ASK

ANNUAL SYMPOSIUM OF KIPS

2026 Program

5.20(수)~23(토)

라카이 샌드파인

주최 kips Korea Information Processing Society 한국정보처리학회

주관 kips Korea Information Processing Society 한국정보처리학회 · 서울대학교 공과대학 전기·정보공학부 · BK FOUR 21 정보기술 미래인재 교육연구단 Education and Research Program for Future ICT Pioneers

후원 KOFST 한국과학기술단체총연합회 · 2025-2026 강원 방문의 해 · GWTO 강원관광재단 Gangwon Tourism Organization · 강릉시 GANGNEUNG CITY · 강릉관광개발공사 Gangneung Tourism Dvlpmnt Corp. · 서울대학교 컴퓨터연구소 INSTITUTE OF COMPUTER TECHNOLOGY · CS Lab Cognitive Systems Lab @SNUHA 지능형 비즈니스 연구실

협찬 Libertron AI & FPGA 임베디드 시스템 설계 전문기업 (주)리버트론 www.libertron.com · COONTEC · kt · 대신정보통신(주) · DESILO · MarkAny · (주)범일정보 BUMIL INFORMATION · CQZ TECHNOLOGY · 아이티센 엔텍 · SK telecom · &company · TGV (주)티씨브이 · Selim 세림TSG · 디엑스 솔루션 · BonC Innovators · BIT 비트컴퓨터 · TRIZN · kpc 한국생산성본부 · BITPLANET · SFACSPACE · SysOne Since 1982 · GlobalTelecom · C2lab · 올포랜드 · UbiTec (주)유비텍 · LIG 시스템 · (주)그린텍아이엔씨 · NEOBRIX · NCT Network Core Technology · WIT (주)우리아이티 Leading company in IT convergence · JWATS AI Satellite Solution 진우에이티에스(주) · (주)태진티엔에스 · suwink · LG U+ · HUAWEI · GL associates · TTA 한국정보통신기술협회 Telecommunications Technology Association

무순

02. 고추 수확 로봇 개발을 위한 방법론 연구 및 실험적 검증 KIPS_C2026A0005
▶ 전하준*(국립경국대학교, 한국전자통신연구원), 황호석, 문애경(한국전자통신연구원)

03. AI 기반 금융감독의 규제체계와 법적 쟁점 연구 - 주요국 비교와 정책적 시사점 KIPS_C2026A0021
▶ 송창훈*, 도성룡(고려사이버대학교)

04. 급격한 노면 마찰 전환 환경에서의 ABS 성능 향상을 위한 거리 기반 NMPC 기법 KIPS_C2026A0049
▶ 정은제*, 김성재, 진예빈, 황성호(성균관대학교)

05. AP 기반 Zonal Architecture 시스템 구현 KIPS_C2026A0077
▶ 박지원*, 양지원, 이지현, 홍성찬, 이채은, 전재욱(성균관대학교)

S6. 멀티미디어처리

01. RoI 기반 장·단기 이중 MAC 연산을 이용한 임베디드 환경에서의 경량 움직임 감지 알고리즘 KIPS_C2026A0177
안재우*, 임승호(한국외국어대학교)

T1-7

5월 21일(목) 09:30~12:00, 5동 1층 호해2 좌장 : 고혜경 교수(청주대학교)

C6. 정보보안

01. OOXML 기반 악성 MS Word 문서 공격 방식의 진화 및 탐지에 대한 연구 KIPS_C2026A0217
천송현*, 최두섭, 임을규(한양대학교)

02. 결제 정책 및 네트워크 인프라 지표 결합을 통한 국가 우회 계정 탐지 기법 KIPS_C2026A0295
▶ 원도경*, 이지은, 신용태(숭실대학교)

