스마트팩토리 IT 및 OT 영역 내 보안위협 관련 데이터 통합 처리 및 관리 아키텍처

정인수[1], 김득훈[2], 곽진[3]
[1]아주대학교 사이버보안학과, 정보보호응용및보증연구실 석박통합과정
[2]아주대학교 소프트웨어융합연구소 박사후연구원
[3]아주대학교 사이버보안학과 교수
jis0727@ajou.ac.kr, kimdh1206@ajou.ac.kr, security@ajou.ac.kr

Architecture for Integrated Processing and Managing Smart Factory IT and OT Area Data

In-Su Jung[1], Deuk-Hun Kim[2], Jin Kwak[3]
[1]ISSA Lab., Dept. of Cyber Security, Ajou University
[2]Inst. for Computiong and Informatics Research, Ajou University
[3]Dept. of Cyber Security, Ajou University

요 약

스마트팩토리는 기존 제조산업과 ICT(Information & Communication Technology)가 융합된 지능형 공장이다. 이는 직접적인 제조공정 과정이 수행되는 OT(Operational Technology) 영역(0~3계층)과 전사업무 관리를 수행하는 IT(Information Technology) 영역(4~5계층)으로 구분되며, 각 영역과 계층이 연결되어 제조·물류·유통 과정의 자동화 및 지능화를 제공한다. 그러나 각 영역과 계층이 연결됨에 따라 보안위협 벡터가 증가하고 있으며, 다영역·다계층 환경인 스마트팩토리에 적합한 대응체계 연구를 위해 영역별 보안위협 관련 데이터를 통합하여 처리 및 관리하는 아키텍처 연구가 필요한 실정이다. 이에 따라 본 논문에서는 스마트팩토리 환경 내 IT 및 OT 영역 장치를 식별하고 보안위협 관련 데이터 통합 처리 및 관리를 위한 아키텍처를 제안한다.

1. 서론

최근 제조산업과 ICT 기술을 융합한 스마트팩토리의 규모가 증가하고 있다. 이는 직접적인 제조공정 과정이 수행되는 OT(Operational Technology) 영역(0~3계층)과 전사업무 관리를 수행하는 IT(Information Technology) 영역(4~5계층)으로 구분되며, 각 영역과 계층이 연결되어 제조공정 자동화 및 지능화를 수행한다[1]. 그러나, 스마트팩토리 영역·계층이 연결됨에 따라 스마트팩토리 구조가 복잡해지고, 이로 인해 보안위협이 발생할 수 있는 보안위협 벡터가 증가하고 있다[1]. 이에 대응하기 위해 스마트팩토리의 다영역·다계층 구조를 고려한 보안위협 대응체계 연구가 필요하며, 영역별 보안위협 관련 데이터를 통합하여 처리 및 관리하는 아키텍처 연구가 필요한 필요한 실정이다. 따라서, 본 논문에서는 스마트팩토리와 스마트팩토리 영역·계층별 장치를 분석하고, 스마트팩토리 IT 및 OT 영역 내 보안위협 관련 데이터를 통합 처리 및 관리하기 위한 아키텍처를 제안한다.

본 논문은 2장에서 스마트팩토리 및 스마트팩토리 내 장치와 보안장비 구성을 분석한다. 3장에서는 스마트팩토리 IT 및 OT 영역 데이터 통합 처리 및 관리 아키텍처를 제안하며, 4장에서 결론을 맺는다.

2. 관련 연구

2.1 스마트팩토리

스마트팩토리는 제품의 설계, 개발, 제조, 유통 및 물류 등 생산의 전 과정에서 ICT 기술을 적용하여 생산성, 품질 등을 향상시킨 지능형 공장이다[2]. 이는 OT 영역인 0~3계층과 IT 영역인 4~5계층으로 나뉜다. OT 영역에는 제조공정에서 생산, 제어, 통제, 작업관리를 위한 시스템이 존재하며, IT 영역에는 외부 네트워크를 통해 스마트팩토리 관리 및 비즈니스 관련 활동을 수행하는 시스템이 존재한다[3]. 이러한 OT 영역과 IT 영역 내 IIoT 기기들의 연결로 제조공정 지능화가 이루어지며, 스마트팩토리의 IT 영역은 스마트시티, 스마트스토어 등과 B2B(Business to Business), B2C(Business to Customer) 등의

형태로 서로 연결되어 유통, 데이터 교환, 프로세스 자동화 등의 서비스를 제공하고 있다. 아래 <표 1>은 스마트팩토리 계층 및 영역별 구성요소를 나타낸다.

