \le 3)$

  · $pk < e, g, h, Y, \mathrm{T}_i, \mathrm{T'}_{i\,(1\le i\le 3)} >$
  · $mk < y, \mathrm{t}_{i_1\,(1\le i\le 3)} >$

Step 2. In the key generation process, the user secret key sk is generated via the user attribute data and the master key. Then sends the public parameter to the CCTV Manager, and send the user pk, ID_{User} , $nonce\ value, sk$.

· $KeyGen(pk, mk, A_U)$: Generate sk
  · $\mathrm{r}_1 \ldots \mathrm{r}_n \in \mathrm{Z}_p$(Random value generation)
  · $\mathrm{r} = \mathrm{r}_1 + \mathrm{r}_2 + .. \mathrm{r}_n$,
  · $\widehat{D} = h^{y-r}$
  · $\mathrm{i} \in \mathrm{N(N} = 1,2 \ldots \mathrm{n}), (D_{i,1} = h^{r_i})_{i\in N}$

  · $sk < S, (D_{i,1})_{i\in N}, \widehat{D} >$

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

Step 3. The CCTV manager generates the access policy AS based on the user attributes, encrypts the video data m in the CCTV with pk and AS, and transmits it to the DVR server.

· $Encrypt(pk, AS, m)$: Generate encrypted video data C

· $s \in Z_p$(Random value generation)

· $\tilde{C} = \mathrm{m} \cdot Y^s, \hat{C} = g^s, \check{C} = h^s$

· If $+\mathrm{d}_i$ is satisfied with the AS, it is $C_i = T_i{}^s$

· If $-\mathrm{d}_i$ is satisfied with the AS, it is $C_i = T^s{}_{n+i}$

· If not both, it is $C_i = T^s{}_{2n+i}$

· $C =< AS, \tilde{C}, \hat{C}, \check{C}, (C_i)_{i \in N} >$

The DVR Server creates the storage space for each CCTV and stores the encrypted video data that is transmitted in real time. The video data of the CCTV stored here has attributes of area A, A police, special, and Traffic.

4.2.2 The User's Video Data Access Phase

In this phase, the user having the attribute of the encrypted video data can access the video data stored in the DVR Server through the AC. The user can decrypt the video data of the encrypted CCTV stored in the DVR Server with the secret key [Figure 9].

Step 1. The user requesting access to the video data encrypts the attributes using his / her nonce value and requests access to the AC. AC authenticates that it is a legitimate user through the list of registered users.

· $k_{nonce}(A_{U*})$: The user encrypts the attribute with a nonce value and requests access.

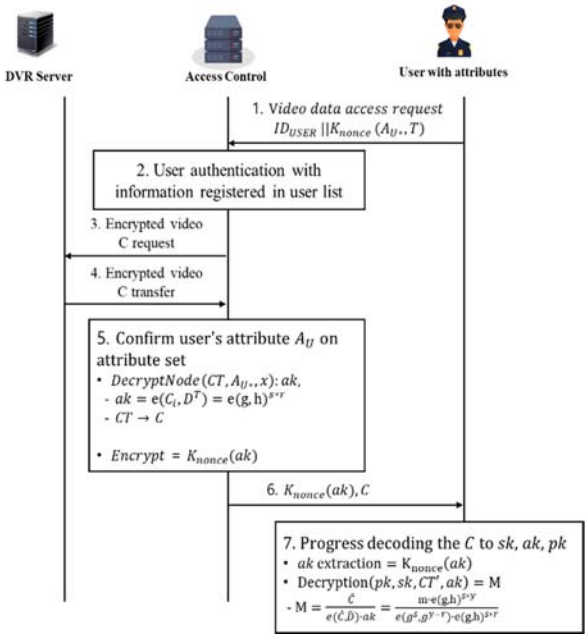

Figure 9: User video data access phase with attribute

Step 2. The AC then determines whether the user's attributes match the attributes of the access policy specified in the video data stored in the DVR Server. If there is a match, a Decryptnode process is performed to generate a decryption key ak. After generating ak, it encrypts ak with the nonce value of the user and sends it to the user together with C'. C' denotes encrypted data that has undergone the Decryptnode process and satisfies the access policy.

