산업융합연구 제20권 제7호 pp. 65-71, 2022
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2022.20.7.065

이벤트 감지를 통한 파일 유출 대응 시스템 설계

신승수
동명대학교 정보보호학과 교수

A Design of File Leakage Response System through Event Detection

Seung-Soo Shin
Professor, Dept. of Information Security, Tongmyong University

요 약 ICT의 발달과 함께 4차 산업혁명 시대가 도래 하면서 데이터의 양은 방대해지고, 빅데이터 기술들이 대두되면서 데이터를 가공, 저장, 처리하는 기술이 중요해지고 있다. 본 논문에서는 산업체와 공공장소 등에서 중요 파일 유출 시 그 피해는 국가적, 재산적으로 심각하기 때문에 모니터링을 통해 이벤트를 감지하고 해시 값을 이용하여 판단하는 시스템을 제안한다. 연구 방법으로는 선택적 이벤트 방식을 사용하여 파일 유출 발생 시 암호화 작업 수행 후 사전에 등록한 해시 값을 비교한 뒤 중요 파일 여부를 판단한다. 특정 이벤트에 대한 모니터링으로 시스템 부하를 최소화하고 Signature를 분석한 후 판별하여 정확성을 개선한다. 데이터베이스에 사전 등록한 해시 값을 비교하여 판별하는 것으로 기밀성을 개선한다. 향후 연구로는 네트워크 및 다양한 경로를 통한 파일 유출 방지를 위한 보안 솔루션 연구가 필요하다.

키워드 : 파일, 이벤트, 암호화, 해시, 탐지

Abstract With the development of ICT, as the era of the 4th industrial revolution arrives, the amount of data is enormous, and as big data technologies emerge, technologies for processing, storing, and processing data are becoming important. In this paper, we propose a system that detects events through monitoring and judges them using hash values because the damage to important files in case of leakage in industries and public places is serious nationally and property. As a research method, an optional event method is used to compare the hash value registered in advance after performing the encryption operation in the event of a file leakage, and then determine whether it is an important file. Monitoring of specific events minimizes system load, analyzes the signature, and determines it to improve accuracy. Confidentiality is improved by comparing and determining hash values pre-registered in the database. For future research, research on security solutions to prevent file leakage through networks and various paths is needed.

Key Words : File, Event, Encryption, Hash, Detection

1. 서론

정보통신기술의 발전과 4차 산업혁명 시대가 시작되면서 산업체의 내부 데이터 및 중요한 기술들은 산업체의 자산이며 경쟁력의 원천이다. 산업체에서 사용하는 데이터양은 급격하게 증가하고 있으며 기업 및 제한 구역에서 기밀 데이터의 유출이 심각하기 때문에 기밀 데이터 유출 방지에 대한 지속적인 연구가 필요하다. 최근 연구 동향으로 파일 접근 로그를 수집하고 이를 바탕으로 파일 접근 화이트리스트를 만들어 파일 접근을 제어하는 연구가 있으며 다양한 접근으로부터 데이터 유출을 보호해야 한다[1].

This Research was supported by the Tongmyong University Research Grants (2020(2020A033-1).
*Corresponding Author : Seung-Soo Shin(shinss@tu.ac.kr)
Received May 9, 2022 Revised June 7, 2022
Accepted July 20, 2022 Published July 28, 2022

데이터 유출은 랜섬웨어, 감염된 PC, 사용자 인증 우회, 패스워드의 추출, 그리고 산업체의 내부자들에 의한 물리적 접근법 등이 있다. 모든 파일의 유출은 산업체 내부자에 의해 이루어지고 자료를 유출하는 대상은 은퇴한 직원, 재직 중인 직원, 협력업체의 직원 등으로 유출되고 있다[2].

