論文2002-39TE-1-11

새로운 침입 패턴을 위한 데이터 마이닝 침입 탐지 시스템 설계

(Design of data mining IDS for new intrusion pattern)

片 奭 範 *, 丁 鍾 根 *, 李 潤 培 **

(Suk Bum Pyeon, Jong Geun Jeong, and Yun Bae Lee)

요 약

침입 탐지 시스템은 침입 판정과 감사 데이터(audit data) 수집 분야에서 많은 연구가 진행되고 있다. 침입 판정은 주어진 일련의 행위들이 침입인지 아닌지를 정확히 판정해야 하고 감사 자료 수집에서는 침입 판정에 필요한 데이터만을 정확히 수집하는 능력이 필요하다. 최근에 이러한 문제점을 해결하기 위해 규칙 기반 시스템과 신경망 등의 인공지능적인 방법들이 도입되고 있다. 그러나 이러한 방법들은 단일 호스트 구조로 되어있거나 변형된 새로운 침입 패턴이 발생했을 때 탐지하지 못하는 단점이 있다. 따라서, 본 논문에서는 분산된 이기종 간의 호스트에서 사용자의 행위를 추출하여 패턴을 검색, 예측할 수 있는 데이터 마이닝을 적용하여 실시간으로 침입을 탐지하는 방법을 제안하고자 한다.

Abstract

IDS has been studied mainly in the field of the detection decision and collecting of audit data. The detection decision should decide whether successive behaviors are intrusions or not , the collecting of audit data needs ability that collects precisely data for intrusion decision. Artificial methods such as rule based system and neural network are recently introduced in order to solve this problem. However, these methods have simple host structures and defects that can't detect changed new intrusion patterns. So, we propose the method using data mining that can retrieve and estimate the patterns and retrieval of user's behavior in the distributed different hosts.

1. 서 론

고속으로 운영되는 네트워크 중심의 방화벽은 침입 시도를 차단하기 위해서 설계된다. 이는 하드웨어를 기반으로 하며 라우터, NIC(Network Interface Card), 통합회로 등에 포함된다. 침입 탐지 시스템(Intrusion Detection System)은 방화벽을 통과한 침입자를 탐지해 내는 기술로써 오용탐지 기술과 비정상 탐지 기술이 있다. (그림1)에서와 같이 데이터 소스 기반의 침입 탐지 기술로서는 호스트 기반과 네트웍 기반으로 나눌 수 있다[1, 9, 11-12].

호스트 기반은 운영체제의 감사 데이터, 즉, solaris의 BSM, pacct, lastlog, sulog, utmp, wtmp 또는 웹서버의 access log 등을 이용하여 탐지하며, 네트웍 기반에서는 libpcap, tcpdump 등의 네트웍 패킷을 이용하여 탐지한다.

기존의 침입 탐지 시스템들은 하나의 통합된 단일 호스트 기반의 형태를 가지고 있다. 이러한 시스템들은 전체 시스템에 걸리는 부하문제, 탐지 모듈의 에러문제, 시스템 확장에 따른 성능 저하 문제 등이 제기되고 있다. 이러한 문제점을 해결하기 위한 방법으로는 탐지

* 正會員, 東岡大學 電子情報科
(Dept. of Electronics & Information Eng., Dongkang College)
** 正會員, 朝鮮大學校 컴퓨터工學部
(Dept. of Computor Eng., Chosun University)
接受日字:2001年6月20日, 수정완료일:2002年3月10日

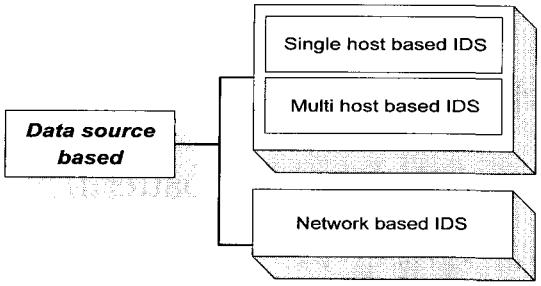


그림 1. 데이터 소스 기반 IDS 분류
Fig. 1. Classification of data source based IDS.