· A_{u*} $Satisfies$ AS ?: If they match, generate decryption key ak.

· If $+\mathrm{d}_i$ is satisfied with the AS, it is $T'_i = t_i$

· If $-\mathrm{d}_i$ is satisfied with the AS, it is $T'_i = t_{n+i}$

· If not both, it is $T'_i = t_{2n+i}$

· $\mathrm{T} = \frac{1}{\prod_{i \in N} T'} = \frac{1}{\prod_{i \in A_{u*}} t_i} = 1$

· $\mathrm{C} = \prod_{i \in N} C_i = g^{s \sum_{i \in A_{u*}} t_{i'}} = g^{s \cdot t}$

· $\mathrm{D} = \prod_{i \in N} D_i = h^{\sum_{i \in N} r_i} = h^r$

· $ak = \mathrm{e}(C_i, D^T) = \mathrm{e}(\mathrm{g}, \mathrm{h})^{s*r}$

· $k_{nonce}(ak)$

Step 3. The user extracts ak from $k_{nonce}(ak)$ received from the AC. Next, the video data encrypted with sk and pk is decrypted to acquire the video data m

· ak extraction = $k_{nonce}(ak)$

·$Decrypt(ak, pk, sk, C')$: Acquired m by decoding video data m

$$\cdot m = \frac{\tilde{C}}{e(\hat{C},\hat{D})\cdot ak} = \frac{\mathrm{m}\cdot \mathrm{e}(\mathrm{g},\mathrm{h})^{s*y}}{e(g^s, g^{y-r})\cdot \mathrm{e}(\mathrm{g},\mathrm{h})^{s*r}}$$

4.2.3 Attribute Revocation Phase Upon User Withdrawal

This is the phase, by removing the attributes of a withdrawn user, it prevents the withdrawn user from accessing the data with the information they already present [Figure 10, 11].

Step 1. The user send a withdrawal, requests to the TTP.

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

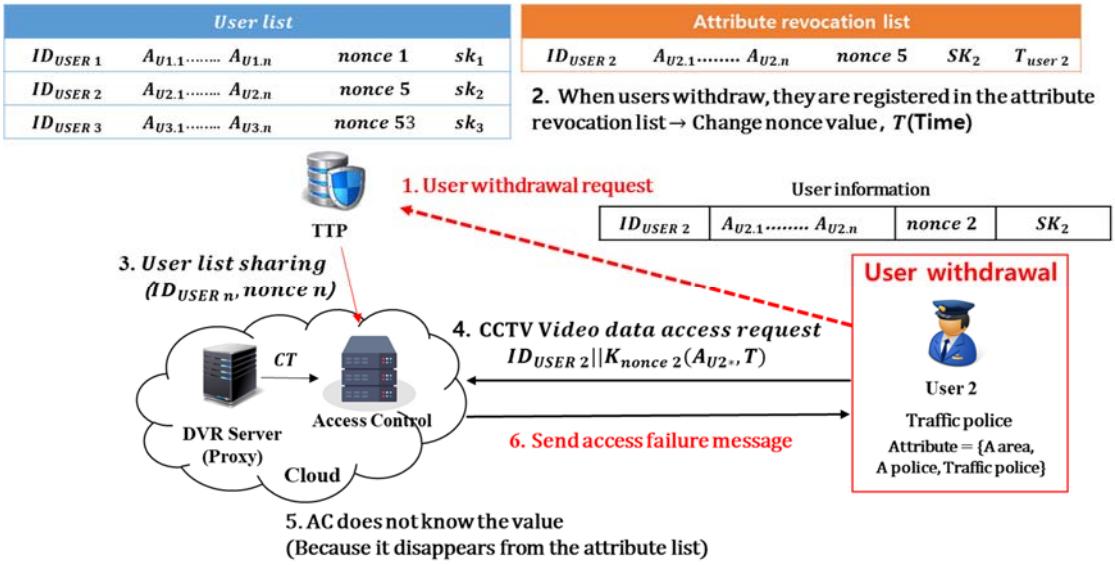

Figure 10: Attribute revocation phase when user withdraws

Step 2. The TTP updates in the user attribute revocation list and changes the nonce value of the withdrawal user. At this time, the nonce value of the user registered in the user list is changed while being synchronized with the user list, and this information is shared with the AC.

