JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 1 : 91~96 Jan. 2014

개인 정보 보호를 위한 화면 캡쳐 방지 모듈 구현

이종혁*

Implementation of anti-screen capture modules for privacy protection

Jong-hyeok Lee*

Department of Computer Engineering, Kyungsung University, Pusan 608-736, Korea

요 약

최근 컴퓨터의 보급과 정보사회의 발달로 인해 개인 신상 정보에 대한 관심이 증대되고, 이와 관련된 정책과 기술이 발전함에 따라서 개인 신상 정보를 보호하려는 시도가 다양하게 이루어지고 있다.

본 논문에서는 컴퓨터를 사용하면서, 개인의 중요한 자료나 신상정보 또는 회사의 기밀 내용을 다루는 기관 및 부서를 대상으로 중요한 자료와 신상정보 및 회사의 기밀을 보호하는 방안을 제안 하였다. 결과적으로 공공기관 또는 개인 컴퓨터 내에서 타인의 정보를 악의적으로 도용하거나 도취하는 것을 방지하고, 기관 내의 시스템들 사이에서 정보가 오가는 동안 중요한 자료와 신상 정보들의 노출을 1차적으로 막을 수 있다.

ABSTRACT

According to the spread of computers and the development of the information society, people are focused on privacy information. As the development of its associated policy and technology, it has been tried various attempts to protect their personal information.

In this paper, we proposed anti-screen capture modules to protect personal information or a company's confidential information for agencies and departments that keeps top security. As a result, we can prevent an illegal use or a stealing of another person's information in a public agency or personal computer. Also modules can stop exposures of top security data and personal information during they communicate with others in their institution's sever system.

키워드 : 화면 캡쳐 방지, 슈퍼 클래싱(전역 후킹), API, 클립보드, 기능키

Key word : Prevent Screen Capture, Super-Classing, API, Clipboard, Function keys

접수일자 : 2013. 10. 19 심사완료일자 : 2013. 11. 11 게재확정일자 : 2013. 11. 25

*** Corresponding Author** Jong-Hyeok Lee(E-mail:jhlee@ks.ac.kr, Tel:+82-51-663-4781)
Department of Computer Engineering, Kyungsung University, Pusan 608-736, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.1.91 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 컴퓨터의 보급의 증가로 사용자의 편의성을 요구하는 일반대중은 인간에게 친숙한 인터페이스(Interface)의 출현을 바라고 있다[1]. 이러한 효과로 인해 컴퓨터 내에는 키보드, 마우스, 혹은 키패드를 이용하여 사용자가 조작할 수 있는 수많은 기능들을 내포하고 있다. 예를 들면 프린트 스크린 기능키, 복사 기능키, 붙여넣기 기능키를 들 수 있다. 이러한 기능들은 유용성과 사용성 등 인간 중심의 컴퓨터를 실현하기 위한 인터페이스로 굉장히 편리하게 사용할 수 있는 반면, 너무나 쉽게 개인의 중요한 자료나, 신상정보를 훔칠 수 있는 기능마저 제공하여 오히려 보안에 대한 역효과가 대두되고 있는 실정이다.

보안의 종류를 간략히 살펴보면 네트워크 보안, PC 보안, 문서 보안, 출력 보안, DB 보안, 물리적 보안이 있으며, PC보안은 사용자가 PC에서 발생할 수 있는 여러 가지 문제들을- 해결하기 위한 솔루션과 통합 보안, Antivirus(바이러스 침투를 방지하기 위한 솔루션), PC 방화벽이 있다. 이러한 보안 정책들이 유지되고 있음에도 불구하고, ‘KT에서 고객정보가 유출되는 보안사고 발생’[2], ‘MBC 정보 수집 프로그램, 금융거래·의료정보 유출사건 발생'[3], ‘게임 앱 위장 개인정보 빼내’[4] 등 개인정보가 유출된 사례가 셀 수도 없이 많이 일어나고 있다. 이런 전차로 우리는 개인정보 및 중요한 자료를 철저히 관리할 필요성이 있다[5].

