데이터 분석을 활용한 랜섬웨어 탐지 시스템 설계

김진욱[O], 이영재[*], 윤정훈[*], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과
e-mail: {wlsdnr0816[O], kronosyuki[*], spzh1592[*]}@mokpo.ac.kr, carpedm@mnu.ac.kr[*]

Design of a Ransomware Detection System Utilizing Data Analytics

Jinwook Kim[O], Youngjae Lee[*], Jeonghoon Yoon[*], Kyungroul Lee[*]
[O]Dept. of Information Security Engineering, Mokpo National University,
[*]Dept. of Information Security Engineering, Mokpo National University

● 요 약 ●

랜섬웨어는 Ransom(몸값)과 Software(소프트웨어)의 합성어로, 데이터를 암호화하여 이를 인질로 금전을 요구하는 악성 프로그램이다. 블랙캣(BlackCat)과 같은 랜섬웨어가 스위스 항공 서비스 기업의 시스템을 마비시키는 공격을 시도하였으며, 이와 같은 랜섬웨어로 인한 피해는 지속적으로 발생하고 있다. 랜섬웨어에 의한 피해 감소 및 방지를 위하여, 다양한 랜섬웨어 탐지방안이 등장하였으며, 최근 행위 기반 침입탐지 시스템에 인공지능 기술을 결합하여 랜섬웨어를 탐지하는 방안이 연구되는 실정이다. 인공지능 기술은 딥러닝 및 하드웨어의 발전으로 데이터를 처리할 수 있는 범위가 넓어지면서, 다양한 분야와 접목하여 랜섬웨어 탐지를 위한 시스템에 적용되고 있지만, 국내는 국외만큼 활발하게 연구되지 않고 연구 개발 단계에 머물러 있다. 따라서 본 논문에서는 랜섬웨어에 감염된 파일에서 나타나는 특징 중 하나인 엔트로피를 데이터 분석에 활용함으로써, 랜섬웨어를 탐지하는 시스템을 제안하고 설계하였다.

키워드: 랜섬웨어(Ransomware), 데이터 분석(Data analysis), 머신러닝(Machine learning), 시스템 설계(System design)

I. 서론

랜섬웨어는 시스템 파일을 포함한 문서 및 이미지와 같은 사용자의 데이터를 암호화하고, 복구에 대한 대가로 금전을 요구하는 악성코드이다. 1989년에 등장한 최초의 랜섬웨어인 AIDS를 시작으로, 최근 랜섬웨어가 유행하기 시작하였으며, 국내에는 2015년 크립토락커(Cryptolocker)의 한글 버전이 유포되면서 사회적인 문제로 드러났다[1]. 이러한 랜섬웨어 중 하나인 블랙캣(BlackCat)은 2023년 7월과 9월에 영국, 일본, 미국의 각 기업을 공격하였으며, 데이터의 몸값과 관련된 협상이 거부되면, 탈취한 데이터를 다크웹에 공개하는 것과 같이 사회적으로 큰 피해가 발생하고 있다[2].

이러한 랜섬웨어를 탐지하기 위하여, 인공지능을 결합한 랜섬웨어 탐지방안과 엔트로피 측정 기반 랜섬웨어 탐지방안이 연구되는 추세이다. 그러나 인공지능을 결합한 랜섬웨어 탐지방안은 행위 기반 침입탐지로, 모델에 따라 높은 탐지 성능이 나타나기도 하지만, 국내에서는 국외만큼 활발하게 적용되지는 않고 연구개발 단계에 머물러 있는 실정이다[3]. 또한, 엔트로피 측정 기반 랜섬웨어 탐지방안은 높은 탐지율과 오탐 및 미탐의 발생이 적은 장점이 있지만, 엔트로피의 임곗값이나 데이터 분석을 통한 학습 모델과 관련된 연구에 집중되어 있어, 접근성 및 사용성 측면 연구가 미흡하다. 이에 따라, 이러한 한계점을 극복하기 위한 방안과 시스템이 요구되는 실정이다[4].

