http://dx.doi.org/10.14400/JDC.2014.12.2.249

행렬기반 RFID 인증 프로토콜의 효율성 및 안정성 분석

신효영*, 황치곤**, 정계동***
경복대학교 IT보안학과*, 광운대학교 컴퓨터과학과**, 광운대학교 교양학부***

An analysis of effectiveness and safety about matrix-based RFID authentication protocol

Hyo-Young Shin*, Chi-Gon Hwang, Kye-Dong Jung*****
Dept. of IT Security, Kyungbok University*
Dept. of Computer Science, Kwangwoon University**
Div. of General Education Information Engineering, Kwangwoon University***

요 약 RFID 시스템은 교통, 출입통제 비롯한 여러 분야에서 활용되고 있다. RFID 시스템에 대한 보안위협 또한 증가하여 정보보안에 대한 연구가 진행되고 있다. 본 논문에서는 행렬기반 RFID 인증 프로토콜을 제안하고 기존에 제안된 프로토콜과 효율성을 비교하고 안전성을 분석한다. 제안된 인증 프로토콜은 도청, 재전송 등의 공격에 안전하며, 서버의 계산량을 줄여 성능면에서 효율이 우수한 장점을 갖는다.

주제어 : RFID, 인증, 행렬, 정보보안

Abstract RFID system is used in several fields such as traffic and access control. The study about RFID security is actively progressed as security threat has been increased. This paper suggests matrix-based authentication protocol. And we analyze the safety of authentication protocol and compares the effectiveness of the protocol with other authentication protocols. The suggested authentication protocol secures from wiretapping attack, replay attack, and spoofing attack, and reduces overload of back-end database so that has efficient performance.

Key Words : RFID, Authentication, Matrix, Information Security

1. 서론

RFID(Radio-Frequency Identification) 기술이란 전파를 이용해 먼 거리에서 정보를 인식하는 기술을 의미한다. RFID 시스템에는 RFID 태그와, RFID 리더가 필요하다. 태그는 안테나와 집적 회로로 이루어지는데, 집적 회로 안에 정보를 기록하고 안테나를 통해 리더에게 정보를 송신한다. 이 정보는 태그가 부착된 대상을 식별하는데 이용된다. 쉽게 말해, 바코드와 비슷한 기능을 하는 것이다. RFID가 바코드 시스템과 다른 점은 빛을 이용해 판독하는 대신 전파를 이용한다는 것이다. 따라서 바코드 판독기처럼 짧은 거리에서만 작동하지 않고 먼 거리

Received 30 December 2013 , Revised 30 January 2014
Accepted 20 February 2014
Corresponding Author: Kye-Dong Jung(Div. of General Education Information Engineering, Kwangwoon University)
Email: gdchung@kw.ac.kr

ISSN: 1738-1916

에서도 태그를 읽을 수 있으며, 심지어 사이에 있는 물체를 통과해서 정보를 수신할 수도 있다.[1,5,6]

데이터베이스는 태그에 관련된 정보를 저장하고 관리하는 역할을 수행한다. 데이터베이스는 연산능력이 낮은 리더나 태그를 대신하여 연산을 수행하기도 하며 리더로부터 수신한 태그의 정보를 통해 태그를 식별하고 수신한 정보의 정확성을 판별하는 역할을 수행한다.

보안 기능이 마련되지 않은 RFID 시스템은 도청, 스푸핑 등의 공격에 취약할 수 있다. 시스템에 대한 공격으로 사용자 정보 등의 자료가 유출될 수 있으므로 시스템 보안장치가 필요하다.

RFID 시스템 보안을 위해 기존에 제안된 기술에는 물리적 보안을 위해 킬 태그, 페러데이 케이지, Active Jamming, Blocking 태그 등이 있다. 도청방지를 위해서는 silent tree-walking, 재암호화 방법 등이 제안되었다. 인증 및 접근제어를 위해 해쉬함수, 암호 알고리즘을 이용하는 방법과 XOR 연산을 이용하는 방법이 제안되었다[1,2,3,9,10].

지금까지 제안된 대부분의 인증 프로토콜은 백엔드 데이터베이스가 태그를 인증하기 위해 데이터베이스에 저장된 모든 태그의 식별정보를 확인해야 하는 절차가 포함되어 있어서 데이터베이스에 많은 연산량을 요구하는 단점이 있다.