Step 3. When the withdrawn user encrypts the attribute by using the existing $nonce$ as a symmetric key and requests access with it, the AC does not know the user's $nonce$ value. Therefore, it cannot decode $k_{nonce}(A_{U*})$ received from the disconnected user.

Step 4. The AC then blocks access to the withdrawn user by sending an access failure message to the user. Also, if the time stamp T is registered in the attribute revocation list, the user cannot access the video data only for the period T, because the nonce value of the user is changed during the registered T period.

4.3 Proposed Scheme 2

As shown in Figure 7, the proposed scheme 2 uses attribute-based proxy re-encryption in the CCTV environment, so that a user who does not have the attribute specified in the previously encrypted video data can access the video data safely. The initial stage of the proposed scheme 2 is based on the proposed scheme 1.

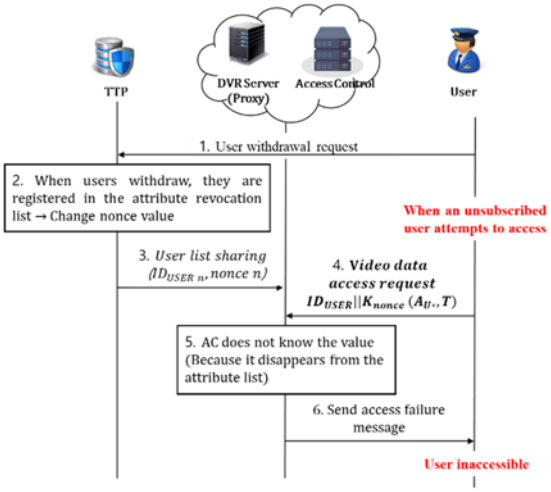

Figure 11: Withdrawn user access phase

4.3.1 User data access with different attributes

When a user with a different attribute access request is requested, the user can access the different attribute video data by re-encrypting the previously encrypted video data based on the access policy of another attribute [Figure 12].

Step 1. The TTP registers a user with a new attribute (Department: Youth) and generates a secret key sk through step 1 of 4.2.1.TTP then sends the registered $ID_{User\,3}$ to the user and requests a new access policy from the CCTV administrator.

Journal of Theoretical and Applied Information Technology
15th September 2019. Vol.97. No 17

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

Step 2. The CCTV administrator generates a new access policy AS' it adds (Department: Youth) and sends it to the TTP.

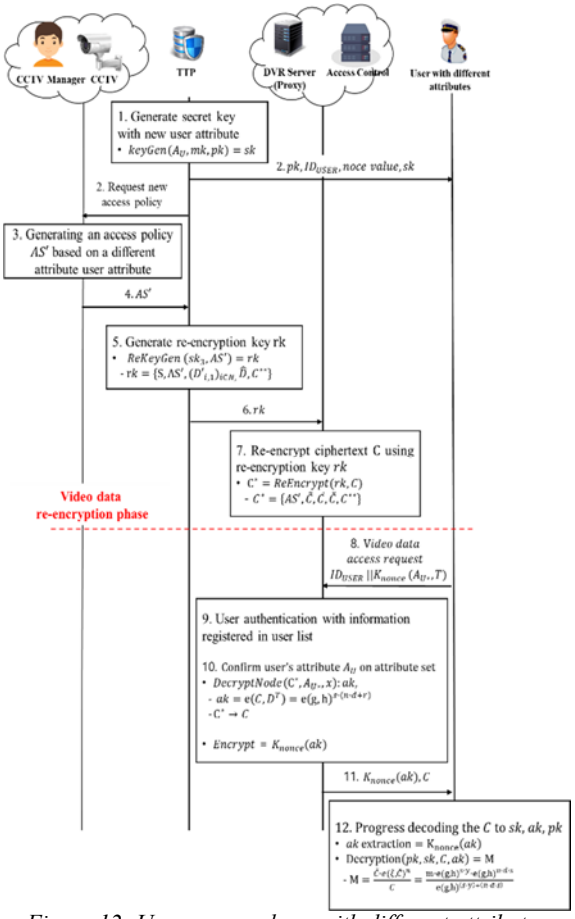

Figure 12: User access phase with different attributes

Step 3. The TTP generates the re-encryption key rk through the AS' received from the CCTV administrator and the secret key sk of the new user, and transmits it to the DVR server.

