CCTV영상 관리를 위한 안전한 접근 제어 방안 연구

이재승*, 김형주*, 전문석*
*숭실대학교 컴퓨터학과
email : ljsa_0322@ssu.ac.kr

Secure Access Control Scheme for CCTV Video Management

Jae-Seung Lee, Hyung-Joo Kim, Moon-Seog Jun
Soongsil University

요 약

CCTV의 다양한 필요성이 대두됨에 따라 CCTV를 통합관리하는 CCTV 통합관제 센터가 늘어나고 있다. 행정안전부는 2015년까지 전국 시군구에 CCTV 통합관제센터 구축을 추진하고 있을 정도로 앞으로도 계속적으로 증가할 예정이다. 하지만 이를 관리할 전문 모니터링 요원이 턱없이 부족한 상황이며, 전문 교육의 부재로 CCTV 영상을 개인적 호기심이나 개인의 이익을 위해 열람하는 경우가 발생하고 있다. 본 논문을 비밀 분산 기법을 이용하여 암호화된 키를 분배하고 요청에 따라 일정 수 이상의 분배키가 모이면 영상 열람권한을 주는 방식으로 설계 하여 관리자가 임의로 영상정보에 접근하는 상황을 방지하였다. 또한 그룹 키를 분배하고 수시로 키 갱신을 함으로서 다양한 보안 위협에 대응 하였다.

1. 서론

범죄예방과 위급상황 발생 시의 대응, 시설물 관리 등의 다양한 필요성에 의해 CCTV를 통합관리하는 CCTV 통합관제센터가 각 지역별로 구축되고 있다. 행정안전부는 2015년까지 전국 시군구 230여 지역에 CCTV 통합관제센터 구축을 추진하고 있음에 따라 CCTV 통합관제센터는 앞으로도 꾸준히 늘어날 것으로 예상되고 있다.

이렇게 구축된 CCTV 통합관제센터는 용도별로 CCTV를 분산 설치하여 방범, 시설물 관리 등에 이용하게 된다.

수집된 영상정보는 CCTV통합관제센터를 통해 실시간 모니터링은 물론 이미 지나간 사건 영상에 대한 열람이 가능하다. 영상의 열람의 경우 수사의 목적으로 경찰서 등에 열람하거나 제공하여 적극 활용될 수 있다. 그러나 현재 CCTV통합관제 센터 전문 관리자의 수가 부족한 상황이며, 전문교육 또한 제대로 이루어지지 않아 공익공무요원이나 지역 내 주민을 동원하여 관리되는 경우가 적지 않다. 이 경우, 전문 교육을 받지 못한 관리자의 전문지식 부족으로 개인적 호기심이나 개인의 이득 등 합리적이지 못한 이유로 영상정보를 열람, 제공하는 상황이 발생함으로서 프라이버시를 침해할 우려를 가지고 있다.

본 논문에서는 비밀 분산 기법을 이용해 키를 분배하여 일정 수 이상의 담당자가 동의하였을 경우 키를 복원하여 영상정보를 열람 할 수 있는 방법을 제시하려고 한다.

2-1. 다항식 키 분배

Predistribution and local Collaboration-based Group Rekeying은 다항식을 이용하여 그룹 내 사용자가 안전하게 그룹 키를 갱신할 수 있도록 한다.

순서 1. 분배자는 t차 다항식 g(x)를 생성하여 그룹 내 사용자에게 전달 한다.

순서 2. 분배자는 이변다항식 e(x,y)를 생성 한다.

$$e_u(x,y) = \sum_{0\le i\le t, 0\le j\le \mu} A_{i,j}x^i y^j$$

순서 3. 분배자는 다항식 y항에는 자신의 아이디 u를 대입하여 t차 다항식을 생성하고 암호화 함으로서 g'(x)를 만든다.

$$g'(x) = g(x) + e_u(x,u)$$

순서 4. 분배자는 e(x,y)의 y에 그룹 사용자의 아이디를 넣어 그룹 사용자에게 전송 한다.

순서 5. 키 갱신이 필요할 경우 x값을 증가 시켜 z를 만들고 e(z,ID)를 계산하여 그룹 내 사용자가 g'(x)를 계산하도록 한다. 본인의 키는 μ+1개의 부분 정보를 받음으로서 μ차 다항식을 복원할 수 있다.

$$\sum_{j=0}^{\mu}(v_i)^j B_j = e_u(c, v_i), (0 \le i \le \mu).$$

$$e_u(c, y) = \sum_{j=0}^{\mu} B_j y^j$$

2-2. Shamir's Secret Sharing

Shamir's Secret Sharing은 원본의 키 s를 n개로 분할하여 분할된 키가 k개 이상이 모이면 본래의 원본 키를 복원할 수 있는 방식이다.

순서 1. 분배자는 s를 상수항으로 하는 k-1차의 다항식 f(k)를 선택한다.

$$f(x)=s+a_1x+a_2x^2+ \cdots +a_{k-1}x^{k-1} \bmod p$$

순서 2. 분배자는 분할된 키를 받는 자를 각각 j(j=1,2…n)로 정하고 f(j)를 분배 한다.

순서 3. f(j)가 k개 이상 모일 경우 s는 복원이 가능하다.