기존에 제안된 인증 프로토콜에는 여러 가지 종류가 존재한다. Lee와 Ahn은 행렬기반의 RFID 인증프로토콜을 제안하였다[7]. 제안된 프로토콜은 태그의 계산량을 감소시켰고, 통신 부하가 줄었으며, 사용자 프라이버시 등의 장점을 제공한다. Yoon과 Ha 등은 행렬기반프로토콜의 취약점을 보완하고자 상호인증이 가능한 인증 프로토콜을 제안했다[8]. 그러나 이 방법은 데이터베이스에서 모든 태그에 대한 연산을 요구하여 태그 수 증가에 따라 데이터베이스 시스템에 부하가 증가되는 단점이 있다.

Shin과 Kim 등은 전체적인 RFID 시스템의 성능을 향상시키기 위해 백엔드 데이터베이스의 연산량을 줄일 수 있는 인증 프로토콜을 제안하였다.[4,9] 본 논문에서는 이 인증 프로토콜의 안전성을 분석하고 효율면에서 다른 인증프로토콜과의 차이점을 분석한다.

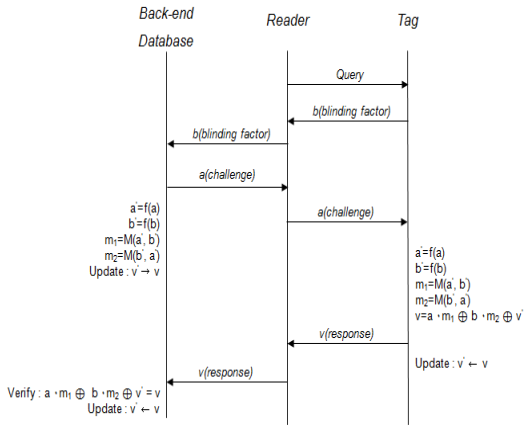
2. 관련 연구

RFID 시스템의 구조와 보안 요구사항, 기존에 수행된 관련 연구들은 다음과 같다.

2.1 Lee와 Ahn의 프로토콜

Lee와 Ahn은 행렬을 기반으로 하는 RFID 인증 프로토콜을 제안하였다. 인증프로토콜을 수행하기 전의 초기화 단계에서 태그와 리더 사이에는 비밀 행렬 $A(n\times n)$ 와 이전 세션에서 계산된 랜덤 값 v'를 공유하고 있다. 이 프로토콜에서는 비밀 행렬 A의 크기 k비트를 증가시켜 $n\times n$ 개수의 소행렬을 생성시켜 복잡도를 높일 수 있다.

Fig. 1은 Lee와 Ahn이 제안한 인증 프로토콜의 인증과정을 보여준다. 이는 상호인증을 제공하지 않아 트래픽분석공격, 위치트래킹공격, 서비스거부공격 등에 취약함을 보인다[7].

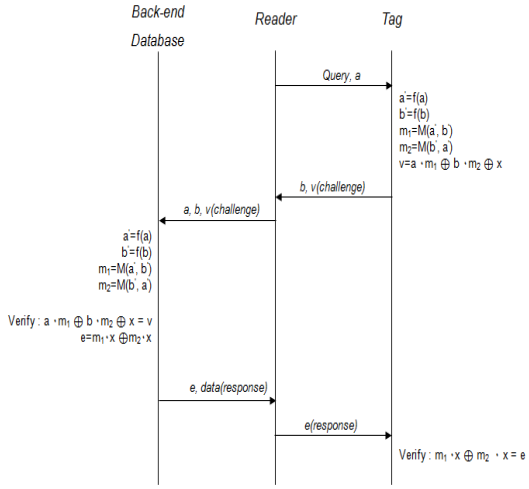


[Fig. 1] Lee and Ahn's matrix-based RFID authentication protocols

2.2 Yoon, Ha, Yoo의 상호인증 프로토콜

Yoon, Ha, Yoo는 Lee 와 Ahn이 제안한 프로토콜의 보안 취약점을 해결하기 위해 상호인증이 가능한 프로토콜을 제안하였다[6].

이 프로토콜에서는 초기화 단계에서 태그와 리더 사이에는 비밀 행렬 $A(n\times n)$ 와 비밀값 x를 공유하고 있다고 가정한다. Fig. 2는 상호인증 프로토콜의 단계를 보여준다.



