Journal of KIIT. Vol. 23, No. 12, pp. 265-273, Dec. 31, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.12.265

편광 시각화 기법을 활용한 시그니처 기반 악성코드 탐지 원리 초등 에듀테크 메커니즘 제안

김진수*, 박남제**

Proposal of an EdTech Mechanism for Elementary Education based on Signature-based Malware Detection using Polarization Visualization Techniques

Jinsu Kim*, Namje Park**

This work was supported by the Korea Foundation for the Advancement of Science and Creativity(KOFAC) grant funded by the Korea government(MOE)

요 약

본 논문은 시그니처 기반 악성코드 탐지의 개념을 초등 수준에서 효과적으로 전달하기 위해, 편광 필터를 활용한 게이미피케이션 기반 에듀테크 메커니즘을 설계하였다. 학습자는 시각적으로 왜곡된 단어들 중 정답 시그니처를 탐색하며, 팀 단위의 단서 공유와 전략적 판단을 통해 실제 탐지 과정의 핵심 구조를 간접적으로 체험하게 된다. 제안 메커니즘은 정보의 제한성과 판단 부담, 정오탐 구분 등의 요소를 학습에 반영함으로써 정보보안 개념의 내재화를 유도하며, 이를 통해 학습자의 몰입과 학습 흥미를 증진시킨다. 또한, 이러한 과정은 학습자에게 실질적인 정보분석 경험과 상황판단 능력을 동시에 제공하여, 시각 인식, 전략적 사고, 협동 문제 해결 역량 향상에 기여할 수 있다. 나아가 초등 교육 단계에서의 정보보안 이해도 확산과 기초 보안 역량 강화에도 긍정적인 효과를 기대할 수 있다.

Abstract

This paper proposes a gamification-based edutech mechanism using a polarizing filter to convey the concept of signature-based malware detection at the elementary level. Learners identify correct signatures among visually distorted words, engaging in team-based clue sharing and strategic decision-making to experience the core detection process. By reflecting factors such as limited information, cognitive load in decision-making, and distinguishing between true and false positives, the approach fosters internalization of information security concepts while enhancing engagement. It also promotes visual perception, strategic thinking, and collaborative problem-solving skills, contributing to improved cybersecurity literacy and basic security competence in early education.

Keywords
malware detection, signature, game-based learning, cybersecurity education, polarized filter

* 제주대학교 사이버보안인재교육원 연구원
- ORCID: https://orcid.org/0000-0003-1009-3928
** 제주대학교 초등컴퓨터교육전공 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

• Received: Aug. 14, 2025, Revised: Oct. 21, 2025, Accepted: Oct. 24, 2025
• Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

정보보안은 디지털 사회에서 필수 소양으로 자리 잡고 있으며, 기초 개념 이해와 역량 함양이 요구되고 있다. 그러나 현재 초등 정보보안 교육은 주로 계도 중심이나 단편적 개념 전달에 머물고 있어 학습자가 보안 원리를 체험적으로 이해하기 어렵다. 기존 에듀테크 교수법은 시뮬레이션이나 단순 시각 자료에 의존하여 학습자의 참여를 이끌지만, 원리의 구조적 이해를 촉진하는 데는 한계가 있다. 따라서 단순 암기를 넘어 보안 사고의 작동 원리와 한계를 탐구할 수 있는 체험적 접근이 요구된다[1][2].

시그니처 기반 악성코드 탐지는 사전에 정의된 패턴을 활용하는 대표적 방식으로, 보안 기초 개념 교육에서 중요한 소재가 된다[3][4]. 그러나 H. Holm의 연구[5]에 따르면 Snort는 알려진 공격에서 평균 54% 탐지율에 그쳤으며, 제로데이 공격에서는 17%에 불과하였다. 이는 시그니처 기반 탐지가 새로운 악성코드에 취약하다는 점을 보여주는 대표적 사례로, 지능형 지속 위협(APT, Advanced Persistent Threat)과 자동화된 변종 악성코드가 확산되면서 이러한 한계가 더욱 뚜렷해지고 있다. 따라서 탐지 개념을 교육할 때는 탐지 원리뿐 아니라 실패와 오탐의 가능성까지 경험적으로 이해시키는 접근이 요구된다.

교육 현장의 수요 또한 이러한 접근의 필요성을 뒷받침한다. 교육부의 2022 개정 교육과정은 디지털 기초 소양을 필수 역량으로 규정하고 있으며, KERIS의 2020 교육정보화 실태조사는 교사의 ICT 활용 역량에 상당한 격차가 존재함을 보고하였다[6][7]. 특히 초등 정보 수업은 주당 1~2차시에 한정되는 경우가 많아, 복잡한 방식보다 간단한 교구와 규칙을 활용한 체험 기반 메커니즘이 효과적인 대안이 될 수 있다.