3. 제안 내용

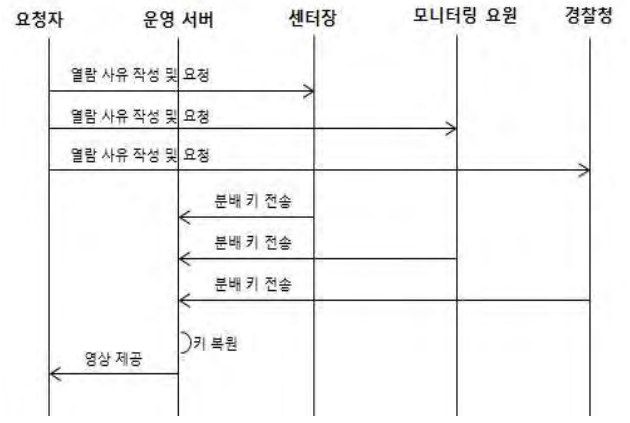
3.1 개요

본 논문에서는 키를 분배하고 영상열람 요청이 들어왔을 경우 일정 수 이상이 동의했을 때 키를 복원하여 영상을 열람할 수 있는 방법을 제안하고 있다. 키를 교환하는 과정에서는 그룹 키를 사용하며 주기적으로 그룹 키를 갱신함으로서 키에 대한 안전성도 보장 한다.

(1) 영상정보 열람을 원하는 요청자는 영상열람 사유서를 전송 한다.

(2) 본 논문은 관리처를 전문 요원과 센터장, 경찰청으로 예시 한다. 각각의 관리처는 열람 사유에 대한 적합성을 판단 후 적절하다고 판단되면 본인의 키를 운영서버로 전송한다.

(3) 일정 수 이상의 키가 모이면 운영서버는 영상에 대한 접근을 허용 한다.



(그림 5) 영상정보 열람 과정

3.2 키 분배 및 전송 방법

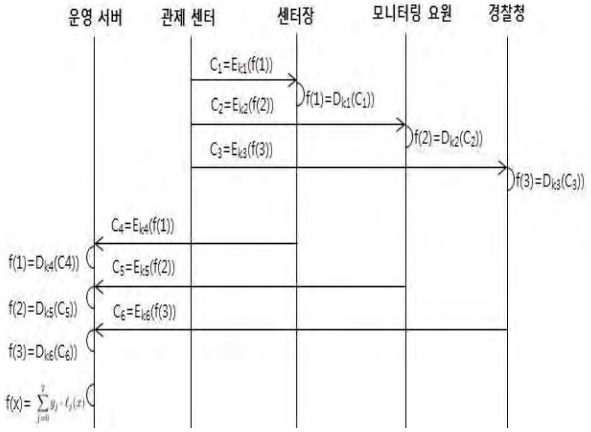
키를 분배하는 방법은 앞에서 나온 k-1차 다항식을 이용한다. 본 논문에서는 예시를 위해 n을 3, k를 2로 설정하여 프로토콜을 구성 하였다.

(1) 관제센터는 s를 상수항으로 하는 k-1차의 다항식 f(k)를 선택한다.

(2) 관제센터는 j의 값을 정하고 f(j)를 전송한다. 본 논문은 센터장은 1, 모니터링 요원은 2, 경찰청은 3으로 j 값을 지정하며 전송할 때 생성한 그룹 키를 통해 암호화를 한다.

(3) 관리처에서 운영서버에 키를 보낼 때, 그룹 키로 암호화 하여 전송한다.

(4) 운영서버는 k개 이상의 분배키가 모이면 라그랑주 다항식을 이용하여 원본 키를 복원한다.



(그림 6) 키 분배 및 전송 방법

3.3 안전성 확보를 위한 키 교환

공격자가 관제 센터에서 센터장에게 보내는 암호문을 탈취하여 추후에 그대로 사용하는 상황이 발생할 수 있다.

본 논문에서는 다항식 키 분배에서 그룹 키 갱신 기법을 이용해 지속적으로 키를 변경함으로서 재사용 공격에 대응 한다.

(1) 운영서버는 t차 다항식 g(x)를 생성하여 그룹 내 사용자에게 전달 한다.

(2) 운영서버는 이변다항식 e(x,y)를 생성 한다.

(3) 운영서버는 다항식 y항에는 자신의 아이디 u를 대입하여 t차 다항식을 생성하고 암호화 함으로서 g'(x)를 만든다.

(4) 운영서버는 e(x,y)의 y에 그룹 사용자의 아이디를 넣어 그룹 사용자에게 전송 한다.

(5) 키 갱신이 필요할 경우 관리처는 x값을 증가 시켜 z를 만들고 e(z,ID)를 계산하여 그룹 내 사용자가 g'(x)를 계산하도록 한다. 본인의 키는 μ+1개의 부분 정보를 받음으로서 μ차 다항식을 복원할 수 있다.

4. 안전성 평가

본 논문에서 제안하는 방법은 키를 분배하여 관리함으로서 하나의 제대로 된 값을 얻어도 영상 열람이 불가능하며 그룹 키를 통해 암호화 되어 전송되기 때문에 도청에 안전하며 수시로 그룹 키를 갱신할 수 있어 키 관리에도 유용하다. 또한 수시로 그룹 키를 갱신함으로서 재사용 공격에도 안전하다.

5. 결론

본 논문은 개인의 프라이버시의 중요성이 대두됨에 따라 CCTV 통합관제센터에서 근무하는 모니터링 관리자가 합리적이지 못한 이유로 영상정보를 열람, 제공하는 상황을 미연에 방지 할 수 있도록 영상정보를 열람할 수 있는 권한을 분배하여 침해 사고가 발생하기 이전에 사전대응을 할 수 있도록 설계하였다. 비밀 분산 기법을 이용하여 키를 분배 하되 그룹키를 통한 암호화와 상호인증 등을 통해 다양한 보안위협에도 대응하였다.

참고문헌

[1] Adi Shamir "How to share a secret" Communications of the ACM, '1979.11.01'
[2] Jean-Paul Berrut, Lloyd N. Trefethen "Barycentric Lagrange Interpolation", Dedicated to the memory of Peter Henric, '2004,02.04'