한국정보전자통신기술학회논문지(jkiiect)'16-10, Vol.9 No.5
논문 16-09-05-439 http://dx.doi.org/10.17661/jkiiect.2016.9.5.439

위치 기반 스마트 관광 서비스를 위한 개인 프라이버시 보호 설계

조국진*, 정은희**

An Individual Privacy Protection Design for Smart Tourism Service based on Location

Cook-Chin Cho*, Eun-Hee Jeong**

요 약 본 논문에서는 위치기반 스마트 관광 서비스를 이용하는 사용자들의 개인 정보 중에서 위치정보를 보호하기 위한 기법을 제안한다. 제안하는 프라이버시 보호 기법은 첫째, 사용자와 관광 서버간에 정보 교환없이 OTK(One Time Key)인 공유 비밀키를 생성하고, 이 공유 비밀키로 데이터를 암호화하여 전달함으로써 사용자와 관광 서버 사이의 메시지 기밀성을 제공한다. 둘째, 사용자와 관광 서버는 사용자 ID, 로그인 시간(timestamp), 그리고 랜덤하게 생성된 난수를 연접하고 해시함수로 해싱하여 OTK를 생성하고, 이 OTK와 XOR 연산을 이용하여 사용자의 위치 정보와 질의어를 암호화하여 전송하므로 사용자와 관광 서버 사이의 메시지 기밀성을 제공한다. 셋째, OTK에 타임스탬프를 추가하여 메시지 재전송공격을 방지한다. 그 결과, 제안하는 개인 프라이버시 보호 기법은 데이터의 기밀성과 사용자의 프라이버시 보호를 제공할 뿐만 아니라 사용자의 위치정보와 행동 패턴 데이터의 안전성도 보장할 수 있다

Abstract This paper proposes the technique to protect the privacy of those who uses Smart Tourism Service based on location. The proposed privacy protection technique (1) generates a shared private key, OTK(One Time Key) without information exchanging Users with a Tourism Server and provides Users and a Tourism Server with message confidentiality by encrypting data with the key, (2) concatenates users' ID, login time(timestamp), and randomly-generated nonce, generates OTK by hashing with a hash function, encrypts users' location information and query by using the operation of OTK and XOR and provides Users and a Tourism Server with message confidentiality by sending the encrypted result. (3) protects a message replay attack by adding OTK and timestamp. Therefore, this paper not only provides data confidentiality and users' privacy protection but also guarantees the safety of location information and behavior pattern data.

Key Words : Data confidentiality, Message confidentiality, One time Key, Privacy protection, Smart Tourism Service

1. 서론

스마트 기기의 확산 및 정보통신기술(ICT: Information Communications Technology) 발전은 사무실에 얽매이지 않아도 되는 자유로운 근무여건을 제공하고, 시·공간의 제한 없이 원하는 관광정보를 습득·공유하게 하는 등 여가환경의 더 나은 기반을 조성하고 있다.

특히, ICT을 기반으로 하는 인터넷과 스마트폰

This work was supported by research fund of Catholic Kwandong University(CKURF-201604300001).
*Department of Tourism Management, Catholic Kwandong University
**Corresponding Author : Department of Regional Economics, Kangwon National University
(jeongeh@kangwon.ac.kr)
Received August 01, 2016 Revised August 23, 2016 Accepted August 24, 2016

을 중심으로 태블릿 PC(Personal Computer)와 통합되어 제공되는 관광정보를 실시간 소통하고 위치정보를 기반으로 내외국인 관광객에게 필요한 맞춤형 서비스를 제공하는 스마트 관광이 본격화되고 있다[1,2].

스마트폰을 활용한 관광서비스의 경우, 서비스 초기에는 교통, 숙박, 지도 등의 단순한 정보를 제공하는데 그쳤다면 현재는 카메라, GPS (Global Positioning System)를 활용하여 증강현실(AR: Augmented Reality)을 접목한 서비스까지 시행되고 있는 만큼 빠르게 발전하고 있다[2].

이렇듯 관광에 ICT를 접목하여 좀 더 나은 여가환경을 제공하고 있는 위치 기반 스마트 관광 서비스가 활성화되고 있지만, 위치 기반 스마트 관광 서비스를 이용하기 위해 제공되는 사용자 위치 정보등과 같은 개인정보로 인해 발생할 수 있는 개인정보 노출과 같은 문제에 대한 해결 방안이 필요하다.

