JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 23, No. 2, pp. 303-308, Feb. 2022

Check for updates

다양한 입력채널 환경에서의 통합보안 시스템구축을 위한 빅데이터 처리 플랫폼에 관한 연구

김 정 범[1]
[1]남서울대학교 빅데이터인공지능학과 교수

A study on big data processing platform for integrated security system in various input channel environments

Jeong-Beom Kim[1]
[1]Professor, Department of Bigdata AI, Namseoul University, Choong Nam Seonghwan DaeHak Ro 1, Korea

[요 약]

다양한 입력채널 환경에서의 통합보안 시스템에 대한 플랫폼은 데이터 처리에 있어서 다량의 데이터를 기반으로 한 로그수집, 분석 기능을 제공해야 한다. 또한 APT 공격과 같은 예상하지 못한 공격에 대하여 유연하게 대응하며 빠른 처리능력을 기반으로 여러 가지 각도에서 상관관계 분석 결과를 도출해야 한다. 주요한 기능으로서 다양한 환경에서 통합보안 관리를 할 수 있는 기능을 제공하고 취약점을 분석하며 자료에 따른 통제 대책 기능을 제공해야 한다. 본 연구에서는 통합관제체계들의 단편적 로그, 일시적 로그의 분석을 넘어선 다양한 입력 채널 환경에서 광대한 데이터에 대한 분석을 빅데이터 플랫폼 기반을 가지고 연구하였다.

[Abstract]

The platform for the integrated security system in various input channel environments should provide log collection and analysis functions based on a large amount of data in data processing. And correlation analysis results should be derived from various angles based on rapid processing capability. As a major function, it should provide a function for integrated security management, analyze vulnerabilities, and provide control measures according to data in various environments. In this study, vast data analysis in various input channel environments, beyond the analysis of fragmentary and temporary logs of integrated control systems, was studied based on a big data platform.

색인어 : 통합보안, 다채널 환경, 빅데이터, 인공지능, 관제시스템

Keyword : Integrated security management, Multi-channel environment, Big data, AI, Monitoring System

http://dx.doi.org/10.9728/dcs.2022.23.2.303

Received 31 December 2021; **Revised** 14 February 2022
Accepted 05 February 2022

***Corresponding Author; Jeong-Beom Kim**
Tel: ※ 개인정보 표시제한
E-mail: jbkim@nsu.ac.kr

Ⅰ. 서 론

1-1 연구배경

모든 산업분야에서 중요시되고 있는 통합보안에 대한 관리는 핵심과제이며 중요한 업무시스템 중의 하나이다. 많은 기업체와 공공기관들이 보안관제 시스템을 활용하여 위협에 최대한 빠르고 정확하게 대응하기 위해서 각 분야별로 다양한 보안 솔루션을 설치하여 운영하고 있으며, 각기 다른 분야에서 서로 다른 목적과 의미를 가지고 보안 관련 시스템을 발전시켜 오고 있다. 다양한 보안 솔루션을 통해 보안에 대한 위협을 원천 차단하고자 하지만, 보안 사고는 지속적으로 발생하고 있다. 이러한 상황에서 기업이나 공공기관이 보유하고 있는 각종 보안제품(방화벽, IPS, VPN) 및 네트워크 장비(서버, 라우터 등)를 상호 연동하여 효율적으로 관리하거나 관제할 수 있는 통합보안관리 시스템이 개발되어 운영되고 있다. 과거 기존 연구에서는 통합로그 관리 솔루션은 대량의 로그 데이터가 쌓일 경우 로그 수집 및 검색 성능이 현저하게 떨어지는 경향이 있다. 이에 대한 문제점들을 보완하기위하여 본 연구배경으로서 기존 보안관제 체계들의 단편적 로그, 일시적 로그의 분석을 넘어선 다양한 입력채널 환경에서 광대한 데이터에 대한 분석을 빅데이터 플랫폼 기반을 가지고 연구하는데 차별성이 있다[1].

