http://dx.doi.org/10.14400/JDC.2015.13.8.315

건강정보를 이용한 OTP 생성 방식 설계

추연수*, 강정호*, 김경훈**, 박재표***, 전문석*
숭실대학교*, 강동대학교**, 숭실대학교 정보과학대학원***

Designed OTP Generation Method Using Health Information

Yeun-Su Choo*, Jung-Ho Kang*, Kyoung-Hun Kim, Jea-Pyo Park***, Moon-Seog Jun***

Dept. of Computer Graduate School Soongsil University*

Dept. of Computer Information, Gangdong University, Seoul, Korea**

Graduate School of Information Sciences Soongsil University***

요 약 온라인 서비스에서 사용자 인증은 정확하고 안전한 서비스를 위해 꼭 필요하다. 이러한 사용자 인증을 위해 OTP(One Time Password)가 많이 활용된다. OTP는 일회성이라는 특성을 만족시키기 위해 분실 및 망실의 위험이 있는 OTP 발생기나 보안카드 등을 사용하여 OTP 생성을 위한 연계 정보를 발생시키거나 최종 OTP 값을 생성한다. 본 논문에서는 u-Health care 시스템에서 수집되는 건강정보를 이용하여 OTP 발생기와 보안카드를 사용하지 않는 OTP 생성방식을 제안한다. 제안하는 방식은 웨어러블 기기를 통해 수집한 건강강보를 OTP 생성에서 사용하는 연계 정보로 활용하는 방식이다. 제안하는 방식으로 생성한 OTP는 같은 인증번호가 얼마나 자주 생성되는지를 확인하는 충돌내성 실험에서 기존의 OTP 생성방식과 비슷한 결과를 나타내어 다양한 온라인 서비스에서 사용될 수 있을 것으로 판단된다.

주제어 : OTP, 융복합 사용자 인증, 건강정보, 충돌내성, u-Health

Abstract User Authentication in Online service is essential for accurate and safe service. For this user authentication, One Time Password(OTP) is frequently used. To satisfy one-time-use characteristic of OTP, Offset information to generate OTP or final OTP value get generated through OTP generator or security card which could be lost. In this study, OTP generation method that bypasses OTP generator or security card by using health information collected from u-Health care system is proposed. Suggestion is that health information collected through wearable devices get utilized to offset information that are applied in OTP generations. OTP generated using suggested methods showed similar results than current OTP generation methods in the collision resistance test which tests how often it generate same authentication numbers, this implies that new proposed method can be applied to various on-line services.

Key Words : OTP, Convergence User Authentication, Health Information, Collision resistance, u-Health

Received 25 June 2015, Revised 28 July 2015
Accepted 20 August 2015
Corresponding Author: Moon seog Jun(Soongsil University)
Email: mjun@ssu.ac.kr

ISSN: 1738-1916

1. 서론

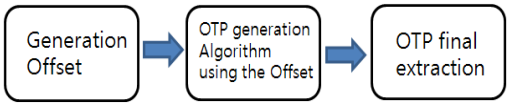
인터넷 뱅킹, 인터넷 쇼핑과 같은 온라인 서비스에서 사용자 인증은 갈수록 중요한 문제이다. 공격자에게 자신의 정보를 노출시키지 않으면서 안전한 사용자 인증을 위해서 공인인증서의 사용, two-channel 인증[1], two-factors 인증[2], OTP(One Time Password)[3,4,5]는 사용자 인증을 위해 생성하는 패스워드를 매번 달리 생성하여 사용자 인증에 사용하고 한번 생성된 패스워드는 다시 사용하지 않는 인증방식으로 인증번호가 노출되더라도 안전하게 사용할 수 있는 방법이다. 하지만, OTP는 다양한 연계정보를 생성하기 위해서 사용자는 OTP 발생기, 보안카드와 같은 별도의 인증 보조 도구를 소지, 관리해야 한다. 또한 이러한 도구들을 분실하거나 물리적인 충격에 의해 고장, 망실되었을 때는 OTP를 사용하지 못하거나 공격자에게 악의적인 목적으로 사용될 가능성도 있어 주의가 필요하다. 이에 본 논문에서는 u-Health care 시스템[6,7,8]에서 수집된 건강정보를 이용한 OTP 생성방식을 제안한다. u-Health care 시스템은 원격에서 사용자들의 건강 정보를 수집하여 건강상태를 체크하고, 진단, 나아가 치료도 가능하게 하는 시스템으로 USN[9] 기술을 바탕으로 구현된다. 이러한 u-Health care의 연구는 치매환자의 돌봄[10], 노인 돌봄 시스템[11], 병원내 진료, 경영지원까지 통합하는 통합지원시스템[12]을 구축하기 위한 연구 등을 다양하게 진행되고 있다. 이 때 다양한 웨어러블(wearable) 기기들이 사용자의 건강정보 수집을 위해 사용된다. 웨어러블 기기들이 수집하는 사용자의 건강정보는 다양한 생활패턴으로 시시가각 변화하기 때문에 OTP 생성 시 중요하게 사용되는 연계정보를 대신할 수 있는 좋은 정보가 될 수 있다.