기업들은 시스템과 네트워크의 보안장비 등 각종 보안시스템을 구축하여 파일 유출을 방지한다. 대기업의 경우 고가의 보안 솔루션 도입과 자체 시스템으로 기밀 데이터 유출을 방지할 수 있지만, 중소기업의 경우 인력, 비용 문제 등의 애로사항이 있다[3,4]. 기업에서 기밀 데이터, 내부정보의 유출 방지는 대부분 DLP(Data Loss Prevention) 솔루션으로 보안 시스템을 구축한다. DLP는 파일 유출을 방지하기 위해 이동식 디스크 또는 저장소를 통제하는 기술이며, EDLP(Endpoint DLP), NDLP (Network DLP), CDLP(Cloud DLP) 등이 있다[5-7]. 많은 기업이 사용하는 만큼 DLP 기술은 기업들의 중요한 보안 솔루션 중 하나이다[8].

본 논문에서는 산업체들이 파일 유출로 인한 피해를 방지하기 위해 중요 파일에 대한 해시 값을 사전에 계산한 뒤, 데이터베이스에 저장하여 실시간으로 중요 파일에 대해서만 선택적 이벤트 방식을 사용하고 판별하는 시스템으로 중요 파일의 유출을 대응한다. 파일 암호화 작업을 할 경우, 병목현상이 발생한다. 병목현상 구간을 분석하고 효율적인 시스템으로 개선하고자 한다.

2. 연구 동향

산업체들의 중요한 기술들이 법률의 보호를 받음에도 산업체들의 파일 유출은 심각할 정도로 증가하고 있으며 산업체들의 파일 유출에 대한 경제적 피해 금액도 상당히 증가하고 있다[9].

2.1 데이터 유출 사례

산업체의 파일과 개인정보 유출 피해는 매년 증가하고 있다. 산업체의 파일 유출 사건을 발생하는 원인 중 하나인 산업스파이는 대기업의 IT 분야에서 중소기업의 정밀기계분야로 변화하고 있는 추세이다[10].

국내의 산업체 파일 유출은 국방과학연구소에서 국가의 중요한 파일 유출에 대한 조사를 2016년부터 2020년까지 한 결과 퇴직자 1,078명 중 46명이 중요한 파일의 유출자이고, 이전에 중요한 파일을 유출한 경험 건수를 포함하면 70명에 이른다. 또한 산업체에 종사하고 있는 중에도 많은 연구원들이 무단으로 중요한 파일 자료를 유출하여 보안규정을 위반하고 있다[11].

해외 사례로 테슬라 회사는 중요한 파일을 유출한 직원을 고소하였다. 유출한 직원은 입사한지 3일 만에 경영 자동화와 관련된 6,000건 이상의 중요한 자료를 유출하고, 신입사원에 대한 중요한 파일을 개인 클라우드 저장소로 유출하였고 회사의 보안 관리자를 통해 유출된 증거 자료를 확보했다. 그는 “회사에서 개인 계정을 쓰면 안 된다고 알려준 사람이 없었다.”며 “단순히 나중에 파일을 열어보려고 개인 계정에 저장한 것”이라고 주장했다[12].

유형별 사례로는 불법적 기술탈취와 거래과정에서의 핵심기술유출이 있다. 먼저, 불법적으로 기술 탈취하는 것은 인가되지 않은 접근방식을 통해 기술을 유출시키는 것이다. 이와 관련해서 주로 산업체의 전·현직 내부 임직원, 외부 경쟁업체, 그리고 협력업체에 의해 발생하는 기술탈취 유형 등이 있다[13,14]. 일반적인 불법 기술유출에 비해 피해 받은 기업에서는 대응이 번거롭다. 이유는 기술유출에 대한 경로와 수법, 주체에 대해 입증이 어렵다. 이에 따라 거래과정에서 파일유출은 사전 조치, 분쟁, 그리고 책임 입증에 대한 종합적인 대책이 필요하다[15].

2.2 데이터 유출 문제점

데이터 유출의 분류는 데이터를 유출하는 사람, 산업체, 제도적, 환경적 측면으로 분류된다. 데이터를 유출하는 사람은 데이터가 유출된 기업의 피해에 비해 처벌 강도가 약하다. 그리고 산업체는 데이터 유출 방지에 대한 보안 의식과 관심이 부족하고, 보안 전담인력, 보안 관리체계 미비, 보안 기술 인력, 그리고 이에 대한 보상체계가 미흡하다[16].