[Fig. 2] Matrix-based RFID mutual authentication protocol

이 인증 프로토콜은 상호인증을 제공하여 트래픽 분석공격을 비롯한 보안 문제점을 해결하였다. 그러나 데이터베이스에 저장된 태그들의 비밀값 x를 모두 대입하는 연산을 수행하여 수신된 v값과 일치하는지를 모든 인증 과정에서 수행해야한다. 이러한 부하는 시스템이 확장되어 태그 수가 증가할수록 부하가 증가되는 단점이 있다.

3. 제안 프로토콜

3.1 용어 정의

제안 프로토콜에서 사용하는 용어들을 다음과 같이 정의한다.

- $Query$: 태그의 응답을 요청하는 리더의 질의어
- TID : 태그의 ID
- $\oplus$: 배타적 논리합 연산

3.2 초기화 단계

제안한 프로토콜을 실행하기 전에 데이터베이스, 리더, 태그에서 초기화해야할 사항들은 다음과 같다.

① 모든 태그에 자신의 식별자로 비밀정보인 TID 값을 저장한다.

② 모든 태그와 데이터베이스는 비밀 키 정보인 x 값을 공유한다.

③ 태그와 데이터베이스 간에는 $n \times n$ 크기 비밀 행렬 $A(=k$ 비트)를 공유한다.

④ 데이터베이스에는 모든 태그의 식별자인 TID 값과 TID별로 할당된 비밀키 정보 x값을 저장한다.

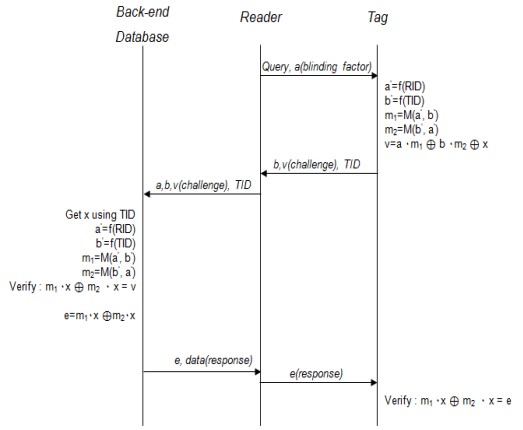
3.3 제안 프로토콜 실행 절차

단계 1. 리더 → 태그 : $Query, a(blinding\,factor)$

리더는 질의어와 함께 랜덤값 $a \in_R (0,1)^k$를 생성하여 태그로 전송한다.

단계 2. 태그 → 리더 : b, v, TID

태그는 리더로부터 질의어와 a를 수신한 후 행렬 A의 소행렬 위치 $a' = f(RID)$, $b' = f(TID)$를 계산한다. 여기서 함수 $f()$는 a와 b가 n보다 작거나 같다는 조건을 만족시키기 위하여 사용한다. 데이터베이스와 공유한 비밀행렬 A로부터 소행렬 $m_1 = M(a', b')$과 $m_2 = M(b', a')$를 생성한다. 생성된 소행렬 m_1과 수신한 a를 $a \bullet m_1$과 같이 AND 연산하고, 소행렬 m_2와 b를 $b \bullet m_2$와 같이 AND 연산한다. 마지막으로 공유 비밀값 x와 XOR 연산을 하여 $v = a \bullet m_1 \oplus b \bullet m_2 \oplus x$를 계산한 후 리더로 TID와 함께 전송한다.



[Fig. 3] Proposed protocol architecture

단계 3. 리더 → 데이터베이스 : a, b, v, TID

리더는 태그로부터 수신한 v를 a, b, TID와 함께 데이터베이스로 전송한다.

단계 4. 데이터베이스 → 리더 : $e, data$

데이터베이스는 저장된 x 값 중에서 리더로부터 수신한 TID에 해당하는 x를 찾는다. 이후 소행렬 위치를 $a' = f(a)$, $b' = f(b)$계산하고, 소행렬 $m_1 = M(a', b')$과 $m_2 = M(b', a')$를 생성한다.

$a \bullet m_1 \oplus b \bullet m_2 \oplus x$를 계산하여 수신한 v와 일치하는지 검증한다. 만일 일치하지 않으면 데이터베이스는 이를 가짜 태그로 판단하고 통신을 종료한다.

두 값이 일치하는 경우 상호인증을 수행하기 위해 데이터베이스는 계산된 m_1과 m_2를 이용하여 $e = m_1 \bullet x \oplus m_2 \bullet x$를 계산한 후 리더로 전송한다. 이 과정을 알고리즘으로 기술하면 다음과 같다.

x = xValue[TID] // Get x using TID
$a' = f(a)$
$b' = f(b)$
$m_1 = M(a', b')$
$m_2 = M(b', a')$
$e = m_1 \bullet x \oplus m_2 \bullet x$
If $(a \bullet m_1 \oplus b \bullet m_2 \oplus x) == v$
  Send e To Reader
Else
  Send Error Message

단계 5. 리더 → 태그 : e

리더는 데이터베이스로부터 수신한 e 값을 태그로 전송한다.

