Journal of Knowledge Information Technology and Systems(JKITS), Vol. 9, No. 2, pp. 247~255, April 2014

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

The User Authentication Method Using Behavioral Characteristics

Yo-Han Choi[1], Hee-Suk Seo[*2], Jin-Sub Park[3]

[1]*Interdisciplinary Program in Creative Engineering, Korea University of Technology and Education*
[2]*School of Computer Science and Engineering, Korea University of Technology and Education*
[3]*Department of Computer Engineering, DaeJeon University*

ABSTRACT

There are studies on biometric based authentication using physiological or behavioral characteristics of the user to improve reliability of user authentication. This study suggests the user authentication method using key input patterns and hand shapes when the user inputs authentication information. When behavioral characteristics are used for user authentication, there is a disadvantage for the authorized user to fail for user authentication and to be prohibited to access the information system. This study suggested a method of granting access to the authority system by differential access in order to solve user authentication failure problems by the authorized user when behavioral characteristics are used for multi-factor authentication. It enables for the authorized user to use the stored information in the information system even though the user fails to authenticate behavioral characteristics by granting the user differentiated authority.

KEYWORDS: User Authentication, Biometrics, behavior, Information Security, Authorization

ARTICLE INFO: Received 6 February 2014, Revised 27 March 2014, Accepted 17 April 2014.

1. 서 론

정보시스템을 안전하게 유지하기 위해서는 정당한 권한을 가진 사용자만이 활용해야 한다. 사용자 인증은 정보 서비스를 이용하는 사용자의 권한을

[*]Corresponding author is with the School of Computer Science and Engineering, Korea University of Technology and Education, 1600, Chungjeol-ro, Byeongcheon-myeon, Dongnam-gu, Cheonan-si, Chungcheongnam-do, 330-708, KOREA.

E-mail address: histone@koreatech.ac.kr

확인하기 위한 기본적인 보안 방법이다[1].

사용자 인증은 사용자가 알고 있는 정보를 기반으로 인증을 수행하는 지식기반, 사용자가 소지하고 있는 인증 매체를 통해 인증을 수행하는 소지기반 그리고 사용자의 생리학적 특징이나 행동학적 특징을 기반으로 인증을 수행하는 생체기반 인증으로 구분할 수 있다[2]. 사용자 인증에 대한 신뢰성을 높이고, 보안성을 강화하기 위해서 서로 다른 인증 방법을 이용하는 Multi-Factor 인증을 활용하기도 한다.

다른 사용자의 정보를 복제, 모방하기 힘든 생체정보를 이용한 인증 방법에 대해 연구되고 있다[4]. 생체기반 인증은 사용자 인증 정보로 사용자 고유의 생체정보를 인증 정보로 활용방법으로 지문, 홍채, DNA 정보 등과 같은 생체학적 특성과 걸음걸이. 키 입력 패턴 등과 같은 행동학적 특성으로 구분할 수 있다[5]. 생체학적 특성을 사용하는 사용자 인증의 경우 인식률이 높다는 장점이 있지만, 사용자가 자신의 생체정보를 활용하는 점에 대한 거부감과 생체 정보를 수집/관리하기 위한 추가적인 비용이 발생하다.

본 논문에서는 사용자에게 거부감이 낮은 행동특성을 이용한 사용자 인증 방법을 설계 하였다. 사용자 인증에 활용하는 행동특성은 각 사용자가 키보드를 이용할 때 나타나는 습관을 활용한다. 사용자의 오랜 키보드 사용으로 형성된 특정키의 사용 빈도, 손 모양을 분석하여 각 사용자의 인증 정보로 활용할 수 있다.

사용자의 행동 특성을 인증 정보로 활용하면 거부감을 줄 일수 있다는 장점[6]이 있지만, 생체학적 특성을 활용하는 인증에 비해 인식률이 떨어진다는 단점이 있다.

본 논문에서는 행동학적 특성을 이용하여 발생하는 낮은 인식률로 인해 인증에 실패하여 사용자의 불편을 유발 시킬 수 있다. 사용자의 불편을 감소시키기 위해 사용자의 권한을 단계적으로 부여하는 방법을 제안한다. Multi-Factor 인증 요소들의 결과를 활용하여 사용자의 권한을 차등적으로 부여한다. 사용자의 권한을 차등적으로 부여하여 사용자가 행동학적 특성에 대한 인증 실패 시 정보 시스템에 접근할 수 없는 불편을 감소시키고, 쉽게 모방할 수 없는 행동학적 특성으로 사용자 구분을 수행하여 보안성을 높일 수 있다.