2장에서는 관련 연구로 기존의 OTP의 생성 방식을 기술하며, 3장에서는 제안하는 상요자의 건강 정보를 이용한 OTP 생성 방식에 대해서 기술하고, 4장은 비교분석, 5장은 결론으로 기술한다.

2. 관련연구

2.1 OTP 설계방식

OTP는 온라인상에서 상대를 인증하기 위한 수단으로 많이 사용된다. OTP는 현재 핸드폰을 이용한 간편 결제, 인터넷 뱅킹 등에서 사용되고 있다. 이러한 OTP는 프로세스는 [Fig. 1][13]과 같다. 첫 단계는 매번 다른 OTP를 얻기 위해서 연계정보를 생성하는 단계이며, 두 번째 단계는 생성된 연계정보를 암호화 알고리즘을 이용하여 암호문을 생성하는 단계이다. 마지막 단계는 생성된 암호문을 OTP 추출 함수를 이용하여 최종 OTP를 생성하는 단계이다[13]. 이러한 프로세스를 가진 OTP 생성 알고리즘은 여러 가지 방식이 존재하지만 가장 많이 쓰고 있는 방식은 이벤트 동기화 방식, 시간동기화 방식, 질의-응답 방식이다.



[Fig. 1] OTP Generation Process

2.1.1 이벤트 동기화 방식

이벤트 동기화 방식은 인증을 요청하는 사용자가 이벤트를 발생시켜 서버에 이벤트 값을 전달하고 이벤트의 특정값을 OTP 생성의 연계정보로 활용하는 방식이 이벤트 동기화 방식이다[14].

2.1.2 시간 동기화 방식

시간 동기화 방식은 계속 변화하는 시간 정보를 연계정보로 활용하는 방식인데, 사용자가 특정한 시점에서 OTP를 발생시켜 인증을 서버에 요청하면, 서버도 사용자가 요청한 동일한 시각 정보를 이용하여 OTP를 발생시켜 인증하는 방식이다. 이 방식은 OTP 발생기와 서버간의 OTP 생성 방식이 일치하기 때문에 사용자가 인증을 요청한 시간이 노출되면 OTP가 노출될 수 있다는 단점이 있다.

2.1.3 질의 응답 방식

질의 응답 방식은 인증기관과 사용자가 미리 합의된 내용의 질문을 서버가 보관하고 사용자의 인증 요청에 미리 합의된 질문을 사용자에게 질의하고 이에 답변하여 연계 정보를 생성한 후 OTP를 생성하는 방식이다. 기존

의 인터넷 뱅킹 시스템에서 미리 배포한 보안 카드의 번호를 질의한 후 질의에 대한 답을 사용자가 입력하였을 때 OTP를 생성하여 인증하는 방식이 이에 속한다. 이 방식은 합의된 질의 내용에 대한 한계가 있으며, 질의 내용에 대한 정보가 노출되면 심각한 보안상의 문제가 발생하는 단점이 있다.

2.2 OTP 추출 알고리즘

OTP 추출 알고리즘은 연계정보를 이용하여 생성된 암호문에서 최종 OTP를 추출해내는 알고리즘을 말한다[13]. 이 알고리즘은 정적 추출 알고리즘과 동적 추출 알고리즘이 있으며, 정적 추출 알고리즘은 생성된 암호문에서 OTP를 생성하기 위해서 항상 같은 순번의 Byte를 추출하는 방법이며, 동적 추출 알고리즘은 추출점을 계산하기 위해서 OTP 생성 알고리즘을 수행한 결과에서 추출점 정보를 찾는 방법이다[13].