제도적 측면에서는 기술에 대한 유출 및 침해행위에 대한 처벌이 미흡, 종합적인 시스템 미비하고, 사전예방에 대한 측면에서 정책지원이 부족하다. 환경적 측면에서는 산업체간 기술협력으로 기술유출 가능성의 증가, IT 환경의 변화에 따른 보안 위협 증가, 산업체의 해외 진출로 기술유출에 대한 위험이 증가하고 있다. 다양한 측면들의 데이터 유출 위협으로부터 사전 대응하는 것이 중요하다[15].

중소기업에서는 내부정보 유출시 수사를 의뢰・고소・고발 및 손해배상을 청구한다. 그리고 보안 관리 시스템을 강화를 해야 하는데 특별한 조치를 하지 않는 경우가 많다. 중요한 파일 유출 시 재발 방지를 위한 조치를 해야 하지만 많은 중소기업들은 조치를 하지 않아 파일 및 기술 유출에 대한 문제가 심각하다. 중소기업의 기술유출 피해액은 감소하듯 하지만 피해는 여전히 지속적이다[17].

2.3 데이터 유출 방지 기술

데이터 유출 방지를 위한 대표 기술로는 DLP가 있다. 데이터의 규칙, 키워드 등과 같은 특정 탐지 기술에 기반 한 엔드 포인트에서 전송 및 사용 등을 탐지하는 기술이다. DLP는 기밀 데이터의 유출을 방지하기 위해 차단되어야 하는 데이터 패턴에 대한 지속적인 갱신을 통해 반영되어야한다[18]. 네트워크 기반 DLP는 Monitor, Prevent 그룹으로 나뉜다. Monitor는 모니터링 방식으로 감시 및 차단 전용으로 다양한 유출 경로에 대해 모니터링이 핵심이다. Prevent는 프록시 방식으로 데이터 유출을 사전 차단하는 방식이다. 대표적으로는 Mail Proxy, DB Proxy가 있다[19].

3. 파일 유출 대응 시스템

파일 유출 대응을 위해 해당 PC의 이벤트를 실시간으로 모니터링하고 이벤트 감지를 통한 파일 유출 대응 시스템을 제안한다.

3.1 시스템 구성도

제안하는 파일 유출 대응 시스템은 클라이언트, 서버, 관리자, 데이터베이스로 구성된다. 클라이언트는 PC에서 파일을 복사하고 이동하는 등에 관한 이벤트를 실시간으로 탐지한다. 그리고 파일의 해시 값을 계산한 후, 중앙 제어 서버를 통해 파일에 대한 해시 값을 검증받고 결과를 삭제 또는 복호화를 한다. 서버는 클라이언트로부터 수신 받은 파일의 해시 값을 데이터베이스를 통해 중요 파일 여부를 검증한다. 관리자는 관리자 프로그램을 통해 중요 파일에 대한 해시 값을 데이터베이스에 등록하기 위해 로그인 후, 중요한 파일을 선택하여 해당 파일의 해시 값을 데이터베이스에 등록한다. 데이터베이스는 중요 파일에 대한 해시 값과 관리자의 계정정보 등이 저장된다. 파일 유출 대응의 구성은 Fig. 1과 같다.

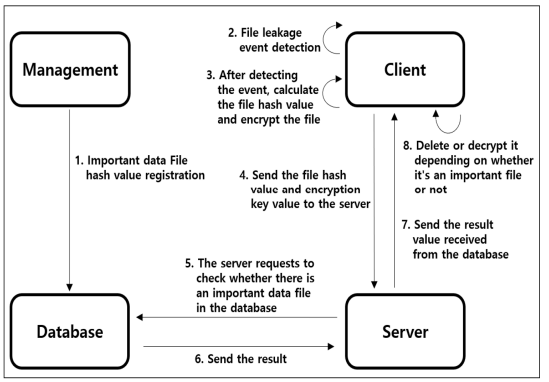

Fig. 1. System Configuration

3.2 시스템 흐름도

모든 중요 파일에 대한 해시 값은 데이터베이스에 저장한다. 중요 파일에 대한 업데이트가 필요할 경우, 관리자가 관리자 프로그램으로 데이터베이스에 중요 파일에 대한 해시 값을 등록한다. 사용자 또는 악의적인 사용자로 인해 이벤트가 발생할 때, 해당 파일을 복사하고 이동하는 명령어를 클라이언트로 전달한다. 클라이언트는 사용자로부터 받은 명령어를 수행하고 파일 복사 또는 파일 이동에 대한 이벤트가 발생한다.