시스템을 기능적, 독립적으로 분할하는 에이전트를 채용해서 다수의 프로세스들로 하여금 각각 독립적인 동작으로 분할된 시스템들을 모니터링한다. 이들은 한 시스템에 침입이 발생할 경우 에이전트들 간의 협력을 통해서 침입을 탐지하도록 구성한다. 이를 위해 에이전트는 다른 에이전트와 상호간의 통신이 가능하며, 침입 탐지 에이전트를 생성한 메인 호스트가 네트워을 제거하기 전까지 활동을 할 수 있어야 한다. 이러한 에이전트는 관리자의 개입 없이 독립적으로 임무를 수행하도록 하여 사용자가 네트워에 접속하고 있지 않은 경우에도 관리자를 대행하여 태스크를 수행한다[13].

본 논문에서는 에이전트가 감사데이터(Audit data)를 수집, 분석하기 위해서 데이터 마이닝 기술을 적용하였다. 대부분의 침입 탐지 시스템은 과거의 침입 데이터를 토대로 탐지하기 때문에 새로운 침입 패턴이 나올 때 이를 탐지하기가 쉽지 않다. 이를 보완하기 위해 최근에는 인공지능기법을 이용하여 새로운 침입 패턴을 생성하는 연구가 진행되고 있다. 데이터 마이닝은 과거의 침입 패턴을 수집하여 일정한 패턴을 생성한 다음 새로운 침입이 발생 할 경우 이를 효율적으로 탐지해 낼 수 있는 기술이다[4-6].

콜롬비아 대학의 JAM(Java Agent for Meta-learning)에서는 비정상 행위 탐지의 학습을 위해 메타 학습 기법을 사용하였다. 데이터 마이닝 기법에서 연관 규칙과 빈번 규칙을 적용할 때 대량으로 생성되는 규칙의 수를 줄이는 것이 문제점이다[7]. 본 논문에서는 이러한 문제점을 해결하기 위해 각각의 호스트에서 발생하는 다량의 감사 데이터중에서 침입 탐지에 필요한 필드(field)만을 추출하여 표준화함으로써 이러한 문제점을 해결하고자 한다.

2. 에이전트기반 침입 탐지 시스템

침입 탐지 시스템에서는 각 모듈에이전트들이 분산되어 있는 호스트들에 대한 모니터링을 하게되며, 비정상적인 행동이라고 의심이 갈 경우 이 사실을 관리자에게 즉각 통보한다. 그리고, 새로운 침입 패턴을 항상 학습하게 된다. 에이전트 학습을 위해서 데이터 마이닝 알고리즘을 적용한다[2-5]. 데이터 마이닝 알고리즘은 과거에서 현재까지의 행동 패턴을 수집하여 분류하는 알고리즘으로 전자상거래 등에서 고객의 구매 패턴을 예측하는데 주로 이용하는 기술이다. 에이전트들은 상호 독립적으로 태스크를 수행하며 사용자들이 로그아웃(log out) 할 때까지 모니터링하여 로그 데이터를 수집한다.

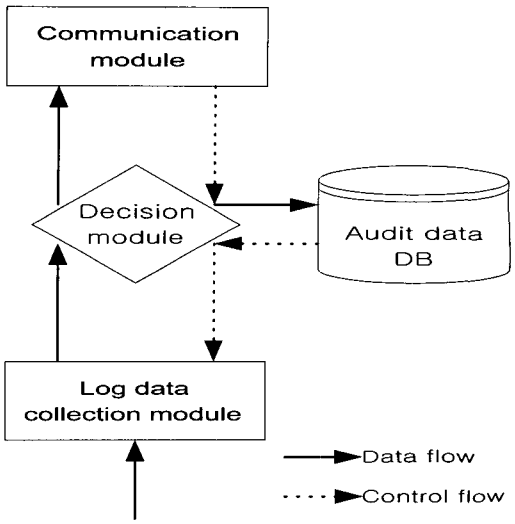


그림 2. 에이전트모듈 내부 구조
Fig. 2. Internal structure of agent module.

수집된 로그 데이터는 침입탐지 메인 호스트에 있는 학습 모듈로 전송되어 각각의 사용자들에 대한 행동패턴을 다양한 각도에서 분류한다. 이렇게 분류된 각 사용자들의 행동패턴은 침입패턴 데이터베이스(Intrusion Pattern DB)에 저장된다음 지속적으로 에이전트와 통신하면서 패턴데이터를 교환한다. (그림2)는 에이전트 모듈의 내부구조를 나타낸 것이다.