1-2 연구목적

본 연구에서는 통합보안관제 시스템에서 제공하고 있는 로그 관제 기능에 빅데이터 시스템을 활용하여 독자적인 로그 저장 및 분석 기술을 기반으로 원본 로그에 대한 실시간 수집 · 저장 · 분석을 갖춘 빅데이터 플랫폼을 구성하기 위하여 가상환경 기반에서 작동하는 방식과 실제 분산 환경에서 운용하는 방식의 2가지 아키텍처로 개발하였다. 아울러 국내에서 경쟁력을 갖추기 위해 개인정보 보호법, 정보통신기반 보호법 등 정부가 기업들에게 요구하는 법적 요구사항을 관리할 수 있도록 개발하였다. 통합보안 관리시스템은 기능별, 제품별로 모듈화된 보안관리 기능을 통합하여 일관적인 사용자 인터페이스를 제공한다. 특히 보안로그에 대한 빅데이터 분석기능으로서 기존의 통합보안 관리시스템이 지원하지 못한 예측기능과 알려지지 않은 공격까지 탐지할 수 있는 통합보안 관리시스템으로 발전시켜야 한다. 시스템 로그, 어플리케이션 로그, 네트워크 로그까지 모든 로그를 통합하여 분석하고 데이터 마이닝 기법과 같은 각종 통계 기법을 적용하고 위협을 경보하여 보안 관제의 효과성과 운영의 효율성을 높이는 방안을 연구하였다[2].

Ⅱ. 본 론

2-1 다양한 입력채널 환경에서의 빅데이터 처리 플랫폼

다양한 입력채널 환경에서의 빅데이터 시스템을 구축하고 최적의 성능을 보장하기 위해서는 서버의 수를 최대화 하여야 한다. 하지만 비용대비 효과적인 시스템을 구축하기 위해서는 가상화를 이용하여 서버 1대만 이용하여 빅데이터 시스템을 구축하는 것을 목표로 서버 가상화로 운영되는 플랫폼을 구축하여야 한다. 또한 가상화 플랫폼은 시스템의 자원을 보다 효율적으로 사용할 수 있으며, 하나의 어플라이언스 형태로 생산이 가능하기 때문에 제품화에 있어서도 기존 플랫폼과 비교하여 차별화가 된다고 볼 수 있다.

1) 시스템 아키텍처

최소의 비용으로 최고의 성능을 얻기 위한 빅 데이터 시스템을 구축하기 위하여 가상화를 통하여 시스템을 구성하였다. 가상화를 이용하면 하나의 Appliance만으로도 빅 데이터 시스템의 구현이 가능하다. 이를 구현하기 위한 Hypervisor로는 Xen을 채택하였다. 이 Xen을 통하여 하드웨어를 전가상화 시킴으로써 여러 개의 가상의 물리적 공간을 형성하고, 그 각각의 공간에 OS를 설치하여 여러 대의 서버로 구성된 것과 동일한 시스템을 구축하였다. Xen은 VMWare나 VPC와는 달리 Full Emulation이 아니기 때문에 Xen위에서 사용할 수 있는 OS가 기본적으로 Linux 계열에 국한되므로 각각의 가상머신에는 기본적으로 Linux OS를 설치하였다. 전체 가상환경을 관리하는 1개의 Master Node와 실제 빅 데이터 시스템의 구성 요소가 되는 여러 대의 Slave Node로 구성되어 있으며, 빅 데이터 시스템에는 아파치 하둡을 채택하였다. 하드웨어 스펙으로서 8개의 2.533 Ghz Intel Xnon CPU, Memory 24Gbyte, 1TByte HDD로 8개의 가상머신을 구축하였다. 시스템상에서 HBase/HDFS를 사용하였고 빅데이터 시스템 데이터베이스와 검색 및 출력 엔진의 역할을 Elastic search가 대신하고 있다. Elasticsearch는 RestApi를 제공하는 등 웹 출력에 강력함을 보이고 있으며 월등한 검색 속도 및 편리한 사용 방법과 Open Source라는 장점들을 보유하고 있기는 하지만 궁극적으로 검색엔진일 뿐 빅데이터 시스템의 역할을 하는 것은 아니므로 추후 HBase/HDFS와 연동된 시스템으로 구성의 수정이 필요하다. 아래 그림에서 빅데이터 처리 플랫폼에 대한 시스템 구조를 정리하였다[3].