본 논문에서는 사용자와 관광 서버 사이에 전송되는 사용자의 위치 정보와 질의어를 OTK (One Time Key)로 암호화하여 전달하거나 저장함으로써 사용자의 위치와 행동 패턴 노출로 인해 발생할 수 있는 개인 프라이버시 침해를 방지 할수 있는 위치기반 스마트 관광 서비스를 위한 개인 프라이버시 보호 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구를 살펴보고, 3장에서는 제안하는 개인 프라이버시 보호 기법을 설명하고, 4장에서는 제안하는 개인 프라이버시 보호 기법의 분석 결과를 설명한다. 그리고 5장에서 결론을 맺는다.

2. 관련연구

2.1 스마트 투어리즘

스마트 투어리즘은 스마트폰으로 대표되는 스마트 기기를 중심으로 서비스되는 SNS, 애플리케이션 등의 채널을 통해 관광객의 시간, 위치, 상황에 맞게 실시간으로 정보를 활용하면서 이루어지는 관광형태를 말한다. 최근 새롭게 등장한 스마트 투어리즘에서는 경험이라는 요소가 강조가 되기 때문에 경험 또는 체험을 사고 파는 관광분야에서 중요한 패러다임으로 발전하고 있다[2,3].

스마트 투어리즘은 그림 1에서 설명하고 있듯이 스마트폰, 태블릿 PC의 애플리케이션이 주도적으로 활용되는 경향으로 출발하여 현재는 기존의 PC기반 인터넷, 웹 그리고 SNS과 연계하여 각 채널들이 통합적으로 사용되는 추세를 보인다[2].

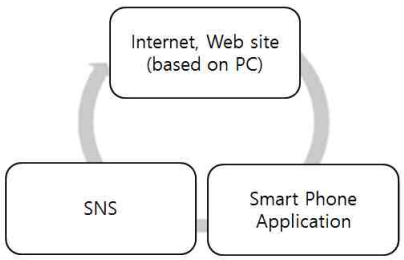

그림 1. 스마트 투어리즘의 일반적인 구조[2]
Fig. 1. The general structure of Smart tourism

스마트 투어리즘의 대표적인 사례로는 첫째, 지도, 교통, 음식점, 숙박 등의 정보를 제공하고 여행지를 추천해주는 한국관광공사의 대한민국구석구석과 Visit Korea가 있다. 둘째, 북한산둘레길, 두발로 2.0 등의 애플리케이션은 오디오, 증강현실 기술을 활용하여 사용자가 어디에 있는지, 무엇을 보고 있는지에 따라 실시간으로 정보를 제공하는 신라역사여행, 국립중앙박물관, 북한산둘레길 등이 있다[2, 4].

즉 사용자는 스마트 투어리즘을 통해 단편적인 정보가 아닌 취향에 맞는 정보만을 선택하여 제공받을 수 있고, SNS과 연결하여 여행 정보를 공유함으로써 여행에 대한 유익한 정보를 제공 받을 수 있다.

2.2 개인 프라이버시 문제

빅데이터 분석은 데이터와 정보의 활용 기회가 증가시키고, ICT 발전으로 인해 고객별 온라인 행위 추적(online behavioral tracking)이 가능해짐에 따라 고객 맞춤형 서비스를 제공하지만, 반면에 개

인 정보와 행위정보 유출로 인한 개인 프라이버시 침해라는 위험이 확대되고 있다[5].

특히, 개인 프라이버시 침해는 빅데이터 분석을 통해 발생하는 가장 큰 위험이다. 기존의 정보 사회에서 수집되는 정보는 주소, 주민번호, 학력, 재산, 병력, 범죄기록, 의료 기록 등의 고정형 정보와 신용카드 내역, 인터넷 활용시간, 접속 사이트 등의 반고정적 정보가 대부분이었으나 빅데이터 분석에서는 개인의 취향, 사고, 행동 패턴뿐만 아니라 감정과 분위기, 본인이 인지하지 못하는 습관이나 버릇까지 수집되고 분석된다. 또한 소셜미디어에 존재하는 메시지뿐만 아니라 접속기록, 검색패턴, 데이터 속성이 기록된 그림자 데이터의 증가는 프라이버시 침해 위험을 더욱 더 확대시킨다[5, 6].

스마트 관광 서비스 또한 스마트 폰에 저장된 개인의 위치정보를 수집하고, 개인이 위치에 따라 맞춤형 관광 정보를 제공하므로 개인 위치 정보와 행위 정보가 유출될 수 있는 가능성이 매우 높다고 볼 수 있다. 따라서, 위치기반 스마트 관광 서비스를 이용하는 사용자들의 위치정보를 보호하기 위한 기법 이 필요하다.

