개인정보보호를 위한 영상 암호화 아키텍처 연구

김정석* **, 이재호*
*서울시립대학교 전자전기컴퓨터공학부
**에스케이텔레콤 AIX 센터 시큐리티랩스
justinkim@uos.ac.kr, jaeho@uos.ac.kr

A Study of video encryption architecture for privacy protection

Jeongseok Kim* **, Jaeho Lee*
*Dept. of Electrical and Computer Engineering, University of Seoul
**Security Labs, AIX Center, SK Telecom

요 약

영상 감시 시스템은 광범위한 영역에서 쉽게 설치되고 있으며, 감시 지역을 녹화한 영상 정보는 대게 인터넷을 통한 클라우드 상의 저장소에서 관리하는 중앙 관리 방식을 사용하고 있다. 그러나 이러한 시스템의 주요한 문제점은 저장 영상의 전송 과정과 저장 대해서 객관적으로 신뢰할 수 있는 방법이 제공되지 않고 있으며, 개인정보보호를 위한 장치 유무와 별개로 모든 권한을 서비스 제공자에게 위임한 상태에서 운영하고 있다는 점이다.

본 연구에서는 공개키 기반 암호화와 블록체인 기반의 키 관리 시스템을 조합한 아키텍처를 이용하여 민감한 정보를 사용자가 안전하게 보호할 수 있는 방안을 제시한다. 제안하는 아키텍처에서는 대칭키를 사용한 블록 암호화(block-cipher) 과정을 통해 영상 정보를 암호화하고, 이때 사용하는 대칭키를 사용자의 공개키로 암호화하여 블록체인의 레저(ledger)로 기록하는 기법을 사용한다. 영상 정보를 암호화하는 과정을 블록체인 네트워크의 특성(분산, 투명성, 데이터 변조 불가)을 활용하여 개인정보 영상의 생성부터 소멸까지 사용자가 추적이 가능하도록 한다.

1. 서론

영상 감시 시스템은 지정한 장소를 상시 녹화하고 있고 불특정 다수의 정보를 수집하는 특성을 가지고 있다. 감시 시스템을 통해 녹화된 영상은 개인정보 혹은 장소에 대한 민감 정보를 저장하고, 시스템 사용자나 서비스 제공자 사이의 개인정보 오남용 방지를 위한 객관적인 관리 시스템 또는 서비스는 부재인 상태이다. 현존하는 클라우드 기반 비디오 영상 감시 서비스들은 공통적으로 영상을 카메라에서 취득한 뒤, 인터넷 구간을 통해 영상 스트림을 전송하여 저장하는 방식을 취하고 있다. 이 때 전송하는 구간에 대해서는 SSL 을 적용하여 안전하게 보호하려 하지만, 서비스 내부에 저장된 영상에 대해서는 방화벽 등을 이용한 접근 차단 외에는 데이터 이동, 복사를 통한 유출에 대해서는 고려하고 있지 못하는 실정이다.

본 연구에서 제안하는 아키텍처는 영상을 저장할 때 영상 암호화 방법을 사용하여, 주어진 키를 알고 있는 경우에만 해당 영상을 재생할 수 있도록 한다. 따라서 본 연구의 목적은 영상 정보를 전송하거나 저장하는 순간부터 이동, 복사, 그리고 삭제할 때까지 일련의 과정을 추적할 수 있는 장치를 마련하여 전체 시스템에서 사용자 신뢰도를 향상시키는데 있다.

2. 관련 연구

영상 감시 시스템은 본질적으로 운영되는 시간 동안 끊임없이 자동적으로 특정 구역을 실시간으로 모니터링하거나 발생한 이벤트를 사건 이후 확인하기 위하여 녹화하는 것을 기반으로 구현 되어있다. 저장된 영상 파일은 카메라가 설치된 장소의 정보와 해당 위치에 방문한 인물들에 대한 정보를 담고 있으며, 경우에 따라서는 개인 정보 혹은 설치된 공간의 민감 정보를 내포하게 된다. 이러한 이유로 저장된 영상 파일에 대한 접근 통제는 대게 시스템에서 권한을 부여 받은 특정 사용자로 한정되도록 설계되어 있다.

개인정보보호를 위한 대표적인 아키텍처로는 G. Zyskind et al.[1]이 블록체인 아키텍처를 기반으로 하는 개인 데이터 보호 방안을 제시하고 있다. 영상과 음성 데이터를 보호하기 위한 방법으로는 MPEG-CENC 표준[2]으로 제시되고 있으며, 단일 혹은 여러 개의

AES Key 를 이용하여 멀티미디어 데이터를 암호화하는 방법으로 통용되고 있다. 이러한 멀티미디어 데이터 암호 기법은 데이터 자체의 보호보다는 Widewine, PlayReady 등과 같은 디지털 저작권 관리(Digital Right Management)의 관점에서 발전하고 있다. Vishwa et al.[3]은 블록체인 기반의 DRM 을 연구하여 저작권을 보호하는 방법을 제시하고 있다.