신영호 등은 공개 데이터베이스인 MySQL에서 개인정보 및 민감한 데이터에 대한 암호화를 통하여 데이터를 저장, 관리하는데 있어서 데이터의 속성에 따라 적절한 암호화 기법을 사용함으로써 암호화를 통한 데이터보호와 함께 속도 등의 성능상의 오버헤드 와 운영, 관리상의 효율을 높이기 위하여 지원하는 암호화 기법에 대하여 연구하였고[6], 안철수 등은 파일 공유 환경에서 사용자 PC 문서의 저장이 안 되도록 하기 위해 API 후킹이 적용된 클라이언트를 설계하고 구현하였으며[7], 박중환 등은 기업 내부의 개인정보 보호시스템(Privacy-i)의 설계를 제시한다. Privacy-i 는 PC 단에서 저장된 개인정보 검출 및 보호 시스템을 구축할 수 있는 서비스를 제공하며 회사 또는 단체 내의 모든 기밀정보를 중앙 집중적으로 관리하고 외부로 유출 되는 것을 방지는 방법을 제시하였다[8].

인터넷의 발달로 인하여 웹을 많이 사용하게 되므로 이를 위한 방안으로 김동례 등은 (1)인터넷상 개인정보 노출점검, (2)웹 어플리케이션 방화벽, (3)개인정보 필터링 시스템, (4)개인정보 종합관리 시스템의 특징 및 적용방안을 제안하였으며[9], 신용녀 등은 원격의료 환경에서 바이오정보 전송에 있어서의 보안 위협으로부터 안전한 원격의료 서비스를 제공하기위한 사용자 인증과, 통신상에서의 정보 획득, 변조, 불법접근 등과 같은 다양한 보안위협으로부터 바이오정보를 보호하기 위한 통합 보안 프레임워크를 제시하였다[10].

NIST(미국표준기술연구소)는 ‘NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing’, 과 ‘NIST SP 800-145 The NIST Definition of Cloud Computing’란 이름의 표준 문서를 발간하였으며, ‘NIST SP 800-146 Cloud Computing Synopsis and Recommendations’를 작성하는 등 클라우드 컴퓨팅 보안 표준 연구를 활발히 진행하고 있다[11-13].

정보화 시대에 진입함에 따라 컴퓨터를 사용하지 않는다는 것은 거의 불가피한 상황이기 때문에 우리는 컴퓨터를 사용하면서 중요한 자료나 개인 정보를 다루는 공공기관이나 개인기관 뿐만 아니라 회사 내의 기밀문서를 다루는 부서는 수 없이 많이 있으며, 이와 같은 곳에서는 개인정보 보호를 위한 프로그램을 이미 도입하여 사용하고 있다. 그러나 정책이 바뀌든지 아니면 새로운 캡쳐 프로그램이 발표되면 이를 수용하기 위하여 프로그램을 바꾸어야 하는 번거러움이 발생한다.

본 연구에서는 PC에서 개인 정보 취급 권한이 없는 자가 개인 정보를 취급하고자 할 경우 이를 보호할 수 있는 실행 모듈인 화면 캡쳐 방지 모듈을 구현하고자 한다.

Ⅱ. 화면 캡쳐 방지와 API 후킹

2.1. 화면 캡쳐 방지의 정의 및 특징

화면 캡쳐 방지란 컴퓨터와 연결된 모니터에서 디스플레이 되는 화면을 컴퓨터에서 제공하는 프린터 스크린 키, 복사 기능키, 붙여넣기 기능키를 통해 화면을 캡쳐 하거나, 마우스 드래그를 통해 정보를 복사하여 옮기는 것을 방지하는 것을 말한다. 위에 기술은 윈도우

즈 운영체제의 이벤트 드리븐 방식에서 후킹 기법을 도입하여, 컴퓨터가 클립보드를 사용하게 될 경우를 백그라운드에서 쓰레드로 실행되고 있던 화면 캡쳐 방지 프로그램이 이를 감지하여 클립보드에 저장되어 있는 화면 캡쳐 내용 또는 텍스트 문서를 비워 주어 붙여넣기 기능키를 사용하여도 화면 캡쳐 내용이나 텍스트 문서가 복사 붙여넣기가 되지 않는다. 그림 1은 화면캡쳐 방지모듈과 이벤트 드리븐 방식의 관계이다.

