상용 비디오 콘텐츠 보호를 위한 일회용 바이오메트릭 키 생성 및 인증 모델

윤성현
백석대학교 정보통신학부

The One Time Biometric Key Generation and Authentication Model for Portection of Paid Video Contents

Sunghyun Yun
Division of Information & Communication Engineering, Baekseok University

요 약 비디오 콘텐츠는 사람의 시각과 청각을 이용함으로 다른 종류의 콘텐츠 보다 이해하기 쉽기 때문에 많은 사람들이 선호한다. 더불어 스마트폰의 보급으로 인터넷을 이용한 비디오 콘텐츠 서비스에 대한 수요가 급증하고 있다. 콘텐츠 거래 활성화를 위해서는 유료 가입자에 대한 인증과 유료 채널로 전송되는 데이터의 보호가 중요하다. 가입자 채널 보호를 위해서는 일반적으로 대칭키 암호 기술이 사용되는데, 안전성을 높이기 위해서 키 값을 주기적으로 변경해야 한다. 또한 다른 사용자에 의한 콘텐츠 불법 이용을 방지하려면 대리 인증이 불가해야 한다. 본 논문에서는 가입자의 바이오메트릭 데이터를 이용한 본인 인증 및 일회용 암호키를 생성하는 모델을 제안한다. 제안한 모델은 바이오메트릭 데이터 등록, 일회용 키 생성, 채널 암호화 및 복호화 단계로 구성된다. 기존의 케이블 TV 콘텐츠 인증 기술인 CAS (Conditional Access System)와의 차이점을 분석하고 인터넷 상거래에서의 응용 분야를 제시한다.

• **주제어** : 바이오메트릭 키, 바이오메트릭 인증, 일회용 패스워드, 전자상거래, 콘텐츠 보호

Abstract Most peoples are used to prefer to view the video contents rather than the other contents since the video contents are more easy to understand with both their eyes and ears. As the wide spread use of smartphones, the demands for the contents services are increasing rapidly. To promote the contents business, it's important to provide security of subscriber authentication and corresponding communication channels through which the contents are delivered. Generally, symmetric key encryption scheme is used to protect the contents in the channel, and the session key should be upadated periodically for the security reasons. In addition, to protect viewing paid contents by illegal users, the proxy authentication should not be allowed. In this paper, we propose biometric based user authentication and one time key generation models. The proposed model is consist of biometric template registration, session key generation and chanel encryption steps. We analyze the difference and benefits of our model with existing CAS models which are made for CATV contents protection, and also provides applications of our model in electronic commerce area.

• **Key Words** : Biometric Key, Biometric Authentication, One Time Password, Electronic Commerce, Contents Security

1. 서론

초고속 인터넷과 스마트폰의 보급으로 인터넷 비디오 콘텐츠에 대한 사용자들의 수요가 급증하고 있다. 유투브, 곰 TV 등과 같은 콘텐츠 제공업자는 스트리밍 기술

이 논문은 2014년도 백석대학교 대학연구비에 의하여 수행된 것임
*교신저자 : 윤성현(shcrpt@gmail.com)
접수일 2014년 9월 23일 수정일 2014년 11월 26일 게재확정일 2014년 12월 12일

을 이용한 VOD(Video On Demand) 서비스를 제공하여 사용자들이 콘텐츠를 다운로드 받으면서 동시에 재생할 수 있도록 한다. 일반적으로 VOD 스트리밍 서비스는 콘텐츠 및 회원 관리가 용이한 서버-클라이언트 방식으로 구축된다 [1].

서버-클라이언트 기반의 비즈니스 모델은 클라이언트, 거래서버 그리고 데이터베이스 서버로 구성된다. 거래서버는 상거래 관련 정책 및 트랜잭션을 처리하고, 데이터베이스 서버는 콘텐츠를 관리하는 역할을 한다. 상거래 활성화를 위해서는 유료 회원에 대한 인증과 상용 콘텐츠의 안전한 분배 방법이 확보되어야 한다 [2, 3].