이에 본 논문은 편광 필터를 활용하여 학습자에게 제한된 단서를 단계적으로 노출시키고, 왜곡된 단어 중 악성코드 시그니처를 유추하는 게임적 상호작용 기반의 체험형 에듀테크 메커니즘을 제안한다. 학습자는 팀 단위로 단서를 수집하고 협력적 추론을 수행하며, 이를 통해 시그니처 탐지의 원리와 한계, 그리고 정탐과 오탐이 발생하는 불확실성 구조를 보다 구체적이고 체험적으로 이해하게 된다.

Ⅱ. 관련 연구 분석

2.1 시그니처 기반 악성코드 탐지 구조와 한계

시그니처 기반 악성코드 탐지는 알려진 악성코드의 고유한 식별 정보(시그니처)를 바탕으로 위협 여부를 판별하는 전통적 탐지 방식이다[8][9]. 안티바이러스 소프트웨어나 침입 탐지 시스템 등에서 널리 활용되며, 보안 교육에서도 가장 기본적인 개념으로 다뤄진다.

본 논문에서는 NIST의 Guide to Intrusion Detection and Prevention Systems에서 제시하는 탐지 흐름의 주요 기능 요소를 참고하여 (1) 이벤트 수집(Input), (2) 데이터 전처리 및 특징 추출(Feature Extraction), (3) 시그니처와의 비교(Matching), (4) 탐지 여부 판별 및 알림(Decision/Alerting)이라는 네 단계로 요약하였다[10][11]. 이러한 체계는 단순한 개념 설명을 넘어, 실제 보안 시스템이 입력 데이터를 처리하여 위협 여부를 판별하는 과정을 명확히 보여준다.

시그니처 기반 탐지는 알려진 공격을 빠르게 탐지할 수 있는 장점이 있지만, 새로운 악성코드나 변종 공격에는 취약하다는 본질적 한계를 지닌다[12][13]. 따라서 교육적 관점에서 이 원리를 다룰 때는 탐지 성공뿐 아니라 탐지 실패와 오탐의 가능성까지 함께 경험적으로 이해시키는 것이 필요하다.

2.2 편광 필터 기반 탐지 과정 시각화 메커니즘

편광(Polarization)은 빛의 진동 방향을 제어하여 특정 방향의 성분만 통과시키는 광학적 현상이다[14][15]. 두 개의 편광 필터를 서로 수직으로 교차시키면 대부분의 빛이 차단되어, 그 뒤에 위치한 패턴이나 글자는 보이지 않는다. 그러나 교차된 필터 사이에 제3의 필터를 45도로 삽입하면 일부 빛이 다시 투과하면서 감춰진 패턴이 부분적으로 드러난다[16][17]. 본 논문에서는 이러한 원리를 활용하여, 악성코드 탐지 과정의 불완전성과 불확실성을 학습자가 직접 체험할 수 있도록 설계하였다.

그림 1은 제안 메커니즘에서 적용한 편광 원리를 보이는 것이다. 수직으로 교차하는 두 편광판은 빛을 차단하여 반대편을 확인할 수 없으나, 교차하는 두 편광판 사이에 45도 각도의 편광판을 추가할 경우, 일부 빛이 통과되어 반대편을 확인할 수 있다.

제안 메커니즘은 시그니처 후보 단어가 인쇄된 A4 시트를 교차 편광 필터로 차단한 상태에서 시작함으로서, 학습자는 필터 아래 아무것도 보지 못한 채로 차례마다 원하는 위치에 45도 각도의 필터를 삽입한다. 삽입된 영역에서만 일부 단서가 드러나며, 이를 통해 해당 단어가 실제 시그니처인지 여부를 추론할 수 있다. 이 과정은 두 개의 팀이 번갈아 가며 수행되며, 각 팀은 제한된 시도 안에서 가능한 한 많은 단서를 확보하고 다른 팀보다 먼저 정답을 찾아내야 한다.

이러한 구조는 NIST에서 제시한 과정을 요약한 한 시그니처 기반 탐지 과정과 직접적으로 대응된다. A4 시트는 입력 데이터(Input)에 해당하며, 45도 필터 삽입은 부분적 단서를 추출하는 특징 추출(Feature extraction)에 해당한다. 드러난 단서를 기존 시그니처 후보와 비교하는 것은 매칭(Matching)에 해당하고, 최종적으로 팀이 정답 여부를 선언하는 과정은 탐지 판정(Decision)에 대응된다. 특히 일부 단서만 드러나고 유사한 후보가 함께 존재하는 상황은 실제 탐지 환경에서의 정탐(True positive), 오탐(False positive), 탐지 실패(False negative)의 구조를 반영한다.