본 논문에서는 높은 탐지율과 오탐 및 미탐의 발생이 적은 장점을 만족하는 머신러닝과 접근성 및 사용성 측면의 한계점을 극복하기 위한 웹 모니터링을 제공하는 랜섬웨어 탐지 시스템을 제안하고 설계하였다. 데이터 분석은 데이터를 수집하고, 수집한 데이터에서 유용한 정보를 추출하고 활용하는 과정이다. 이러한 데이터 분석을 활용하기 위한 기술로는 4차 산업혁명의 대표적인 빅데이터, 머신러닝, 딥러닝이 있으며, 패턴 인식과 예측, 복잡한 문제 해결 등을 제공하는 데이터 분석의 강력한 모델을 학습시키고 활용한다면, 랜섬웨어 탐지에 매우 효과적일 것으로 판단된다. 그뿐만 아니라, 사용자 관점에서의 접근성 및 사용성 측면에서, 사용자들에게 시각적으로 편리하게 랜섬웨어의 탐지 및 상태를 확인하는 웹 모니터링 기능을

제공하며, 이를 통하여 랜섬웨어 감염 상태 및 감염 파일을 확인하고, 사용자의 컴퓨터를 관리할 수 있다.

II. 랜섬웨어 탐지 시스템 설계

1. 전체 시스템 설계

제안하는 랜섬웨어 탐지 시스템의 전체 시스템 설계를 그림 1에 나타내었다.

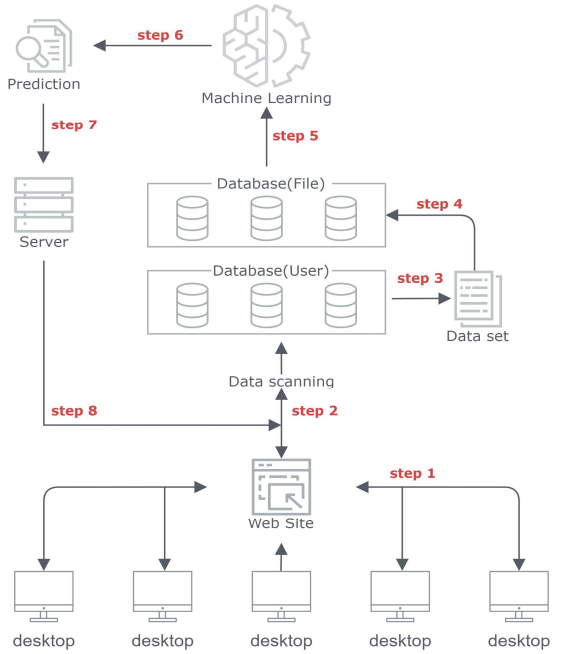

Fig. 1. 전체 시스템 설계

사용자의 전자기기(desktop)는 웹 사이트에 접속하여 사이트에서 제공하는 파일 스캐닝 도구를 설치한다 (Step 1). 설치한 파일 스캐닝 도구는 사용자의 전자기기에 저장된 전체 파일을 스캔하고(Step 2), 스캔한 파일에서 수집된 메타데이터를 데이터베이스 (User)로 전송한다. 해당 메타데이터는 데이터 분석을 더욱 효과적으로 처리하기 위하여, 전처리하여 데이터셋을 생성하고(Step 3), 데이터베이스(File)에 저장한다(Step 4). 이와 같이, 데이터베이스(File)에 저장된 데이터셋을 통하여, 랜섬웨어 감염을 탐지하기 위한 데이터 분석 중 하나인 머신러닝 모델을 학습한다(Step 5). 학습된 머신러닝 모델을 통하여, 지속적으로 사용자의 전자기기에 저장된 파일들을 대상으로 랜섬웨어 감염 여부를 예측하며 (Step 6), 랜섬웨어에 감염된 것으로 판단된 파일의 정보를 서버로 전달한다(Step 7). 마지막으로, 파일의 개수, 감염 진행도, 감염 결과를 시각화하여 웹 페이지에 출력함으로써, 사용자는 랜섬웨어 감염 상태를 모니터링한다(Step 8).