침입 탐지 시스템들은 한 개의 침입 탐지 프로세스에 의해 침입 탐지를 수행하므로 시스템의 부하는 물론 한 프로세스의 결함이 전체 시스템의 성능을 떨어

뜨리는 문제점을 가지고 있다. 이에 대한 해결책은 다중 에이전트를 이용하여 분산 시스템 전체에서 시스템에 대한 감시와 자료 수집, 탐지 등의 작업을 수행토록 하는 것이다. 또한, 이들 침입 탐지 시스템들은 자체적인 학습 기능이 없으므로 시스템의 환경 변화나 새로운 공격 유형이 나타날 때 유연하게 대처할 수 없다. (그림3)은 일반적인 실시간 침입 탐지 시스템의 구조를 나타낸 것이다[10].

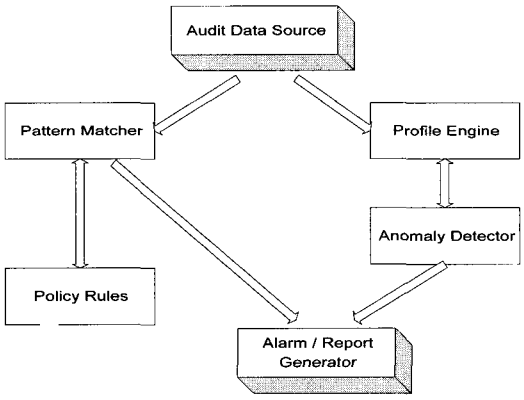


그림 3. IDS의 일반적인 구조도
Fig. 3. General structure of IDS.

일반적인 IDS 구조는 탐지 규칙에 의해 수집된 감사 데이터를 패턴 매칭하여 침입을 탐지하며 거의 모든 IDS에서 이러한 원리를 따르고 있다[10].

1. 데이터 마이닝 탐지 기술

데이터 마이닝 알고리즘은 과거에서 현재까지의 행동 패턴을 수집하여 분류하는 알고리즘으로 전자상거래 등에서 고객의 구매 패턴을 예측하는데 주로 이용하는 기술이다.

침입 탐지 시스템에서 분산되어 있는 호스트들의 행위를 모니터링하고 침입을 감시하기 위해서는 대용량의 감사 데이터(Audit Data)를 검사해야 한다. 특히, 이기종 간의 감사 데이터를 참고하기 위해서는 각 운영체제마다 감사 데이터 포맷이 다르기 때문에 상당한 부하를 가질 수 있다[11-12].

따라서, 대용량의 감사 데이터로부터 시스템의 행위를 탐지해 내기 위해 효과적이고 지능적인 분석도구가 필요하며 이를 위해 데이터 마이닝 기법이 효과적이다. 데이터 마이닝 기법에서는 데이터 아이템을 여러개의 미리 정의된 범주에 할당하여 시스템 사용자나 프로그램에 대해 정상과 비정상의 데이터를 수집하여 훈련시킴으로써 전체 로그 데이터의 양을 줄이고, 시스템이 아직까지 경험하지 않은 데이터를 정상과 비정상으로 분류하도록 학습시킨다. 이때, 시스템에서 발생하는 행위들에 대해 순차적인 패턴을 추출하고 빈번하게 발생하는 행위에 대해 시간적인 통계자료를 측정한다.

감사 데이터로부터 패턴을 추출하고 모델 집합을 만들기 위해 데이터 마이닝 알고리즘을 적용한다. 먼저, 초기의 감사 데이터 집합은 전처리 과정과 요약을 거쳐 몇가지 기본적인 특징을 포함하고 있는 레코드로 생성된다. 예를들어, timestamp, duration, source IP address, destination IP address, ports, and error flags 등을 포함한다. 그런 다음, 데이터 마이닝 알고리즘은 이러한 특징들 사이에 연관되어 있는 패턴과 레코드들 사이에 빈번하게 발생하는 사건들을 계산한다. 정상 행위와 관련된 일련의 패턴들과 침입에 관련되어 있는 패턴들은 계속적으로 분류되어 추가된다.

2. 침입 탐지를 위한 감사데이터 학습

비정상 탐지를 위한 기계학습 방법의 어려움은 알려져 있지 않은 패턴과 알려진 패턴의 한계를 정하는 것이다. 훈련데이터에 있어서 비정상 패턴에 대한 별다른 예를 가지고 있지 않은 상태에서는 기계학습 알고리즘은 훈련 데이터에 있는 알려진 패턴에 대한 한계를 구분할 수 없다. 일반적으로, 비정상과 오용 탐지를 구분하기란 쉬운 일이 아니다. 비정상 탐지는 전형적으로 비통제된 학습 방법을 사용하는 반면에, 오용 탐지에서는 통제된 분류 방법을 사용한다.

