KOSDI
ISSN : 1976-2208 (Print)
ISSN : 2671-5287 (On-line)
www.sodi.or.kr

Journal of the Society of Disaster Information
Vol. 17, No. 1, pp. 176-183, March 2021
https://doi.org/10.15683/kosdi.2021.3.31.176

Original Article

스마트팩토리 확산을 위한 비파일시스템(None File System) 기반의 차세대 데이터보호에 관한 연구

A Study on Next-Generation Data Protection Based on Non File System for Spreading Smart Factory

김승용[1] · 황인철[2]* · 김동식[3]
Seungyong Kim[1], Incheol Hwang[2]*, Dongsik Kim[3]

[1]Professor, Department of Management Information System, Korea National University of Transportation, Chungju, Republic of Korea
[2]Director, Secuware Inc., Cheongju, Republic of Korea
[3]Director, KCC Corporation, Seoul, Republic of Korea

*Corresponding author: Incheol Hwang, ichwang@secuware.co.kr

ABSTRACT

Purpose: The introduction of smart factories that reflect the 4th industrial revolution technologies such as AI, IoT, and VR, has been actively promoted in Korea. However, in order to solve various problems arising from existing file-based operating systems, this research will focus on identifying and verifying non-file system-based data protection technology. **Method:** The research will measure security storage that cannot be identified or controlled by the operating system. How to activate secure storage based on the input of digital key values. Establish a control unit that provides input and output information based on BIOS activation. Observe non-file-type structure so that mapping behavior using second meta-data can be performed according to the activation of the secure storage. **Result:** First, the creation of non-file system-based secure storage's data input/output were found to match the hash function value of the sample data with the hash function value of the normal storage and data. Second, the data protection performance experiments in secure storage were compared to the hash function value of the original file with the hash function value of the secure storage after ransomware activity to verify data protection performance against malicious ransomware. **Conclusion:** Smart factory technology is a nationally promoted technology that is being introduced to the public and this research implemented and experimented on a new concept of data protection technology to protect crucial data within the information system. In order to protect sensitive data, implementation of non-file-type secure storage technology that is non-dependent on file system is highly recommended. This research has proven the security and safety of such technology and verified its purpose.

Keywords: None File System, Data Protection, Ransomware, Storage, Secure Area

요 약

연구목적: 우리나라 최근 4차 산업 혁명의 핵심 기술인 인공지능(AI), 사물인터넷(IoT), 가상현실(VR) 등을 제조 환경에 반영한 스마트공장 도입이 활발히 추진되고 있다. 그러나 기존 운영체제 기반의 파일 시스템에서 발생하는 각종 문제점을 해결하고자 비파일시스템 기반의 데이터보호 기술을 연구·검증하고자 한다. **연구방법:** 본 연구에서는 운영체제에 의해 식별되거나 제어되지 않는 보안저장부와 디지털 키 값의 입력에 따라 보안 저장부를 활성화할 수 있는 방법연구와 BIOS 동작 시 연결을 위한 입출력 정

Received | 19 February, 2021
Revised | 4 March, 2021
Accepted | 15 March, 2021

보만 제공하는 제어부를 설정하고 보안 저장부의 활성화에 따라 제2 메타 데이터를 사용한 맵핑 동작을 수행할 수 있도록 비파일형태의 구조를 연구함. **연구결과:** 첫째, 비파일시스템 기반의 보안 저장부의 생성과 데이터 입출력 시 데이터 손상 여부를 샘플 데이터의 해시함수 값과 일반 저장부 및 보안 저장부의 해시함수 값을 비교하여 일치하는 것을 확인하였음. 둘째, 보안 저장부의 데이터 보호 성능 실험에서는 원본 파일의 해시함수 값과 랜섬웨어 활동 이후의 일반 저장부와 보안 저장부의 해시함수 값을 비교하여 악성코드인 랜섬웨어로부터 데이터 보호 성능을 확인함. **결론:** 본 연구는 국가적으로 추진하고 있는 스마트팩토리 구축 사업을 통해 기업에 도입되고 있는 정보시스템 내의 중요 데이터를 보호하기 위한 새로운 개념의 데이터 보호 기술을 구현하고 실험하였다. 정보보안의 목적인 중요 데이터의 보호를 위해 기존의 저장 개념과 달리 파일 시스템에 비의존적인 비파일 형태의 보안 저장부 생성기술을 구현하였고 그 안전성을 검증하였음.