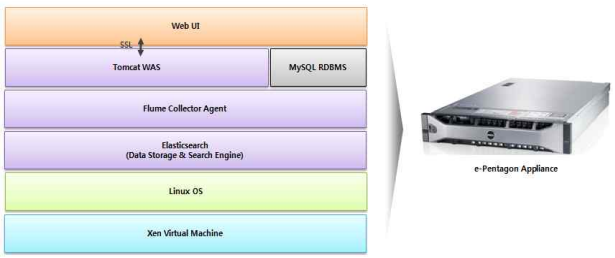

그림 1. 빅데이터 처리 플랫폼에 대한 시스템 아키텍처
Fig. 1. System Architecture of Big Data Process Platform

2) 분산시스템 기반의 빅데이터 플랫폼 개발

다양한 입력채널 환경에서의 빅데이터 플랫폼은 시스템 자원의 병목현상이 발생할 수 있다. 따라서 어느 정도 이상의 데이터나 복잡한 분석프로그램을 수행할 경우 처리속도 문제가 발생할 수 있다. 따라서 이러한 문제를 해결하기 위해 시스템의 병목현상과 대량의 데이터를 처리하기 위한 분산처리 기반의 다중 플랫폼을 개발하였다. 또한 최신 버전인 하둡 2.7.1 버전의 구조를 적용하여 이전 버전에 비해 빠른 성능과 가용성을 높였다. 하둡2.x 이후부터는 하둡 클러스터를 액세스하는 데 필요한 일관성 있는 수행과 보안을 제공하는 데이터 가브넌스 툴이자 리소스관리툴인 MapReduce2.0이라는 YARN 방식을 적용하였다. 아래 그림에서 데이터 처리 방식이 나타나 있다[4].