분산 환경에서 컨텐츠를 암호화하고 사용자의 키를 관리하는 방법에 대해서는 블록체인 기반의 PKI(Public Key Infrastructure)[4]를 사용자-서비스 간의 신원확인 및 데이터 보호에 사용하는 방안이 제시되고 있다. 또한 민감한 데이터를 보호하는 방법에 대한 연구는 EMR(Electronic Medical Records)처럼 정보의 소유자가 아닌 제 3 자가 데이터를 수집하고 처리할 때 발생할 수 있는 정보 보호 이슈[5]를 해결하고자 새로운 아키텍처를 수립하기도 하였다.

또한 실질적인 데이터를 관리하는 상황에 있어서, 블록체인 기반의 접근 방법은 위변조가 불가능하고 개인정보보호에 사용이 가능하다는 것을 이야기하지만, 시스템을 설계할 때 보호하려는 데이터의 크기보다는 기록하는 데이터의 수에 따라 전체 시스템의 성능이 좌우된다는 연구 결과[6]를 고려하여 영상 암호화 아키텍처를 제안하고자 한다.

3. 영상 스트림 접근 제어

데이터를 보호 방법은 데이터에 허가된 사용자가 접근하는 것을 제어하는 것과 위변조를 방지하는 두 가지 측면에서 접근할 수 있다. 그러나 본 제안 아키텍처에서는 영상을 획득하는 카메라가 설치된 장소와 획득한 영상을 서비스 제공자가 구성한 클라우드 기반의 저장소로 자동적으로 전송되는 특성을 고려하여 EMR 의 경우와 비슷하게 제 3 자에 의하여 생성된 데이터를 관리하는 방안을 제시하고자 한다.

또한 네트워크 단절 상황에서도 영상 유실을 막고자 카메라 내부에 일정 시간 동안 저장하는 경우에도 해당 데이터를 보호하기 위하여 서비스 전반에 걸쳐 영상 암호화 방법을 적용하도록 설계하였다.

4. Compound Identity 의 복잡성

비대칭 암호화는 둘 이상의 관련자간의 공개키와 개인키를 사용하고 있으며, 암호화 데이터 전송이전에 공개키의 교환은 필수적인 절차이다. 그렇기 때문에 서로간의 공개키를 통하여 서로를 식별하는 *Compound Identity* 를 구성하게 된다. Compound 집합은 공개키(pk)와 개인키(sk)의 2-tuple 혹은 완전한 식별데이터를 요구하는 경우 5-tuple(공개키, 개인키, 상대방 공개키와 개인키, 공유하는 대칭키)로 구성된다. 그러나 이러한 집합은 단순히 양방향 데이터 교환을 위해서는 강력한 암호화 메커니즘을 제공하는 기반이 되지만, 사용자와 다수의 서비스간의 경우로 환산한다면, Compound Identity 자체의 복잡도는 *O(n!)*으로 수렴하게 된다.

$$
\begin{aligned}
Compound^{(public)}_{u,s_1,s_2,\ldots,s_n} = \\
Compound^{(public)}_{u,s_1} + \ldots + Compound^{(public)}_{u,s_n} + \\
Compound^{(public)}_{s_1,u} + \ldots + Compound^{(public)}_{s_1,s_n} + \\
\ldots \\
Compound^{(public)}_{s_n,u} + \ldots + Compound^{(public)}_{s_n,s_{n-1}}
\end{aligned}
$$

Equation 1 Complexity of Compound Identity

영상 감시 시스템은 사용자가 직접 컨텐츠를 생성하는 것이 아니라, 카메라와 시스템이 자동적으로 생성하는 구조이기 때문에, 사용자-서비스 혹은 사용자-카메라간의 Compound Identity 를 구성한다고 하면, 이러한 복잡도의 증가는 시스템의 구성을 저해하는 요소가 된다.

5. 제안 아키텍쳐

Compound Identity 의 복잡도는 공개키를 공유를 필요로하는 양방향의 데이터 보호 채널을 구성하기 때문에 발생하게 된다. 영상 감시 시스템에서는 카메라와 사용자간의 관계상 사용자만이 카메라의 영상을 확인할 수 있도록 한정하여 Compound Identity 의 복잡도를 획기적으로 낮추도록 하였다.