클라이언트는 사용자 PC를 모니터링 하여 해당 파일의 복사와 이동이 발생할 경우, 원본 파일의 해시 값을 계산한 후, 클라이언트가 16자리 문자열의 대칭키를 생성하여 해당 파일을 암호화한다. 그리고 클라이언트는 대칭키를 서버의 공개키로 암호화하여 암호화한 대칭키와 파일의 해시 값을 서버로 전송한다. 서버는 클라이언트로부터 수신 받은 파일의 해시 값을 서버가 계산한 해시 값과 비교하여 일치하면 데이터베이스로 질의하여 중요 파일 여부를 검증한다. 이후 데이터베이스의 검증 결과에 따라 서버는 일반 파일일 경우 복호화 명령어를 전송하고 중요 파일의 경우 삭제 명령어를 전송한다. 파일 유출 대응은 Fig. 2와 같다.

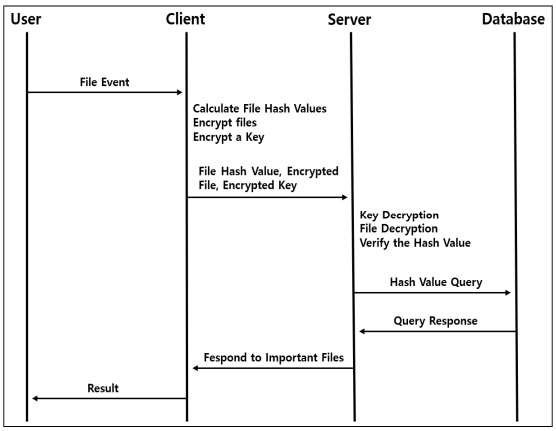

Fig. 2. System flow Chart

3.3 시스템 시뮬레이션

중요 파일 유출 대응을 위한 시뮬레이션은 환경 구성, 파일 유출 시나리오로 구성된다.

3.3.1 시스템의 환경 구성

시스템 시뮬레이션을 위한 하드웨어는 CPU 3.60GHz Octa Core, RAM 16GB, 네트워크 1000Mbps이다. 그리고 소프트웨어의 운영체제는 Windows 10 Pro 20H2, 언어는 C# .Net Framework 4.7.2를 사용한다. 데이터베이스는 MySQL 8.0.24로 구축한다.

3.3.2 시스템의 시나리오

이벤트 감지를 통한 파일 유출 대응을 위한 시스템의 시나리오는 클라이언트가 실행 중인 PC에 파일 복사 및 이동 이벤트가 발생할 경우, 유출 대상 파일을 암호화 작업을 한다. 그 후 파일의 해시 값을 계산하여 서버로부터 중요 파일 여부를 검증 받는다. 파일 유출 대응을 위한 시스템의 시나리오는 다음과 같다.

① 관리자는 사전에 관리자 프로그램을 사용하여 중요 파일의 해시 값과 경로를 데이터베이스에 저장한다.

② 관리자는 서버를 실행하고 클라이언트의 접속을 기다린다.

③ 사용자 및 악의적인 사용자가 중요 파일에 대한 유출 시도가 일어날 때, 클라이언트는 해당 파일을 대칭키로 암호화한다. 서버의 공개키로 암호화한 대칭키, 해당 파일의 해시 값, 그리고 경로를 서버로 전송한다.

④ 서버는 클라이언트로부터 암호화된 키를 개인키로 복호화하고, 복호화한 대칭키로 암호화된 데이터를 복호화한다. 이후 데이터의 해시 값을 계산하여 클라이언트로부터 받은 해시 값과 비교하여 검증한다. 해시 값이 일치하면 데이터베이스로 중요 파일 여부를 질의한다.