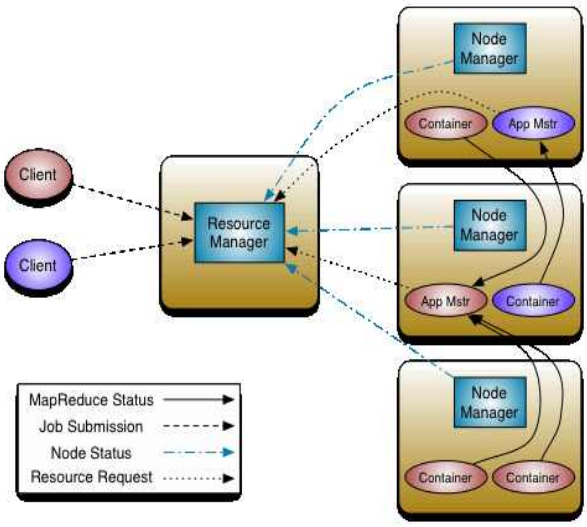

그림 2. 데이터 처리 방식
Fig. 2. Application Process

3) 다양한 입력채널 환경에서 빅데이터 처리 과정

빅데이터 처리 방안은 하둡 기반의 데이터 처리 방식을 채택하여 유연한 Scale-Out을 지원하며 빠른 속도로 데이터를 처리할 수 있다. 가상화를 통하여 8대의 서버를 구축하였으며 하나의 마스터 노드와 7개의 슬레이브 노드를 구축하였다. 하둡의 특성상 수평적 확장 구조로 시스템을 구현하였으며 3개 데이터 중복성을 가지도록 시스템을 구현하였다. 따라서 2개의 노드(NODE)가 장애가 발생하더라도 데이터를 복구할 수 있도록 구현하여 가용성을 높였다. 관계형 데이터베이스에서는 하둡에서 처리한 데이터에 대한 요약정보나 실시간 조회를 필요로 하는 데이터를 저장하여 웹으로 서비스를 제공한다. 빅데이터에는 정형, 반정형, 비정형의 3가지 유형으로 데이터가 분류되는데 로그 수집 자료는 정형의 데이터에 가깝다. 일부 이벤트 로그는 반정형으로도 볼 수 있다. 구축된 빅데이터 플랫폼은 다양한 데이터 형식의 데이터를 수집하며 대용량인 경우에도 처리 및 분석할 수 있는 가상화 기반의 단일 어플라언스 형태이다. 각각의 Agent에서 수집한 대량의 데이터를 하둡에 저장하고 MapReduce를 통하여 분산처리한 결과를 관계형 데이터베이스에 저장하여 웹컨텐츠로 제공한다. 분산환경 빅데이터 처리 플랫폼을 위해 하둡의 최신버전인 2.7.1버전을 기반으로 4개의 클러스터 시스템을 기본으로 구성하였으며, 첫 번째 노드에는 ESM Manager 엔진이 작동되고 두 번째는 관계형 데이터베이스와 원시로그저장을 위한 Collector 가 작동된다. Collector는 Agent가 수집한 원시로그를 저장하고 분석을 위해 하둡의 HDFS로 저장한다. 세 번째 노드에는 Agent가 구동되고 있으며 해당 서버에 대한 성능정보등을 수집하고 있다. 네 번째 서버는 하둡서버만 구동되고 있다. 하둡에 저장된 데이터는 HDFS에 저장되고 HBASE를 통하여 테이블 구조로 저장되며, 필요시 쿼리를 통하여 분석이 가능하다. 로그데이터에 대한 정형화는 Agent에서 이루어지며 정형화된 로그는 관계형 데이터베이스와 빅데이터 시스템에 저장되어 분석되어진다. HBASE는 랜덤하게 실시간으로 하둡에 있는 데이터에 접근이 가능하며 HBASE 쿼리를 통하여 특정시점에 데이터를 질의할 수 있다. Agent에서 수집한 로그는 HBASE에서 빅 테이블로 만들어져 분석을 위한 기본자료로 사용된다. 시스템 아키텍처로 사용된 하드웨어와 소프트웨어는 다음과 같다. 보다 빠른 성능으로 제품화시 차별화를 위하여 DRAM 방식의 SSD를 적용하였다. JSM은 256G로 메모리 디스크라 상당히 빠른 속도를 보여준다.[5]

2-2 빅데이터 분석 기반 통합보안관제 시스템 구축결과

빅데이터 분석 기반 통합보안관제 시스템은빅데이터 플랫폼 하둡의 에코 시스템인 SQOOP을 이용하여 통합보안 관제 관리의 관계형 데이터베이스와 연동하여 이벤트 자료를 HDFS로 옮기거나 HDFS 분석자료를 관계형 데이터베이스로 가져가서 웹클라이언트에 제공할 수 있도록 개발하였다. 또한 범용적이면서 기존의 HIVE나 HBASE보다 빠른 속도로 작업을 수행할 수 있는 클러스터용 연산 플랫폼인 SPARK를 적용하여 시스템의 성능을 높였다. SPARK는 1.5Gbyte 데이터에 대하여 HBASE에 비해 대략 10배 이상의 성능개선을 보였다. SPARK는 메모리 기반이므로 메모리에 따라 그 성능의 차이가 두드러질 것으로 예상된다. 누적된 이벤트 정보를 관계형 데이터베이스에서 처리하면 시간과 자원의 소모가 크지만 이를 빅데이터 플랫폼에서 처리하면 성능이나 시간이 크게 개선되는 것을 확인하였다. 또한 요약정보 또는 과거자료를 분석하는 일은 실시간 처리를 요구하지 않으므로 하둡에서 처리 후 일부는 관계형 데이터베이스로 제공하거나 HIVE를 통하여 사용자가 조회할 수 있게 하였다. 현재까지 이용한 하둡의 에코 시스템중 SPARK가 가장 좋은 성능을 보였으며 계속해서 SPARK를 기반으로 개발이 진행되고 있다. 통합보안관제 시스템 구축 결과는 아래 표와 같다[6].