3. 제안하는 건강 정보를 이용한 OTP 생성 방식

2장에서 언급한 단점을 해결하기 위한 건강 정보를 이용한 OTP 생성 방식을 제안한다. 제안하는 OTP 생성 방식은 u-Health care 시스템이 구현되어 u-Health care 시스템을 사용자가 사용한다는 가정을 전제로 한다. 다양한 웨어러블 기기와 가정마다 갖추어진 u-Health care 시스템을 위한 건강 정보 수집 기기들을 통해 수집된 건강 정보가 가정의 u-Health care 센터에 모이게 된다. OTP를 생성할 수집된 다수의 건강 정보는 <Table 1>과 같이 저장된다.

〈Table 1〉 Health Information

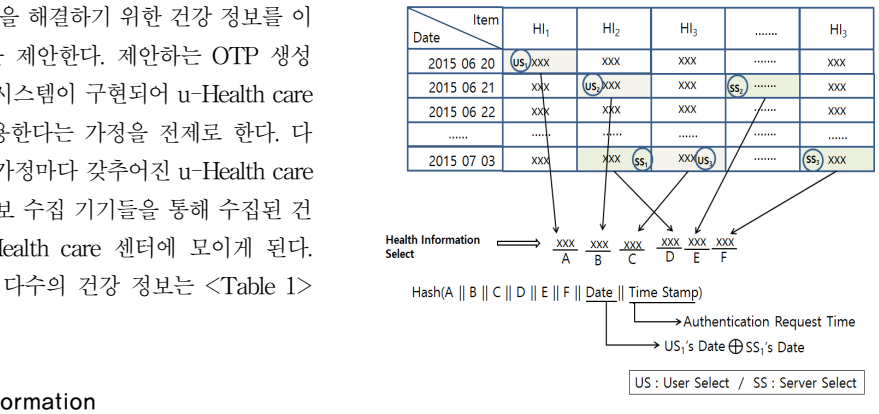
Item / Date	Weigh (kg)t	Blood Pressure (mmhg)		...
		SBP	DBP	...
2015 06 30	86.4	115	78	...
2015 07 01	86.2	119	80	...
2015 07 02	86.0	113	76	...
2015 07 03	86.3	116	79	...
...	...	...	...	...

이 건강 정보는 해당 날짜 정보와 Time Stamp와 함께 OTP 생성을 위한 연계 정보로 활용되고, OTP 생성 알고리즘을 이용하여 OTP 값을 생성한 후, 날짜 정보와 Time Stamp를 이용하여 특정 바이트를 추출한 후 최종 OTP 값이 만들어진다.

3.1 건강 정보를 이용한 OTP 생성

OTP 생성은 2단계를 거쳐 생성된다. 1단계는 연계정보 생성, 2단계는 OTP 생성 알고리즘을 이용한 OTP 값 생성이다.

① 1단계 연계 정보 생성 : OTP 생성을 위해 6개의 건강정보가 선택되며, 6개의 정보는 사용자에 의해서 3개, 인증서버에서 랜덤하게 3개 결정된다. 6개의 건강정보는 OTP 생성이 요청된 시간 값(Time Stamp)과 날짜정보와 함께 연계정보로 활용된다. 여기서 날짜정보는 사용자에 의해서 선택된 건강정보의 첫 번째 건강정보의 날짜와 인증서버에 의해서 선택된 건강정보의 첫 번째 건강정보의 날짜가 XOR 연산된 값이다. 이러한 3가지 정보(건강정보, 시간정보, 날짜정보)연접하여 Hash 함수를 거쳐 OTP 연계정보를 생성한다.



[Fig. 2] Generation Offset Information

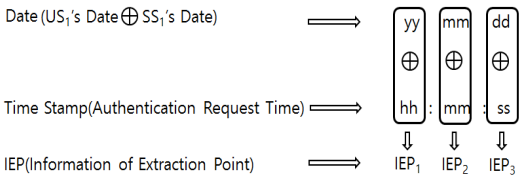
② 2단계 OTP 생성 알고리즘을 이용한 OTP 값 생성 : 1단계에서 생성된 연계정보는 OTP 생성 알고리즘을 이용하여 암호문을 생성한다. 본 논문에서는 생성 알고리즘으로 256비트 AES 알고리즘을 이용하여 암호화한 후 OTP값을 생성한다. 256비트의 key 값은 서버와 사전 협의 하에 Key를 나누어가진다.