따라서 본 논문에서 제안하는 편광 필터 기반 시각화는 단순한 광학 실험을 넘어서, 협력과 경쟁을 기반으로 한 상호작용 속에서 탐지 과정의 본질을 경험하도록 설계된 에듀테크 메커니즘이다. 이는 학습자가 탐색, 판단, 의사결정 과정을 거치며 보안 사고의 본질을 학습할 수 있도록 유도한다[18][19].

2.3 관련 연구 분석

사이버보안 에듀테크 분야에서는 게임 기반 학습이 학습자의 보안 개념 이해와 관심도 증진에 효과적이라는 연구가 다수 보고되고 있다. GenCyber 캠프를 대상으로 한 G. Jin et al.[20]는 고등학생을 대상으로 다양한 보안 게임을 활용한 교육 모듈을 운영하고, 참가자 설문 결과 게임 기반 학습이 보안 개념 인지와 관심도 증진에 효과적이라는 결과를 도출하였다. J. Vykopal et al.[21]은 CTF (Capture-the-Flag) 게임을 대학 교육 환경에서 활용하여 보안 개념의 이해를 증진하고 학습자의 참여도를 높이는 효과를 확인하였다. Nkongolo[22]는 남아프리카 전통 보드게임 ‘Morabaraba’를 변형한 CyberMoraba를 활용하여 사이버보안 인식을 높이는 교육적 효과를 보고하였다. 이들 연구는 게임 요소가 학습자의 몰입과 개념 내재화에 효과적임을 보여준다.

본 논문은 이와 같이 시뮬레이션을 통한 직관적 이해 접근을 기반으로 하되, 초등 학습자의 인지적 특성을 고려한 게임적 구조와 협력적 탐색 방식을 적용하여 보다 교육적 효과성을 극대화하는 데 중점을 두었다.

III. 편광 시각화 기반 악성코드 시그니처 탐지 초등 에듀테크 메커니즘 제안

3.1 에듀테크 개념적 설계

시그니처 기반 악성코드 탐지는 이미 알려진 악성코드의 고유 패턴을 데이터베이스와 비교하여 위협 여부를 판정하는 전통적 방식이다.

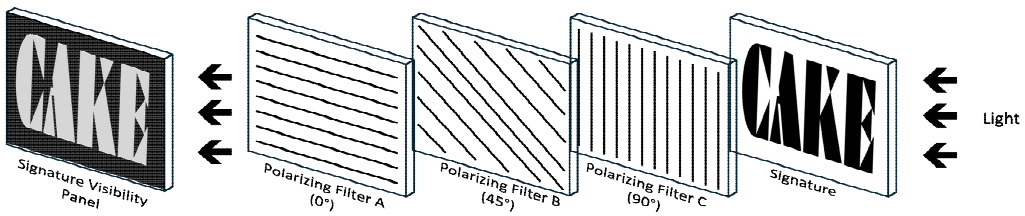


그림 1. 편광 필터 기반 단계적 노출 개념
Fig. 1. Architectu concept of stepwise exposure using a polarizing filter

이 과정은 일반적으로 악성 행위의 특징을 시그니처로 정형화하고, 이를 탐지 엔진에 등록하며, 대상 파일과 트래픽 및 로그와 실시간으로 비교한 뒤, 일치 여부를 판정하는 절차로 구성된다. 탐지 결과는 정탐(True positive), 오탐(False positive), 미탐(False negative)으로 구분되며, 각 경우는 보안 시스템의 성능과 신뢰성에 직접적인 영향을 미친다. 이러한 기법은 알려진 위협에 대해서는 높은 효율성을 보이지만, 등록되지 않은 새로운 악성코드나 변종에 대해서는 탐지가 불가능하다는 근본적 한계를 가진다. 따라서 탐지 과정은 본질적으로 불확실성을 수반하며, 보안 분석가는 제한된 단서를 바탕으로 신중하게 판단해야 한다.