3. 개인 프라이버시 보호 기법 설계

위치기반 스마트 관광 서비스를 사용하는 사용자의 정확한 위치 정보가 데이터베이스 서버에 저장하기 때문에 서비스 이용자가 방문한 장소와 시간을 파악하여 개인 정보를 획득할 수 있으므로 개인 프라이버시가 노출될 가능성이 매우 높다.

본 논문에서는 위치기반 스마트 관광 서비스를 이용하는 사용자들의 개인 정보 중에서 위치정보를 보호하기 위한 기법을 설계한다. 그림 2는 제안하는 개인 프라이버시 보호 기법을 위한 위치기반 스마트 관광 서비스 시스템의 처리절차를 전반적으로 설명하고 있다.

우선, 사용자는 위치기반 스마트 관광 정보 서비스 시스템에 회원 가입하여 사용자의 아이디와 패스워드를 관광 서버에 등록한다. 그리고 관광 서버는 사용자의 위치 정보에 기반을 둔 관광 정보를 수집하고, 그 정보를 사용자의 스마트 폰에 제공한다. 또한 관광 서버는 사용자가 질의한 정보를 사용자의 스마트 폰에 제공하기도 한다.

이때 사용자와 관광 서버는 사용자의 위치 정보와 질의어를 OTK(One Time Key)로 암호화하여 전달하거나 저장함으로써 사용자의 위치와 행동 패턴 노출로 인해 발생할 수 있는 개인 프라이버시 침해를 방지 한다.

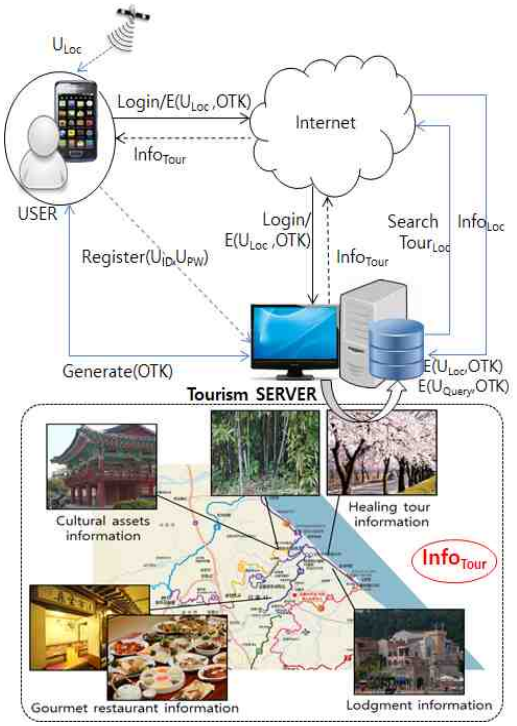

그림 2. 위치기반 스마트 관광 서비스 시스템 구조
Fig. 2. The structure of location based smart tourism service system

3.1 OTK(One Time Key) 생성

사용자의 위치를 기반으로 관광정보를 사용자의 스마트 폰에 제공하기 위해서는 스마트 폰의 GPS를 이용하여 수집한 위치정보를 관광 서버에 전달하거나 사용자가 입력한 질의어를 관광 서버에 전달한다. 이때, 사용자의 위치 정보와 질의어의 노출을 방지하기 위해 암호화하여 전달하거나 관광 서버에 저장하는데 비밀키가 필요하다.

본 논문에서는 사용자가 위치기반 스마트 관광 정보 서비스를 이용하려고 할 때마다 일회용키를 생성하고, 이 일회용키를 비밀키로 사용하도록 제안한다.

본 논문에서 제안하는 OTK(One Time Key)를 생성하는 절차는 다음과 같다.

[단계 1] 사용자는 위치기반 스마트 관광 정보 서비스 시스템에 로그인을 한다. 이때 로그인 시간을 OTK의 timestamp로 이용한다.

[단계 2] 사용자는 랜덤하게 난수인 nonce를 생성한다.

[단계 3] 사용자는 nonce의 무결성 검증을 위해 사용자의 아이디, 패스워드, 그리고 nonce를 연접한 후 해시함수로 해싱하여 hn을 생성한다.

$$hn = h(U_{ID} \| U_{PW} \| nonce)$$

[단계 4] 사용자는 hn, nonce를 관광 서버에 전달하고, 사용자의 ID, 로그인 시간(timestamp), 그리고 nonce를 연접한 후 해시함수로 해싱하여 OTK를 생성한다.

$$OTK_U = h(U_{ID} \| \ Timestamp \ \| nonce)$$

[단계 5] 관광 서버는 사용자로부터 전달받은 hn을 이용하여 nonce의 무결성을 검증하기 위한 hn'를 생성한다.

$$hn' = h(U_{ID} \| U_{PW} \| nonce)$$

이때, 관광 서버가 사용한 사용자의 아이디와 패스워드는 사용자로부터 전달받은 것이 아니라 사용자가 로그인할 때 검증한 아이디와 패스워드를 이용한다.