표 1. 빅데이분석 기반 통합보안관제 시스템 구축 결과
Table 1. Result of Integrated Security Monitoring System based on Big Data Analysis

Classification	collect cycle	method	test target	test result
Syslog	Real time	Push	fire wall	8500 Agents/sec. (syslog)
			web wall	
			Hacking Detect system	
			UTM	7500 Agents/sec. NXG-4000)
			VPN	
			unix/linux	
SNMP	Real time	GET / Trap	Switch	6500 Agents/sec. (trap)
			Router	
			Wireless Network AP	7500 Aagents/sec. (SNMP)
JDBC	1 sec	Polling	MS-SQL	8500 Agents/sec.
			Oracle	9500 Agents/sec.
			MySQL	7800 Agents/sec.
File Update	1 sec	Polling	IIS	5500 Agents/min. (280Kbyte)
			tomcat	
			messages	
			simple text file	

2-3 빅데이터 분석 결과화면

원시로그 분석시스템은 방화벽 및 UTM 장비에서 발생하는 다량의 로그데이터에 대하여 분석한 결과를 조회할 수 있는 화면이다. 기존의 관계형 데이터베이스가 분석에 많은 시간이 소요되는 관계로, 빅 데이터를 분석하기 위해 SPARK로 데이터를 분석하는 기능을 구현하였다. SPARK는 지금까지의 하둡 에코시스템 중 가장 좋은 성능을 보여 주었다. 본 연구에서는 SPARK 시스템을 이용하여 댜량의 원시로그를 분석하였다. Security gateway 3000, Anlab_Turst Guard, Penta Security 에서 발생하는 수집한 로그 파일을 하둡의 HDFS 파일로 변환하여 처리한 결과이다. 수집한 이벤트에 대하여 장비별 고유주소인 IP 어드레스로 분석한 화면이 아래에 나타나 있는데 출발지와 목적지를 비교하여 특정한 출발지에 집중된 목적지 혹은 그 반대의 경우 등 분석할 가치가 있는 정보를 찾을 수 있다. 원시 로그에 대하여 현재 분석이 가능한 기능은 다음의 테이블에 정리되어 있다. 현재는 원시로그 및 이벤트를 수집하여 분석하는 기능이 개발되어 있으며 현재 분석 가능한 정보는 다음과 같다. 장비간의 연관분석 등 사용자 요구 및 원시로그 분석가능 항목과 보안상의 필요에 따라 확장이 가능하다. 로그수집을 Agent가 설치된 서버, 즉 Agent 서버에서 로그를 수집하는 Agent 방식과 Agent가 설치가 불가능한 경우 syslog, SNMP를 통해 로그를 수집하여 저장하는 Agentless식 으로 로그수집이 가능하다. 현재 원시로그 암호화 전송, 실시간 관제를 위한 메모리 공유, 이벤트 과다 발생시 메모리 최적화 부분과 로그 파싱 및 이벤트 수집 모듈, 이벤트 상관 분석에 대한 개발이 완료되었다. Agent는 가동시 필요한 모든 정보를 읽어 환경을 인식하고 다른장비 또는 동일 장비에서 수집한 원시 로그를 파싱 처리한다. 또한 이벤트 룰에 따라 이벤트를 발생시키거나 장비의 성능 임계치를 초과한 경우 매니저로 해당 정보를 전송한다.

표 2. 원시로그 빅데이터 분석
Table 2. Original Log Big Data Analysis

Classification	Description	min	hour	day	month
IP address	IP connection count	0	0	0	0
	disconnect IP count	0	0	0	0
	permission IP count	0	0	0	0
	2D relative count	0	0	0	0
	IP traffic status	0	0	0	0
event analysis	event count	0	0	0	0
	relative event count	0	0	0	0
performance information	memory	0	0	0	0
	CPU	0	0	0	0
	disk	0	0	0	0
	traffic	0	0	0	0
SNMP	TRAP	0	0	0	0
black list	connection status	0	0	0	0
SYS LOG	event count	0	0	0	0
	event analysis	0	0	0	0
	key event count	0	0	0	0
	search keywords	X	X	X	X
other	file change	0	0	0	0