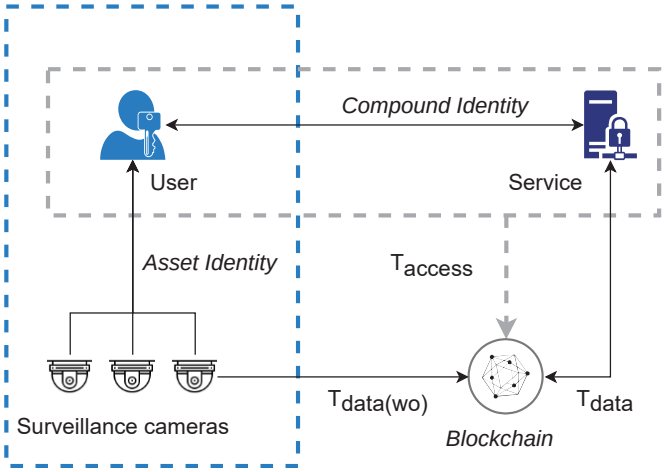

Figure 1 Overview of privacy protection architecture for surveillance system

1) ***Asset Identity***: Algorithm 1 에서는 **사용자-카메라** 혹은 **사용자-암호화된 비디오**의 관계를 설정하여 사용자의 공개키와 영상 암호화에 사용할 대칭키만을 조합하는 *Nonce* 개념을 소개하고 있다.

카메라 혹은 서비스가 생성한 Nonce 를 기반으로 영상 파일을 암호화하는 경우 대칭키 정보는 사용자 만이 알 수 있게 된다. 그렇기 때문에 영상 파일을 공개된 공간으로 전송하거나 사고에 의하여 유출된다고

하더라도 사용자의 개인키에 대한 어떠한 정보도 얻을 수 없게 되며, 이는 영상 정보를 복호화 할 수 없다는 것을 의미한다.

$$Asset_{u,a} = (pk^{u}_{sig}, Nonce^{a}_{pk(enc)})$$
$$Asset_{u,a_1,a_2 \ldots a_n} = (pk^{u}_{sig}, Nonce^{A}_{pk(enc)})$$

Equation 2 Asset Identity

Nonce 는 사용자가 정보의 소유권을 가진 장치나 서비스 등 사용자의 공개키를 획득할 수 있는 제 3 자에 의해서 생성이 가능하며, 사용자는 대칭키를 관리해야하는 부담에서도 동시에 벗어날 수 있다. 또한 Nonce 생성에는 단지 사용자의 공개키만을 요구하기 때문에 사용자와 암호화 채널을 구성해야하는 영상 감시 카메라 혹은 영상 정보를 처리하는 서비스가 증가함에도 그 복잡도는 여전히 *O(n)*으로 수렴한다.

Require: $A \neq \emptyset$
1: **procedure** ASSETIDENTITY(U, A)
2: **if** $(pk^{U}_{sig}, sk^{U}_{sig}) = \emptyset$ **then** ▷ U executes
3: $(pk^{U}_{sig}, sk^{U}_{sig}) \leftarrow \mathcal{G}_{sig}()$
4: $sk^{U}_{enc} \leftarrow \mathcal{G}_{enc}()$ ▷ only U keeps
5: **end if**
6: **for each** $a_k \in A$ **do**
7: $Nonce \leftarrow \mathcal{G}_{nonce}()$ ▷ only a_k keeps
8: $Nonce^{a_k}_{enc} \leftarrow Encrypt(pk^{U}_{sig}, Nonce)$
9: **end for**
10: **return** $(pk^{U}_{sig}, Nonce_{enc})$
11: **end procedure**

Algorithm 1 Generating *Asset Identity*

2) ***Protocol***: 개인정보보호를 위해 생성하는 일련의 정보는 블록체인 메모리(*L*)에 저장하는 것을 기본 전제로 한다. 영상 스트림의 경우, 영상 정보를 대게 그 사이즈가 크기 때문에 *L* 에 저장하는 것보다는 일반적인 저장소(*ds*)에 저장하고, 해시 함수(*H*)를 통해 매핑한 정보를 *L* 에서 관리하도록 한다. Nonce 에 대한 공유 혹은 허가 정보를 *L* 에 기록하여, 개인정보보호 관점에서 저장된 영상의 접근 제어뿐만 아니라 영상 정보의 생성부터 소멸까지 전반적인 라이프 사이클에 대한 추적이 가능하도록 한다.