단계 6. 태그

태그는 공유 비밀값 x와 소행렬 m_1, m_2를 이용하여 $e' = m_1 \bullet x \oplus m_2 \bullet x$를 계산한다. e'와 수신한 e가 동일하면 태그는 리더를 인증하게 되어 상호 인증이 이루어진다.

4. 안전성 및 효율성 평가

제안한 프로토콜의 안전성을 RFID 시스템의 보안 요구사항에 따라 분석하고 기존 프로토콜과 비교한 효율성은 다음과 같다.

4.1 안전성

4.1.1 상호 인증(Mutual Authentication)

제안한 프로토콜은 태그와 리더가 서로 합법적인지 상호 인증하는 기능을 제공한다.

제안 프로토콜의 단계 4에서 데이터베이스는 리더로부터 수신한 v값이 데이터베이스에 저장된 x를 이용한 $a \bullet m_1 \oplus b \bullet m_2 \oplus x$ 연산값과 일치하는 지 검사한다.

단계 6에서 태그는 자신이 계산한 $e' = m_1 \bullet x \oplus m_2 \bullet x$와 수신한 e값을 비교한다. 이 두 단계에서 태그와 리더사이에 공유한 비밀값 x는 추측 불가능한 랜덤 값을 사용하므로 공격자가 알 수 없다. 따라서 제안 프로토콜은 안전한 상호 인증을 수행한다.

4.1.2 도청 공격(Eavesdropping Attack)

도청 공격은 공격자가 태그와 리더간에 송수신되는 통신 내용을 도청한 후 태그에 저장된 비밀정보를 알아내고자 하는 공격이다.

제안 프로토콜에서 공격자는 메시지의 통신 과정에서 TID, v, e를 도청할 수 있다. 그러나 도청한 내용으로부터 공격자는 태그와 리더의 데이터베이스 간에 공유된 비밀행렬 A와 비밀값 x를 유추할 수 없다. x를 구하기 위해서는 공격자가 $v = a \bullet m_1 \oplus b \bullet m_2 \oplus x$와 $e = m_1 \bullet x \oplus m_2 \bullet x$로부터 소행렬 m_1과 m_2를 구할 수 있어야 한다. 그러나 비밀행렬 A는 태그와 데이터베이스만 알고 있기 때문에 공격자는 A를 알지 못하는 한 소행렬 m_1과 m_2를 구할 수 없다. 따라서 제안한 프로토콜은 도청공격에 대하여 안전하다.

4.1.3 재전송 공격(replay attack)

재전송 공격은 공격자가 리더와 태그 사이의 통신 내용을 도청 한 후 이를 재전송하여 합법적인 태그로 인증

받으려는 공격이다.

제안 프로토콜에서 공격자가 v값을 가로채 재전송함으로써 재전송 공격을 시도할 수 있으나, 공격자는 소행렬 m_1, m_2를 알 수 없으므로 e'값을 구할 수 없어 정당한 태그로 인증 받을 수 없다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

4.1.4 스푸핑 공격(Spoofing Attack)

스푸핑 공격은 공격자가 정당한 태그로 위장하여 리더로부터 인증에 필요한 정보를 획득하거나 이를 이용하여 정당한 태그나 리더로 인증받는 공격이다.

제안 프로토콜에서 공격자가 리더와 태그 간에 공유된 비밀행렬 A와 비밀값 x를 얻을 수 있으면 스푸핑 공격을 수행할 수 있다. 그러나 공격자는 리더와 태그가 안전하게 저장하고 있는 A와 x를 얻을 수 있는 방법이 없다. 또한 송수신되는 메시지에 포함된 비밀값 x는 소행렬 m_1과 m_2에 의해 보호되어 있다. 따라서 제안한 프로토콜은 스푸핑 공격에 대해 안전하다.

4.1.5 트래픽 분석공격(Traffic Analysis Attack)

트래픽 분석 공격은 공격자가 도청을 통해 수집한 정보를 통해 태그의 이동경로를 추적 할 수 있는 공격이다.