[단계 6] 관광 서버는 사용자로부터 전달받은 hn과 관광 서버가 5단계에서 생성한 hn'가 일치하는지를 비교한다. 비교 결과가 참이면 관광 서버는 사용자의 ID, 로그인시간, 그리고 nonce를 이용하여 OTK를 생성하고 OTK 생성 절차를 종료한다.

$$OTK_S = h(U_{ID} \| \ Timestamp \ \| nonce)$$

만약, 비교 결과가 거짓이면 OTK 생성에 실패하였음을 사용자에게 알리고 단계 2로 이동한다.

그 결과, 사용자와 관광 서버는 동일한 OTK를 갖게 된다. 사용자는 위치정보와 질의어를 OTK로 암호화하여 관광 서버에 전달하면 관광 서버는 관광 서버의 OTK로 복호화하여 위치기반 관광 정보를 사용자에게 전달하고, 전달받은 위치정보와 질의어를 OTK로 암호화하여 관광 서버 데이터베이스에 저장한다.

3.2 데이터 암·복호화 절차 설계

본 논문에서 제안하는 데이터 암·복호화 절차는 다음과 같다.

[단계 1] 사용자의 스마트폰은 GPS를 이용하여 사용자의 위치 정보를 수집한다.

[단계 2] 수집된 사용자의 위치정보는 OTK를 이용하여 암호화한다. 이때 빠른 처리를 위해 본 논문에서는 XOR 연산 기법을 이용한다.

$$E(U_{Loc}, OTK) = OTK \oplus Position(x, y)$$

[단계 3] 사용자는 암호화된 사용자의 위치정보를 서버에 전달한다.

[단계 4] 관광 서버는 사용자로부터 전달받은 암호문을 서버의 OTK로 복호화한다.

$$\begin{aligned} & E(U_{Loc}, OTK) \oplus OTK \\ & = OTK \oplus Position(x,y) \oplus OTK \\ & = Position(x,y) \end{aligned}$$

즉, 사용자와 관광 서버는 로그인할 때 생성한 각각의 OTK를 이용하여 위치정보와 질의어를 암호화하여 전달하거나 관광 서버 데이터베이스 저장한다.

4. 분석

현재 우리나라뿐만 아니라 세계적으로 인터넷을 기반으로 했던 IT기술이 스마트폰, 소셜 네트워크 서비스(SNS: Social Network Service)의 발전으로 그 영역을 확장하면서 기존의 획일적이고 제한적인 정보에서 탈피하여 경험자들이 직접 정보를 만들고 공유하는 소비자 중심의 스마트 관광이 본격

화 되어가고 있다.

하지만, SNS를 통해 서로의 관광 정보를 공유하거나 위치기반의 스마트 관광이 본격화되면서 사용자의 위치가 노출되거나 행동 패턴이 노출될 가능성도 또한 증가하고 있다.

본 논문에서는 OTK를 설계하고, OTK로 사용자의 위치 정보와 질의어를 암호화하여 처리함으로써 위치기반 스마트 관광 서비스를 위한 개인 프라이버시 보호하는 기법을 제안하였다.

4.1 데이터 기밀성

제안하는 프라이버시 보호 기법은 3.1절에서 사용자와 관광 서버 사이의 일회용 키인 OTK를 생성하고, 이 OTK로 스마트폰이 탐지한 사용자의 위치정보와 사용자가 관광 서버에 요청하는 검색 질의어를 암호화하여 전달함으로써 데이터 기밀성을 제공한다. 특히, 이 OTK는 사용자와 관광 서버가 서로 교환하는 것이 아니라, 사용자와 관광 서버가 각자 보유한 정보로 OTK를 생성하도록 설계함으로써 OTK의 노출을 방지하였다.

4.2 개인 프라이버시 보호

제안하는 프라이버시 보호 기법에서는 사용자의 위치정보와 질의어를 암·복호화시키는 비밀키인 OTK를 사용자가 로그인할 때마다 다르게 생성하도록 설계하였다. 그리고 사용자의 스마트 폰이 수집한 위치 정보를 관광 서버에 전달할 때, 이 OTK로 암호화시켜 전달하도록 설계함으로써 개인 프라이버시를 보호할 수 있다.

또한, 사용자 아이디와 패스워드가 노출된다고 하더라도 관광 서버 데이터베이스에는 OTK로 암호화된 정보가 저장되어 있기 때문에 위치 노출로 인한 프라이버시를 보호할 수 있으며 사용자가 로그인될 때마다 새로운 OTK가 생성되기 때문에 사용자의 프라이버시 침해를 최소화시킬 수 있다.