핵심용어: 비파일시스템, 데이터보호, 랜섬웨어, 저장장치, 보안영역

서 론

2016년 세계경제 포럼의 의장인 클라우스 슈밥(Klaus Schwab)이 4차 산업혁명이라는 용어를 처음 사용한 이후 정보통신기술(ICT)의 발달과 더불어 세계 각국에서는 다양한 분야에서 4차 산업혁명을 적용하고 있다. 특히, 4차 산업 혁명의 핵심기술인 인공지능(AI), 사물인터넷(IoT), 가상현실(VR) 등을 제조 환경에 반영한 스마트공장 도입에 노력을 기울이고 있다.

Jang (2014)의 보고서에 따르면 미국은 '첨단제조업파트너십(AMP) 2.0' 통해 미국 제조업 부문을 활성화하고 있으며, 중국은 13차 5개년 계획(2016~2020)의 제조업 육성을 위한 산업정책으로 '중국제조 2025(Made In China 2025)'를 발표하여 추진하고 있다(You, 2017).

이러한 스마트공장은 최근 IT 영역과 OT 영역의 통합 등으로 보안위협이 높아지고 있는 상황이다(Bae, 2019).

한국인터넷진흥원이 발행한 '스마트공장 사이버보안 가이드'(Kim, 2019)에 따르면, 스마트공장은 IT영역과 OT영역이 융합되어 효율을 높인 시설인 만큼 기존의 IT 보안 위협과 해당 보안 위협에 의해 야기된 OT영역 보안 위협, 그리고 외부 인터넷망과 직접 연결됨으로 발생되는 OT영역에 대한 다양한 해킹사고가 있을 수 있다.

대표적으로 제조기반의 기업들을 중심으로 보안 솔루션이 적용되기 어려운 산업용 설비가 외부 인터넷망에 직접 연결되어 악성코드에 감염되거나, 설비관리자가 사용자의 의사에 반해 악의적인 목적으로 펌웨어 업그레이드 또는 단순 점검을 위한 방문 시 USB를 활용하여 악성코드를 설치하는 방법 등을 통한 공격을 들 수 있다. 그리고 이러한 해킹을 통해 스마트공장 내 생산 공정의 핵심기술정보, IoT 센서 기반 공정에서 수집된 빅데이터, 제품생산과 관련된 각종 레시피 정보 등의 기밀정보 유출이 발생할 수 있으며, 이외에도 악의적인 생산 중단을 통한 매출 손실, 작업자의 안전을 위협하는 인명피해 사고를 유발할 수 있다(Jeong et al., 2020; Hwang et al., 2018).

Table 1은 보안 위협에 의해 발생된 대표적인 보안사고 사례를 보여준다.

이러한 보안사고를 예방하기 위해 개발하거나 도입한 기존의 보안솔루션들은 컴퓨터 시스템에 기본적으로 설치되는 운영체제에 매우 종속적인 기술을 사용하고 있다. 완벽한 보안기능을 실현하기 어렵고 운영체제의 취약점이 노출된 경우 보안 솔루션까지 무력화되는 문제도 안고 있다(Kim et al., 2007).

선행연구(Quan et al., 2015)에서는 파일시스템을 구성하는 메타데이터의 위치에 대한 정보를 암호화하는 방식으로 저장 방식을 구현하여 운영체제가 메타데이터의 위치를 식별할 수 없게 하여 저장된 데이터에 무단 접근하는 것을 방지하는 연구를 진행하였다.

본 연구에서는 파일시스템을 탑재하지 않는 보안 저장부를 구현하여 기존 운영체제 기반의 파일시스템에서 발생하는 각

종 문제점을 해결하고자 비파일시스템 기반의 데이터보호 기술을 연구·검증하고자 한다.