⑤ 서버는 데이터베이스의 검증 여부에 따라 클라이언트로 중요한 파일의 경우 삭제, 일반 파일의 경우 복호화 명령어를 전송한다.

3.4 시스템 구현

제안한 시스템은 관리자, 클라이언트, 서버 데이터베이스로 구현한다. 클라이언트는 파일 유출 이벤트 탐지, 해시 값의 계산, 파일 암호화 및 결괏값에 따른 삭제 또는 복호화 작업을 한다.

3.4.1 관리자

관리자 프로그램은 다음과 같이 진행된다. 관리자는 ID 및 PW를 입력하면 데이터베이스로부터 검증한다. 검증이 완료된 관리자는 프로그램에 파일 삭제 및 추가 명령을 통해 작업한다.

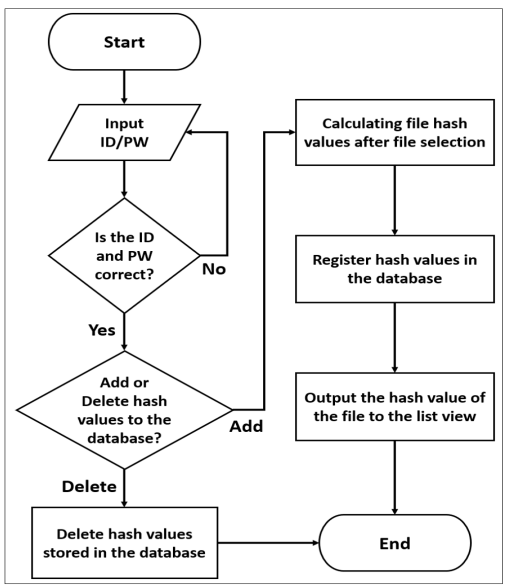

Fig. 3. Manager flow Chart

삭제 명령을 할 경우, 해당 파일의 해시 값을 삭제한

다. 파일에 대한 해시 값을 추가할 때 해당 파일의 해시 값을 계산한다. 계산된 파일의 해시 값을 데이터베이스에 추가한다. 데이터베이스에 추가된 파일의 해시 값을 리스트 뷰로 출력한 후 종료 단계로 진행된다. 또한 데이터베이스와의 연동을 위한 Module이 필요하다. 관리자 프로그램은 Fig. 3과 같이 진행한다.

3.4.2 클라이언트

클라이언트는 8단계로 진행되고 과정은 Fig. 4와 같이 진행한다.