모든 전송은 SSL을 이용하여 암호화 통신으로 이루어져 보안을 강화하였다. Agent는 원시로그를 콜렉터에 전송하고 콜렉터는 이를 시스템에서 지정한 위치에 보관한다. 빅데이터 처리를 위해 저장이 필요한 경우 스케줄러 프로그램이 하둡의 HDFS로 저장한다. 매니저는 웹 사용자 즉 클라이언트에서 설정한 각종 시스템 정보나 파싱정보를 Agent로 전송한다. 이를 위해 메니저는 웹서버 접속시 메모리를 할당하고 시스템 가동시 메모리에 대한 읽기, 쓰기 작업을 통해 에이전트와 통신한다. 웹클라이언트가 변경한 정보 역시 매니저의 메모리에 기록되고 데이터베이스에 저장된후 에이저트로 전송된다. 아래 표에 원시로그 분석결과를 정리하였다[7][8].

2-4 다채널 관리 와 모니터링

다채널 관리를 위한 관제 화면으로 네트워크 구성도로 이루어진 맵과 관리 대상 장비에서 발생하는 이벤트를 관제하는 이벤트 모니터링 화면으로 구성되어 있다. 맵 구성은 [보안정책] - [맵 에디터]에서 가능하며 맵은 권한이 있는 사용자가 관제 가능하다. 관제 맵 상에서 구성된 대상 장비에서 오류 및 이벤트가 발생 시 해당 오류 및 이벤트에 대해 맵 모니터링 화면에서 이벤트 발행을 경보하고 해당하는 장비 아이콘에 이벤트 발생을 알리는 상태를 표시한다. 맵과 함께 별도의 팝업 창으로 실시간 통계 기능을 제공한다. 장비별 현재 장비에 대해서 발생하는 이벤트를 조회하는 [현재장비 모니터링], 각 장비의 CPU, 메모리, 디스크, 트래픽 정보를 제공하는 [성능 모니터링], 해당 장비가 사용 중인 프로세스를 조회하는 [프로세스 모니터링], 해당 장비에 이벤트 발생 횟수를 산출하는 [TopN 모니터링], 현재 시점부터 6개월 전까지의 블랙리스트 발생 건수와 비율을 보여주는 [블랙리스트], 해당 장비의 정보를 보여주는 [등록정보]가 있다. 맵 모니터링 화면에서는 발생한 이벤트를 최근 날짜순으로 최대 300건까지 출력된다. 시스템, 임계치, 연관분석 이벤트의 경우 별도의 탭에서 확인할 수 있도록 하였다. 또 전체 발생 이벤트에 대해서 이벤트 위험도에 따라 분류할 수 있도록 하였다. 아래 그림에서 다채널관리에 대한 내용을 표시하였다[9]- [12].