이와 같은 기술적 절차는 교육적 맥락에서 체험 가능한 형태로 변환될 필요가 있다. 제안하는 에듀테크 메커니즘은 시그니처를 단어 형태로 단순화한 뒤, 이를 격자 구조로 분해 및 왜곡하여 학습자에게 제시한다. 학습자는 수직으로 교차된 편광 필터 위에 45도 각도의 필터를 삽입하여 제한된 단서를 확보하고, 이를 종합해 정답 시그니처를 추론해야 한다. 이 과정에서 정탐은 정답 선언, 오탐은 감점, 미탐은 정답 미도출로 대응된다. 학습자는 제한된 정보 속에서 전략적으로 탐색하고 협력적으로 판단하는 과정을 경험함으로써, 보안 탐지에서 요구되는 정확성, 신중함, 그리고 불확실성 관리의 개념을 자연스럽게 습득하게 된다. 결과적으로 제안된 메커니즘은 단순한 흥미 유발을 넘어, 정보보안 탐지의 핵심 원리를 교육적으로 재현할 수 있는 사례로 제시될 수 있다.

3.2 제안 에듀테크 메커니즘 적용 편광 원리

편광 필터 기반 시각화는 악성코드 탐지의 본질적 특징인 불완전한 단서와 불확실성 속 판단을 학습자가 체험하도록 설계되었다.

편광 필터 구성은 그림 2의 원리를 기반으로 한다. 전체 탐지 영역은 4×4 격자로 구획되어 있다. 두 장의 기본 편광판은 수직으로 교차해 대부분의 정보를 차단한 상태로 배치되며, 학습자는 보조 편광판을 준비된 격자 중 하나의 크기에 맞추어 삽입한다. 이때 삽입된 영역에서만 일부 문자의 단서가 드러나도록 설계되어 있으며, 각 시도는 단일 격자에 국한된다. 이러한 표준화된 구조는 활동의 난이도를 일정하게 유지하는 동시에, 필터 조작과 단서 획득 과정을 명확히 대응시켜 학습자의 체험 효과를 극대화한다.

이 과정은 실제 탐지 환경의 사고 구조를 반영한다. 학습자는 제한된 정보로 추론을 수행해야 하고, 유사한 후보와의 혼동 속에서 정탐과 오탐을 구분해야 한다. 또한 정답 시도에는 리스크가 존재하기 때문에, 단서를 더 수집할지 혹은 결정을 내릴지를 전략적으로 판단해야 한다.

따라서 제안 메커니즘은 단순한 시각적 효과를 넘어, 협력적 탐색·정보 공유·전략적 의사결정을 포함하는 교육 활동으로 확장된다. 이는 실제 보안 분석가가 직면하는 탐색, 판단, 의사결정 과정을 모의적으로 경험하게 함으로써, 학습자가 보안 탐지 개념을 깊이 이해하도록 돕는다.

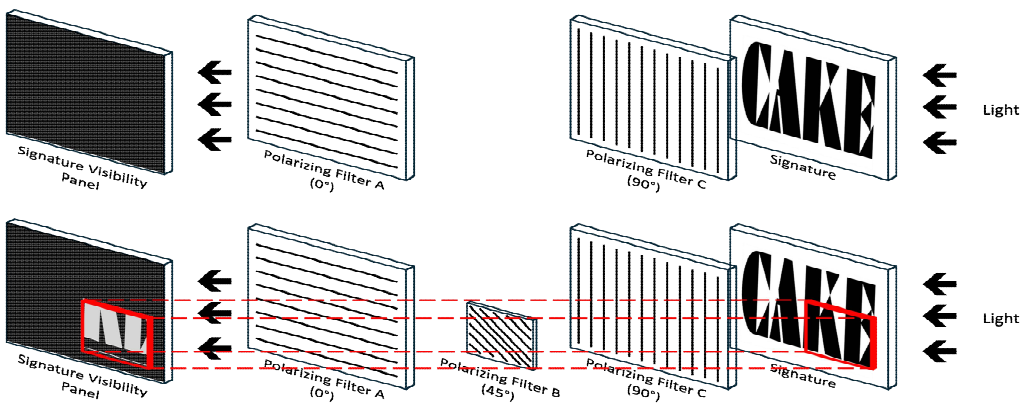


그림 2. 편광 필터 삽입 전후 시각적 변화

Fig. 2. Visual changes before and after inserting a polarizing filter

3.3 실습 활동 설계

제안된 실습 활동은 편광 필터를 활용하여 제한된 단서를 단계적으로 드러내고, 학습자가 이를 기반으로 악성코드 시그니처를 추론하도록 구성되었다. 활동은 팀 단위 협력 구조로 진행되며, 이는 실제 보안 탐지 과정에서 요구되는 협의와 판단을 교육적으로 모사하기 위함이다.