· $RekeyGen(sk, AS')$: Generate rk

· $sk < S, (D_{i,1})_{i\in N}, \widehat{D} >$

· $d \in Z_p$(Random value generation)

· $\xi \in g^d, \widehat{D'} = \widehat{D}$

· i ∈ N, $D'_{i,1} = D_{i,1} \cdot h^d$

· $rk < S, AS', (D'_{i,1})_{i\in N}, \widehat{D}, C^{**} >$

· C^{**} is the ciphertext of ξ in the access policy AS'

Step 4. The DVR Server re-encrypts the previously encrypted video data with the received rk.

· $ReEncrypt(rk, C)$: Re-encrypt encrypted video data C.

· If $+d_i$ is satisfied with the AS, it is $T'_i = t_i$

· If $-d_i$ is satisfied with the AS, it is $T'_i = t_{n+i}$

· If not both, it is $T'_i = t_{2n+i}$

· $T = \frac{1}{\prod_{i\in N} T'} = \frac{1}{\prod_{i\in A_{u*}} t_i} = 1$

· $C = \prod_{i\in N} C_i = g^{s\sum_{i\in A_{u*}} t_{i'}} = g^{s\cdot t}$

· $D = \prod_{i\in N} D'_i = h^{d+\sum_{i\in N} r_i} = h^{n\cdot d+r}$

· $E = e(C, D^T) = e(g, h)^{s\cdot(n\cdot d+r)}$

· $\bar{C} = e(\hat{C}, \hat{D}) = e(g^s, h^{y-r}) \cdot e(g, h)^{s\cdot(n\cdot d+r)}$

$= e(g, h)^{(s\cdot y)+(n\cdot d\cdot s)}$

· $C^* =< AS', \tilde{C}, \bar{C}, \check{C}, C^{**} >$

Step 5. When the user having the attribute of Youth and the department requests the video data from AC. At this time, it is determined based on the registered user information whether or not it is accessible through authentication. The procedure is the same as Step 2 in 4.2.2.

· A_{u*} $Satisfies$ AS ?: If they match, generate decryption key ak.

· $ak = e(C, D^T) = e(g, h)^{s\cdot(n\cdot d+r)}$

· $k_{nonce}(ak)$

Step 6. The user extracts ak from $k_{nonce}(ak)$ received from the AC. Next, the video data re-encrypted with sk and pk is decrypted to decrypt the video data m

· ak extraction = $k_{nonce}(ak)$

· $Redecrypt(ak, pk, sk, C^{*\prime})$: = Acquired m by decoding video data m

$\cdot m = \frac{\tilde{C}\cdot e(\xi, \check{C})^n}{C} = \frac{m\cdot e(g,h)^{s\cdot y}\cdot e(g,h)^{n\cdot d\cdot s}}{e(g,h)^{(s\cdot y)+(n\cdot d\cdot s)}}$

Step 7. When a user withdraws, register the withdrawn user in the attribute revocation list, as in 4.2.3. After that, the user is blocked from accessing the period registered in the revocation list.

5. ANALYSIS OF PROPOSED SCHEMES

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

This proposed scheme is an access control technique using attribute-based encryption and attribute-based proxy re-encryption to securely access stored video data in CCTV environment. The proposed method satisfies the security requirements required in Chapter 3 through Table 1, and can effectively block the access of the withdrawn user compared to the CP-ABE scheme considering the withdrawn user. In addition, compared to the existing CP-ABPRE scheme through Table 2, the overall amount of computation is reduced to improve the efficiency of encryption and decryption computation. The detailed description of the security and efficiency aspects of the proposed scheme is as follows.

5.1 Security Analysis

· **User collusion:** Since the proposed schemes generates a secret key based on attributes and random functions when generating a secret key in TTP, the secret key sk cannot be derived from only the attributes of the user. Also, the nonce value known only to the user and the AC is used as a symmetric key to request data access, and the key ak is also used in data decoding. Therefore, even if sk is deduced through collusion between users, data m cannot be decoded.