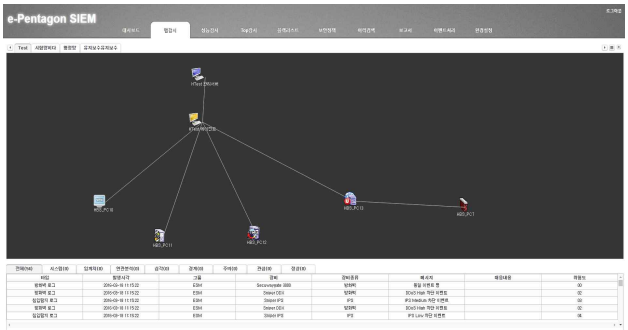

그림 3. 다채널관리 관제
Fig. 3. Multi Channel Monitoring

Ⅲ. 결 론

기존의 통합관제체계들의 단편적 로그, 일시적 로그의 분석을 넘어선 광대한 데이터에 대한 분석을 목표로 과제를 추진하였다. 이를 위해 먼저 기반이 되는 빅데이터 플랫폼 구축 및 운영 기술을 확보하였는데 빅데이터 플랫폼중 하나인 하둡의 다양한 에코시스템에 대한 기술력을 습득하였으며 필요한 에코시스템을 적용하여 개발을 진행하였다. 특히 가상화 및 물리적 분산 기반의 2가지 구축 기술로 사이트의 규모에 따라 어플라이언스 형태로 공급할 수 있도록 패키징화하여 고객들이 저비용으로 빅데이터 시스템을 구축할 수 있게 제공할 계획이다. 또한 통합관제의 기본 기능인 원시로그 수집, 저장 및 처리하는 기술과 이를 빅데이터 분석 시스템으로 분석하는 기능을 개발하였으나 아직은 데이터에 대한 깊이 있는 이해도와 분석기능의 고도화가 필요하다. 네트워크 토플로지를 맵으로 그려내는 기능은 사용자가 쉽게 사용할 수 있도록 개발하였는데 많은 시간과 노력을 투자한 만큼 편리하게 이용될 것으로 예상된다. 다른 웹화면 역시 HTML5기반의 UI로 브라우져에 독립적인 기능으로 작동 되도록 개발하였으며 대쉬보드 구성기술과 자바의 객체 전송 및 메모리 공유 기술을 통하여 안정적으로 모듈간에 필요한 데이터를 공유하도록 하였다. 차후 연구에서는 인공지능 기술을 기반으로 하여 다채널 환경에서 효율적인 빅데이터처리 와 관련한 통합보안 시스템 구축 방법에 대해 연구하고자 한다.

감사의 글

“이 논문은 2021년도 남서울대학교 학술연구비 지원에 의해 연구되었음.”

참고문헌

[1] J. B. Kim, “A Study on the Development of Next Generation Intelligent Integrated Security Management Model using Big Data Technology”, *International Journal of Security and Its Applications*, Vol. 9, No. 6. pp. 218-219, June 2015. http://dx.doi.org/10.14257/ijsia.2015.9.6.21

[2] J. .B. Kim, “A Study on the Successful Implementation about Vulnerability Supplementation and Effective Recovery from Damage related with Web Appllication ”, *Asia-pacific Journal of Multimedia Service Convergent with Art, Humanities and Sociology*, Vol. 6 No 1, pp. 53-60, Feb. 2016. http://dx.doi.org/10.14257/AJMAHS 2016.02.22

[3] H. J. Kang, “A Study on Analysis of Intelligent Video

Surveillance Systems for Societal Security," *The Journal of Digital Contents Society*, Vol.17, No. 4, pp. 273-278, June 2016. https://doi.org/10.9728/dcs.2016.17.4.273

[4] J. .B. Kim, "A Study on the Development of the Emergent System Recovery in Effective Way from Hacking Attacts or Security Incidents", *International Journal of Security and Its Applications*, Vol. 8, pp. 188-189, August 2015. http://dx.doi.org/10.14257/ijsia.2015.9.8.15

[5] I. G. Chun, *Deep Learning Express*, SaengNung Pub. ch. 8. pp. 318-322, July 2021.

[6] Seung-Byung Chae, *Human information filter in the era of big data curation,* Samsung Economic Research Institute, pp. 8-10. August 2011.

[7] S Charles P Pfleeger & Shari Lawrence Pfleeger, *Security Computing,* Mcgrow hill Pub. pp. 697-810. Jan. 2007.

[8] Jim Davis, Gloria J. Miller, Allan Russel, *"Information Revolution"*, John Wiley & Sons, Inc., pp. 52-55. Dec. 2006

[9] SK C&C Shim Tak-gil, *Big data search and analysis technology insight*, Kwangmooon Pub. pp. 29-51. Feb. 2011

[10] Sea Wisenutrch, *Discovering the future with Big Insight from Big Data*,, John Wiley & Sons, Inc., pp. 60-62. March 2011.

[11] O'Reilly, *Hands-On Machine Learning with Scikit-Learn , Keras & TensorFlow*, Hanbit Media, pp. 783-801. May 2020.

[12] W. S. Cho, *Information Security,* HongNeung Publisher, pp. 25–36, June 2003.

김정범(Jeong-Beom Kim)

1980년 : 서울대학교 물리교육학과 (이석사)
1996년 : 연세대학교 대학원(경영학석사)
2011년 : 숭실대학교 IT정책경영학과(공학박사)

1983년～1994년 : IBM Korea 근무
1996년～2000년 : SAP Korea 근무
2014년～현 재 : 남서울대학교 대학원, 빅데이터인공지능학과 주임교수(전공주임)
※관심분야 : 인공지능(AI)