2. 관련 연구

2.1 시스템 구조

정맥인식은 손등이나 손목의 정맥 모양으로 신원을 식별하는 방법이다. 정맥은 쌍둥이라도 서로 다르기 때문에 정맥 인식을 사용자 인증 요소로 사사용할 경우, 신뢰성 높은 사용자 인증이 가능하다.

그림1 손가락 정맥인식 장치
Figure 1. Finger vein recognition device

최근에는 손목에 분포되어 있는 정맥이 아닌 손가락에 분포되어 있는 정맥을 인식하는 방법에 대해 연구[7]되고 있다. 손목을 인식하는 것에 비해 사용자의 거부감이 덜할 수 있다. 혈관은 피하에

존재하므로 위조나, 훼손, 마모, 오염 등으로부터 자유롭고, 육안으로는 식별이 어려우므로 특별한 장비에 의하여 촬영하여야 한다.

새로운 정합 알고리즘을 이용한 손가락 정맥 인식 방법[8] 연구에서는 손가락 정맥영상을 지역적 히스토그램 균등화에 의하여 전처리하고, 이것을 세선화 처리하여 선 형태의 정맥을 얻는다. 이렇게 얻어진 선 형태의 정맥선 영상에 HS정합 알고리즘(HeeSung's Matching Algorithm)이라고 명명된 새로운 정합 알고리즘을 적용하여 정맥의 정합 여부를 분별한다.

2.2 서명 인식

서명인식은 전자패드에 직접 서명하는 방법으로 사내 결제 등에 이용한다. 서명의 물리적 특성을 이용하거나 서명할 때 펜의 움직임, 속도, 압력 등을 동적으로 파악하는 방법이 연구 중에 있다[9]. 생리적인 접촉이 없고 개인신상 정보를 데이터베이스로 저장하지 않아도 되기 때문에 이용자가 부담을 덜 느끼는 장점이 있다. 현재 이 메일을 보내거나 전자패드를 이용한 전자결제에 활용되고 있다.

인식은 서명을 하는 속도, 가속, 획의 순서 등을 포함한 변할 수 있는 것들을 분석함으로써 이루어진다. 서명은 보안을 제공하지만 서명 모양을 복제할 수 있다는 문제가 있다. 이것이 서명 인증이 고도의 보안 제품에 적용되기 어려운 점이다.

2.3 손동작 인식

사람의 손동작이나 손 모양은 인식하여 인간과 기계와 상호작용하는 방법으로 사용되고 있다. 사용자의 손 모양 인식은 비전시스템의 발전과 함께 2D영상을 기반에서 3D를 이용한 인식으로 연구가 진행되고 있다.

손모양 인식 기술은 카메라를 이용하여 사용자의 손 모양을 촬영하여 분석하는 방법이다. 사용자의 손 모양에서 특징점을 추출하거나 사용자의 체스쳐를 인식하는 기술이다[10]. 사용자의 손 모양은 주변 상황에 따라 인식률이 떨어 질수 있다는 단점이 있다.

보다 정확한 사용자의 손 모양을 인식하기 위해서 깊이 영상을 획득 할 수 있는 키넥트를 활용하여 사용자의 손 모양을 인식하기 위한 연구가 이루어 지고 있다. Kinect 기반 손 모양 인식을 위한 손 영역 검출에 관한 연구에서는 사용자의 손 모양 인식하기 위해 컬러 영상과 깊이 영상을 함께 사용한다. Kinect 의 깊이 영상에서 깊이에 따라 주변의 사물과 사용자의 손을 구분하고 컬러 영상을 이용하여 손 모양을 추출한다.