먼저 학습자들은 두 개의 팀을 구성한다. 사전에 협의한 방법에 따라 팀별 순서를 정한다. 이후 학습자에게 편광판에 의해 가려진 시그니처 A4 용지와 공개된 단어로 구성된 4개의 정답후보 시그니처를 제공한다. 단어는 시각적으로 왜곡되어 있으며, 유사한 패턴을 가진 오답이 포함되어 있어 단순 식별이 아니라 세밀한 추론이 필요하다.

게임의 진행은 각 팀이 차례대로 편광 필터를 격자의 원하는 위치에 삽입하는 방식으로 이루어진다. 삽입된 위치에서만 일부 단서가 드러나며, 학습자는 이를 바탕으로 팀 내에서 분석과 토의를 수행한다. 이때 단서는 한 번 확인된 이후 재사용할 수 없고, 정답을 선언할 수 있는 기회는 차례당 한 번으로 제한된다. 정답일 경우 3점을 획득하며 라운드는 즉시 종료되지만, 오답일 경우 1점이 차감되고 탐색은 계속 이어진다. 동일한 오답을 반복 제출할 수는 없으며, 모든 팀은 이러한 과정을 거쳐 점수를 누적하게 된다. 최종적으로는 3~5개 라운드의 점수를 합산해 우승 팀을 결정한다.

그림 3은 본 논문에서 제안하는 실습 활동의 전체 흐름을 시각적으로 나타낸 것이다. 이러한 구조는 실제 보안 탐지 과정의 본질을 교육적으로 반영한다. 일부 단서만을 근거로 판단해야 하는 제한적 상황, 유사 패턴 속에서 정답을 식별해야 하는 추론 과정, 그리고 오탐과 정탐의 결과가 가져오는 성과 차이를 학습자가 직접 경험할 수 있게 한다. 또한 단서가 편광 필터의 특정 방향에서만 드러나도록 설계되어, 물리적 조작과 정보 해석의 연계성을 강화하였다. 아울러 단서 정보는 격자 내에 무작위로 배치되어 있어 전략적 탐색과 협동적 의사결정이 요구된다. 결과적으로 본 활동은 학습자가 단순히 정답을 찾는 경험을 넘어, 정보보안 탐지에서 중요한 신중함, 정확성, 불확실성 관리를 체험할 수 있는 교육적 장치를 제공한다.

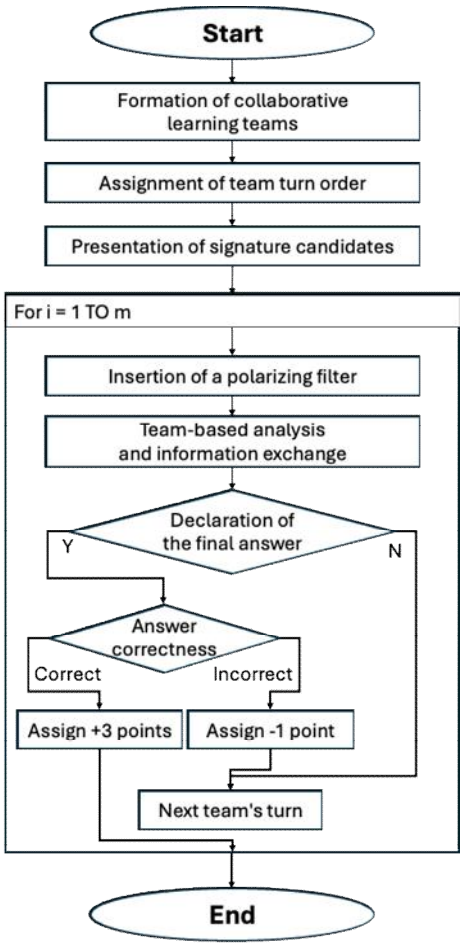


그림 3. 제안 방법론 순서도
Fig. 3. Proposed methodology flowchart

IV. 효과성 분석

4.1 정성적 효과성 분석

본 논문에서 제안한 편광 필터 기반 에듀테크 메커니즘은, 학습자가 제한된 단서를 수집하고 정답을 추론하는 과정에서 정탐, 오탐, 미탐과 같은 탐지 결과의 불확실성을 자연스럽게 체험할 수 있도록 설계되었다. 이는 단순한 이론적 설명을 넘어 탐지 원리와 한계를 구조적으로 이해하도록 돕는 장치이다.