제안 프로토콜은 데이터베이스에서의 인덱스로 사용하기 위한 TID를 전송하는 과정에서 공격자에가 이를 도청할 수 있다. 공격자는 이 값을 이용하여 위치 추적에 이용할 수 있는 위험이 존재한다. 따라서 제안 프로토콜은 트래픽 분석 공격에 대해 취약하다.

4.1.6 위치 트래킹 공격(Location Tracking Attack)

위치 트래킹 공격은 공격자가 태그의 위치 변화를 감지함으로 인해 태그 소유자의 이동 경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다.

제안 프로토콜은 트래픽 분석공격에서와 동일하게 도청된 TID값에 의해 태그의 위치가 노출될 수 있으므로 위치 트래픽 공격에 대해 취약하다.

제안한 프로토콜은 트래픽 분석 공격에서 지적한 사항과 같이 a와 b가 랜덤하게 발생되어 공격자가 특정한 태그의 위치를 쉽게 식별할 수 없다.

4.1.7 서비스 거부 공격(Denial of Service Attack)

서비스 거부 공격은 공격자가 많은 계산이 요구되는 요청을 하거나, 이전 세션에서 갱신되는 값을 올바른 값으로 갱신하지 못하도록 방해하여 리더와 태그가 정상적인 서비스를 수행하지 못하도록 하는 공격이다.

제안 프로토콜은 리더와 태그 간에 XOR 연산만을 이용하여 상호 인증함으로써 많은 계산이 요구되지 않으며 데이터베이스에서 태그에 대한 v값을 검색하는 시간을 줄였다. 또한 매 세션마다 리더와 태그 사이에 상호 인증을 완료 한 후에 갱신을 필요로 하는 값이 없다. 따라서 제안한 프로토콜은 서비스 거부 공격에 대해 안전하다.

<Table 1>은 제안한 프로토콜을 XOR 연산을 기반으로하는 HB+ 프로토콜, Lee와 Ahn의 프로토콜, Yoon, Ha 그리고 Yoo의 프로토콜과 안전성을 비교한 것이다. 제안한 프로토콜은 트래픽분석 공격과 위치 트래킹 공격에서는 취약함을 나타냈으나 다른 공격들에 대해서는 안전함을 보여주었다.

〈Table 1〉 Safety comparison of related protocols

attack \ protocols	HB+	Lee-Ahn	Yoon-Ha-Yoo	proposed protocol
Mutual Authentication	×	×	○	○
Eavesdropping Attack	○	○	○	○
Replay Attack	○	○	○	○
Spoofing Attack	×	○	○	○
Traffic Analysis Attack	×	×	○	×
Location Tracking Attack	×	×	○	×
Dos Attack	○	×	○	○

4.2 효율성

RFID 시스템은 데이터베이스, 리더, 태그로 구성된다. 리더는 먼저 태그에 질의를 하고 태그는 이에 대한 응답을 리더로 보낸다. 리더는 데이터베이스로 태그의 응답을 전송한다.

〈Table 2〉 Effectiveness comparison of proposed protocol

protocol / operation	Yoon-Ha-Yoo			proposed protocol		
	DB	reader	tag	DB	reader	tag
matrix operation	2	0	2	2	0	2
XOR operation	2n+1	0	3	3	0	3
AND operation	2n+2	0	4	4	0	4
random number generation	0	1	1	0	0	0
number of communication	5			5		

n : Stored in the database, the number of tags

제안 프로토콜은 인증 과정에서 데이터베이스에서의 연산 수를 줄이기 위해 태그를 등록할 때 사전에 TID를 인덱스로 비밀값 x를 저장한다. 이는 기존 프로토콜에서 데이터베이스가 수신한 v값과 일치하는 x가 존재하는지 검색하기 위한 연산 횟수를 줄여준다. <Table 2>는 제안 프로토콜이 기존 프로토콜보다 데이터베이스에서의 XOR과 AND 연산이 각각 $2n+1$에서 3회로, $2n+2$에서 4회로 줄었음을 알 수 있다.

5. 결론

RFID는 통행료 징수 등의 교통시스템, 상품 이력 관리 등의 분야에서 널리 이용되고 있다.

RFID의 정보보안을 위해 인증 및 접근제어를 위해서 해쉬함수, 암호 알고리즘을 이용하는 방법과 XOR 연산을 이용하는 방법들이 제안되었다. Lee와 Ahn은 행렬기반 인증프로토콜을 제안하였고, Yoon, Ha, Yoo은 행렬기반의 상호인증 프로토콜을 제안하였다. Yoon, Ha, Yoo의 인증프로토콜은 보안성 면에서 기존의 Lee와 Ahn의 프로토콜을 보완하였으나, 백엔드 데이터베이스에게 부하를 많이 주는 단점을 가지고 있다.