<표 1> 스마트팩토리 계층 및 영역별 구성요소

영역	계층	계층 명	구성요소
OT	0	현장 장치	센서, 액추에이터, 로봇, 생산 장비, etc.
	1	공정 제어	PLC, DCS, RTU, IED, etc.
	2	공정 통제	SCADA, HMI, OWS, Mobile, etc.
	3	생산 관리	MES, PLM, WMS, POP, Historian, etc.
IT	4~5	전사 관리	ERP, CRM, SCM, Groupware, etc.

스마트팩토리 환경 내 보안 장비는 내·외부 네트워크를 대상으로 패킷 필터링, 상태 기반 모니터링, 애플리케이션-프록시 게이트웨이, 가상 사설망 등을 제공하는 방화벽, 네트워크에서 발생하는 트래픽 모니터링 기반 침입 탐지 및 대응 시스템인 IPS(Intrusion Prevension System), 일반적인 네트워크 방화벽과 달리 웹 애플리케이션에 대한 SQL Injection, XSS 등의 웹 공격을 차단하고 정보유출방지, 부정접근방지, 위변조 방지 등의 기능을 제공하는 WAF(Web Application Firewall) 등의 보안 장비로 구성되어 있다.

또한, APT(Advanced Persistent Threat), DDoS(Distributed Denial of Service), 해킹 메일 등에 대응하기 위한 보안 장치와 백신, 로그 관리 시스템 등을 기반으로 스마트팩토리 내 보안위협을 관리 및 대응하고 있다[3,4].

2.2 빅데이터 처리 프로세스

스마트팩토리 환경 내 보안위협 관련 데이터를 처리하기 위한 빅데이터 처리 프로세스는 아래와 같다[5].

Step 1~2. 소스 및 수집

데이터 발생원으로부터 안정적인 저장소로 수집하는 기능 수행

Step 3. 저장

수집된 데이터를 안정적으로 저장하는 저장소, 비구조적 데이터 저장소에서 원본 데이터를 실시간으로 저장, 조회 처리를 하기 위한 저장소 및 구조적 저장소 또는 검색엔진 기술 활용

Step 4. 처리

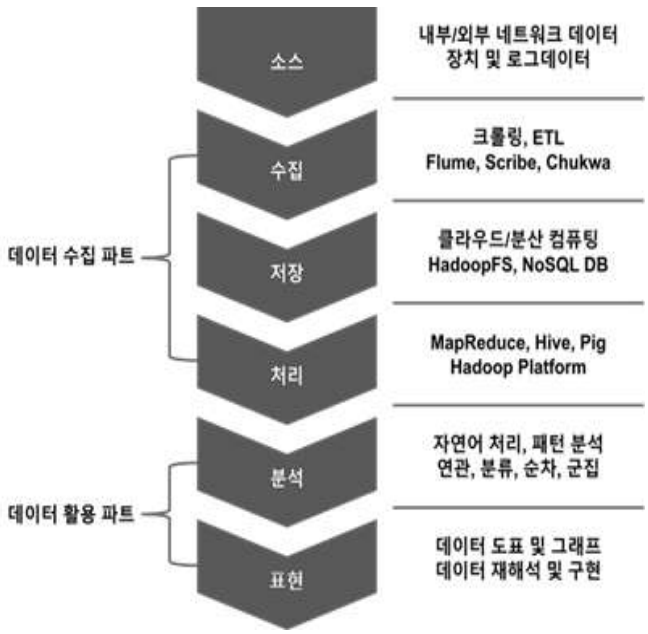
데이터 수집과 동시에 분석 수행 및 단순한 aggregation 연산 수행, 복잡하고 다양한 분석 수행, 대용량 처리를 위한 분산, 병렬처리, 단순 텍스트로부터 그래프 분석까지 다양한 분석 모델 지원