4.3 재전송 공격 탐지

제안하는 프라이버시 보호 기법에서는 사용자의 ID, 로그인 시간(timestamp), 그리고 랜덤하게 생성된 난수(nonce)를 해싱함수로 해싱하여 OTK를 생성하도록 설계하였다. 따라서, 이 OTK는 사용자가 로그인할 때마다 timestamp가 변경되기 때문에 다르게 생성된다. 따라서 악의의 사용자가 OTK로 암호화시킨 위치정보를 반복적으로 관광 서버에 전달하는 재전송 공격을 방지함으로써 제안하는 프라이버시 보호 기법은 데이터의 안전성을 제공한다고 할 수 있다

5. 결론

본 논문에서는 일회용 비밀키이자 공유 비밀키인 OTK를 설계하고, 이 공유 비밀키 OTK로 사용자의 위치 정보와 질의어를 암호화하여 관광 서버에 전달하거나 관광 서버 데이터베이스에 저장함으로써 위치기반 스마트 관광 서비스를 위한 개인 프라이버시 보호 기법을 제안하였다.

제안하는 프라이버시 보호 기법은 첫째, 사용자와 관광 서버간에 정보 교환없이 OTK인 공유 비밀키를 생성하고, 이 공유 비밀키로 데이터를 암호화하여 전달함으로써 사용자와 관광 서버 사이의 메시지 기밀성을 제공한다.

둘째, 사용자와 관광 서버는 사용자 ID, 로그인 시간(timestamp), 그리고 랜덤하게 생성된 난수를 연접하고 해시함수로 해싱하여 OTK를 생성한다. 그리고 이 OTK를 암호화키로 사용하여 사용자의 위치정보 또는 질의어를 암호화하여 전송하므로 사용자와 관광 서버 사이의 메시지 기밀성을 제공한다.

셋째, OTK는 로그인할 때마다 새로 생성되고고, 이때 OTK에 로그인 시간을 timestamp로 추가하기 때문에 메시지 재전송공격을 방지한다.

그 결과, 제안하는 개인 프라이버시 보호 기법은 데이터의 기밀성과 사용자의 프라이버시 보호를 제공할 뿐만 아니라 사용자의 위치정보와 행동 패턴 데이터의 안전성도 보장할 수 있다.

REFERENCES

[1] Jeong-Hee Lee, Tak-Gyun Ahn, Hong-Min Kim, Tourism Information System focusing on smart tourism, *Saromi*, 2012.

[2] Chulmo Koo, Seung-Hun Shin, Kee-Hun Kim, Namho Chung, "Analysis of Case Study for Smart Tourism Development : Korea Tourism Organization's Smart Tourism Case," *JOURNAL OF THE KOREA CONTENTS ASSOCIATION*, Vol.15, No.8, pp.519-531, August, 2015.

[3] E. Sternberg, "The Iconography of the Tourism Experience," *Annals of TourisM Research*, Vol.24, No.4, pp.951-969, April, 1997.

[4] Korea Tourism Organization, Korea Tourism Organization, *Internal management assessment report*, 2012.

[5] Sang-Chan Kim, Jae-Jung Kang, "Online Marketing and Protection of Personal Data in the Age of Big data," *Law and Policy*, Vol.21, No.1, pp.97-126, March, 2015.

[6] Sang-oh Yun, "Big data and risk information society," *Communication Books*, pp.59, June, 2013.

저자약력

조 국 진(Cook-Chin Cho) [정회원]

- 1982년 8월 : 경희대학교 경영대학원 관광경영학과 (경영학석사)
- 1994년 2월 : 경기대학교 대학원 관광경영학과 (경영학박사)
- 1983년 3월 ~ 1984년 2월 : 진주실업전문대학 관광과 전임강사
- 1984년 3월 ~ 1991년 2월 : 경북실업전문대학 관광과 부교수
- 1991년 3월 ~ 현재 : 가톨릭관동대학교 관광스포즈대학 관광경영학과 정교수

<관심분야>
경영학, 스마트 관광, 빅데이터

정 은 희(Eun-Hee Jeoong) [종신회원]

- 1998년 2월 : 관동대학교 일반대학원 전자계산공학과 (공학석사)
- 2003년 2월 : 관동대학교 일반대학원 전자계산공학과 (공학박사)
- 2003년 9월 ~ 현재 : 강원대학교 지역경제학과 교수

<관심분야>
전자상거래 보안, 빅데이터, 헬스케어, IoT 보안