03. CKKS 기반 암호화된 MLP에서 Packing전략과 Bootstrap 설정에 따른 성능 평가 KIPS_C2026A0378
▶ 김나은*, 오현영(가천대학교)

C7. 개인정보보호

01. 암호화된 LLM추론을 위한 효율적인 동형암호 기반 행렬 곱셈 기법에 대한 연구 KIPS_C2026A0139
주유연*, 최영한, 이동주, 백윤흥(서울대학교)

02. 동형암호를 활용한 유사도 기반 정보 검색 연구 동향 분석 KIPS_C2026A0173
최영한*, 주유연, 백윤흥(서울대학교)

03. Design and Implementation of a Blockchain Smart Contract-Based On-Device MyData Platform KIPS_C2026A0245
Jaeyoung Lee*(aSSIST University), Ahreum Hong(Kyung Hee University)

04. 사용성과 프라이버시를 고려한 차등 이미지 압축 기법 KIPS_C2026A0160
▶ 안예현*, 전아영, 이일구(성신여자대학교)

S1. 소프트웨어공학

01. ROS2 기반 실시간 시퀀스 공유를 통한 소형 이동체 군집 주행 기반 기술 구현 KIPS_C2026A0078
▶ 이하준*, 조용인, 이채민, 전희연, 박효진, 전재욱(성균관대학교)

02. 웹 애플리케이션의 자동 런타임 결함 탐지를 위한 강화학습 기반 지능형 에이전트 메커니즘 KIPS_C2026A0222
▶ 이하은*, 강소현, 김장환, 서채연, 김영철(홍익대학교)

03. 대형 언어 모델들(LLM)과 인간 코드의 품질 비교 분석 KIPS_C2026A0224
▶ 박성호*, 박성진, 김장환, 서채연, 김영철(홍익대학교)

T2-1

5월 21일(목) 13:00~15:00, 5동 1층 해운1 좌장 : 박기웅 교수(세종대학교)

C6. 정보보안

01. iOS AOP 펌웨어 런타임 패치 기법 연구 KIPS_C2026A0213
정승민*, 류재철(충남대학교)

02. 차원 추정과 차등 프라이버시를 활용한 IoT 데이터에서의 프라이버시 보존 기법 KIPS_C2026A0237
김재철*, 손윤식(동국대학교)

웹 애플리케이션의 자동 런타임 결함 탐지를 위한 강화학습 기반 지능형 에이전트 메커니즘

이하은[1], 강소현[2], 김장환[3], 서채연[4], 김영철[5*]
홍익대학교 소프트웨어융합학과 학부생[1,2]
홍익대학교 소프트웨어융합학과 교수[3,4,5*]
{haeum815[1], rkdthgus1019[2]}@gmail.com, {lentoconstante[3], chaeyun[4], bob[5*]}@hongik.ac.kr

Reinforcement Learning-based Intelligent Agent Mechanism for Automated Runtime Defect Detection in Web Applications

Ha Eun Lee[1], So Hyeon Kang[2], Janghwan Kim[3],
Chaeyun Seo[4], R. Young Chul Kim[5*]
Dept. of Department of Software and Communications Engineering[1,2,3,4,5*]

요 약

기존의 공개 홈페이지 취약점 및 오류 점검은 인력과 도구에 의존하여 막대한 시간과 비용이 소모된다. 특히 단일 페이지 애플리케이션 및 마이크로서비스 아키텍처의 확산으로 웹 환경이 복잡해지면서 기존 정적 테스트는 구조적 한계에 직면하였다. 우리는 이를 개선하고자 근접 정책 최적화(PPO) 알고리즘 기반의 멀티모달 자율 탐색 시스템을 제안한다.제안하는 방법은 문서 객체 모델(DOM) 정보, 서버 로그, 스크린샷 등 이종 데이터를 가중치 기반으로 통합하여 상태 인지 성능을 극대화하였다. 또한 음의 보상 전략을 적용해 기존 방식으로는 포착하기 어려운 비결정적 결함을 능동적으로 측정한다. 자체 실험을 통해 핵심 결함을 성공적으로 측정하며 실효성을 입증하였고, 향후 대형 언어 모델(LLM)을 연동하여 자동화된 지능형 품질 보증(QA) 체계로 확장할 계획이다.