3.2 최종 OTP 추출 방식

3.1절에서 생성된 OTP 값에서 최종 OTP값을 추출하기 위해 건강정보 사용자 선택날짜와 서버 선택날짜, 인증 서버에 인증을 요청한 시간(Time Stamp)을 활용한다.

서버와 사용자의 건강정보 선택날짜와 사용자가 인증을 요청한 시간을 XOR 연산한 값에 mod 연산하여 추출점을 구한다. 최종 OTP 추출 방식은 2단계로 구성되어 있다.

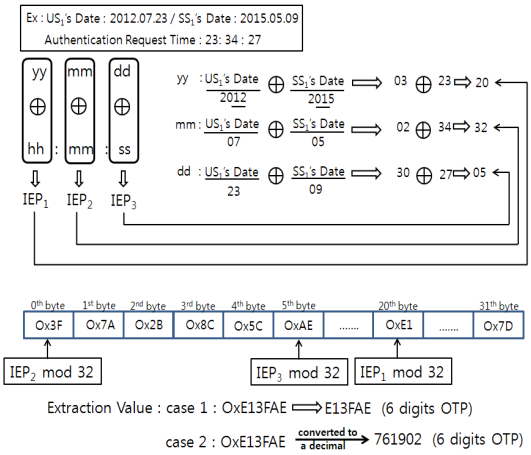
① 추출지점 선정 단계 : 건강정보 선택날짜는 YY년 MM월 DD일로 표현이 가능하며, 인증 요청시간은 hh시 mm분 ss초로 표현이 가능하다. 서버의 건강 정보 선택날짜와 사용자의 건강정보 선택 날짜의 각 성분끼리 XOR연산하여 결과를 얻는다. 이 결과의 각 성분과 사용자가 서버에 인증을 요청한 시간의 각 성분을 다시 한번 XOR 연산하여 추출지점(IEP : Information of Extraction Point) 3개를 선정한다. [Fig 3]은 이 과정을 그림으로 보인 것이다.



[Fig. 3] Selection of Extract Point

② 최종 OTP 결정 단계 : 본 단계는 IEP 3개를 통해 OTP 생성알고리즘으로 생성한 OTP 생성 값에서 최종 OTP를 선정하는 단계이다. 이전 단계에서 선정된 IEP 3개와 OTP 생성 값의 Byte 순서를 매칭하여 해당 Byte의 값을 OTP 최종 값으로 결정한다. 선정된 IEP는 32byte의 결과 값에 매칭시키기 위해 mod 연산을 거친다. [Fig. 4]는 이 과정을 그림을 통해 예를 들어 보인 것이다.

3개의 IEP가 각각 20, 30, 05로 정해졌을 때, 각각을 32로 mod 연산을 하면, 20, 0, 05로 값이 변경되며, 차례로20번째, 0번째, 5번째 byte가 최종 OTP로 결정된다.



[Fig. 4] Gerneration of OTP(One Time Password)

3.1 절의 단계를 거쳐 생성된 OTP 생성 값이 그림의 byte와 같다고 할 때, OTP 생성은 최종 E13FAE 또는 761902이다.

4. 비교분석

제안하는 OTP 생성방식은 기존의 OTP 생성 방식에서 사용하였던 OTP 발생기, 보안카드와 같은 보조 도구들이 필요하지 않다. 물론 u-Health care 센터에 모이는 사용자의 건강정보를 열람하기 위해서 u-Health care 센터에 접속이 필요하지만 OTP 발생기 등을 소지하고 있어야 하는 기존의 방식보다는 더 간편해졌다. 또한 개인의 건강정보가 u-Health care 시스템에 의해 많이 수집된다면 연계정보의 랜덤성은 더욱 커진다. 조금의 변화에도 다른 결과를 보여주는 Hash 함수를 특성을 고려하면 매일 매일 변화하는 건강정보는 아주 좋은 연계정보가 될 수 있다. 또한 OTP는 6자리 이상의 숫자 또는 문자로 구성되어 있어야 하는 표준도 만족한다. 더욱이 3.2절에서 제한한 OTP 추출지점 정보를 4개 이상으로 늘리면 6자리 이상의 인증번호도 충분히 가능하다.