· **Camouflage attack:** In the proposed scheme, the re-encrypted video data can only be accessed and decrypted with the attributes of the user and the secret key of the user. Therefore, the attacker cannot decrypt the video data even if is acquired by eavesdropping. In addition, the TTP registers the user in the user attribute revocation list when a user leaves, and shares the changed the nonce value with the AC. Communication between the user and the AC is performed by using the nonce value of the user registered in the user attribute revocation list as a symmetric key. Thus, even if the disconnected user accesses the AC with other users attributes, the AC does not recognize the access request message and blocks access.

· **Access control for unauthorized users:** In the proposed scheme, the user is initially registered in the TTP to access the data. It also requests access to the AC to access the encrypted data stored on the DVR Server. The AC compares the attributes of the user with the attribute of the access policy specified in the encrypted video data and transmits the ciphertext to the matching user. In this way, access by unauthorized users is blocked.

· **Video data integrity and confidentiality:** In this proposed scheme, the confidentiality of the data is strengthened by encrypting the CCTV video data based on attributes. The video data can be decrypted only with the attribute of the user matching the attribute of the encrypted video data and the secret key, so that the integrity of the video data is guaranteed.

5.2 Efficiency

The proposed scheme has the following advantages over the CP-ABE approach in traditional cloud environments. This proposed scheme blocks

Table 1: Security analysis of existing scheme and proposed scheme

Scheme / Items	Sekhar Scheme [8]	Zhu Scheme [9]	Xu Scheme [10]	Yang Scheme [11]	Ramesh Scheme [12]	The Proposed Scheme
User Collusion	safe	safe	safe	safe	safe	safe
Camouflage attack	unsafe	unsafe	unsafe	safe	safe	safe
Attribute Revocation	not considered	not considered	not required	satisfied	not required	satisfied
Key, Ciphertext Updates	not considered	not considered	update all keys and ciphertext	update all keys and ciphertext	update all keys	not required

Table 2: Comparison of Proposed Scheme Calculation Requirement

Scheme / Items	Liang scheme [4]	Luo Scheme [5]	Seo Scheme [6]	The Proposed Scheme
Encryption	$(n+3)E+2M$	$(n+2)E+2M$	$(n+5)E+1M$	$(n+3)E+1M$
Decryption	$(n+2)C_e+M$	$(2n)C_e+3M$	$2C_e+(3n+2)E+2M$	$2C_e+(2n+1)E+M$
Re − encryption	$(n+1)C_e+M$	$(2n+1)C_e+(n+1)M$	$2C_e+(3n)E+M$	$2C_e+(2n)E+2M$
Re − decryption	$(n+3)C_e+4M$	$(2n+1)C_e+5M$	$3C_e+(3n)E+4M$	$2C_e+3E+2M$

C_e : *Pairing operation*; n : *Number of attributes*; E : *Exponentiation operation*; M : Multiplication operation

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

access by users who have been withdrawn from AC and the user list. This effectively improves the inefficiency of updating other users' keys and stored ciphertexts when users withdraw from the existing system. In addition, Table 2 compares the proposed method with the existing attribute-based proxy re-encryption scheme, Liang scheme [4], Luo scheme [5], and Seo scheme [6]. In Table 2, the proposed scheme has reduced the overall amount of computations in encryption, decryption, re-encryption and re-encryption compared to other CP-ABPRE methods. First of all, there is the disadvantage of increasing the amount of operation because the pairing operation increases with the number of attributes in the existing Liang scheme [4] and Luo scheme [5]. Therefore, in the proposed scheme, encryption, decryption, re-encryption, and re-encryption can be computed regardless of the number of pairing operations and attributes, thereby solving the problem of increasing the number of computations according to the number of attributes.