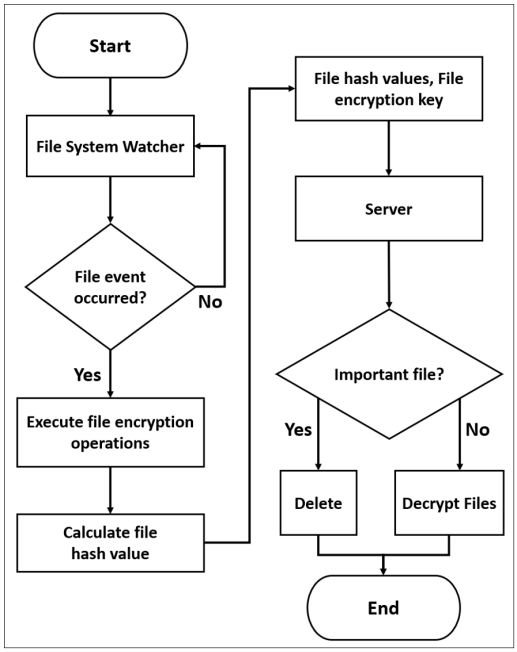

Fig. 4. Client flow Chart

① 사용자 또는 악의적인 사용자가 해당 파일을 복사하고 이동하는 이벤트가 발생할 때, 파일 시스템 와쳐는 파일의 이벤트를 탐지한다.
② File Copy Event 모듈에서는 해당 파일을 복사하고 이동하는 이벤트를 탐지한다.
③ 클라이언트는 16자리 문자열의 대칭키를 생성하고, Rijndael Managed를 사용하여 파일을 암호화한다.
④ 클라이언트는 유출 파일에 대한 해시 값을 계산한다.
⑤ 클라이언트는 파일의 해시 값과 서버의 공개키로 암호화한 대칭키를 JSON 형태로 변환한다.
⑥ 클라이언트는 해시 값, 암호화된 파일, 공개키로 암호화한 대칭키를 서버로 전송한다.
⑦ 클라이언트는 서버로부터 결괏값을 수신한다.
⑧ 클라이언트는 검증 결괏값에 따라 파일을 삭제 또는 복호화를 한다.

3.4.3 서버

서버는 5단계로 진행되고 Fig. 5와 같이 진행한다.
① 서버는 최초 실행 시 키 쌍이 필요하다. 공개 키 알고리즘에서 개인키는 RSAPrivateKeyGen로 생성하고, 공개 키는 RSAPublicKeyGen로 생성한다.
② 서버에서 TCP Listener는 중요 파일의 해시 값 검증을 위해 클라이언트의 접속을 기다린다.
③ 클라이언트가 서버에 접속하면 서버는 다수의 네트워크를 관리하기 위해 동적으로 Thread를 생성한다. 그리고 서버는 클라이언트에게 공개키를 전송한다.
④ 서버는 클라이언트로부터 받은 해당 파일의 해시 값 및 암호화 키를 데이터베이스에 질의한다.
⑤ 서버는 데이터베이스에 질의한 결괏값을 클라이언트에게 전송한다.

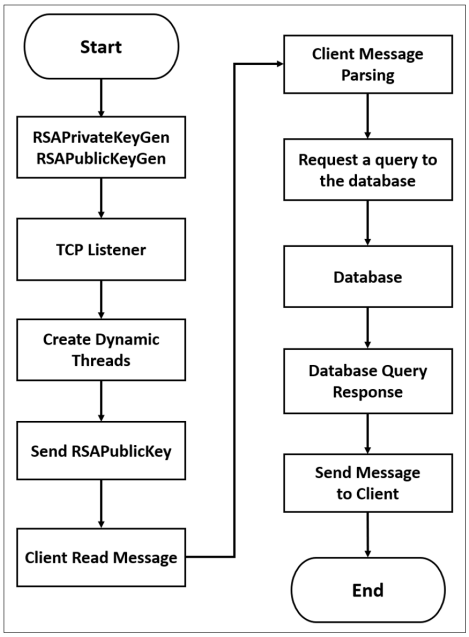

Fig. 5. Sever flow Chart

4. 분석

제안한 시스템은 사전에 지정한 중요 파일 대한 해시 값을 서버에 미리 등록하고 파일에 대한 이벤트가 발생할 경우 해시 값을 비교하여 판단하고 해당 파일을 복호화 또는 삭제를 진행한다. 이때 암호화 작업 중 시스템에서는 CPU에 대한 병목현상이 발생한다. 따라서 파일에 대한 종류별 그리고 파일의 용량에 따라 암호화 작업에 필요한 소요 시간 분석이 필요하다.

기업이나 국가의 중요한 파일 등은 문서 파일 형식으로 저장되는 것이 대부분이다. 본 논문에서는 문서 파일 형식으로 쓰이는 PDF, HWP, DOC, PPT, XLS 파일 확장자를 분석하고, 파일에 대한 크기는 문서 파일의 용량을 10MB, 15MB로 지정하여 분석한다. 제안한 시스템은 클라이언트 내에 모듈인 암호화/복호화 Module 이용하여 파일을 암호화한다. 파일을 암호화하기 위해 랜덤한 문자열 16자리 대칭키를 생성한다. 분석을 위해 대칭암호를 이용하여 100개씩의 PDF, HWP, DOC, PPT, XLS 확장자별 파일을 암호화한다.