OTP 생성 방식은 연계정보를 이용하여 OTP를 생성하게 된다. 연계정보는 선택되어진 후에 Hash 함수를 거치게 된다. 연계정보의 랜덤성은 OTP의 충돌가능성을 낮추게 된다. MD5(Message Digest 5)[15], SHA(Secure Hash Algorithm)[16]와 같은 Hash 함수는 어떤 값을 이

용하여 수행하느냐에 따라 매번 다른 값을 가질 수 있다. 본 논문에서 제안하는 OTP 생성방식은 연계정보를 건강정보로 활용하고 있게 때문에 상당히 다양한 건강정보를 활용할 수 있다. u-Health care 시스템과 연계된 디바이스들과 간단한 웨어러블 기기를 이용하여 u-Health care 센터로 다양한 건강정보가 보이게 되는데 향후 더 많은 디바이스들이 u-Health care 시스템과 연계된다면 더 많은 연계정보를 확보할 수 있을 것을 판단된다. 현재 제안하는 OTP 생성방식에서 활용할 수 있는 사용자의 건강정보는 대략 7~8개 수준이다. 7~8개의 건강정보도 매일 매일 오랜 시간동안 축적되면 선택할 수 있는 경우의 수는 대단히 많아진다. 이렇게 많은 연계정보를 이용할 수 있는 제안하는 OTP 생성 방식은 매우 다양한 인증번호를 생산해낼 수 있다.

OTP는 한번만 사용하고 폐기되어야 하기 때문에 한번 사용된 인증번호가 중복되어 사용된다면 보안상 큰 위험요소가 된다. 따라서 기존의 OTP 생성 방식과 제안하는 OTP 생성방식의 충돌내성 실험을 진행하였으며, 실험의 결과는 <Table. 2>와 같다. 충돌내성 실험은 1,000개의 인증번호를 생성하는 동안 몇 개의 충돌이 생기는지 실험하였다.

〈Table 2〉 Result of Collision resistance

Generation Time	Existing Methods	Proposed Methods
1000	0	1
2000	1	1
3000	1	1
4000	2	2
5000	3	2
6000	3	3

제안하는 OTP 생성방식은 기존의 방식과 유사한 충돌내성을 가지고 있는 것으로 나타났다. 하지만, 제안하는 OTP 생성방식은 u-Health care 시스템의 사용 기간이 늘어나면 연계정보로 활용할 수 있는 경우의 수, 즉 사용자의 건강정보는 늘어난다. 이에 따라 기존의 OTP 생성방식보다 충돌내성 실험에서 좋은 결과를 도출할 수 있다.

5. 결론

기존의 OTP의 번거로움들을 해결하고 u-Health care 시스템에서 수집된 정보들을 이용하여 쉽게 사용할 수 있는 OTP 생성 방식을 본 논문에서 제안하였다. 4장에서 기술한 것처럼 제안된 OTP 생성 방식은 기존의 OTP보다 충돌내성 실험에서 좋은 결과를 보였다. 또한 기존의 OTP가 가지고 있는 OTP 발생기, 보안카드 등의 OTP 보조 수단들을 소지하지 않아도 된다는 장점이 있다. 따라서 본 논문에서 제안한 건강정보를 이용한 OTP 생성 방식은 기존의 OTP 알고리즘을 대체할 수 있을 것으로 판단된다. 하지만 본 논문에서 제안된 OTP 생성방식은 u-Health care 시스템이 적용되어 있어야 한다는 한계가 있으며, 연계정보로 사용하는 건강정보는 사용자의 개인정보이므로 이러한 개인정보를 외부로 유출시키지 않을 수 있는 방안의 추가적인 연구가 필요하다.

REFERENCES

[1] Han-na You, Jae-Sik Lee, Jung-Jae Kim, Jae-Pio, Moon-Seog Jun, A Study on the Two-Channel Authentication Method which Provides Two-way Authentication using Mobile Certificate int Internet Banking Environment, The Journal of Korea Information and Communications Society, Vol. 36, No. 8, pp. 939-946, 2011.