Table 1. Cases of security incidents caused by security threats

시기	대상	피해 내용
2019	벨기에 이스코 인더스트리	랜섬웨어 감염으로 인한 생산 시스템 마비
2019	노르웨이 노르스크 하이드로	랜섬웨어 감염으로 인한 생산 차질
2018	대만 TSMC	USB를 통한 악성코드 감염으로 하루 동안 일부 공장 내 생산 라인 가동 중단
2017	석유, 철강, 자동차 제조공장 등	워너크라이, 페트야 랜섬웨어 확산
2017	미국 달라스 비상 사이렌	무선통신망의 해킹으로 인해 달러스의 비상 사이렌이 15시간 동안 가동
2017	일본 자동차	혼다 자동차 사야마 공장 워너크라이 랜섬웨어 감염, 약 48시간 동안 엔진 생산과 조립 중단
2016	미국 전력	랜섬웨어가 첨부된 이메일을 통한 스피어 피싱 공격이 발생, 내부 네트워크 감염 확산으로 회사 시스템 일시 중단
2016	미국 수처리 회사	PLC 조작을 통해 수처리 관련 화학물질의 양을 조작, 2백 50만명 이상의 고객 지불정보 유출
2015	한국 교통시설	항만, VTS, 지하철, 대중교통 관련 시설에 대한 공격 발생

데이터 저장방식

전통적인 데이터 저장방식은 Fig. 1과 같은 구조를 가진다. 물리적인 디스크에 데이터 저장공간을 구성하기 위해 파티션 테이블, 파일 테이블 등 메타 데이터를 저장하는 논리적인 파티션을 구성하게 되는데 이 테이블의 메타 데이터는 자체적으로 암호화되지 않으므로 손쉽게 역분석이 가능하다. 또한 이러한 논리적 파티션의 위치 및 메타 데이터는 항상 일정하게 표준으로서 오프셋이 지정되어 있어 데이터 복구 또는 디지털 포렌식 분석을 통해 중요 데이터들이 복원되어 유출될 수 있으며, 해킹 또는 악성코드에 의해 중요 데이터가 유출되거나 위변조될 수 있다.

즉, 운영체제에 의해 생성된 파일시스템을 탑재한 저장장치는 어떠한 데이터 보호 기술을 적용하더라도 파일 형태로 존재하기 때문에 다양한 위협요소에 의한 데이터 손상 및 인가되지 않은 데이터 접근이 가능하다.

Fig. 1. Traditional data storage method

상기 문제점을 근본적으로 해결하기 위해 본 연구에서 제안하는 데이터보호 기술의 구조는 Fig. 2와 같다.

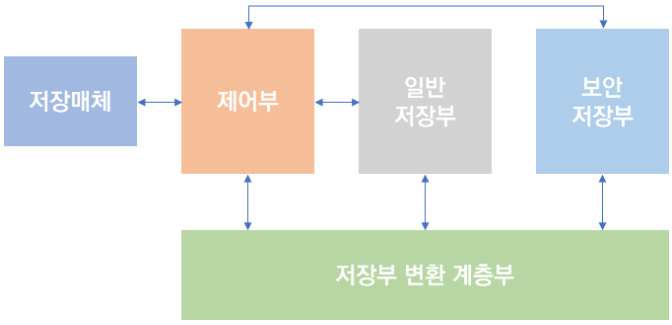


Fig. 2. Data protection technology configuration diagram

첫째, 일반 데이터를 저장하는 일반 저장부는 윈도우즈, 리눅스 등 운영체제가 인지할 수 있도록 파티션 정보에 의해 저장부의 위치와 크기가 정의된다. Fig. 3에서 보는 바와 같이 일반적으로 파티션 정보는 디스크의 0번 섹터인 MBR(Master Boot Record)에 정의되어 있으며, 해당 섹터의 511~512Byte 위치에 기록된 특별한 시그니처(0x55AA)에 의해 인식된다.