이와 같은 체험 중심 학습 방식은 여러 연구에서 학습 효과와 학습자 참여도를 높이는 것으로 확인

되었다[22]. E. Ebrahimi et al.[23]에서는 초중등 학생을 대상으로 한 사이버보안 게임 및 플랫폼이 추상적 개념 이해와 몰입도 증진에 효과적이라는 사례가 다수 보고되었다. 또한 D. Ondrušková and R. Pospíšil[24]에서는 체코 초등학생을 대상으로 한 사이버보안 인식 교육 실험에서 교육 직후 이해도 향상과 위험 인식 개선 효과를 확인하였다. 더불어 M. Lamond et al.[25]에서는 스코틀랜드 초등교사 설문조사 결과, 교사의 ICT 역량과 교육 자료 제공 여부가 교육 효과에 직접적 영향을 미친다고 보고하였다.

따라서 본 메커니즘은 물리적 교구(편광 필터), 제한적 단서 노출, 팀 기반 상호작용을 결합함으로써 학습자의 몰입과 추론 과정을 강화하고, 교사의 자료 활용성을 높여 보안 개념 이해와 참여를 동시에 촉진할 수 있다는 점에서 교육적 효과성을 가진다.

4.2 기존 기법과의 비교

기존의 사이버보안 교육은 주로 시뮬레이션 소프트웨어나 디지털 자료를 활용하여 개념을 전달하는 방식이 중심이었다. 이러한 방식은 직관적 이해와 흥미 유발에는 효과적이지만, 학습자가 직접 조작하거나 물리적으로 개입하는 체험적 요소가 적고, 탐지 과정의 불확실성이나 판단 구조를 몸으로 느끼는 경험을 제공하기에는 한계가 있다[26][27].

반면 본 연구에서 제안하는 편광 기반 메커니즘은 물리적 교구를 활용하여 학습자가 필터를 직접 삽입하고 단서를 확보하는 참여적 활동을 포함함으로써 학습자의 몰입과 참여를 높인다. 탐지 과정에서 정탐, 오탐, 미탐의 구조적 불확실성을 체험하고, 팀 간 협력과 전략적 판단을 요구하는 구조는 기존의 관찰 중심 교육 방식과 뚜렷이 구별된다.

이러한 차별성은 최근 교육 연구에서도 유사하게 확인된다. W. Lazarov et al.[28]에서는, Cyber Range 플랫폼을 통해 가상 네트워크 환경에서 게임화된 학습이 학생들의 참여도와 이해도, 실습 효과를 유의미하게 향상시켰다고 보고하였다. 또한 J. Vykopal et al.[29]에서는 실습 중심 환경이 학습자에게 현실성 있는 탐구와 피드백 기회를 제공함으로써 이해도가 증가된 바 있다. 마지막으로 T. K. Damenu et al.[30]에서는 다수의 게임 기반 수업 사례에서 어린 학습자들이 보안 개념 인식과 동기 측면에서 긍정적인 결과를 확인하였다.

따라서 제안된 메커니즘은 기존 교육 기법이 가진 수동적·관찰 중심적 특성과 달리, 학습자가 탐지 원리와 한계를 체험적으로 습득하고, 전략적 의사결정 및 협력적 학습 과정을 경험할 수 있도록 한다는 점에서 교육적 차별성과 강점을 지닌다.

V. 결 론

본 논문에서는 새롭고 직관적인 편광 필터 기반 체험형 에듀테크 메커니즘을 통해 시그니처 기반 악성코드 탐지 과정을 교육적으로 효과적이고 시각적으로 구현하는 방법을 제안하였다. 제안된 접근 방식은 추상적 개념 설명에 의존하는 기존 보안 교육의 한계를 보완하고, 초등 학습자가 직접 조작과 추론을 통해 탐지 원리와 한계를 보다 체계적으로 이해할 수 있도록 설계하였다.

제안된 메커니즘은 정탐, 오탐, 미탐이라는 탐지 결과를 학습자가 게임적 규칙 속에서 체험하도록 하여, 정보보안의 본질적 불확실성을 인식하게 한다. 또한 물리적 교구와 팀 단위 활동을 결합함으로써 학습자의 참여와 몰입을 강화하고, 탐색·판단·의사결정이라는 보안 분석 사고 과정을 교육적으로 재현하였다. 이는 단순한 지식 전달을 넘어 정보보안 교육의 개념적 내재화와 협력적 학습 효과를 동시에 촉진하는 장점이 있다.

제안 방법론은 시그니처 기반의 악성코드 탐지 기법에 대해 초등 피교육자를 대상으로 수행할 수 있는 방법론이나, 이를 교육하는 교육자에게는 기술적인 이해가 요구된다. 따라서 향후 연구에서는 교육자가 제안 방법론의 기술적 배경과 탐지 원리를 보다 직관적으로 이해하고 수업에 적용할 수 있도록 지원하는 개념적 설명 도구나 교수 가이드라인의 개발이 요구된다.