본 논문에서 제안하는 사용자의 행동 특성에 이용한 사용자 인증 방법은 SkinColor를 기반으로 인식한다. 정확한 사용자의 손동작을 인식하기 위한 방법이 아니기 때문에 조명에 의해 손실된 손 영역을 복원하지는 않았다. 사용자의 손 영역의 피부색과 주변의 조명 조건을

그림 2 Kincet를 이용한 사용자 손 모양 인식
Figure 2. The user's hand shape recognition using Kincet

3. 사용자 행동 특성에 이용한 사용자 인증

Multi-Factor 인증은 다양한 사용자 인증 방법을

복합적으로 사용하여 사용자 인증의 신뢰성을 높이는 방법이다. 하지만 정당한 권한을 가진 사용자여도 단 하나의 인증 요소를 충족하지 못하면 인증에 실패한다. 이러한 방법은 인증의 신뢰성을 높일 수 있지만 사용자의 불편이 증대시킬 수 있다. 특히 행동특성을 사용자 인증 요소로 사용하는 경우 사용자 주변의 환경에 따라 사용자의 행동 특성이 달라져 인증을 성공하지 못할 수 있다.

본 논문에서는 Multi-Factor 인증이 가지는 신뢰성을 유지하면서 사용자의 불편을 감소시키기 위해 행동특성을 이용한 사용자 인증 방법을 제안한다.

사용자가 인증 정보를 입력하는 과정을 웹캠과 키로거 기능을 이용하여 수집한다. 수집된 정보는 <그림 3>과 같이 손 모양, 사용한 키 정보, 입력한 문자열 정보로 구분하여 분석한다. 각 인증 요소의 성공 여부에 따라 사용자에게 부여하는 권한을 차등적으로 제공하는 방법을 통해 인증의 신뢰성과 사용자의 편의성을 확보하였다.

사용자 인증 정보로 손 모양을 활용하기 때문에 사용자는 기존의 ID/PW기반 인증 이외에 추가적인 인증 정보를 제공한다는 것을 인지하지 못한다.

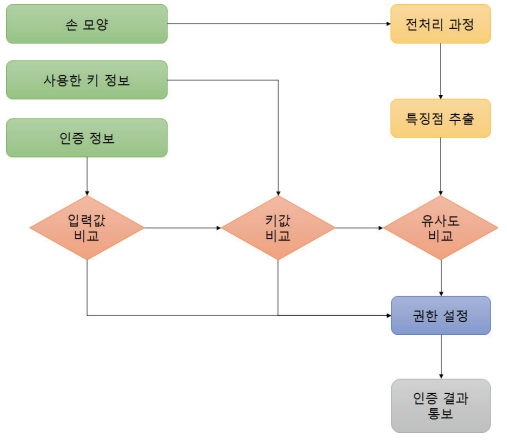


그림 3 권한 부여 프로세스
Figure 3. Authorization process

3.1 사용자 인증 요소

본 연구에서는 사용자 인증 요소로 사용자의 ID/PW와 사용자가 키보드를 이용할 때의 손 모양을 인증 요소로 선택하였다.

기존에 인증 정보로 많이 사용되고 있는 ID/PW는 사용자의 지식 기반 인증 요소로 과거부터 많아 사용되던 인증 방법이다. 따라서 사용자가 ID/PW를 통한 인증에 쉽게 접근 할 수 있다는 장점이 있다.

하지만, ID/PW를 이용한 인증은 타인에게 쉽게 노출될 수 있고 인증 정보를 알고 있는 사람은 누구나 사용자 인증을 수행할 수 있다는 단점이 존재한다. 이러한 단점을 해결하기 위해서 ID/PW와 다른 인증 요소를 결합한 Multi-Factor인증을 통해 인증의 신뢰성을 높이기 위한 연구가 진행되고 있으며, 본 논문에서는 사용자의 행동 특성을 활용한다.

각각의 사용자는 자신만의 오랜 습관을 통해 개인의 고유한 행동학적 특성을 형성한다. 본 논문에서는 사용자가 오랜 기간 키보드를 사용하면서 형상된 사용자의 손 모양과 인증 정보를 입력하기 위해 사용한 키보드의 키 정보를 인증 정보로 활용한다.

3.1.1 사용 키 정보 분석

사용자가 사용한 키 정보를 획득하기 위해 사용자 누른 키의 Keys Enumeration 값을 수집한다. Keys Enumeration 값을 수집하기 때문에 키보드를 눌러 화면에 인지할 수 있는 문자, 숫자 이외에도 Home, End 키와 같은 특수키에 대한 정보도 수집할 수 있다.