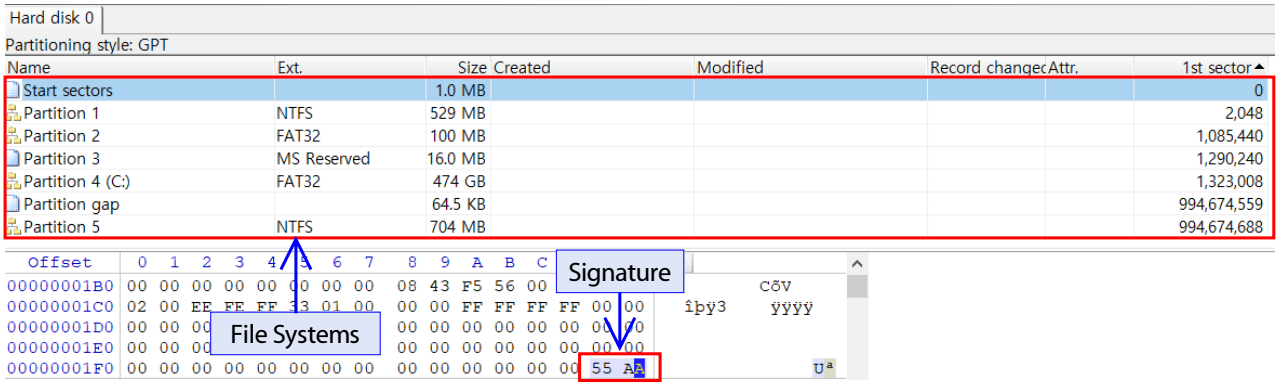


Fig. 3. Start sector"s signature

정의된 파티션은 포맷 과정을 통해 운영체제가 데이터를 입출력할 수 있도록 하는 파일시스템을 탑재한다. 파일시스템은 운영체제에 따라 지원되는 파일시스템이 다르다. Fig. 3과 같이 윈도우즈의 경우 일반적으로 NTFS(New Technology File System), FAT32(File Allocation Table 32), exFAT(Extended FAT) 등의 파일시스템을 사용하며, 리눅스의 경우 Ext2/3/4 파일시스템이 일반적으로 사용된다. 이렇게 생성된 일반 저장부는 운영체제가 드라이브로 인식할 수 있도록 드라이브 레터를 할당받게 되며, 운영체제는 드라이브 레터를 기반으로 데이터의 입출력을 제어한다.

둘째, 보안 저장부는 앞서 기술한 일반 저장부와 달리 운영체제에 의해 파일시스템을 생성하지 않는다. 따라서 해당 보안 저장부는 데이터 입출력을 위한 드라이브 레터가 없으며, 일반 저장부와 달리 운영체제는 해당 영역에 데이터를 입출력할 수 없다. 해당 영역은 암호화된 가상 드라이브를 가지고 있으나 운영체제에 의해 식별되거나 제어되지 않는다. 데이터 입출력 이벤트 발생 시 보안 저장부의 모든 데이터는 실시간 암복호화 과정을 거치게 된다.

셋째, 제어부는 디지털 키 값의 입력에 따라 보안 저장부를 활성화하고 보안 저장부의 활성화에 따라 접근 운영체제로의 정보 제공 여부를 결정한다. 제어부는 BIOS 동작 시 일반 저장부의 연결을 위한 제1 입출력 정보 및 보안 저장부의 연결을 위

한 제2 입출력 정보 중 제1 입출력 정보만을 제공한다. 즉, 디지털 키 값이 없으면 보안 저장부는 활성화되지 않아 보안 저장부 내의 데이터는 물론 보안 저장부의 존재조차 알 수 없게 된다.

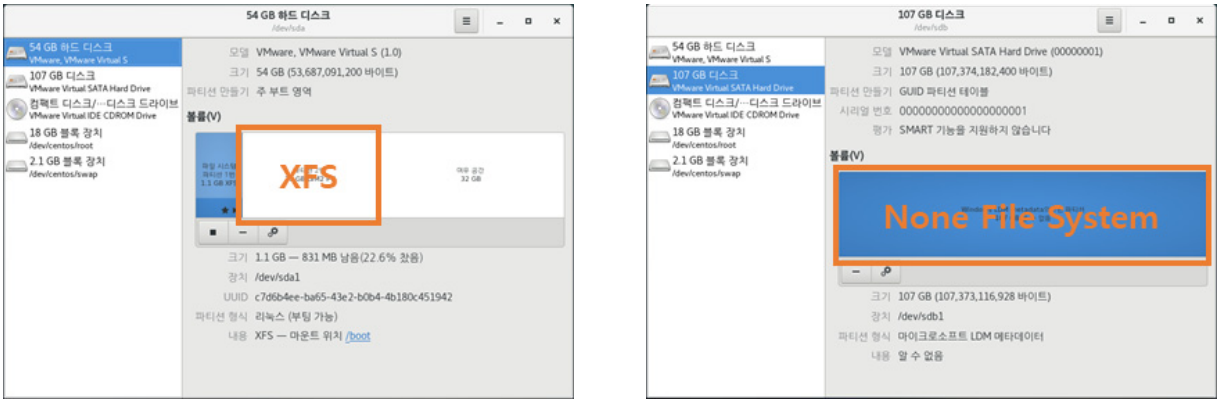
넷째, 저장부 변환 계층부는 일반 저장부의 어드레스 맵핑(address mapping)을 위한 제1 메타 데이터 및 보안 저장부의 어드레스 맵핑을 위한 제2 메타 데이터를 저장하고, 보안 저장부의 활성화에 따라 제2 메타 데이터를 사용한 맵핑 동작을 수행한다. 즉, 운영체제가 보안 저장부를 인식하게 한다.