References

[1] E. Choi and N. Park, "A Comprehensive Case Study of Security Education for Information Security Personnel", Korean Society for Internet Information, Vol. 26, No. 1, pp. 93-102, Feb. 2025. https://doi.org/10.7472/jksii.2025.26.1.93.

[2] S. Ryu, J. Kim, and N. Park, "Study on Trends and Predictions of Convergence in Cybersecurity Technology Using Machine Learning", Journal of Internet Technology, Vol. 24, No. 3, pp. 709-725, May 2023.

[3] D. V. Jesús, J. M. Calle, A. E. Alonso, R. E. Alonso, and G. Madinabeitia, "On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks", Applied Sciences, Vol. 12, No. 2, pp. 852, Jan. 2022. https://doi.org/10.3390/app12020852.

[4] J. Kim and N. Park, "Suggestions for a Blockchain-based Smart Factory Data Verification Mechanism to Enhance Cloud Data Reliability", Journal of Convergence Science, Technology, and Society, Vol. 2, No. 2, pp. 45-449, Dec. 2023. https://doi.org/10.56366/jcsts.2023.2.2.45.

[5] H. Holm, "Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?", 2014 47th Hawaii International Conference on System Sciences, IEEE, Waikoloa, HI, USA, Jan. 2014. https://doi.org/10.1109/HICSS.2014.600.

[6] Ministry of Education, "Exploring the 2022 Revised Elementary School Curriculum Organization and Operation", Ulsan Metropolitan Office of Education, 2024. https://use.go.kr/edu/user/bbs/BD_selectBbs.do?q_bbsSn=2318&q_bbsDocNo=20240605112518873.

[7] E. Choi, J. Kim, and N. Park, "An Analysis of the Demonstration of Five-Year-Long Creative ICT Education Based on a Hyper-Blended Practical Model in the Era of Intelligent Information Technologies", applied sciences, Vol. 13, No. 17, pp. 9718, Aug. 2023. https://doi.org/10.3390/app13179718.

[8] J. Kim, "A Study on Developing Digital Literacy Education Guidelines Linked to the Curriculum", Korea Education and Research Information Service (KERIS), 2023. https://www.keris.or.kr/main/ad/pblcte/selectPblcteRRInfo.do?mi=1138&pblcteSeq=13665.

[9] J. Kim, E. Choi, and N. Park, "A Proposal for a Mobility-Control Data Transfer Mechanism Based on a Block Network Utilizing End-to-End Authentication Data", Mathematics, Vol. 12, No. 13, pp. 2073, Jul. 2024. https://doi.org/10.3390/math121320730.

[10] C. Greco and M. Ianni, "A cross-architecture malware detection approach based on intermediate representation", Journal of Information Security and Applications, Vol. 93, pp. 104117, Sep. 2025. https://doi.org/10.1016/j.jisa.2025.104117.

[11] K. Scarfon and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology, Feb. 2007. https://doi.org/10.6028/NIST.SP.800-94.

[12] S. Das, S. Saha, A. T. Priyoti, E. K. Roy, F. T. Sheldon, and A. Haque, "Network Intrusion Detection and Comparative Analysis Using Ensemble Machine Learning and Feature Selection", IEEE Transactions on Network and Service Management, Vol. 19, No. 4, pp. 4821-4833, Dec. 2021. https://doi.org/10.1109/TNSM.2021.3138457.

[13] J. Kim, E. Choi, B. G. Kim, and N. Park, "Proposal of a Token-Based Node Selection Mechanism for Node Distribution of Mobility IoT Blockchain Nodes", Sensors, Vol. 23, No. 19, pp. 8259, Oct. 2023. https://doi.org/10.3390/s23198259.

[14] E. Choi, J. Kim, and N. Park, "A Case Study of SW · AI Education for Multicultural Students in Jeju, Korea: Changes in Perception of SW · AI", Applied sciences, Vol. 13, No. 17, pp. 9844, Aug. 2023. https://doi.org/10.3390/app13179844.

[15] P. R. Kothamali and S. Banik, "Limitations of Signature-Based Threat Detection", Revista de Inteligencia Artificial en Medicina, Vol. 13, No. 1, pp. 381-391, Mar. 2022.

[16] T. Sascha, "Polarization and polarimetry: a review", arXiv preprint arXiv:1401.1911, Jan. 2014. https://doi.org/10.48550/arXiv.1401.1911.