비디오 스트리밍은 실시간 전송을 요구하기 때문에 TCP 대신 UDP 프로토콜을 사용하며, 채널 암호화를 위해서 상대적으로 속도가 빠른 대칭키 기반의 암호화 기법이 사용된다 [1].

VOD 기반의 비즈니스 모델이 성공하기 위해서는 콘텐츠 저작자, 판매자 그리고 사용자로 구성되는 각 구성요소간에 서비스 가치 및 수익의 선순환 구조가 만들어져야 한다. 수익모델의 안전성이 입증되면 보다 많은 저작자들이 콘텐츠를 생산하게 되고, 이에따라 콘텐츠 사용자들은 양질의 콘텐츠를 접하게 되며 이는 곧 수요 증가로 이어지게 된다.

유료 가입자 인증과 안전한 콘텐츠 분배를 위한 주요 보안 요구사항을 알아보면 다음과 같다.

첫째로, 가입자 인증에 대해서 살펴본다. 기존의 ID, 패스워드 기반 인증은 사람이 기억하고 있는 것으로 해당 사용자를 인증하는 방식이다. 스마트폰과 같은 모바일 기기를 이용하여 온라인으로 콘텐츠를 서비스를 받는 비즈니스 모델에서는, 제 3자가 유료 가입자의 정보를 이용하여 대리 인증이 가능하다. VOD 기반의 비즈니스 모델이 성공하기 위해서는 대리 인증이 불가한 가입자 인증 기법의 도입이 필수적이다. 최근에는 기기 인증 방식을 도입하여 해당 기기에서만 서비스를 받을 수 있도록 하는 방법이 적용되고 있지만, 이 방식의 단점은 사용자 입장에서 등록된 기기만 사용해야 하는 불편이 따르기 때문에 선호하지 않는다는 것이다. 보안성을 높이기 위하여 규제나 사용조건이 많아지면 사용성이 떨어지게 되어 오히려 콘텐츠 산업 활성화를 저해한다. 보안성을 높이면서 사용성을 확보할 수 있는 인증 기법이 필요하다.

둘째로, 안전한 콘텐츠 분배에 대해서 살펴본다. 스트리밍 콘텐츠는 무결성 보다는 서비스가 끊기지 않아야 하는 실시간성이 더욱 중요하다. 따라서, 가입자 채널 암호화 및 복호화를 위해서 속도가 빠른 알고리즘의 선택이 중요하다. 넓은 대역폭을 요구하는 고화질 대용량 콘텐츠의 경우에 연산 성능이 낮은 모바일 기기에서 재생하려면 XOR 연산을 이용한 스트림 암호를 이용해야 한다. 스트림 암호의 안전성은 생성된 키스트림의 길이와 임의적 성질에 기반한다. 안전성과 실시간성을 동시에 만족하기 위해서는 키스트림을 주기적으로 변경해주고 임의의 값을 만들어 낼 수 있는 외부 입력이 있어야 한다. 단순히 의사 난수 함수를 이용하여 키스트림을 생성하는 것은 해당 함수가 생성하는 난수열의 특성을 분석하는 암호 해독 공격에 취약하다 [4].

CAS (Conditional Access System)는 케이블 TV 가입자를 위한 가입자 인증 시스템이다 [5]. 가입자의 셋탑박스에 콘텐츠 전송 서버의 마스터 키를 내장하여, 이 키를 기반으로 주기적으로 채널 암호화 키를 변경한다. 암호화 키의 업데이트는 서버에서 주도함으로 서버의 키 업데이트 방법이 노출되면 전체 시스템에 영향을 미치게 되고 셋탑박스의 마스터 키를 모두 교체해야 하는 불편이 따른다.

본 연구에서는 사용자 고유의 바이오메트릭 데이터를 이용하여 가입자 인증과 함께 일회용 세션키를 생성할 수 있는 모델을 제안한다. 사용자의 시스템 사용성을 높이면서 거래 모델의 안전성을 강화하는 것이 본 연구의 목표이다. 제안한 모델은 바이오메트릭 인증 기법을 도입하여 대리 인증이 불가능하고, 사용자 고유의 바이오메트릭 데이터를 이용하여 세션키를 생성함으로써 서버 의존도를 최소화한다.