Step 5. 분석

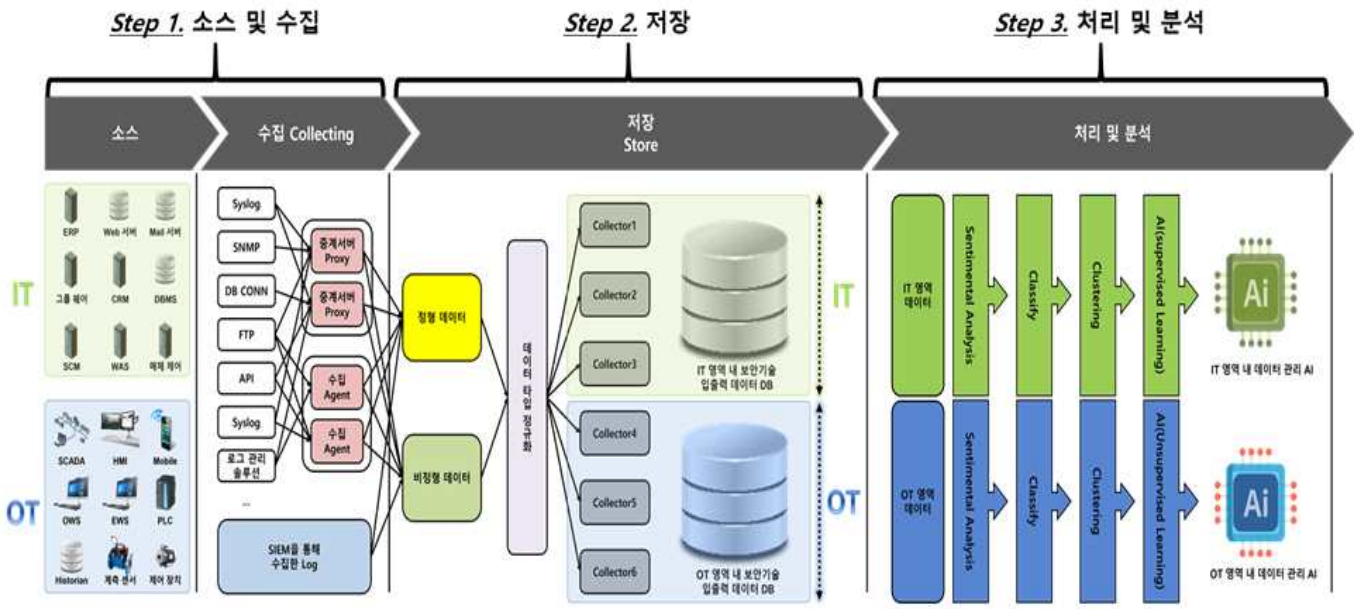
Cluster, Classification 등과 같이 데이터 마이닝을 위한 라이브러리 및 도구 활용, 전체 클러스터에 대한 관제 및 모니터링

Step 6. 리포트

수행한 빅데이터 처리 프로세스 기반 결과 가시화 및 데이터 관련 자료 작성



(그림 1) 빅데이터 처리 프로세스



(그림 2) 스마트공장 IT/OT 데이터 통합 처리 및 관리 아키텍처

3. 스마트팩토리 영역별 데이터 통합 처리 및 관리 아키텍처

스마트팩토리 내 보안위협 관련 데이터는 위협정보 습득 및 처리의 한계와 정적 분석 결과를 기반으로 만들어지는 IOC(Indicators of Compromise)의 한계로 인해 원활한 수집 및 분석에 어려움이 있다. 이에 따라, 대량으로 생산되는 위협정보를 수집 및 분석하고 위협 행위를 동적으로 분석해 위협에 효과적으로 대응하기 위한 스마트팩토리 IT 및 OT 영역 내 보안위협 관련 데이터 통합 처리 및 관리 아키텍처를 도출한다.

스마트팩토리 환경 내 존재하는 보안위협 관련 데이터 처리 및 관리를 위해서는 스마트팩토리 환경 내 존재하는 제어 장치 및 보안기술에 대한 입출력 데이터를 기반으로 DB가 구축되어야 한다. 스마트팩토리 환경 내 보안위협 관련 데이터는 각 장치 및 보안기술마다 상이한 데이터 형태를 가지며, IT 및 OT 영역별 데이터의 특성 또한 상이하다. 이러한 데이터들을 처리 및 관리하기 위한 본 아키텍처의 과정은 다음과 같다.

Step 1. 소스 및 수집

장치 및 보안기술에서 요구하는 입출력 데이터의 포맷에 따라 활용될 수 있는 수집 도구들을 활용하며, 이에 대하여 중계 서버 Proxy, 수집 Agent 방식을 활용하여 수집한다. 또한, 최근 스마트팩토리 내 도입되어 보안위협 관련 데이터 수집 및 분석에 활용되는 SIEM 장비를 통해 얻을 수 있는 데이터도 활용한다.

Step 2. 저장

수집한 데이터에 대하여 정형 데이터 및 비정형 데이터로 구분한다. 보안기술을 통해 생성된 입출력 데이터 중 일반적으로 정형화된 형태의 데이터는 정형 데이터 세션으로, 정형화되지 않은 데이터는 아래 비정형 데이터 세션으로 이동하게 된다. 이후 아래 도출하는 입출력 데이터 정규화 방안을 통해 데이터 정규화를 수행한 후 데이터 분산 처리 및 관리가 가능한 6개의 Collector들로 분산 저장하게 된다. 각 Collector에 저장된 보안기술 입출력 데이터들은 IT 영역과 OT 영역을 구분하여 저장하게 된다. 스마트팩토리는 IT 영역과 OT 영역으로 구분되어 제조공정 과정이 수행됨에 따라 각 영역별 보안기술 입출력 데이터 모델을 구분하고자 하였으며, 이를 통해 각 영역별 보안기술 데이터의 통합적인 관리가 가능하다.