사용자가 인증 암호를 'SEcr3t' 로 설정하고, 이때 사용한 키 정보가 '(NP3)3 (LS)t(HE)(CL)se(RS)C

(RS)r' 를 이용하여 설정하였다. 악의적인 사용자가 정상 사용자를 사칭하기 위해 '(RS)s(RS)ecr(D3)3(RS)t' 와 같이 인증 값을 입력하였다. 사용자의 패스워드 문자열은 SEcr3t로 같지만, 사용한 키가 서로 달라 악의적인 사용자는 2단계 권한을 부여 받게 된다.

표 1. 특수키에 대한 키값
Table 1. The key value for the special keys

특수키 명	약어	키값
Home	HE	36
End	ED	35
left SHIFT	LS	160
right SHIFT	RS	161
CAPS LOCK	CL	20
NumPad	NP0~9	-
숫자열	D0~9	-

3.1.2 사용자의 행동 정보

본 논문에서 활용하는 사용자의 행동학적 특성은 사용자가 키보드를 사용하는 손 모양이다. 사용자의 주변 환경이나 자주 사용하는 키에 따라서 사용자가 키보드로 특정한 문자를 입력할 때 손모양이 달라진다는 점을 활용한다. 사용자의 손 모양을 촬영하기 위해서 추가적으로 웹 카메라가 설치하였다. 실험의 정확도를 높이기 위해 사용자를 손을 제외한 영역을 단일 색으로 조성하였다. 또한 사용자의 피부색과 주변의 조명의 색에 따라서 전처리 과정 후 영상에서 추출되는 특징점이 달라져 좀 더 신뢰성 높은 사용자 인증 수행이 가능하다.

<그림 5>는 서로 다른 사용자가 동일한 키(B)를 입력할 때의 손 모양을 촬영하고, 영상으로부터 특징점을 추출한 결과이다.

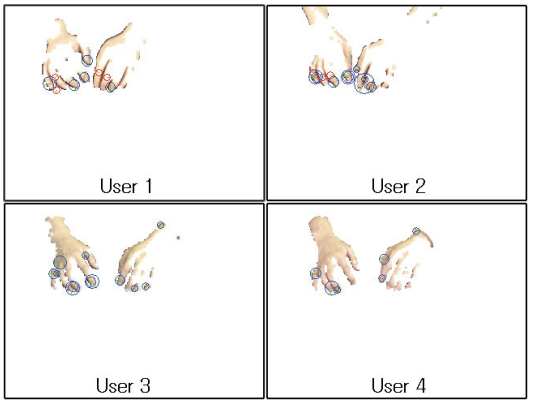


그림 5. 각 사용자의 특징점 비교
Figure 5. Comparing each feature point of the user

<그림 6>은 추출한 특징점으로 사용자 등록과정에 획득한 영상과 인증 과정에 획득한 영상을 비교한 결과이다. 동일 사용자의 경우 일치하는 특징

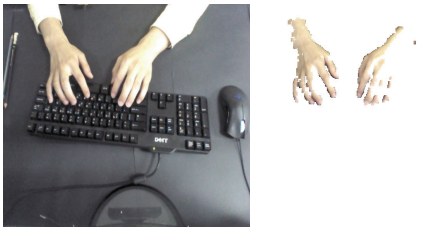


그림 4. 사용자 행동 특성
Figure 4. Behavioral characteristics of users

그림 6. 사용자 특성 비교 결과
Figure 6. Comparison of the results

점이 존재하지만, 다른 사용자의 경우 특징점이 일치하지 않는 것을 확인 할 수 있다.

3.2 인증 결과에 따른 권한 차등 부여

본 논문에서는 사용자 인증의 요소로 사용자의 ID/PW와 행동학적 특성을 이용한 Multi-Factor 인증 방법을 기준으로 사용자 권한을 차등 부여하는 방법을 설계하였다.

사용자 인증을 위해서 먼저 사용자가 입력한 문자열에 대한 일치 여부를 검증한다. 사용자가 입력한 문자열이 다른 경우 1단계 권한을 부여하고 인증을 과정을 그만둔다. 1단계 권한은 사용자가 입력한 패스워드가 다른 경우로 사실상 인증이 거부된 경우이다. 사용자가 입력한 문자열이 같은 경우 2단계 권한을 부여하고 사용자가 문자열을 입력하는데 사용한 키를 비교한다.