따라서 변형된 패턴의 공격이 발생할 경우 이를 탐지해 내지 못한다. 본 논문에서는 변형된 새로운 유형의 공격이 발생할 경우, 이 공격 패턴을 즉시 학습시킴으로써 새로운 공격에 대응하고자 한다. 새로운 공격 패턴이 발생할 경우 이미 분류되어 있는 침입 패턴 집합에 계속적으로 추가시킨다.

(그림4)의 알고리즘에서와 같이 H_2는 새로운 침입 패

```
if (H1(x)=normal) ∨ (H1(x)=anomaly) then
  if H2(x)=normal
    then output ← H1(x)(normal or anomaly)
    else output ← new_intrusion
else output ← H1(x)
```

그림 4. 침입 탐지 학습 알고리즘
Fig. 4. Learning algorithm for intrusion detection.

턴과 정상 데이터로부터 학습된 추가된 분류자이다[2]. 위의 알고리즘에서 결정 규칙은 출력을 위해서 평가된다.

H_1은 존재하는 침입 탐지 시스템 모델이고, H_2는 최근에 발견된 새로운 침입 패턴을 위해 훈련된 새로운 모델이다. H_1에서는 정상과 비정상 패턴만을 확인하고, 새로운 침입을 확인할 수 없기 때문에 대부분의 패턴들은 비정상과 오용으로 분류한다. 그러나, H_2는 새로운 침입과 정상 데이터로 분류한다. 이때 새로운 침입 패턴의 양이 적기 때문에 H_2는 다른 데이터로부터 침입 패턴을 쉽게 분류할 수 있다[3].

3. 제안된 시스템의 구조

데이터 마이닝 알고리즘을 탑재한 에이전트 기반 침입 탐지 시스템의 구조는 (그림5)와 같다[12]. audit data DB에는 데이터 마이닝 알고리즘으로 학습된 감사 데이터가 저장되어 있으며, 감사 데이터의 학습과 확정은 오프라인(off-line) 작업으로 수행된다. 새로운 패턴의 공격이 나타날 때 data mining generator에서 침입 패턴을 생성하여 audit dtata DB에 저장한다. 기존의 시스템에서는 data wearhouse를 사용하였으나 본 논문에서는 audit data DB를 사용하여 datamining generator에서 생성된 audit data를 저장하게 하였고, data processor에서는 이기종에서 생성하는 로그데이터를 하나의 표준양식으로 변형하도록 하였다.

(그림6)과 같이 data processor는 각기 다른 환경의

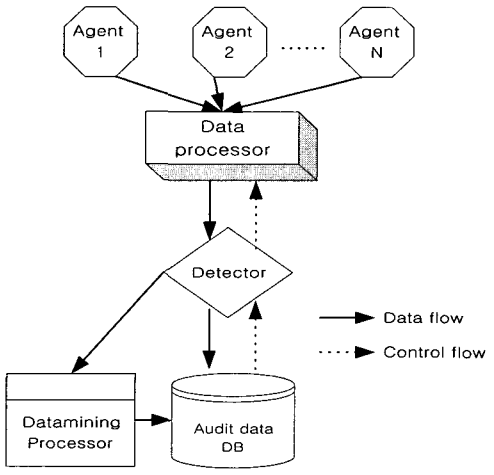


그림 5. 제안된 IDS 구조
Fig. 5. Suggested IDS structure.

운영체제에서 수집되는 로그 데이터중에 필요한 필드만을 추출하여 하나의 포맷(format)으로 변형시킴으로써 Detector가 다른 운영체제들 간의 로그 데이터를 탐지하는데 별다른 작업 없이 수행하도록 하여 시스템의 부하를 최소화하도록 한다. 본 논문에서 제안한 감사 자료 표준화를 위해 각기 다른 OS인 Linux와 AIX 기종의 OS에서 생성되는 로그파일을 표준화하였다.

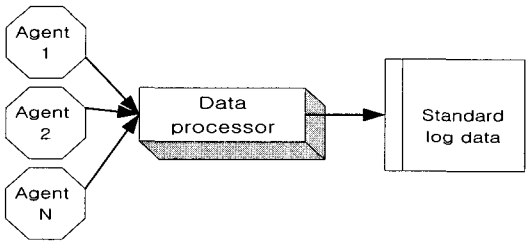


그림 6. 데이터프로세서에 의한 감사데이터 표준화
Fig. 6. Audit data standardization by data processor.