6. CONCLUSIONS

In this paper, we proposed a video data access control scheme using attribute-based encryption and attribute-based proxy Re-encryption to solve security threats in CCTV environment. The proposed scheme, are safe from a variety of security threats because the video data is encrypted with an attribute based encryption. In addition, by using the nonce value given by TTP as a symmetric key to access DVR Server, users can solve camouflage attacks that can occur through other users' attributes in the existing scheme. When a user withdraws from a system, the user is registered in the user attribute revocation list managed by the TTP and the users nonce value is changed to share the list with the AC. This allows the AC to grant user access to the DVR server. This improves overall computational efficiency, because it eliminates the process of updating other user's secret keys and ciphertexts when removing users from the traditional approach. Finally, only users authorized to access the recorded video data on CCTV can access it, ensuring the confidentiality and integrity of the video data. Also, through attribute-based proxy re-encryption techniques, users with other attributes in addition to registered users can securely access the video data.

Future research will focus on improving efficiency by comparing computation with existing schemes. As the number of attributes increases, ciphertext and size increase, so it is necessary to investigate a lightweight CP-ABE scheme that can reduce the computational complexity. Additionally because a user's attribute in attribute-based encryption is privacy, research to protect a user's attribute by adding anonymity to that user's attribute is required in the attribute-based proxy re-encryption technique presented in this paper.

ACKNOWLEDGMENTS:

This research was supported by the MSIT(Ministry of Science, ICT),Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403)supervised by the IITP(Institute for Information & communications Technology Promotion) and Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A1B03935917)

REFRENCES:

[1] Xia. Z, Zhang. L, "Attribute-Based Access Control Scheme with Efficient Revocation in Cloud Computing Multi-authority scheme based CP-ABE with attribute revocation for cloud data storage", *China Communications,* vol. 13, no. 7, 2016 , pp. 92-99.

[2] Bethencourt. J, Sahai. A, Waters. B, "Ciphertext-policy attribute-based encryption", *In Security and Privacy, SP'07. IEEE Symposium on*, 2007, pp. 321-324.

[3] Cheung. Ling, Nwport. Calvin, "Provably secure ciphertext policy ABE", In: *Proceedings of the 14th ACM conference on Computer and communications security*, ACM, 2007. p. 456-465.

[4] X. Liang, Z. Cao, H. Lin, J. Shao, "Attribute-based proxy re-encryption with delegating capabilities," *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, 2009, pp. 276-286.

[5] S. Luo, J. Hu, Z. Chen, "Ciphertext Policy Attribute-Based Proxy Re-encryption," *Information and Communications Security*, vol. 6476 of LNCS, 2010, pp. 401-415.

[6] H. Seo, H. Kim, "Attribute-based Proxy Re-encryption with a Constant Number of Pairing Operations," *Journal of Information and Communication Convergence Engineering*, vol. 10, no. 1, 2012 , pp. 53-60,

[7] Chandar. P. Praveen, D. Mutkuraman, M. Rathinrai, "Hierarchical attribute based proxy re-encryption access control in cloud computing", In: *Circuit, Power and Computing Technologies*

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

(ICCPCT), 2014 International Conference on. IEEE, 2014. pp. 1565-1570.

[8] Sekhar. B. R, Kumar. B. S, Reddy. L. S, PoornaChandar. V, "CP-ABE based encryption for secured cloud storage access", *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, 2012, pp. 1-5.

[9] Zhu. S, Yang. X, "Protecting data in cloud environment with attribute-based encryption", *International Journal of Grid and Utility Computing,* vol. 6, no. 2, 2015, pp. 91-97.

[10] Xu. Z, Martin. K. M, "Dynamic user revocation and key refreshing for attribute-based encryption in cloud storage", *In Trust, Security and Privacy in Computing and Communications, 2012 IEEE 11th International Conference on, IEEE,* 2012, pp. 844-849.

[11] Yang. K, Jia. X, "Attribute-based Fine-Grained Access Control with Efficient Revocation in Cloud Storage Systems", *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ACM, 2013*, pp. 523-528.

[12] Ramesh, D, Priya. R, "Multi-authority scheme based CP-ABE with attribute revocation for cloud data storage", *In Microelectronics, Computing and Communications (MicroCom), 2016 International Conference on, IEEE*, 2016, pp. 1-4.

[13] Chung. P. S, Liu. C. W, Hwang. M. S, "A Study of Attribute-based Proxy Re-encryption Scheme in Cloud Environments". *IJ Network Security*, vol. 16, no. 1, 2014, pp. 1-13.