사용자가 매 세션마다 입력하는 바이오메트릭 데이터는 그 모양이 유사하지만 동일하지는 않기 때문에 임의 값 발생을 위한 입력 소스로 이용할 수 있다. 입력된 템플릿은 MD5 또는 SHA-1 해쉬 함수를 이용하여 해쉬함으로써 입력소스 간의 종속성을 최소화 시킨다. 해쉬 및 암호 함수의 안전성은 입력소스와 출력소스 간의 확산도로 결정되는데, 입력 값이 1비트라도 차이가 나게 되면 완전히 다른 결과 값을 보여주는 특성이 있다 [4].

2 장에서 바이오메트릭 사용자 인증 모델에 대해서 살펴보고, 3 장에서 바이오메트릭 기반의 일회용 키 생성 모델을 제안한다. 4 장에서 기존의 CAS 모델과 비교 분석하고, 5 장에서 결론을 제시한다.

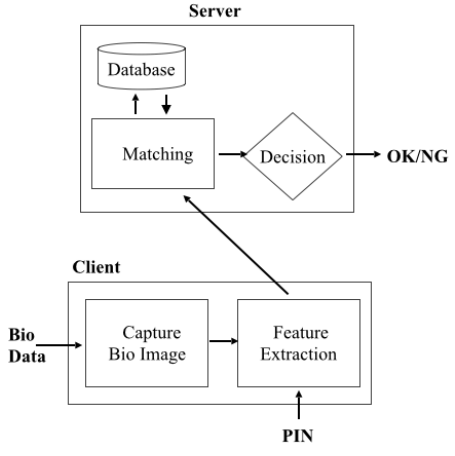
2. 관련연구

사용자 인증은 제 3자에게 본인임을 입증하는 기술이다. 보편적으로 가장 많이 사용되는 방법은 사람이 기억하고 있는 것을 기반으로 그 사람임을 입증하는 패스워드 방식이다. 패스워드 기반 인증을 위해서 사용자는 먼저 자신의 아이디와 패스워드를 서버에 등록해야 한다. 서버 공격 또는 전송중인 패스워드를 보호하기 위하여 패스워드는 데이터베이스에 해쉬값으로 저장되어야 하고 전송중인 데이터는 암호화되어야 한다 [4].

하지만 사람의 기억에 의존하는 인증 방식은 다른 사람이 대리로 인증할 수 있는 위험요소가 있기 때문에, 콘텐츠 스트리밍 기반의 비즈니스 모델에는 적합하지 않다. 아이디와 패스워드를 공유하여 저작물을 여러 사람이 불법적으로 공유할 수 있다. 그 결과로 저작자 및 판매자의 수익이 감소하고 이에 따라서 저작 의욕이 저하되어 양질의 콘텐츠를 생산할 수 없고, 따라서 콘텐츠 수요자도 줄어들게 되는 악순환을 따르게 된다.

바이오메트릭 인증은 사용자가 가지고 있는 고유의 신체 정보를 이용하여 인증하는 것으로 대리 인증이 불가능하다 [6]. 특히, 카메라 및 지문인식 센서가 내장된 스마트폰의 폭 넓은 보급은 모바일 콘텐츠 거래 모델에 바이오메트릭 인증 기법의 도입을 가능하게 한다 [7].

바이오메트릭 인증을 위해서는 먼저 사용자가 자신의 바이오메트릭 데이터를 서버에 등록해야 한다. 지문, 홍채 등의 신체 정보는 각 개인마다 고유하기 때문에 한 번 도용되면 다시 사용할 수 없기 때문에 바이오메트릭 데이터는 원본 형태로 저장되면 안되고 취소 가능한 형태로 변형하여 데이터베이스에 등록되어야 한다 [8, 9].



[Fig. 1] Server based Biometric Authentication

바이오메트릭 기반 사용자 인증은 사용자가 입력한 바이오메트릭 데이터와 서버에 등록된 데이터를 비교하여 그 유사도를 평가함으로써 결정된다. 입력된 데이터는 동일인의 것이어도 매번 스캔할 때 마다 차이가 있기 때문에 서버에 등록된 데이터와 얼마나 유사한 지를 비교해서 판단해야 한다.