3) ***Data Transaction***: *Asset Identity* 절차를 통하여 Asset 으로 분류되는 카메라는 Nonce 정보를 가지고 있기 때문에, $Nonce_{enc}$와 Asset 정보(*a*)를 암호화된 미디어 파일(M_{enc}) 내의 메타데이터로 기록하여 암호화된 미디어 파일 단독으로 off-chain 을 통해 공유 가능한 상태가 된다.

Algorithm 2 는 StoreSecureDataTX 를 이용한 데이터 저장소와 블록체인 메모리간의 상호 운영에 대한 절차를 설명하고 있다. 위에서 언급한대로 암호화된 미디어에 기록된 Nonce 는 아무런 제약없이 추출이 가능한 메타데이터이기 때문에 본 연구에서 제안하는 시스템은 카메라 내부 혹은 클라우드 기반의 데이터 저장 서비스를 블록체인 네트워크 혹은 암/복호화 과정과 분리하여 수행할 수 있도록 하여 시스템의 확장성을 고려하고 있다.

Require: $M_{enc} \neq 0$
1: **procedure** STORESECUREDATATX(pk^{k}_{sig}, M_{enc})
2: $(a_p, Nonce^{p}_{enc}) \leftarrow Parse(M_{enc})$
3: **if** $ValidateAsset(pk^{k}_{sig}, a_p, Nonce^{p}_{enc}) \neq True$ **then**
4: **return** $\emptyset$
5: **end if**
6: $h_{M_{enc}} \leftarrow \mathcal{H}(M_{enc})$
7: $L[\mathcal{H}(pk^{k}_{sig})] \leftarrow L[\mathcal{H}(pk^{k}_{sig})] \cup h_{M_{enc}}$
8: $ds[h_{M_{enc}}] = M_{enc}$
9: **return** $h_{M_{enc}}$
10: **end procedure**

Algorithm 2 Storing secure data

StoreSecureDataTX 내에서 수행하는 ValidateAsset 은 트랜잭션 내에서 비즈니스 로직이 개입할 수 있는 보조적인 장치로 사용되고 있으며, 이를 통하여 사용자, Asset, Nonce 정보가 일치하는지 확인할 때 블록체인 네트워크에 M_{enc}에 대한 접근 상황을 추적할 수 있다.

암호화된 미디어의 저장이 완료된 이후 Algorithm 3 은 ds 와 H 를 이용하여 M_{enc}를 획득한 후 복호화를 수행하는 과정을 설명하고 있다. 또한 제 3 자에의한 복호화 요청에도, *CheckPolicy* 를 정의하여 본래 Asset 의 소유주인 사용자에게 요청을 허가할지 결정할 수 있도록 하여, M_{enc}의 복호화 과정을 블록체인 네트워크에 기록할 수 있도록 한다. 또한 사용자가 허가할 수 있는 권한의 종류는 downloadable, readable 등으로 세분화하여 세밀한 권한 제어가 가능하도록 한다.

요청자가 M_{enc}를 획득한 이후에도 ValidateAsset 을 수행하여 사용자가 허가한 경우에 한하여 평문의 대칭키를 획득 가능하도록 하여 미디어 파일의 획득과 복호화 과정을 분리하여 추적할 수 있다.

Require: $m \neq 0$
1: **procedure** LOADSECUREDATATX(pk^{k}_{sig}, m)
2: $(h_{M_{enc}}, x_p) \leftarrow Parse(m)$
3: **if** $CheckPolicy(pk^{k}_{sig}, x_p) \neq True$ **then**
4: **return** Error
5: **end if**
6: **if** $h_{M_{enc}} \in L[\mathcal{H}(pk^{k}_{sig})]$ **then**
7: $M_{enc} \leftarrow ds[h_{M_{enc}}]$
8: $(a_p, Nonce^{p}_{enc}) \leftarrow Parse(M_{enc})$
9: **if** $ValidateAsset(pk^{k}_{sig}, a_p, Nonce^{p}_{enc}) \neq True$ **then**
10: **return** $\emptyset$
11: **end if**
12: **end if**
13: **return** $(pk^{k}_{sig}, h_{M_{enc}}, a^{p}, Nonce^{p}_{enc})$
14: **end procedure**

Algorithm 3 Loading secure data

4) ***Tracing Transaction***: 영상 정보의 생성 이후 M_{enc}의 소유권 이전과 소멸에 대한 관리를 위한 트랜잭션으로 대용량의 미디어 파일의 반복적인 암복호화 과정

없이 Nonce 정보를 추가하여 off-chain 상에서도 전달 과정을 Algorithm 4 를 통해 제시하고 있다.