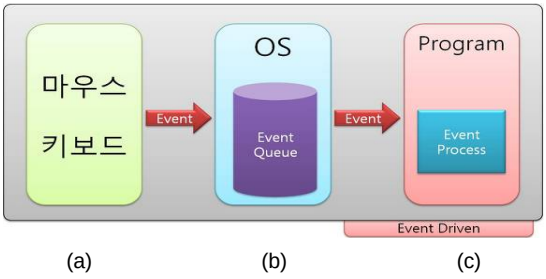


그림 1. 화면 캡쳐 방지 모듈과 이벤트 드리븐 방식과의 관계 (a) 입력 (b) 후킹 (c) 클립보드 비움
Fig. 1 Relation of prevent screen capture modules and Event-Driven system (a) Insert (b) Hooking (c) Clipboard Empty

2.2. WIN32 API 후킹

API는 후킹기술을 가능하게 해주는 모듈 중 하나이다. 후킹 기술은 크게 서브 클래싱(쓰레드 후킹), 슈퍼 클래싱(전역 후킹)으로 나눌 수 있다. 서브 클래싱(쓰레드 후킹)은 윈도우 프로시저로 보내지는 메시지를 중간에 가로채는 기법으로 특정한 쓰레드에서 발생하는 메시지만을 가로챈다. 슈퍼 클래싱(전역 후킹) 같은 경우는 모든 쓰레드에서 발생하는 메시지를 가로 챌 수 있다. 메시지 기반의 윈도우즈에서는 운영체제와 응용 프로그램, 또는 응용 프로그램 사이나 응용 프로그램 내부의 컨트롤끼리도 많은 메시지를 주고받는다. 일반적으로 시스템에서 메시지가 발생하면 운영체제가 관리하는 메시지 큐에 모두 저장된다. 따라서 메시지 후킹 프로그램의 과정은 메시지 큐에 들어온 메시지를 메시지 후킹 프로세스가 가로채어 응용프로그램으로 전달되지 못하도록 하는 방법을 사용한다. 메시지 후킹 프로세스를 통해 메시지를 가로채고 Hook_Process를 통해 최종 응용 프로그램에 전달하기 전에 메시지를 가로채어 임시 공유 메모리상에 저장하고 실행을 보류시킨다. 이후 시스템은 사용자에게 Win32 API 메시지의 사용권한이 허가되었을 경우 응용프로그램에게 전달하여 원하는 동작을 수행하게 되며, 허가 되어 있지 않을 경우 Win32API 메시지를 공유 메모리에서 삭제함으로써 응용 프로그램에서 메시지를 인식 할 수 없도록 한다. 윈도우 메시지가 발생했을 때 후킹 되는 과정을 그림 2에 나타내었다.

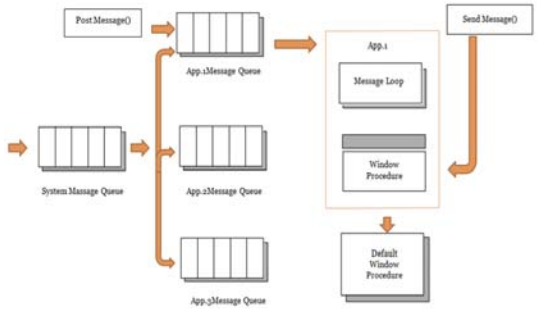


그림 2. 윈도우 메시지 후킹
Fig. 2 Window message hooking

Ⅲ. 모듈 구현

3.1. 구현 방법

화면 캡쳐 방지 모듈을 구현하기 전에 우선 모든 스레드에서 발행하는 윈도우 메시지를 가로 챌 수 있도록 슈퍼 클래싱(전역 후킹) 기법을 사용하여 전역 후킹 모듈을 구현하였다. 후킹 모듈 같은 경우는 반드시 dll형식으로 만들어 실행 시켜야 한다. dll형식의 파일을 실행시키기 위해서는 다른 응용 프로그램에 추가 종속시켜 훅 체인을 설치하도록 해야 한다. 훅 체인을 설치함으로 인해 후킹 시에 자신이 만든 메시지 프로시저로 변경이 가능해 진다. 설치 함수는 그림 3과 같다.

```
HHOOK SetWindowsHookEx(
    int idHook,             // type of hook to install
    HOOKPROC lpfn,          // address of hook procedure
    HINSTANCE hMod,         // handle to application instance
    DWORD dwThreadId        // identity of thread to install hook for
);
```