파일 유출 대응을 위해 클라이언트 프로그램에서 암·복호화 Module로 파일을 암호화할 때, 과도한 CPU 사용으로 인해 해당 파일을 암호화하기 때문에 소요 시간이 전체 평균 암호화 작업의 소요 시간보다 증가함으로 병목현상이 발생한다. 암호화 작업의 소요 시간을 측정하기 위해 암호화 횟수를 10회에서 100회로 변경하고 10MB, 15MB 파일을 대상으로 병목현상을 분석한다.

첫 번째, 10MB 파일의 분석은 다음과 같다. 파일 종류별 동일한 방법으로 round에서 암호화할 때 소요 시간을 x, round 횟수를 i, 전체 round의 평균 시간을 t_3라 한다. 전체 round의 평균 시간을 천장함수를 사용하여 초 단위로 표현한다. round 횟수(i) 10번을 100번으로 변경하여 전체 round의 평균 시간(t_3)을 계산한다. 10MB 문서 파일의 병목현상 측정결과 평균값이 가장 낮은 HWP는 8 round에서 4,300초를 제외하고, 나머지 1~7 round 9~10 round까지 4,000초로 일정하다. 평균값이 가장 높은 DOC는 6, 7 round에서 5,800초를 제외한 나머지 round는 병목현상이 발생하여 파일을 암호화 작업의 소요되는 시간이 일정하지 않다. 10MB 파일의 대한 병목현상은 Fig. 6과 같다.

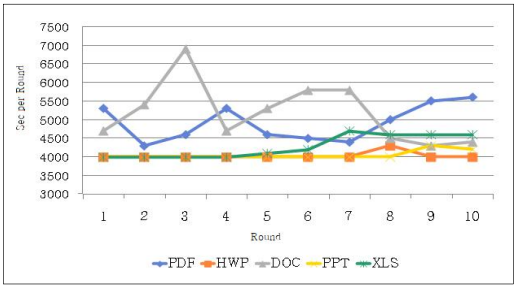

Fig. 6. 10MB file throttling

두 번째, 15MB 파일의 병목현상은 동일한 계산 방법을 이용하고, 15MB인 파일을 100회 암호화 작업한 후 병목현상을 분석한다. 15MB 파일의 병목현상 결과 평균값이 가장 낮은 PDF는 1과 6 round에서 5,810초, 3 round에서 5,790초를 제외하고, 나머지 round에서는 5,800초로 일정하다. 그리고 XLS는 5와 9 round에서 7,200초로 평균값이 가장 높고, 이를 제외한 나머지 round에서는 암호화하는 소요시간이 일정하지 않다. 15MB 파일의 병목현상은 Fig. 7과 같다.

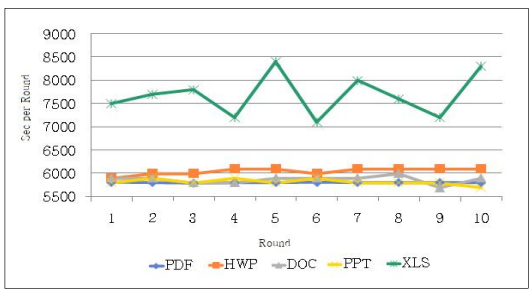

Fig. 7. 15MB file throttling

5. 결론

기업의 기밀 파일의 경우 유출 시에는 국가적, 경제적으로 피해가 심각하다. 본 논문에서는 중요 파일 유출 대응을 위한 시스템을 제안했다. 제안한 시스템은 클라이언트, 서버, 관리자, 데이터베이스로 구성되며, 클라이언트가 설치된 PC에서 파일에 대한 복사, 이동하는 등에 관한 이벤트를 실시간으로 탐지한다. 중요 파일 유출 시 특정 이벤트에 대한 지속적인 모니터링을 통해 시스템 부하를 최소화하기 위해 해당 파일을 확장자별로 분류하지 않고, 시그니처를 분석하여 정확성을 개선했다.

향후 연구로는 중요 파일 유출 시 다양한 경로를 통

한 유출을 방지하기 위해 네트워크 영역인 E-메일, 웹하드, P2P, SNS 등을 포함한 이벤트를 실시간으로 탐지하기 위해 통합솔루션 연구가 필요하다.