제시된 알고리즘의 6 번째 라인에서 설명하듯 M_{enc}^{t} 는 $Nonce_{enc}^{k}$와 $Nonce_{enc}^{t}$의 정보를 모두 가지고 있기 때문에 사용자 k 와 t 는 M_{enc}^{t}를 복호화 할 수 있으나, 이 과정에서 M_{enc}^{t}를 복호화는 필요로 하지 않는다.

Require: $T \neq \emptyset \vee m \neq 0$
1: **procedure** TRANSFERSECUREDATATX(pk_{sig}^{k}, T, m)
2: $(pk_{sig}^{k}, h_{M_{enc}}, a^{p}, Nonce_{enc}^{p}) \leftarrow LoadSecureDataTX(pk_{sig}^{k}, m)$
3: $M_{enc} \leftarrow ds[h_{M_{enc}}]$
4: **if** $M_{enc} \neq \emptyset$ **then**
5: $(pk_{sig}^{t}, Nonce_{enc}^{t}) \leftarrow AssetIdentity(T, a^{p})$
6: $M_{enc}^{t} \leftarrow M_{enc} \cup Nonce_{enc}^{t}$
7: $h_{M_{enc}^{t}} \leftarrow StoreSecureDataTX(pk_{sig}^{t}, M_{enc}^{t})$
8: **end if**
9: **return** $h_{M_{enc}^{t}}$
10: **end procedure**

Algorithm 4 Transferring secure data

영상 감시 시스템에서 또다른 주요 이슈는 생성된 영상 정보를 영구히 제거하는 것이다. 제안된 시스템에서도 임의로 저장한 M_{enc}의 복사를 제한할 수 있는 방법은 없으나, Algorithm 5 는 Nonce 자체를 무효화하여 결과적으로는 M_{enc}의 복호화 방법을 차단하는 간접적인 절차를 통해 해당 영상 정보에 접근을 영구히 제거하는 방안을 제안한다.

물론 Nonce 조차도 임의의 공간에 별도로 보관하는 경우 무효화된 M_{enc}를 복호화 하려는 시도는 가능하나 일반적으로 난수 생성기(Random Number Generator)를 통해 생성된 값으로 공격의 대상이 되는 모든 M 에 대하여 무효화 이전에 예측 불가능한 Nonce 를 별도의 시스템에서 관리하는 것은 사실상 불가능에 가깝다.

1: **procedure** INVALIDATESECUREDATATX($pk_{sig}^{k}, h_{M_{enc}}$)
2: $M_{enc} \leftarrow ds[h_{M_{enc}}]$
3: $(a_{p}, Nonce_{enc}^{p}) \leftarrow Parse(M_{enc})$
4: $M_{enc} \leftarrow M_{enc} - Nonce_{enc}^{t}$
5: **if** M_{enc} has no $Nonce$ **then**
6: $ds[h_{M_{enc}}] = \emptyset$
7: **end if**
8: **end procedure**

Algorithm 5 Invalidating secure data

6. 결론

사회 안전을 위하여 널리 사용되고 있는 영상 감시 시스템의 시스템 자체가 개인정보보호를 위해 보호되어야 하는 대상이 되고 있다. 시간이 지남에 따라 더 많은 사용자와 시스템이 관련되기 때문에 악의적인 접근과는 상관없이 실수에 의해서도 민감한 영상이 공유되는 상황은 발생할 수 있으나 시스템에 대한 접근 차단 외에는 뚜렷한 보호장치는 없는 상태이다. 본 연구에서 제안한 아키텍처는 영상 정보에 보다 중점을 두어 사용자의 제어권 안에서 영상 정보 제공이 가능하도록 하여 개인정보를 보호하는데 목적을 두고 있다. 그러나 제안된 아키텍처는 영상 감시 시스템 뿐만 아니라 추후 연구를 통하여 데이터의 생성과 소유가 분리되는 일반적인 경우에도 적용할 수 있을 것으로 기대된다.

참고문헌

[1] G. Zyskind, O. Nathan, and A. ’. Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184, May 2015.

[2] ISO/IEC 23001-7:2016, Part 7: Common encryption in ISO base media file format files In *Information technology – MPEG systems technologies* Retrieved from https://www.iso.org/standard/68042.html

[3] Alka Vishwa and Farookh Hussain. A blockchain based approach for multimedia privacy protection and provenance. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1941–1945, Nov 2018.

[4] R. Wang, J. He, C. Liu, Q. Li, W. Tsai, and E. Deng. A privacy- aware pki system based on permissioned blockchains. In *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, pages 928–931, Nov 2018.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25– 30, Aug 2016.

[6] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Com- puting (CCGRID)*, pages 468–477, May 2017.