그림 7. 사용자 권한 부여 단계
Figure 7. User Authorization step

사용자가 인증 정보를 입력하기 위해 사용한 키가 사용자 등록 단계에서 사용한 키와 동일한지 비교한다. 사용자가 사용한 키가 등록 단계에서 사용한 키와 다른 경우 2단계 권한을 부여하고 인증을 그만두게 되며, 동일한 경우 3단계 권한을 부여한다.

모든 데이터에 대한 접근이 가능한 4단계 권한은 사용자가 입력한 인증정보와 행동 특성이 모두 일치 하는 경우에 부여한다.

3.3 권한에 따른 접근 가능 데이터 예

사용자 인증 결과를 단순히 성공 혹은 실패로 판단한 경우 정상 사용자의 인증 정보를 알고 있는 악의적인 사용자에 의해서 시스템 전체의 정보가 유출될 수 있는 위협이 존재한다. 이러한 위협을 대비하기 위해 인증 결과를 성공 실패가 아닌 사용자에게 부여하는 권한을 단계별로 구분하였다.

본 연구에서는 사용자에게 부여하는 권한 단계를 4단계로 구분접근 할 수 있는 데이터를 제한하였다.

인증 결과로 데이터에 접근 할 수 있는 권한 단계로 정보를 제공한다. 1단계 권한은 사용자 인증에 실패한 단계로 어떠한 정보도 확인할 수 없다. 2단계 권한은 다른 정보에 비해 상대적으로 중요하지 않은 정보는 확인 할 수 있지만, 중요 정보들에 대해서는 일부만 확인 가능하다.

1단계 권한

***	***
***	*** ***
***	*** ***

2단계 권한

이름	주소
홍*동	천안 *** ...
최*한	부산 *** ...

3단계 권한은 정보 시스템에 있는 정보들을 확인 가능하다. 하지만 정보의 수정이나 삭제는 불가

능 하다. 4단계 권한은 사용자의 권한 내에서 확인할 수 있는 모든 정보에 대해 확인이 가능하고, 수정/삭제 등의 작업도 가능하다.

3단계 권한 (수정/삭제 불가)

이름	주소
하성철	천안 동남구 *** ...
최요한	부산 진구 *** ...

4단계 권한 (수정/삭제 가능)

이름	주소
하성철	천안 동남구 병천면 ...
최요한	부산 진구 양정동 ...

4. 결 론

본 연구에서는 개인정보나 기업의 기밀정보를 보호하기 위해 사용자의 행동 특성을 이용한 사용자 인증 방법을 설계 하였다. 기존에 주로 사용되던 아이디와 패스워드를 이용한 인증 방법에 사용자가 입력에 사용한 키에 대한 정보와 키보드 입력과정에서 나타나는 사용자 고유의 손 모양을 활용하여 사용자 인증을 수행한다. 사용자가 설정한 패스워드가 노출되어도 사용자가 패드워드 입력에 사용하는 각 키들의 정보나 입력 시 나타나는 개인의 고유한 손동작까지는 모방하기 어렵다.

본 연구에서는 사용자의 행동 특성 중 주로 사용하는 키보드의 키와 키보드를 입력할 때의 손 모양을 이용한 인증 방법을 설계하였다. 사용자가 설정한 인증 정보와 손 모양을 이용해 인증을 수행하여 2-factor 인증과 같은 보안성을 가지면서 OTP등과 같은 사용자가 휴대하여야 하는 추가적인 장비가 필요하지 않다.

본 연구가 사용자가 보유하고 있는 다양한 정보를 활용하여 사용자 인증에 대한 보안성을 높이면서 사용자의 편의를 증대 시킬 수 있는 연구의 초석이 될 수 있을 것으로 판단된다.

References

[1] Jun, and Xiong, *Application of user identity authentication technology in computer in information security,* Information Security and Technology 6, 2013.

[2] Ector, and Boudewijn, *Master thesis: User-centric privacy in de SURFfederatie*, 2009.

[3] Sokabe M1, Fraser CS, and Hershey JW., *The human translation initiation multi-factor complex promotes methionyl-tRNAi binding to the 40S ribosomal subunit,* Nucleic acids research Vol. 40, No. 2, pp. 905-913, 2012.

[4] C.-T. Li, and M.-S. Hwang, *An efficient biometrics-based remote user authentication scheme using smart cards,* Journal of Network and Computer Applications Vol. 33, No. 1, pp. 1-5, 2010.