(그림7)은 각각의 OS에서 추출하여 로그 프로세서를 통해 변환된 표준화된 감사 데이터의 구조를 보여주고 있다.

```
struct std_audit_data {
        unsigned long   tseq;
        char            hostname[32];
        char            remotehost[32];
        char            ttyname[16];
        char            cmd[18];
        char            jobname[16];
        char            dellog;
        char            errlogin;
        char            errorflagd;
        time_t          timestamp;
        long            syscall;
        long            errno;
        char            port;
        long            pid;
```

그림 7. 감사 데이터 표준 형식
Fig. 7. Standard format of audit data.

4. 제안된 시스템 분석 및 환경

본 실험에서는 펜티엄 II266MHz에서 Red Hat linux 6.0 운영체제와 IBM AIX기종을 사용하였다. 데이터 마이닝을 이용해 침입을 탐지하기 위한 실험을 위해 setUID를 이용하여 root의 권한을 획득하려고 할 때 사용되는 명령어들을 로그 데이터로 수집한다.

다음은 setUID를 이용하여 root의 권한을 획득하기위해 사용되는 명령어들에 대한 대응표를 작성한다.

표 1. 초기 DB 명령 대응표
Table 1. The first DB command table.

명령유형	id	ls-l	find	more	su	./	whoami
대응값	A	B	C	D	E	F	H

setUID를 사용하여 root 권한을 획득하는 순서는 다양하기 때문에 유사한 접근 시도를 유형별로 분석하여 알려진 침입 방법인지 새로운 유형의 침입 방법인지를 판별한다. 표2는 setUID를 이용하여 root 권한을 획득하는 유형을 나타낸 것이다.

표 2. setUID 사용 유형
Table 2. Using pattern setUID.

상태 / ID	S1	S2	S3	S4
jkcom	A	B	C	F
yblee	B	C	D	F
psbum	C	F	H	B
yhkim	B	C	F	A

(표2)의 명령집합은 순서가 고려된 명령 집합이다. 이 표에서 침입유형 X에 대해서 전체 트랜잭션에서 X가 차지하는 비율을 나타내는 지지도와 침입유형 X가 포함되는 트랜잭션의 비율을 나타내는 신뢰도의 임계값(threshold)을 2로 주었을 때 다음과 같은 최종 감사데이터를 생성해낸다. 임계값이라는 것은 최소의 지지도와 신뢰도를 표시하는 것으로 임계값을 높이게되면 침입유형 X를 포함하는 순서패턴을 많이 발견하게 된다. 하지만 임계값이 높을수록 긍정적 경함의 발생 확률이 높아진다.

표 3. 감사 데이터 생성
Table 3. Audit data generation.

명령순서	{B, C, F}
빈도수	2

(표3)의 결과는 최소지지도를 1로 했을 때 (표1)에서 {B,C,F}의 연속된 패턴이 나타나는 빈도수를 표시한 것이다.

마지막으로 생성된 감사데이터는 IDS DB에 저장되어 이와 같은 침입 사건이 발생할 때 이를 탐지한다. 임계값의 조정은 시스템 관리자에 의해 사용자의 수나 시스템 처리 능력에 따라 변화시킬 수 있게 하였다.

5. 결론 및 향후 연구 방향

본 연구에서는 알려지지 않은 새로운 침입 패턴을 탐지하도록하는 방법에서 데이터 마이닝과 감사데이터 표준화 방법을 제안하였다. 데이터 마이닝 알고리즘의 분류 알고리즘으로 정상과 비정상 패턴을 분류하여 탐색할 로그 데이터의 양을 줄였고 비정상 패턴중에 변형된 비정상 패턴을 추측하여 침입을 탐지해내도록 하였다. 또한, 접속 상태에 라벨을 붙임으로써 알려지지 않은 새로운 침입 패턴을 추측하게 할 수 있게 하였다. 분산된 환경에서 여러 호스트를 탐지해내기 위해 독립적으로 동작할 수 있는 에이전트를 사용하였으며, 로그 데이터 표준화 단계에서는 각각 다른 기종에서 발생되는 다량의 로그 데이터를 하나의 로그데이터 형식으로 표준화함으로써 침입 탐지 호스트에서 각각 다른 OS의 로그데이터를 별도로 검사해야 했던 작업을 최소화 하였다.