그림 1은 서버 기반의 바이오메트릭 인증 단계를 보여준다. 서버-클라이언트 기반의 모바일 상거래에 적합한 바이오메트릭 인증 모델이다. 사용자 특징 정보와 PIN 정보가 네트워크를 통해서 클라이언트에서 서버로 전송되며 서버에서 이를 가지고 데이터베이스에 등록된 사용자 특징정보를 비교하여 사용자 인증을 수행한다. 인터넷과 같은 공중망으로 전송되는 사용자의 민감한 정보는 암호화 및 서명 등 정보보호 기법의 적용이 필수적이다.

3. 일회용 바이오메트릭 키 생성

본 장에서는 스마트폰의 바이오메트릭 센서를 이용하여 가입자 인증과 함께 일회용 세션키를 생성하는 프로토콜을 제안한다.

정의 1. GF(p)는 암호학적으로 안전한 유한체이고 g는 GF(p) 상에서 정의된 생성자로 위수 p-1을 갖는다 [10]. p는 큰 소수로 모듈라 연산의 법이다.

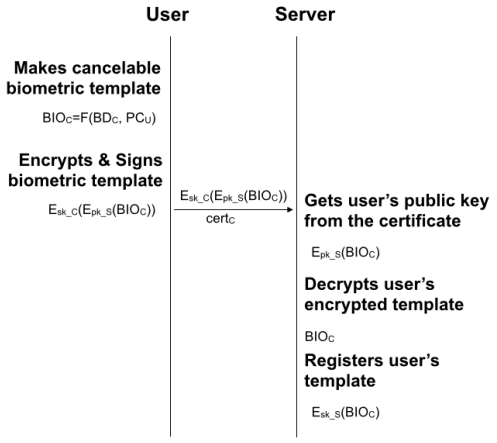
가정 1. 사용자 바이오메트릭 템플릿을 등록 및 관리하는 데이터베이스와 바이오메트릭 인증을 담당하는 신뢰할 수 있는 상거래 서버가 존재한다. 상거래 서버와 구매자는 정의 1의 GF(p)를 공유하고 개인키 및 공개키는 다음과 같다.

User	Private key	Public key	Biometric template
Server	$sk_S < p$	$pk_S \equiv g^{sk_S} \bmod p$	$E_{pk_S}(BIO_C)$
Customer	$sk_C < p$	$pk_C \equiv g^{sk_C} \bmod p$	$E_{pk_C}(BIO_C)$

가정 2. 상거래 서버와 구매자는 PKI 인증 기관으로부터 공개키에 대한 인증서를 발급받는다.

User	Private key	Public key	Cert
CA	$sk_{CA} < p$	$pk_{CA} \equiv g^{sk_{CA}} \bmod p$	$E_{sk_{CA}}(pk_S)$ $E_{sk_{CA}}(pk_C)$

3.1 바이오메트릭 템플릿 등록



[Fig. 2] Biometric Template Registration

사용자는 패스코드를 이용하여 취소가능한 바이오메트릭 템플릿을 생성한다. 패스코드는 사용자가 임의로 생성한 난수 값으로 템플릿이 도용되었을 때 동일한 신체정보로 템플릿을 재생성하여 등록할 수 있도록 한다.

단계 1: 사용자는 자신의 바이오메트릭 데이터와 패스코드를 입력하여 취소가능한 템플릿을 생성한다. BD_C는 사용자가 입력한 바이오메트릭 템플릿, BIO_C는 취소가능한 템플릿, F는 변형함수, PC_U는 사용자 패스코드이다.

$$BIO_C = F(BD_C,\ PC_U)$$

단계 2: 사용자는 자신의 공개키 pk_C를 이용하여 BIO_C를 암호화하고 스마트폰에 저장한다.

단계 3: 사용자는 상거래 서버의 공개키 pk_S를 이용하여 BIO_C를 암호화하고 자신의 개인키로 서명한다. 사용자는 인증서와 함께 서명된 템플릿을 서버로 전송한다.