실험설계

이러한 저장기술구조를 기반으로 운영체제에 비종속적인 비파일시스템의 보안 저장부의 생성과 생성된 보안 저장부 내 데이터가 데이터 위협 요인으로부터 안전하게 보호되는지 검증하고자 한다.

본 연구를 위해 일반 저장부와 보안 저장부를 설정하였다. 실험에 사용된 PC환경은 반복적 실험을 위해 동일한 환경 구성과 초기화가 용이한 가상머신 프로그램을 사용했다. 가상머신 프로그램을 사용하면 추가적인 설정없이 해당 가상머신 파일의 통제를 통해 실험환경을 구성할 수 있으며, 실험 후 초기 환경 구성을 위해 스냅샷을 사용함으로써 매우 빠르게 실험을 진행할 수 있는 장점이 있다.

Fig. 4. A에서 보는 것과 같이 가상디스크에 파티션을 설정하여 운영체제를 설치하였고, 동일 가상디스크에 일반 저장부를 생성하여 XFS 파일시스템을 탑재하여 기존의 일반적인 PC환경을 구현했다. 그리고 Fig. 4. B와 같이 해당 가상 머신에 보안 저장부를 설정하기 위해 가상디스크를 추가하였고 별도의 파일시스템을 탑재하지 않았다. 일반 저장부와 달리 보안 저장부에 파일 시스템을 탑재하지 않았기 때문에 드라이브 레터가 나타나지 않아 가상머신에서는 일반 저장부만 존재하는 것으로 보이게 된다.



<A. Normal Area> <B. Secure Area>

Fig. 4. Comparison of normal area and secure area

첫 번째 실험에서는 Fig. 5와 같이 보안 저장부에 가상의 드라이브가 생성되는지 여부와 해당 보안 저장부에 데이터가 정상적으로 입출력되는지 확인하는 실험을 하였다. 먼저, 60GB의 샘플 데이터를 생성한 후 해시함수 값을 추출하였다. 그리고 디지털 키 값을 통해 보안 저장부를 활성화하고 어드레스 맵핑(Address Mapping)을 통해 가상 드라이브를 마운트하였다.

샘플 데이터를 보안 저장부에 마운트된 가상 드라이브에 복사한 후 다시 해시함수 값을 추출하였다. 보안 저장부에 저장된 샘플 데이터를 일반 저장부로 복사한 후 다시 해시함수 값을 추출하여 3개 함수를 상호 비교하였다. 본 실험은 총 10회를 실시하였고 실험과정에서 발생된 에러는 없었다. 이를 통해 보안 저장부에 가상의 보안 드라이브가 생성되고, 데이터 입출력 시 데이터의 손상 및 누락이 없는지 확인하였다.