1. 서론

최근 단일 페이지 애플리케이션 및 마이크로서비스 아키텍처의 확산은 웹 상태 공간을 확장하고 소프트웨어의 복잡도를 심화시켰다[1]. 현대 웹의 복잡한 UI와 동적 로직은 고정 경로만 검증하는 정적 테스트 방식에 구조적 한계를 유발하며, 잦은 스크립트 파손에 따른 유지보수 비용 증가 및 비결정적 결함 측정의 취약성으로 CI/CD 신뢰성을 저해한다[2][3][4].

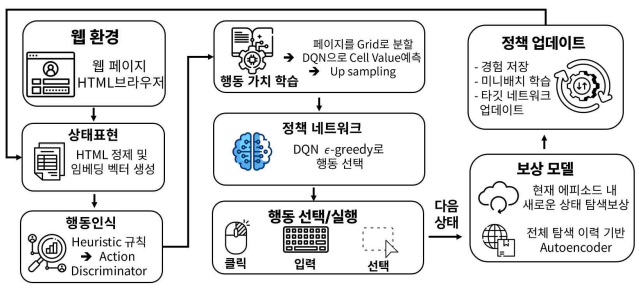
우리는 이를 개선하고자 강화학습(RL) 기반 자율 탐색 시스템을 제안한다. 제안하는 방법은 실행 중 예외 상황과 로그를 보상 신호로 활용하는 동적 학습으로 비정형 경로를 능동 추적한다[5]. 이를 통해 신뢰도를 높이고 결함 측정 자동화로 경제성을 확보하여 자율 품질 보증(QA) 패러다임으로의 전환을 도모한다[1][3].

특히 LLM을 활용한 지능형 테스트 생성 연구[6]를 참고하여, 탐색을 넘어선 자동화된 분석 체계의 기틀을 마련하고자 한다.

우리는 다음과 같이 논문의 체계를 구성하였다. 2장에서는 관련 연구로 WebRLED의 성과와 한계를 분석하고, 3장에서는 PPO 알고리즘 및 가중치 최적화 기반의 멀티모달 시스템 설계를 다룬다. 4장에서는 자체 테스트베드 적용 사례를 통해 결함 측정 성과를 확인하며, 5장에서는 전체 요약 및 향후 LLM 연동 계획을 기술한다.

2. 관련 연구

우리가 분석한 WebRLED는 딥 강화학습(DRL) 기반 웹 자율 탐색 도구다[5].



(그림 1) 딥 강화학습 기반 웹 GUI 자동 테스트 시스템의 전체 아키텍처 및 동작 흐름

그림 1처럼 HTML 임베딩으로 상태를 표현하며,

Heuristic 규칙과 (Multi-Layer Perceptron, MLP) 다층 퍼셉트론 기반 판별기로 행동을 인식한다[5]. 특히 액션 미정렬 문제를 개선하기 위해 페이지를 격자 단위로 분할 학습하며, Upsampling 기술로 행동 가치를 산출해 DQN epsilon-greedy 정책에 반영한다[5]. 보상은 Episodic과 Autoencoder 기반 Global Reward를 결합해 설계했다. 실험 결과 탐색 시간을 46% 단축하며 695개의 고유 결함을 측정했다[5]. 해당 연구는 콘솔 에러 측정을 통한 탐색의 유효성을 입증하였으나, 로직 모순 인지 및 원인 분석 역량 면에서는 추가적인 개선 가능성을 시사한다[5].