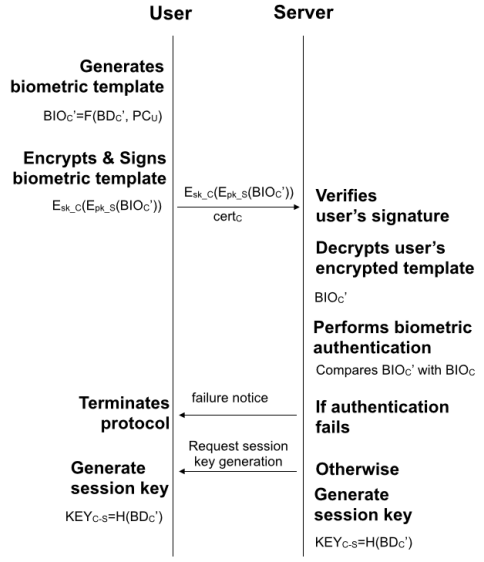
$$(E_{sk_C}(E_{pk_S}(BIO_C)),\quad cert_C)$$

단계 4: 서버는 사용자의 인증서 $cert_C$에 있는 공개키를 검증하고 $E_{sk_C}(E_{pk_S}(BIO_C))$를 복호화 한다.

단계 5: 서버는 자신의 개인키 sk_S로 $E_{pk_S}(BIO_C)$를 복호화하한다.

단계 6: 서버는 사용자의 바이오메트릭 템플릿을 자신의 개인키로 서명하여 사용자 인증서와 함께 데이터베이스에 등록한다.

3.2 사용자 인증 및 일회용 키 생성



[Fig. 3] User Authentication and One Time Session Key Generation

사용자는 서버 인증을 받기 위하여 자신의 바이오메트릭 데이터와 패스코드를 스마트폰에 입력하여 취소 가능한 템플릿을 만들고 이를 서버로 전송한다. 서버는 데이터베이스에 등록된 사용자 템플릿과 수신된 템플릿을 비교하여 사용자 인증을 한다. 인증이 성공하면 서버와 사용자는 공유한 바이오메트릭 템플릿을 이용하여 일회용 세션키를 생성한다.

단계 1: 사용자는 스마트폰으로 바이오메트릭 인증을 위한 인증값을 생성한다. BD_C'는 사용자가 입력한 바이오메트릭 템플릿, BIO_C'는 취소가능한 템플릿, F는 변형함수, PC_U는 사용자 패스코드이다.

$$BIO_C' = F(BD_C'\ ,\ PC_U)$$

단계 2: 사용자는 BIO_C'를 서명하고 서버의 공개키로 암호화한다. 사용자는 $(E_{sk_C}(E_{pk_S}(BIO_C')))$와 인증서를 서버로 전송한다.

단계 3: 서버는 사용자의 공개키로 서명을 검증하고 자신의 개인키로 암호화된 BIO_C'을 추출한다.

데이터베이스에 등록된 BIO_C와 BIO_C'의 유사도를 계산하여 사용자 인증을 수행한다. 인증에 성공하면

단계 4로, 그렇지 않으면 인증 실패 메시지를 사용자에게 전달하고 프로토콜을 종료한다.

단계 4: 서버와 사용자는 BIO_C'을 이용하여 다음과 같이 일회용 세션키를 생성한다. BIO_C'은 매 인증 세션마다 사용자가 생성한 취소가능한 템플릿이고, H는 암호학적으로 안정한 해쉬 함수인 MD5 또는 SHA-1이라고 가정한다.

$$KEY_{C-S} = H(BD_C')$$

4. 비교 분석 및 응용

제안한 일회용 세션키 생성 모델과 기존의 CAS 모델에 대해서 분석하고 응용에 대해서 기술한다.