본 논문에서는 태그 ID를 이용하여 인증절차를 수행할 때 백엔드 데이터의 연산량을 줄이기 위한 인증 프로토콜을 제안하고 이에 대한 안전성과 효율성을 분석하였다.

제안된 프로토콜은 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격에 안전함을 보여주었을 뿐만 아니라 상호인증을 제공한다. 백엔드 데이터베이스의 계산량을 줄여 시스템 효율면에서도 다른 방법들보다 우수함을 보여주었다.

REFERENCES

[1] A. Jules, R. L. Rivest, and M. Szydlo " Selective Blocking of RFID Tags for Consumer Privacy", In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, 2003

[2] H. Gillbert, M. Robshaw, H. Sibent, "Active attack against HB+: a probably secure lightweight authentication protocol", Electronics Letters, 13th October, vol. 41, No. 25, 2005.

[3] S. L. Garfinkel, A. Jules and R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security and Privacy, vol. 3, pp.34-43, May/June 2005.

[4] Hyoyoung Shin, Kyedong Jung, Chigon Hwang, "A Study on the effectiveness of matrix-based authentication protocol", The 3rd International conference of convergence technology 2013, July 3-6, 2013.

[5] R. Chandramouli, T. Grance, R. Kuhn, "Security Standards for the RFID Market ", IEEE Security & Privacy, Dec. 2005.

[6] Christian Flockermeier, Sanjay Samara, "An Overview of RFID System Interfaces and Reader Protocols", 2008 IEEE International Conference on RFID, pp.232-pp.240, April, 2008

[7] Su Youn Lee, Hyo Beom Ahn, "A Study on Secure Matrix-based RFID Authentication Protocol", Journal of information and security. Vol. 6, No.1, pp.83-90, 2006.

[8] Eun-Jun Yoon, Kyeoung-Ju Ha, Kee-Young Yoo, "Robust Matrix-based RFID Mutual Authentication Protocol", The Journal Of Korea Information And Communications Society, Vol. 33, No. 11, 2008.

[9] Ik-Su Kim, "Hash Function-based Secure

Authentication Protocol for Improving Efficiency in RFID System", The Journal Of Korea Information And Communications Society, Vol. 34, No. 4, pp.428-434, 2009.

[10] Eun Young Choi, Dong Hee Choi, Jong In Lim, Dong Hoon Lee, "Efficient authenticate protocol for very Low-Cost RFID", Journal of the Korea Institute of Information Security and Cryptology, Vol. 15, No. 5, 2005.

신 효 영(Hyo-Young Shin)

- 1986년 2월 : 광운대학교 전자계산학과(이학사)
- 1988년 2월 : 광운대학교 전자계산학과(이학석사)
- 1998년 8월 : 광운대학교 전자계산학과(이학박사)
- 1988년 2월 ~ 1993년 8월 : LG 소프트 연구소
- 1994년 2월 ~ 현재 : 경복대학교 IT보안과 부교수
- 관심분야 : 네트워크 보안, 분산 시스템
- E-Mail : hyshin@kbu.ac.kr

황 치 곤(Chi-Gon Hwang)

- 1995년 2월 : 창원대학교 경영학과(학사)
- 2004년 8월 : 광운대학교 정보통신학과(공학석사)
- 2012년 8월 : 광운대학교 컴퓨터과학과(공학박사)
- 2006년 1월 ~ 현재 (주)인찬 연구원
- 관심분야 : XMDR, 클라우드 컴퓨팅, DBaaS, 서비스 상호운용, 온톨로지, 멀티미디어
- E-Mail : duck1052@kw.ac.kr

정 계 동(Kye-dong Jung)

- 1985년 2월 광운대학교 전자계산학과(이학사)
- 1992년 2월 광운대학교 산업정보학과(이학석사)
- 2000년 2월 광운대학교 컴퓨터과학과(이학박사)
- 1993년 3월 ~ 2004년 12월 광운대학교 정보과학원 교수
- 2005년 3월 ~ 현재 광운대학교 교양학부 교수
- 관심분야 : XML, 분산시스템, 분산 컴퓨팅기술, 이동에이전트, 클라우드 컴퓨팅, DBaaS
- E-Mail : gdchung@kw.ac.kr