그림 3. 훅 프로시저 설치 함수
Fig. 3 Hook procedure installed function

화면 캡쳐 방지 모듈은 크게 세 가지로 구성하였다. 첫째, 전체 방지 기능 구현 방법은 백그라운드에서 실행되고 있는 캡쳐 방지 모듈이 프린터 스크린 키가 사용되는지를 O/S 상에서 감시하고 있다가 이를 감지하게 될 경우 클립보드 내용을 모두 비워 버리는 방식을 사용하였고, 복사기능(Ctrl + V)키 역시 화면 캡쳐 방지 모듈이 O/S 상에서 감시하고 있다가 Ctrl키를 감지하게 되면 클립보드로 접근하여 안의 내용을 모두 비워버리는 방법을 사용하였다. 둘째, 부분 방지의 기능 구현의 경우 프린터 스크린 키를 감지하면 클립보드에 저장된 내용을 잠시 DC에 보관한 후, 방지 하고자 하는 특정 영역에 접근하여 RGB의 색깔을 덧 입혀 줌으로써 특정 부분에는 흰색 또는 어두운 색으로 채우는 형식으로 구현 하였다. 가로챈 메시지를 사용자가 만든 메시지로 바꿔주는 함수는 그림 4와 같다.

```
LRESULT CallNextHookEx(
  HHOOK hhk,        //handle to current hook
  int nCode,        //hook code passed to hook procedure
  WPARAM wParam,    //value passed to hook procedure
  LPARAM lParam     //value passed to hook procedure
);
```

그림 4. 훅 체인 함수
Fig. 4 Hook chain function

마지막으로 시중에 배포 사용되고 있는 캡쳐 지원 프로그램을 사전에 등록하여 두고 용의자가 등록된 프로세스들을 실행시켰을 때 이들의 실행을 막도록 하였다. 또한 이 프로그램은 MFC를 기반으로 만들었지만 VB 등 다른 모듈에서도 실행하기 위해서 ATL COM이라는 방식을 사용하였다.

3.2. 구현 알고리즘

캡처방지 기능을 실행시키면 구현 방법에서 설명한 것과 같이 후킹함수들이 윈도우상에서 눌러지는 버튼들을 감지한다. 감지를 하는 도중 원하는 키 값을 누르게 되면 전체방지의 경우 클립보드에 있는 내용들을 지우게 되며, 부분방지의 경우 화면을 DC에 저장한 후 부분영역을 특정한 값으로 치환 한 후 이를 클립보드에 저장한다. 만약 원하는 키 값을 누르게 되지 않으면 계속해서 윈도우 버튼을 감시하게 된다. 그림 5는 화면 캡쳐 방지 모듈의 흐름도이다.

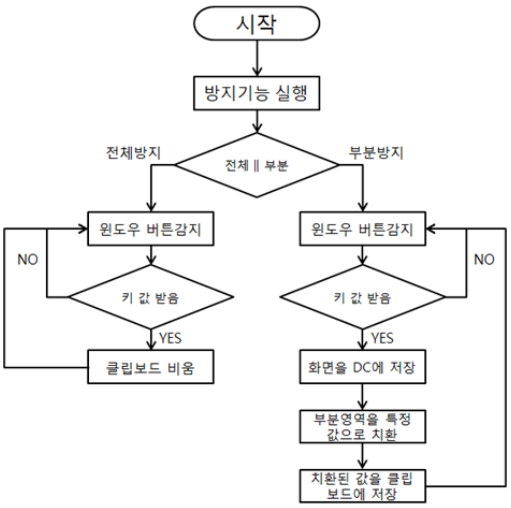


그림 5. 화면 캡쳐 방지의 흐름도
Fig. 5 Flowchart of the prevent screen capture

3.3. 실험 결과

dll 형태의 모듈 개발은 다른 응용 프로그램 내부에서 수행되고 있으므로 메인화면은 없고 모든 것을 환경설정 창에서 처리 할 수 있어야 한다. 본 모듈의 환경 설정 창을 그림 6에 나타내었다.