향후 연구과제로는 실시간 침입 탐지를 위한 학습의 최적화 방안을 모색하고, 네트워크상의 비정상 탐지를 위한 방안에 대한 연구가 지속적으로 필요하다. 또한 새롭게 나타나고 있는 해킹 패턴에 대응할 수 있는 다각적인 시각에서의 대처 방안이 연구되어야 한다.

참 고 문 헌

[1] A. Ghosh and A. Schwartzbard. "A study in using neural networks for anomaly and misuse detection". In proceedings of the Eighth USENIX security Symposium, 1999.

[2] T. Fawcett and F. Provost. "Adaptive fraud detection Data Mining and Knowledge Discovery". 1:291-316, 1997.

[3] T. Lane and C. E. Brodley. "Temporal sequence learning and data reduction dor anomaly detection". In Processsing of the fifth ACM

Conference on Computer and Communications Security, pages 150-158, 1998.

[4] W. Lee, S. J. Stolfo. "Data mining approaches for intrusion detection". In Proceding of the 1998 USENIX security Symposium, 1998.

[5] W.Lee, S.J.Stolfo, and K.Mok, "A Data Mining Framework for Building Intrusion Detection Models", 1999 IEEE Symposium on security and Privacy, 1999.

[6] Sandeep Kumar, gene Spafford. "A Pattern Matching Model for Misuse Intrusion Detection", Proceedings of the 17th National Computer Security Conference, October 1994.

[7] T. lane and C. E. Brodley. "Detecting abnormal: Machine learning in computer security", Technical Report TR-ECE 97-1, Prudue University, West Lafayette, IN, 1997.

[8] Jai Sundar B. Spafford E, "Software Agents for Intrusion Detection," Technical Report, Purdue University, Department of Computer Science, 1997.

[9] Crosbie M, Spafford E, "Defending a Computer System using Autonomous Agents," Technical Report, Purdue University, Department of Computer Science, 1996.

[10] Wenke Lee, Salvatore J.Stolfo, Philip k.Chan, "Real Time Data Mining-based Intrusion Detection". In proceedings of IEEE symposium on research in security and privacy, 2000.

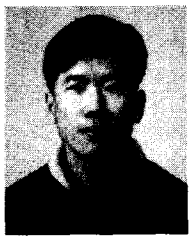
[11] 은유진, 박정호, "침입 탐지 기술 분류 및 기술적 구성요소", 정보보호센터 정보보호 뉴스 1998.7 통권 13호.

[12] 편석범,정종근, 이윤배, "데이터 마이닝 기법을 적용한 최적 침입 탐지 모듈 설계", 1999. 춘계정보과학회 논문집

[13] 편석범, 정종근, 이윤배, "패턴 추출 에이전를 이용한 분산 침입 탐지 시스템 모델 설계 및 성능 평가", 2000,12 대한전자공학회 논문지(TE권)

저 자 소 개

片 奭 範(正會員) 第38卷 TE編 第4號 參照



丁 鍾 根(正會員)

1995년 : 조선대학교 전자계산학과 졸업(이학사). 1997년 : 조선대학교 대학원 전자계산학과 졸업(이학석사). 1999년 3월~현재 : 조선대학교 대학원 전자계산학과 대학원 박사과정. 1999년 3월~2001년 현재 : 동강대학 전자정보과 겸임교수. <관심분야 : 인공지능, 전문가 시스템, 데이터베이스, 정보보안, 전자상거래, 바이러스, 멀티미디어>

李 潤 培(正會員)

1980년 : 광운대학교 전자계산학과 졸업(이학사). 1983년 : 광운대학교 대학원 전자계산학과 졸업(이학석사). 1993년 : 숭실대학교 대학원 전자계산학과 졸업(공학박사). 1988년 4월~현재 : 조선대학교 컴퓨터공학부 교수. 1999년 7월~2000년 현재 : 광주광역시 시정정책자문회의 위원. 1996년 7월~2000년 현재 : 광주광역시 및 전라남도 지역 정보화 추진위원, 2000년~2000년 현재 : 광주교육신문사 회장, 1997년 9월~2000년 2월 : 조선대 정보과학대학장, 1996년 12월~1997년 2월 : 호주 타스마니아대학 초청교수. <관심분야 : 인공지능, 전문가시스템, 멀티미디어, 데이터베이스, 정보보안, 바이러스>