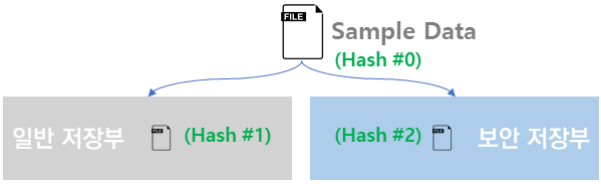


Fig. 5. Comparison of data hash function values of normal area and secure area

두 번째 실험에서는 Fig. 6과 같이 일반 저장부와 보안 저장부에 동일한 샘플 데이터를 저장한 후 랜섬웨어(Ransomware)로부터 데이터가 안전하게 보호되는지 확인하였다. 먼저 샘플 데이터의 해시함수 값을 추출하여 기록하고, 일반 저장부와 보안 저장부에 동일한 샘플 데이터를 저장하였다. 이후 대표적인 데이터 침해 요인인 랜섬웨어 3종을 준비하였다. 랜섬웨어는 다양한 산업분야에서 데이터 침해를 일으키고 있으며, 정보시스템 내 중요 데이터 형식의 파일을 고도의 암호화 기술로 암호화한다. 본 실험에서 사용한 랜섬웨어는 실제 랜섬웨어 피해를 본 사용자의 PC에서 획득한 악성코드 파일이다. 랜섬웨어를 실행시킨 후 일반 저장부와 보안 저장부에 저장된 샘플 데이터의 해시함수 값을 각각 추출하여 초기 샘플 데이터의 해시함수 값과 비교하여 데이터 침해 여부를 확인하였다.

한 종의 랜섬웨어 실험이 종료되면 가상머신의 스냅샷을 초기 상태로 복원하여 동일한 실험환경으로 만들었다. 이러한 방법으로 총 30회 실험하였으며, 3종의 랜섬웨어를 통해 보안 저장부의 데이터 보호 성능을 확인하였다.

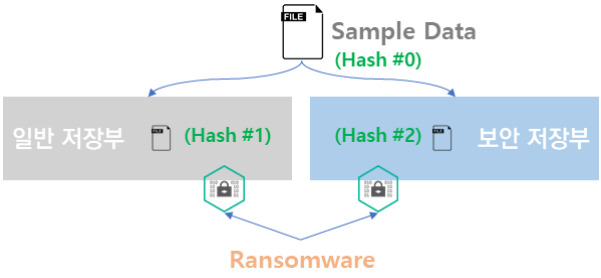


Fig. 6. Comparison of data hash function values after ransomware infection

실험결과

상기의 연구 방법으로 실험한 결과 두 가지의 연구 결과를 얻을 수 있었다.

첫째, 비파일시스템 기반의 보안 저장부의 생성과 데이터 입출력 시 데이터 손상 여부에 대한 연구에서는 Table 2에서 보는 바와 같이 샘플 데이터의 해시함수 값과 일반 저장부 및 보안 저장부의 해시함수 값이 일치하는 것을 볼 수 있다. 이는 보안

저장부에 가상 드라이브가 생성되었으며, 가상 드라이브를 대상으로 데이터 입출력 시 데이터의 손상 또는 누락이 발생되지 않고 일반 저장부와 같은 프로세스를 수행함을 알 수 있다.

Table 2. Comparison of hash function values of normal area and secure area

	Contents	Hash(MD5)
Sample File	Sample_Origin	cedf7858cb98f4e26fe34fe0d66b7a01
Normal area	Sample_Origin	cedf7858cb98f4e26fe34fe0d66b7a01
Secure Area	Sample_Origin	cedf7858cb98f4e26fe34fe0d66b7a01

둘째, 보안 저장부의 데이터 보호 성능을 실험한 결과 Table 3과 같은 결과를 얻을 수 있었다. 실험을 위한 원본 파일의 해시함수 값과 랜섬웨어 활동 이후의 일반 저장부와 보안 저장부의 해시함수 값을 비교한 결과이다. 결과적으로 보안 저장부는 일반 저장부와 달리 대표적인 악성코드인 랜섬웨어로부터 데이터 보호 성능을 보였다.

이는 일반 저장부와 달리 보안 저장부는 운영체제가 인식하는 별도의 파일 시스템을 탑재하지 않았기 때문에 드라이브 레터(예를 들어 윈도우즈의 경우 C:\ 등)가 맵핑되지 않는다. 따라서 랜섬웨어가 샘플 데이터의 존재를 알 수 없기 때문에 공격 대상이 없게 되는 것이다.

Table 3. Comparison of hash function values of normal area and secure area after ransomware infection