Step 3. 처리 및 분석

스마트공장의 IT 영역은 주로 공장 내부의 생산을 관리하는 생산정보시스템과 전사 업무 관리 및 인터넷 서비스를 제공하기 위한 장치로 구성되어 있으며, 4~5계층을 의미한다. 또한, Ethernet을 통해 내·외부 네트워크와 연결되어있는 외부망으로 구축되어있다. IT 영역은 스마트공장 내·외부에 대한 서비스를 제공하고, 전체적인 관리 및

비즈니스 관련 활동에 필요한 기능을 수행한다. 이와 같이 IT 영역은 일반적으로 외부 네트워크와 연결된 환경들과 유사하다. 이에 따라, 생성되는 입출력 데이터 관리를 위해서 지도 학습을 활용하는 것이 더욱 효율적이다. 스마트공장의 OT 영역은 주로 제어설비 장치로 구성되어 있으며, 0~3계층을 의미한다. 또한, Fieldbus, 산업용 Ethernet, Modbus, Profinet 등과 같은 산업용 네트워크를 기반으로 외부 네트워크와 구분된 폐쇄망으로 구축되어 있다. OT 영역 내 각 계층은 생산과 관련된 현장 장치로 구성된 0계층, 현장 장치들의 상태정보 수집 및 제어 명령 전달을 수행하는 1계층, 모니터링 및 공정 통제를 수행하는 2계층, 공장 또는 시설 단위로 전체 모니터링을 수행하고 최종 제품을 생산하기 위한 작업을 관리하는 3계층으로 구성되어 있다. 이와 같이 OT 영역은 일반적인 기타 환경들과 상이한 구조를 가지고 있다. 이에 따라, 생성되는 입출력 데이터 관리를 위해서 비지도 학습을 활용하는 것이 더욱 효율적이다.

위 아키텍처는 스마트팩토리 내 장치, 보안 장비 및 계층 구조를 고려하여 도출되었으며, 아키텍처 기반 보안위협 관련 데이터 처리 및 관리 내용을 정리한 것은 아래 표와 같다.

<표 2> 보안위협 관련 데이터 처리 및 관리 방안

단계	설명
Source and Collect	스마트공장 내 보안 장비 또는 계층별 장치 식별
	Syslog, SNMP, API, SIEM, 로그 관리 솔루션 등을 활용한 로그 데이터 수집
	중계 서버 Proxy, 수집 Agent로 분류된 로그 데이터를 분산 처리 시스템으로 전송
Store	수집한 장치 및 보안기술 데이터 분산 처리와 정형화
Process and Analyze	스마트팩토리 IT 및 OT 영역별 데이터 대상 Sentimental Analysis, Classify, Clustering, AI(IT 영역은 지도 학습, OT 영역은 비지도 학습) 기반 데이터 처리 및 분석

본 아키텍처는 Syslog, SNMP, DB CONN, FTP, API 등과 같은 도구를 활용하여 스마트공장 내 보안 장비 또는 계층별 장치의 로그 데이터를 수집할 수 있다. 수집되는 로그 데이터는 중계 서버, 수집 Agent에 의해 데이터가 수집되며, AI를 활용하여 이기종 보안기술 데이터를 분석하기 위해 정형화 및 분산 처리 과정을 진행한다. SIEM 장비는 관제 시스템으로써 장치에 대한 로그를 수집하고 분산 처리 과정을 진행한다. 이와 같은 아키텍처를 기반으로 스마트공장 내 보안기술 데이터 및 장치 기반 데이터 분석을 위한 로그 데이터를 수집 및 분석할 수 있으며, 분산 처리, 정형화, 학습 과정을 통해 스마트공장 통합보안관제 시스템에 적용 가능하다.

4. 결론

본 논문에서는 스마트팩토리를 분석하고, 스마트팩토리 환경 및 특징을 고려한 보안위협 관련 데이터 통합 처리 및 관리 아키텍처를 도출하였다. 이를 통해 수집·처리·관리되는 데이터를 기반으로 스마트팩토리 내 발생 가능한 보안위협에 신속하게 대응할 수 있으며, 추후 본 아키텍처의 고도화를 통해 스마트팩토리 환경에 적용 가능한 자동대응체계 구축 연구를 수행할 것이다.

사사문구

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-01806, 스마트공장 보안 내재화 및 보안관리 기술 개발)

참고문헌

[1] Deloitte, “Cyber security for smart factories”, 2019.

[2] KISA, “스마트공장 보안 모델 PART1_요약본”, Apr. 2022.

[3] KISA, “스마트공장 보안 모델 PART2_요약본”, Apr. 2022.

[4] KISA, “스마트공장 사이버보안 가이드”, Dec. 2019.

[5] 한국IR협의회, “데이터 시각화 - 빅데이터 중요성 부각에 따른 데이터시각화 관심 증가”, Aug. 2021.