[5] S.-L. Wang, and A. W. Liew, *Physiological and behavioral lip biometrics: A comprehensive study of their discriminative power,* Pattern Recognition, Vol. 45, No. 9, pp. 3328-3335. 2012.

[6] Drosou, A., D. Ioannidis, K. Moustakas, and D. Tzovaras, *Unobtrusive behavioral and activity-related multimodal biometrics: the ACTIBIO authentication concept,* The Scientific World Journal 11, pp. 503-519. 2011.

[7] A. Jain, A. Ross, and S. Prabhakar, *An introduction to biometric recognition,* IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics, Vol. 14, No. 1,

2004.

[8] H. S. Kim, and J. H. Cho, *A method for finger vein recognition using a new matching algorithm*, Journal of Korea Information Science Society, Vol. 37, No. 11, 2010.

[9] A. Boyko, and G. Rozorynov, *Signature based authentication,* IEEE International conference on Modern Problems of Radio Engineering, Telecommunications and Compute Science. pp. 300, 2010.

[10] J. H. Kim, J. H. Lim, and S. H. Moon, *The effect of visual feedback on one-hand gesture performance in vision-based gesture recognition system,* Journal of the Ergonomics Society of Korea, Vol. 31, No. 4, pp. 551-556. 2012.

행동학적 특성을 이용한 사용자 인증 방법 설계

최요한[1], 서희석[2], 박진섭[3]

[1] *한국기술교육대학교 창의융합공학협동과정*
[2] *한국기술교육대학교 컴퓨터공학부*
[3] *대전대학교 컴퓨터공학과*

요 약

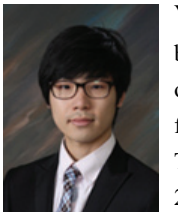
사용자 인증의 신뢰성을 높이기 위해 사용자의 생리학적 특성이나 행동학적 특성을 활용한 생체기반 인증에 대한 연구가 이루어지고 있다.

본 논문에서는 사용자가 인증 정보를 입력할 때 나타나는 키 입력 패턴과 손 모양을 이용한 사용자 인증 방법을 제안한다.

사용자 인증에 요소로 행동학적 특징을 이용하는 경우 정당한 권한을 가지고 있는 사용자도 사용자 인증에 실패하여 정보 시스템에 접근 할 수 없다는 단점이 있다. 본 논문에서는 행동학적 특성을 Multi-factor인증에 사용하면서 발생하는 정당한 사용자의 인증 실패의 문제점을 해결하기 위해 각 인증 요소의 성공 여부에 따라 사용자가 정보 시스템에 접근 할 수 있는 권한을 차등적으로 부여하는 방법을 제안한다. 사용자의 권한을 차등적으로 부여하여 행동학적 특성에 대한 인증이 실패한 경우에도 정당한 사용자가 정보 시스템에 저장된 정보를 사용할 수 있도록 하였다.

감사의 글

이 논문은 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2010-0021951).



Yo-Han Choi received the bachelor's degree in the School of Internet Media Engineering from the Korea University of Technology and Education in 2012. He received the M.S. degree in the Department of Computer Science and Engineering from Korea University of Technology and Education in 2014. Now He is a Ph.D. course student at the Interdisciplinary Program in Creative Engineering from Korea University of Technology and Education, Cheonan, Korea. His current research interests include mobile Security, Information Security, User Authentication. He is a member of the KKITS.

E-mail address: yhchoi@koreatech.ac.kr

Hee-Suk Seo received the bachelor's degree in the Department of Industrial Engineering from the Sungkyunkwan University in 2000. He received the M.S. degree and the Ph.D. degree in the Department

of Electronic, Electrical and Computer Engineering from Sungkyunkwan University in 2002 and 2005, respectively. He is now a professor in the Department of Computer Science and Engineering, Korea University of Technology and Education, Korea. His research interests include malicious code analysis, modeling & simulation, network security and intelligent system. He is a member of the KKITS.

E-mail address: histone@koreatech.ac.kr

Jin-Sub Park received the bachelor's degree and M.S. degree and the Ph.D. degree in the Department of Electronic, Electrical and Computer Engineering from Chungang University in 1980 and 1982 and 1991, respectively. He is now a professor in the Department of Computer Engineering, Dae Jeon University, Republic of Korea. His research interests include ISMS, network & security. He is a member of the KKITS.

E-mail address: jspark@dju.ac.kr