2. 기능 및 구성요소

랜섬웨어 탐지 시스템은 웹 모니터링을 위하여, 그림 2와 같이 웹 페이지, 파일 스캐닝 도구, 랜섬웨어 감염 상태 및 탐지기능을 제공하며, 머신러닝을 통하여 랜섬웨어 감염 여부를 예측하는 기능을 제공한다.

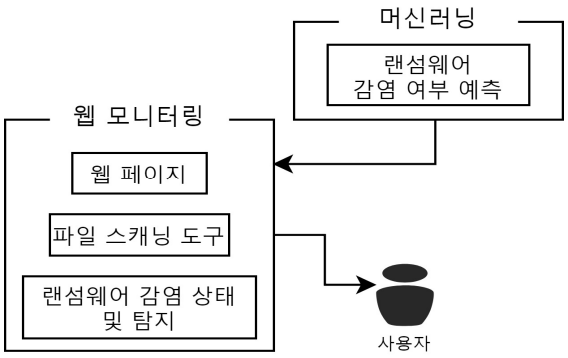

Fig. 2. 탐지 시스템에서 제공하는 핵심 기능

웹 페이지는 사용자 계정에 따른 웹 페이지를 제공하며, 사용자와 관련된 파일의 메타데이터 정보를 보호하기 위하여 암호화한다. 파일 스캐닝 도구는 사용자의 전자기기에 저장된 파일의 메타데이터를 스캔하며, 해당 데이터를 기반으로 웹 페이지에서 파일의 목록을 시각화한다. 랜섬웨어 감염 상태 및 탐지는 머신러닝을 활용하여 랜섬웨어 감염 여부를 예측하고, 예측 결과를 기반으로 감염 상태와 탐지 결과를 시각화한다.

3. 랜섬웨어 탐지를 위한 유즈케이스 설계

제안하는 랜섬웨어 탐지 시스템을 위한 유즈케이스 설계는 그림 3과 같다.

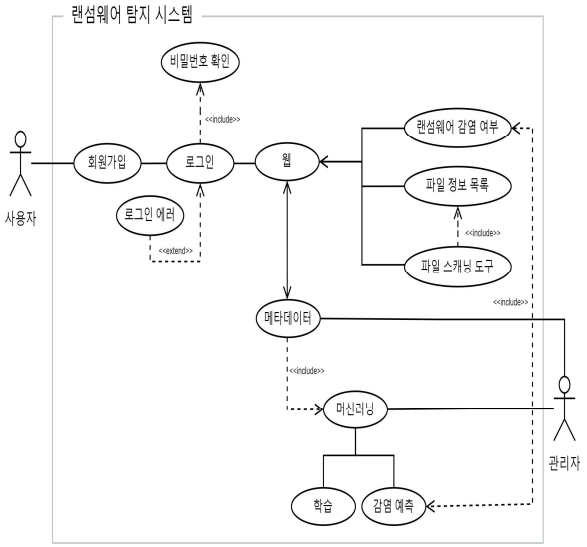

Fig. 3. 랜섬웨어 탐지 시스템 유즈케이스

사용자는 회원가입 및 로그인을 통하여 웹 서비스를 제공받으며, 웹에서는 랜섬웨어 감염 여부 확인, 파일 정보 목록 확인, 파일 스캐닝 도구 설치 기능을 제공한다. 웹은 설치된 파일 스캐닝 도구를 통하여 사용자의 전자기기에 저장된 파일의 메타데이터를 수집하고, 수집된

파일의 정보를 모니터링하도록 시각화한다. 이와 같이 수집된 메타데이터는 시각화뿐만 아니라, 전처리 과정을 통하여 머신러닝 모델을 학습하기 위한 데이터로 활용된다. 데이터 학습은 전처리된 데이터를 기반으로 머신러닝 모델을 활용하여, 사용자의 전자기기에 저장된 파일들의 랜섬웨어 감염을 예측하며, 그 결과를 웹 페이지로 제공한다. 이러한 데이터는 사용자의 정보가 포함되므로, 안전하게 보호되어야 하며, 이를 위하여 관리자가 데이터를 관리하고 보호한다.