[2] Shirly Lee, Ivy Ong, HyoTaek Lim, HoonJae Lee, International Journal of KIMICS, Vol. 8, No. 4, pp 427-432, 2010.

[3] DOI: http://www.ietf.org/rfc/rfc2289.txt

[4] DOI: http://www.ietf.org/rfc/rfc4226.txt

[5] DOI: http://www.ietf.org/rfc/rfc6238.txt

[6] TTA, u-Health Service Reference Model , TTA, 2010

[7] TTA, Information Security Reference Model for u-Health Service, TTA, 2011.6

[8] So-Yeon Min, Byung-Wook Jin, "Disign of Integrated Authentication Scheme for Safe Personal Information Management in a U-Health Environment", Journal of the Korea Academia-

Industrial cooperation Society, Vol 15, No 6, pp.3865-3871, 2014

[9] M. Tubaishat, S. Madria, Sensor Networks: An Overview, IEEE Potentials, Vol. 22, Issue. 2, 20-23, 2003.

[10] Dong-Min Shin, Dong-Il Shin, Dong-Kyoo Shin, Development of u-Health Care System for Dementia Patients, The Journal of Korea Information and Communications Society, Vol. 38C, No. 12, pp.1106-1113, 2013.

[11] Hyeon-Suk Jang, Tae-Hak Ban, Se-Cheol Jang, Hoe-Kyung Jung, Journal of the Korea Institute of Information and Communication Engineering, Vol. 17, No. 11, pp. 2693-2698, 2013.

[12] Yun-Young Sok, Seok-Hun Kim, Integrated Medical Information System Implementation for the u-Healthcare Service Environment, Journal of the Korea Contents Association, Vol. 14, No. 5, pp.1-7, 2014.

[13] TTA, Algorithm Profile for a one-time password, TTA, 2012.12

[14] TTA, Road map for the one time password standards,TTA, 2011.12

[15] R. Rivest "The MD5 message digest alrogithm." Requests for Comments(RFC) 1321, 1992.

[16] Behrouz A. Forouzan, Cryptography and Network Security(International Edition), pp.377-398, McGraw-Hill, 2008.

추 연 수(Choo, Yeun Su)

- 2003년 8월 : 호서대학교 컴퓨터 공학과(공학사)
- 2005년 8월 : 숭실대학교 컴퓨터학과(공학석사)
- 2005년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 관심분야 : 컴퓨터통신, 정보보안, 사용자 인증, 암호학
- E-Mail : lets-priase@hanmail.net

강 정 호(Kang, Jung Ho)

- 2000년 2월 : 서울과학기술대학교 컴퓨터공학과(공학사)
- 2002년 2월 : 서울과학기술대학교 컴퓨터공학과(공학석사)
- 2013년 12월 : 숭실대학교 컴퓨터학과 박사
- 관심분야 : NFC, Secure Coding
- E-Mail : kjh7548@naver.com

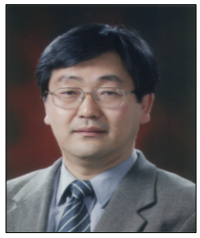
김 경 훈(Kim, Kyoung Hun)

- 2000년 2월 : 삼육대학교(이학사)
- 2002년 8월 : 경희대학교 전자계산공학(공학석사)
- 2012년 9월 : 경희대학교 전자계산공학(공학박사)
- 2012년 3월 ~ 현재 : 강동대학교 컴퓨터정보과 조교수
- 관심분야 : 형상관리, 의료시스템, 콘텐츠
- E-Mail : iioii@gangdong.ac.kr

박 재 표(Park, Jae Pyo)

- 1998년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2004년 9월 ~ 2009년 8월 : 숭실대학교 정보미디어기술연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학 교수
- 관심분야 : 컴퓨터 통신, 정보보안, 포렌식, 암호학
- E-Mail : pjerry@ssu.ac.kr

전 문 석(Jun, Moon Seog)



- 1989년 2월 : University of Maryland Computer Science (공학박사)
- 1991년 2월 : New Mexico State University physical Science Lab 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수
- 관심분야 : RFID, PKI
- E-Mail : mjun@ssu.ac.kr