	Contents	Hash(MD5)
Sample file	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7
Normal area1	PKचप चc ? _Q # Sample_Origin.txtҕ? ҕ AEҕ V?-ҧjW_뙡?pV?K Dk 暻멢?? 볣ㅗ*PKҕҕ चc ? _Q # ҕ Sample_Origin.txtҕ? ҕ AEҕ PKवप॰ ҕ ҕ J]	61b6206a609f3b2b12645cbcf268dec1
Secure area1	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7
Normal area2	PKचप चc ? _Q ' Sample_Origin.txtҕ? ҕ AEҕ oB^p쌹g?3?5ҧ?햩e旒 *?u귟प॰'쿓뻻 CXPKҕҕ चc ? _Q ' ҕ Sample_Origin.txtҕ? ҕ AEҕ PKवप॰ ҕ ҕ J a	150ee612606fcd2b25b33e86f00d4d5e
Secure area2	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7
Normal rea3	PKचप चc ? _Q + Sample_Origin.txtҕ? ҕ AEच ?뎉?`捌 f 뾆 음 9 譁 V(S@알J뀖?g%/|?화??PKҕҕ चc ? _Q + ҕ Sample_Origin.txtҕ? ҕ AEच PKवप॰ ҕ ҕ J e	f7af52e4a989c41f81f07f7b2168a23d
Secure area3	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7

결 론

본 연구에서는 국가적으로 추진하고 있는 스마트팩토리 구축 사업을 통해 기업에 도입되고 있는 정보시스템 내의 중요 데이터를 보호하기 위한 새로운 개념의 데이터 보호 기술을 구현하고 실험하였다. 전통적으로 데이터는 파일시스템 상의 데이터 저장영역에 기록하고 있다. 일반 데이터는 물론 가상머신 내의 데이터 또한 가상머신 파일에 기록되기 때문에 파일시스템에 의존적이다. 이러한 이유로 그 동안 다양한 정보보안 및 데이터 보호 솔루션이 개발되어 공급되었음에도 데이터 침해 사례를 접하고 있는 것이다.

본 연구에서는 정보보안의 목적인 중요 데이터의 보호를 위해 기존의 저장 개념과 달리 파일 시스템에 비의존적인 보안 저장부 생성기술을 구현하였고 보안 저장부 내의 데이터 보호 성능을 일부 검증하였다. 비파일시스템 형태의 보안 저장부에 중요 데이터를 저장하기 때문에 어떠한 악성코드 및 해커가 중요 데이터의 존재 여부를 파악할 수 없어 공격 자체가 무의미해진다.

본 연구에서는 랜섬웨어를 통해 샘플 데이터의 암호화 여부를 중요 보호 성능으로 실험하였다. 그러나 데이터 침해요소는 매우 다양하기 때문에 다른 침해요소를 추가적으로 적용하여 본 연구에서 제시한 보안 저장부의 데이터보호 성능을 추가적으로 검증할 필요가 있다.

그럼에도 본 연구에서 구현한 기술을 스마트팩토리 정보 시스템에 적용한다면 데이터 침해로부터 중요 데이터를 보호하여 안정적인 시스템 운영이 가능할 것으로 기대한다.

Acknowledgement

본 연구는 2020년 한국교통대학교 지원을 받아 수행하였음.

References

[1] Bae, M.-H. (2019). Analysis of Security Trends in Smart Factories in Major Countries and Implications. IITP, Weekly ICT Trends Vol. 1920, Korea.

[2] Hwang, H., Seo, Y., Jeon, T., Kim, C. (2018). “Design and implementation of an urban safety service system using realtime weather and atmosphere data.” Journal of Korea Multimedia Society, Vol. 21, No. 5, pp. 599-608.

[3] Jang, Y. (2014). Accelerating U.S. Advanced Manufacturing. KIAT, Vol. 2015-55, Korea.

[4] Jeong, M.G., Lee, S.H., Kim, C.S. (2020). “A study on the safety index service model by disaster sector using big data analysis.” Journal of the Korea Society of Disaster Information, Vol. 16, No. 4, pp.682-690.

[5] Kim, J.G., Kim, T.E., Choi, J.W., Kim, W.G., Lee, J.S. (2007). “Vulnerability analysis and research on digital contents storage system.” Journal of Information and Security, Vol. 7, No. 4, pp. 36-41.

[6] Kim, S.-H., (2019). Smart Factory Cyber Security Guide for Internalizing Security of ICT Convergence Products and Services in the Factory Field, KISA, Korea.

[7] Quan, S.G., Kwon, Y.G., (2015). “Design and Implementation of Virtual and Invisible Private Disk(VIPDISK) having Secure Storage Device.” Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 4, pp. 781-792.

[8] You, Y.-S. (2017). China’s ICT Industry and Policy Trends in Preparation for the 4th Industrial Revolution. IITP, Vol. S17-05, Korea.