표 1은 제안한 모델과 CAS 모델을 비교한 것이다. CAS 모델은 셋탑박스와 콘텐츠 서버가 마스터키를 공유하여 서버와 유료 가입자 간의 채널을 암호화하여 보호한다. 세션키를 알고있는 유료 가입자에게 서비스를 제공할 수 있지만, 유료 가입자가 다른 사용자에게 인증 정보를 대여할 수 있는 단점이 있다. 서버와 가입자 간의 세션키는 서버에서 주기적으로 업데이트 하여 키 안전성을 강화하고 있지만, 콘텐츠 서버 해킹에 의해서 마스터 키가 노출되면 이전의 모든 암호화된 콘텐츠가 노출되고, 모든 가입자들의 마스터키를 새로 갱신해야 하는 부담이 따른다.

〈Table 1〉 Functional Comparison

Functions	CAS Model	Proposed Model
Is the paid customer can get the service ?	O	O
Is proxy authentication is possible ?	O	X
Is the session key updated periodically ?	O	O
Who updates the key ?	Server	Customer
Is the sessino key secure against server hacking ?	X	△

제안한 모델은 사용자 바이오메트릭 데이터를 이용하여 인증정보와 세션키를 생성한다. 바이오메트릭 인증을 하기 때문에 대리 인증이 불가능하고 유료 가입자에게만 해당 서비스를 제공할 수 있다. 더불어, 세션키는 가입자가 요구하는 매 세션마다 가입자에 의해서 생성되는 일회성을 갖는다. 서버 해킹으로 서버 정보가 노출되어도 해당 세션의 콘텐츠만 유출되기 때문에 위험을 최소화할 수 있다.

제안한 모델은 대리 인증이 허용되지 않으며 일회용 패스워드가 요구되는 상거래 응용 분야에 적용될 수 있다. 인터넷 뱅킹에서의 OTP를 이용한 계좌 인증, 전자선거 시스템에서의 사용자 인증 [11, 12], 스마트폰을 이용한 화상 회의 등에 적합하다.

5. 결론

본 논문에서는 바이오메트릭 기반의 일회용 세션키 생성 모델을 제안하였다. 제안한 모델은 바이오메트릭 템플릿 등록, 사용자 인증 및 일회용 키 생성 프로토콜로 구성된다. 제안한 모델과 기존의 케이블 TV 가입자 관리 시스템인 CAS를 비교 분석하였고, 제안한 모델이 개인 프라이버시 보호가 요구되는 응용과 일회용 패스워드가 요구되는 응용에 적용될 수 있음을 제시하였다.

References

[1] Streaming media, http://en.wikipedia.org/wiki/Streaming_media

[2] Laudon, Kenneth C, Jane P, Management Information Systems 12/E: Managing the Digital Firm, Pearson Education Asia, ISBN-10 : 027375453X

[3] Quirky Business Model, http://www.quirky.com

[4] M. Stamp, Information Security Principles and Practice, Wiley-Inerscience, 2006.

[5] CAS, http://en.wikipedia.org/wiki/Conditional_access#Conditional_access_systems

[6] C. Vivaracho-Pascual, J. Pascual-Gaspar, On the Use of Mobile Phones and Biometrics for Accessing Restricted Web Services, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, pp. 1-10, 2011.

[7] Apple Support, iPhone 5s: Using Touch ID, http://support.apple.com/kb/HT5883

[8] ITU-T X.1088, A Framework for Biometric Digital

Key Generation, ITU-T, 2008.
[9] N. Ratha, J, N. Ratha, J. Connell, R. Bolle,"Enhancing security and privacy in biometric-based authentication systems,"IBM Systems Journal, Vol. 40, No. 3, pp. 614-634, 2001.
[10] D. M. Burton, Elementary Number Theory, McGraw-Hill Science/Engineering/Math, 2010.
[11] Q. Zhang, J. N. Moita, K. Mayes andK. Markantonakis, "The secure and multiple payment system based on themobile phone platform," presented at Workshop Inf. Secur. Appl., JejuIsland, Korea, 2004.
[12] Tepandi, "Wireless PKI Security andMobile Voting, "IEEE Computer, Vol. 43, No. 6, pp. 54-60, 2010.

저자소개

윤 성 현(Sunghyun Yun) **[종신회원]**

- 1994년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학석사)
- 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG전자 중앙연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수

<관심분야> : 모바일 보안, 바이오메트릭 인증, DRM, 전자선거