REFERENCES

[1] H. S. Lee, D. J. Kim, H. J. Lee & D. H. Hwang. (2021). A File Access Control System Based on File Access Logs for Ransomware Response and Data Loss Prevention System. *Korea Computer Congress 2021.*

[2] J. S. Lee & K. H. Lee. (2014). A Study on Security Container to Prevent Data Leaks. *Journal of The Korea Institute of Information Security & Cryptology, 24(6),* 1225-1241. DOI :10.13089/JKIISC.2014.24.6.1225

[3] G. J. Shin, G. H. Jung, D. M. Yang & B. H. Lee. (2017). A USB DLP Scheme for Preventing Loss of Internal Confidential Files. *Journal of the Korea Institute of Information and Communication Engineering, 21(12),* 2333-2340. DOI : 10.6109/jkiice.2017.21.12.2333

[4] M. B. Hyun & S. J. Lee. (2016). The Proactive Threat Protection Method from Predicting Resignation Throughout DRM Log Analysis and Monitor. *Journal of The Korea Institute of Information Security & Cryptology, 26(2),* 369-375. DOI : 10.13089/JKIISC.2016.26.2.369

[5] B. J. Jeon, D. B. Yoon & S. S. Shin. (2017). Improved Integrated Monitoring System Design and Construction. *Journal of Convergence for Information Technology, 7(1),* 25-33. DOI : 10.22156/CS4SMB.2017.7.1.025

[6] J. H. Choi & S. Y. Rhew. (2005). Monitoring System of File Outflow through Storage Devices and Printers. *Journal of the Korea Institute of Information Security & Cryptology, 15(4),* 51-60.

[7] J. U. Choi, Y. J. Lee & J. M. Park. (2012). E-DRM-based Privacy Protection Technology for Overcoming Technical Limitations of DLP-based Solutions. *Journal of the Korea Institute of Information Security & Cryptology, 22(5),* 1103-1113.

[8] J. H. Ko, G. S. Lee, H. Y. Kim & N. G. Kim. (2020). A Log Management System of Removable Storage Devices Based on Blockchain. *Journal of Korean Institute of Information Technology, 18(7),* 51-56.

[9] H. B. Chang. (2015). A Study on The Countermeasure by The Types through Case Analysis of Industrial Secret Leakage Accident. *Convergence security journal, 15(7),* 39-45.

[10] Police. (2021). *Police Statistical Yearbook.* (Online). https://www.police.go.kr

[11] The JoongAng. (2020). Available online: https://news.joins.com/article/23883461

[12] Insight. (2021). Available online: https://www.insight.co.kr/news/322291

[13] M. R. Lee. (2017). *A study on the improvement plan of monitoring system for preventing inside information loss of Korean firms overseas.* Sungkyunkwan University.

[14] J. H. In. (2015). *Research on DLP security policy with case study of internal information leakage.* Dankook University.

[15] S. J. Ahn. (2016). *Countermeasures to strengthen technology protection capabilities of SMEs.* Industry-Academic Cooperation Foundation of Sungkyunkwan University.

[16] H. H. Heo. (2007). *Small and medium-sized enterprise technology leakage cases and response strategies.* Korea Industrial Technology Promotion Association.

[17] Ministry of SMEs and Startups. (2021). *Amount of damage from technology leakage*(Online). https://www.ultari.go.kr/portal/introduce/realTechProtect.do

[18] S. J. Yoo. (2018). A Study on DLP System for Preventing Internal Information Leakage. *Convergence security journal, 18(5),* 121-126.

[19] H. R. Yoo, G. J. Shin, D. M. Yang & B. H. Lee. (2018). A Digital Secret File Leakage Prevention System via Hadoop-based User Behavior Analysis. *Journal of the Korea Institute of Information and Communication Engineering, 22(11),* 1544-1553. DOI : 10.6109/jkiice.2018.22.11.1544

신 승 수(Seung-Soo Shin) [정회원]

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

- 관심분야 : 암호프로토콜, 네트워크 보안, U-헬스 케어, IoT, 데이터분석
- E-Mail : shinss@tu.ac.kr