4. 데이터 분석을 활용한 랜섬웨어 탐지 방안

4.1. 기존 미끼 파일 기반 랜섬웨어 탐지 방안 한계점

미끼 파일 기반 랜섬웨어 탐지 방안은 랜섬웨어가 파일을 암호화하는 특징을, 사용자의 중요한 파일이 아닌, 의미가 없는 미끼 파일에 적용하도록 유도하는 방안이다. 랜섬웨어가 사용자의 중요한 파일을 암호화하기 전, 디스크에서 가장 처음 접근하도록 유도된 디렉터리를 생성하고, 그 디렉터리에 미끼 파일을 저장한다. 이후, 랜섬웨어가 미끼 파일에 접근하여 암호화 또는 파일을 변조하려고 하는 순간을 탐지하여 랜섬웨어를 탐지한다.

이 기술은 허니팟(Honeypot)이라고 불리며, 암호화가 시작되기 전에 감염을 탐지하고 차단하는 기회를 제공함으로써, 랜섬웨어에 의하여 발생하는 피해를 최소화할 수 있다. 그러나 이 방식은 랜섬웨어가 미끼 파일에 먼저 접근하지 않거나, 우회하는 경우, 랜섬웨어 감염을 탐지하지 못하는 한계점이 존재한다[5].

4.2. 데이터 분석 기반 랜섬웨어 탐지 방안

이 방안은 랜섬웨어 탐지를 위하여, 파일의 메타데이터, 특히, 엔트로피 정보를 데이터 분석에서 이용하며, 여기에서 엔트로피는 데이터의 균일성을 의미한다. 만약 어떠한 값이 0부터 8까지의 범위에 포함될 경우, 엔트로피 값이 0에 가까우면 데이터가 균일하지 않은 것을 의미하고, 엔트로피 값이 8에 가까우면 데이터가 균일한 것을 의미한다. 이러한 데이터의 균일성은 암호문에서 뚜렷하게 나타나며, 암호문은 데이터가 균일하게 나타나도록 설계되었으므로, 높은 엔트로피 값을 가진다. 이와 같은 암호문의 특징으로 인하여, 랜섬웨어에 감염된 파일은 엔트로피가 높아지는 경향을 보이며, 파일의 엔트로피를 측정함으로써 랜섬웨어에 감염된 파일의 탐지가 가능하다. 상기 특징을 토대로, 파일 포맷별 엔트로피를 측정한 결과를 그림 4에 나타내었다.

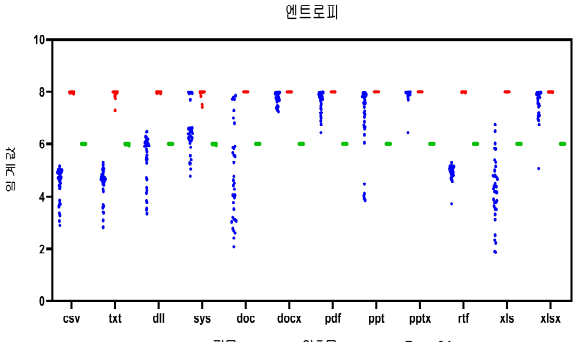

Fig. 4. 파일 포맷에 따른 엔트로피 측정 결과

그림을 살펴보면, 파일 포맷에 따라 매우 다양하게 평문과 암호문을 구분하는 엔트로피 임곗값을 도출할 수 있다. 이는 암호문이 높은 엔트로피를 가지는 특징으로 인하여, 랜섬웨어에 감염된 파일을 탐지할 수 있지만, 암호문의 엔트로피를 조작하기 위하여, base64 인코딩 기법을 적용함으로써, 랜섬웨어 탐지를 무력화하는 방안이 등장하였다[6]. 그뿐만 아니라, 평문과 거의 유사한 엔트로피를 가지도록 base64 인코딩 기법을 포함한 다양한 인코딩 기법을 적용함으로써, 엔트로피 기반 랜섬웨어 탐지 방안을 무력화하는 방안도 등장하였다[7].