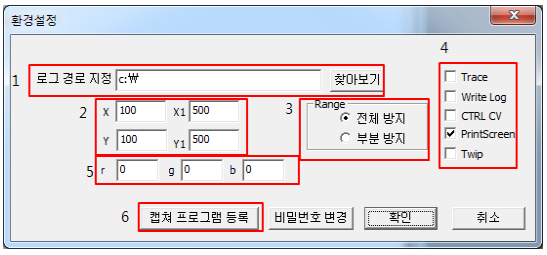


그림 6. 환경 설정 화면
Fig. 6 Configuration screen

설정 창에서 각 부분의 기능은 아래와 같이 정하였다.

1) 사용자의 사용 이력관리를 위한 로그 경로를 지정하는 부분.
2) 개인정보가 표시되어져 있는 부분만 보이지 않게 하기 위하여 영역을 지정하는 부분. (초기 단위는 픽셀)
3) 부분방지 혹은 전체방지 기능을 지정 하는 부분.
4) 관리자의 편리를 도모하기 위하여 각종 기능을 선택하여 사용 할 수 있도록 하는 부분.

5) 지정된 부분 방지 영역에 출력되는 색상을 바꿀 수 있게 하는 부분.
6) 최근 배포되고 있는 캡쳐 프로그램이지만 실행을 방지하고자 할 때 그 실행파일명을 추가할 수 있는 부분.

그림 7과 같은 자신의 개인 정보를 기록한 이력서를 파일로 컴퓨터에 저장해 두었으며 이를 대상으로 본 모듈의 기능들을 테스트를 하였다.

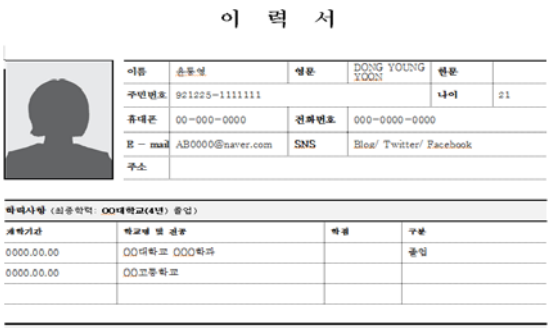


그림 7. 개인 이력서 파일
Fig. 7 Personal history file

개인 이력서 파일에 화면 캡쳐 방지 모듈을 종속시켜 전체 방지 기능을 수행한 결과를 그림 7에 나타내었다. 이력서의 모든 정보는 보이지 않고 검게 출력됨을 알 수 있었다.

그림 8. 전체 방지 기능을 수행한 결과
Fig. 8 The result of performing full protection

개인 이력서 파일에서 개인 정보 영역에만 부분 방지 기능을 적용하였을 경우의 결과를 그림 8에 나타내었다. 이력서 파일 중에서 사용자가 지정한 영역의 정보만 보이지 않고 검게 출력됨을 알 수 있었다.

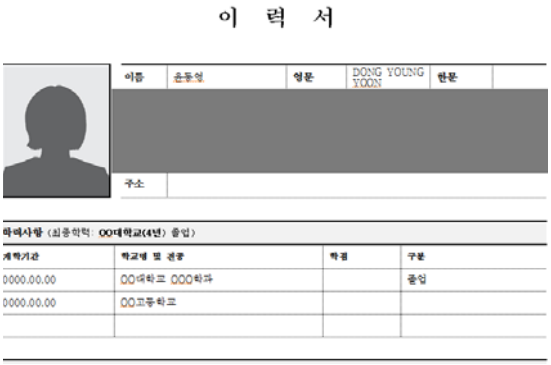
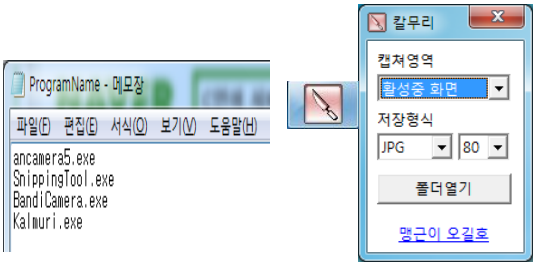


그림 9. 부분 방지 기능을 수행한 결과
Fig. 9 The result of performing partial protection

마지막으로 시중에 배포 사용되고 있는 캡쳐 지원 프로그램의 일종인 '칼무리'를 등록한 결과를 그림 10에 나타내었으며, 등록된 파일에 'Kalmuri.exe' 파일이 존재하므로 이 프로그램을 실행시켰을 때 이들이 실행되지 않음을 확인할 수 있었다.