[17] J. Kim, Y. Jung, and N. Park, "A Proposal for Elementary Education Methods based on Color Phenomena for Understanding the Principles of Quantum Communication", The Journal of Korean Institute of Information Technology, Vol. 22, No. 12, pp. 191-200, Sep. 2024. https://doi.org/10.14801/jkiit.2024.22.12.191.

[18] R. C. Jones, "Transmittance of a Train of Three Polarizers", Journal of the Optical Society of America, Vol. 46, No. 7, pp. 528-533, 1956. https://doi.org/10.1364/JOSA.46.000528

[19] F. Logiurato, "Teaching Light Polarization by Putting Art and Physics Together", arXiv preprint arXiv:1803.09645, Mar. 2018. https://doi.org/10.48550/arXiv.1803.09645.

[20] G. Jin, M. Tu, T. H. Kim, J. Heffron, and J. White, "Evaluation of Game-Based Learning in Cybersecurity Education for High School Students", Journal of Education and Learning (EduLearn), Vol. 12, No. 1, pp. 150, Feb. 2018. https://doi.org/10.11591/edulearn.v12i1.7736.

[21] J. Vykopal, V. vábenský, and E. C. Chang, "Benefits and Pitfalls of Using Capture the Flag Games in University Courses", Proc. of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, pp. 752-758, Mar. 2020. https://doi.org/10.1145/3328778.3366893.

[22] N. Mike, "CyberMoraba: A game-based approach enhancing cybersecurity awareness", arXiv preprint arXiv:2403.10118, Mar. 2024. https://doi.org/10.48550/arXiv.2403.10118.

[23] E. Ebrahimi, M. Pare, G. Stoker, and S. White, "Cybersecurity Early Education: A Review of Current Cybersecurity Education for Young Children", Proc. of the 17th International Conference on Computer Supported Education, Porto, Portugal, Vol. 1, pp. 822-833, Apr. 2025. https://doi.org/10.5220/0013501000003932.

[24] D. Ondrušková and R. Pospíšil, "The good practices for implementation of cyber securityeducation for school children", Contemporary Educational Technology, Vol. 15, No. 3, Feb. 2023. https://doi.org/10.30935/cedtech/13253.

[25] M. Lamond, S. Prior, K. Renaud, and L. A. Wood, "Teachers' perspectives and practice of cybersecurity education in primary schools", Discover Education, Vol. 4, No. 312, Aug. 2025. https://doi.org/10.1007/s44217-025-00471-0.

[26] M. Y. Chu, Y. W. Park, S. H. Noh, S. J. Heo, and W. W. Huh, "Development of 1:1 customized Smartphone Education Application for the Elderly using Generative AI", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 24, No. 4, pp. 15-20, Aug. 2024. https://doi.org/10.7236/JIIBC.2024.24.4.15.

[27] Y. Zhen, K. M. Gwak, and Y. J. Rho, "A Study on Metaverse Framework Design for Education and Training of Hydrogen Fuel Cell Engineers", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 24, No. 1, pp. 207-212, Feb. 2024. https://doi.org/10.7236/JIIBC.2024.24.1.207.

[28] W. Lazarov, T. Schafeitel-Tähtinen, J. Squillace, Z. Martinasek, A. Coufalikova, M. Helenius, P. Gallus, and R. Fujdiak, "Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education", Technology, Knowledge and Learning, Apr. 2025. https://doi.org/10.1007/s10758-025-09840-y.

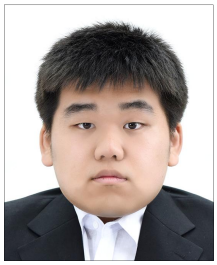
[29] J. Vykopal, P. Čeleda, P. Seda, V. Švábenský,

and D. Tovarňák, "Scalable Learning Environments for Teaching Cybersecurity Hands-on", 2021 IEEE Frontiers in Education Conference (FIE), Lincoln, NE, USA, Oct. 2021. https://doi.org/10.1109/FIE49875.2021.9637180.

[30] T. K. Damenu, İ. Z. Gökbay, A. Covaci, and S. Li, "Cyber Security Educational Games for Children: A Systematic Literature Review", arXiv preprint, arXiv:2508.17414, Aug. 2025. https://doi.org/10.48550/arXiv.2508.17414.

저자소개

김 진 수 (Jinsu Kim)



2024년 8월 : 제주대학교 융합정보보안학과(공학박사)
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : ETRI 정보보호연구단 선임연구원
2009년 1월 ~ 2010년 8월 : UCLA Post-Doc., ASU Research Scientist
2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수, 대학원 융합정보보안협동과정 교수
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드