이와 같은 무력화 방안을 해결하기 위하여, 인코딩된 파일의 엔트로피가 평문과 유사하더라도, 랜섬웨어에 감염된 파일을 탐지하는 방안이 요구되며, 본 논문에서는 머신러닝과 같은 데이터 분석을 통하여 랜섬웨어를 탐지하는 방안을 도입하고, 이를 통하여, 높은 탐지율을 제공하는 랜섬웨어 탐지 시스템을 구축하는 것이 목표이다.

III. 결과

최근 랜섬웨어 탐지 방안은 인공지능을 결합한 방안이나 엔트로피 측정을 활용한 방안과 같은 다양한 방안들이 연구되는 추세이다. 그러나 이러한 탐지 방안들은 국내에서 아직 활발하게 사용되지 않거나 학습 모델과 관련된 연구에 집중되어 있고, 효율성 및 편의성과 관련된 연구는 미흡한 실정이다.

따라서, 본 논문에서는 기존의 랜섬웨어 탐지방안의 한계점을 극복하기 위하여, 엔트로피와 같은 데이터 분석을 활용한 랜섬웨어 탐지 시스템을 제안하였다. 제안하는 방안은 데이터 분석으로 패턴 인식과 예측, 복잡한 문제 해결 능력이 뛰어난 인공지능의 머신러닝이나 딥러닝을 활용하여 랜섬웨어를 탐지한다. 또한, 사용자의 편의성과 관련하여, 웹 사이트를 제공함으로써 사용자는 자신의 컴퓨터 상태를 쉽게 파악할 수 있으며, 랜섬웨어 감염 여부에 따라 빠른 대처가 가능할 것으로 판단된다.

본 논문에서 제안한 방안은 랜섬웨어 탐지와 관련하여 우수한 결과를 가질 것으로 예상되며, 향후, 머신러닝이나 딥러닝과 같은 데이터 분석 성능을 향상시키기 위한 방안을 연구할 예정이다. 더 나아가 랜섬웨어를 탐지하는 모듈로써, 새로운 탐지 프로그램을 설계하고 개발할 예정이며, 이러한 결과물들을 통하여 랜섬웨어를 탐지하는 통합 시스템을 구축할 예정이다.

ACKNOWLEDGEMENT

이 성과는 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2021R1A4A2001810). 본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역 혁신 사업의 결과입니다.(2021RIS-002, 1345370809)

REFERENCES

[1] Korea Internet & Security Agency, "Ransomware Response Guidelines," https://www.kisa.or.kr/402/form?postSeq=2299, accessed on December 1, 2023.

[2] Korea Internet & Security Agency, "Ransomware Trend - Third quarter for 2023," https://seed.kisa.or.kr/kisa/Board/165/detailView.do, accessed on December 1, 2023.

[3] Y. Lee, H. Choi, D. Shin, and J. Lee, "Deep Learning based User Anomaly Detection Performance Evaluation to prevent Ransomware," Journal of Software Assessment and Valuation, Vol. 15, No. 2, pp. 43-50, Dec. 2019.

[4] K. Lee, J. Lee, S. Lee, and K. Yim, "Effective Ransomware Detection Using Entropy Estimation of Files for Cloud Services," Sensors, Vol. 23, No. 6, 3023, Mar. 2023.

[5] K. Kug, Y. Ryu, and S. Shin, "Implementation of reliable dynamic honeypot file creation system for ransomware attack detection," Journal of convergence security, Vol. 23, No. 2, pp. 27-36, Jun. 2023.

[6] J. Lee and K. Lee, "A Method for Neutralizing Entropy Measurement-Based Ransomware Detection Technologies Using Encoding Algorithms," Entropy, Vol. 24, No. 2, 239, Feb. 2022.

[7] T. McIntosh, J. Jang-Jaccard, P. Watters, and T. Susnjak, "The Inadequacy of Entropy-Based Ransomware Detection," International Conference on Neural Information Processing, pp. 181-189, Dec. 2019.