(a) (b)

그림 10. 캡쳐 프로그램 등록 (a) 프로그램 등록 (b) 실행 결과
Fig. 10 Registration of capture program (a) Program registration (b) Execution result

Ⅳ. 결 론

본 논문에서는 PC보안에 중점을 두어 화면 캡쳐 방지 모듈을 구현하여 컴퓨터를 사용하면 개인의 정보나 중요한 자료를 다루는 기관을 대상으로 개인 정보 및 중요한 자료가 기관 시스템을 통해 오가는 동안 고의로 개인 정보가 유출 되는 것을 1차적으로 막기 위한 해결 방안을 제시하였다. 또한 화면 캡쳐 방지 모듈은 기존에 개인 정보나 중요한 정보를 다루는 프로그램에 DLL

형태로 추가하여 캡쳐 방지 기능을 수행하도록 구현되어 별도의 환경을 구축할 필요가 없는 장점이 있다.

화면 캡쳐 방지 모듈로 인해 정보의 기밀성을 보장하여 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하여 비밀 보장을 유지하고, 원치 않는 정보의 공개를 막을 수 있다. 정보에 대한 무결성을 유지하여 정보의 수정할 수 없도록 하며, 가용성 또한 높여 정보에 접근하려 하고자 할 때 방해 받지 않고 정보를 보안할 수 있다.

감사의 글

이 논문은 2013학년도 경성대학교 학술연구비 지원에 의하여 연구된 것으로서, 관계부처에 감사드립니다.

REFERENCES

[1] S. Y. Shin and T. K. Kwon, “A Study of HCI technologies for privacy”, *Review of KIISE Korea Institute of Information Science and Engineers*, vol. 27, no. 12, pp. 68-77, Dec. 2009.

[2] T. H. Hwang, Security incidents Dilemma. KT can not see a solution specifically, [Internet]. Available: http://search.etnews.com/etnews, 2012. 07. 31

[3] J. J. Lee, MBC Information gathering program went out to financial transactions, and medical information, [Internet]. Available: http:// www.mediatoday.co.kr/news/Media Today, 2012. 09. 24.

[4] M. J. Back, Goes out personal privacy by App stomach, [Internet]. Available: http: //www.focus.co. kr

[5] Y. I Cho, “Information Privacy and Intelligent Agency Technology,” *Review of Korean Institute of Information Technology, vol. 6, no. 1, pp. 29-35, Jan. 2008.*

[6] Y. H Shin and J. C. Ryou, "Study on adoption of suitable encryption scheme according to data properties on MySQL Database," *Proc. of the KIISE Korea Computer Congress 2010, vol. 37, no. 1(D), pp. 77-80, Jan. 2010.*

[7] C. S. Ahn and J. G. Shon, "Design and Implementation of a Hooking Client for Document Security in File Sharing Environments based on SMB Protocol," *Proc. of the KIISE Korea Computer Congress 2009, vol. 36, no. 1(D), pp. 61-65, Jan. 2009.*

[8] J. H. Park, N W. Jo, K. H. Lee and I. H. Choi, "Development of Personal Information Protection Systems in company," *Review of KIISC Korea Institute of Information Security and Cryptology, vol. 18, no. 6, pp. 28-33, Jun. 2008.*

[9] D. R. Kim, K. C. Sim and M. S. Jeon, "Personal information protection system compared to the Privacy Act," *Review of KIISC Korea Institute of Information Security and Cryptology, vol. 21, no. 6, pp. 16-23, Jun. 2011.*

[10] Y. N. Shin and M. G. Chun, "Personal Information Protection for Biometric Verification based TeleHealth Services," *Korean Institute of Intelligent Systems, Vol. 20, No. 5, pp. 659-664, Oct. 2010.*

[11] NIST, "NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing,” 2011. 01.

[12] NIST, "NIST SP 800-145 The NIST Definition of Cloud Computing,” 2011. 01.

[13] NIST, "NIST SP 800-146 Cloud Computing Synopsis and Recommendations,” 2011. 05.

이종혁(Jong-hyeok Lee)

1975년 부산대학교 전자공학과 학사
1980년 부산대학교 대학원 석사
1991년 부산대학교 대학원 전자계산기전공 박사
1990년~현재 경성대학교 컴퓨터공학부 교수
※관심분야 : 인공지능, 증강현실, 정보보안