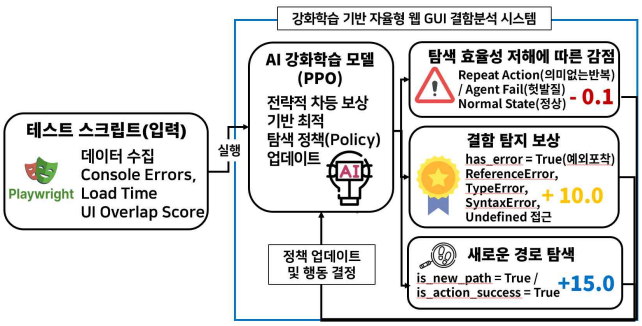
3. 강화학습 기반 자율형 에이전트 및 결함 분석 시스템 설계

3.1 시스템 개요 및 통합 아키텍처

우리는 관련 연구에서 소개한 연구인 WebRLED 메커니즘을 참고하고, 강화학습 알고리즘을 DQN에서 Proximal Policy Optimization(PPO) 알고리즘으로 변경한 PPO 기반 웹 애플리케이션 오류 탐색 중심의 자율 탐색 시스템을 제안한다. 제안하는 방법은 DOM 정보, 서버 로그, 스크린샷 등 서로 다른 성격의 데이터 소스를 통합하는 과정에서, 현재 탐색 맥락에 따라 유의미한 정보에만 선별적으로 집중하는 가중치 최적화 기법을 도입하여 웹 상태 인지 성능을 혁신적으로 개선하였다. 우리가 채택한 PPO는 클리핑 기법으로 정책 업데이트 폭을 제한하여 학습 안정성을 보장한다. 이는 가치 함수 발산이나 진동 위험이 있는 DQN 방식과 대조적으로, 정책을 직접 최적화하여 복잡한 웹 환경의 불안정성을 안정적으로 관리한다. 이러한 정책 변동 억제는 에이전트가 신뢰도 높은 탐색 경로를 일관되게 학습하여 최적 정책에 도달하게 하는 핵심 요소다.

(그림 2) 강화학습 기반 자율형 웹 어플리케이션 결함 분석 시스템 아키텍처

그림 2에서 제시된 바와 같이, 우리는 시스템 아키텍처의 학습단계에 집중하여 에이전트가 복잡한 동적 웹 환경에서 자율적으로 결함을 측정하고 경로를 최적화하는 메커니즘을 구축하였다. 특히 학습한 오류 패턴을 바탕으로 결함이 발생하기까지의 전 과정을 능동적으로 탐색하도록 설계하여, 결함의 인과관계를 명확히 규명하고 오류 파악의 용이성을 확보하였다. 이를 통해 에이전트는 고정된 시나리오에 의존하지 않고, 실제 실행 환경에서 발생하는 예외 상황을 기반으로 결함 가능성이 높은 비정형 경로를 능동적으로 추적하며 탐색 성능을 강화한다.



(그림 3) PPO 알고리즘 기반 최적 탐색 메커니즘

3.2 근접 정책 최적화 기반 자율 학습 및 차등적 보상 설계

우리는 에이전트의 학습 안정성과 정책 최적화를 위해 PPO를 핵심 엔진으로 활용한다.

그림 3은 에이전트와 AI 서버 간의 유기적 통신 및 전략적 차등 보상 산출 메커니즘을 보여준다.제안하는 방법은 멀티모달 데이터를 수집해 세 가지 분기로 보상을 산출한다.

첫째, 예외 결함을 측정했을 때 +10.0을 부여해 결함 유발 경로를 강화한다. 둘째, 새로운 경로 탐색 시 가장 높은 +15.0의 보상으로 능동적 탐색 확장을 유도한다. 반면, 무의미한 반복 행동이나 새로운 발견이 없는 정상 상태가 지속되면 탐색 효율성 저해로 간주하여 -0.1의 음의 보상을 부과한다. 이러한 차등 보상은 PPO 정책 업데이트에 실시간 반영되어, 에이전트가 결함 가능성이 높은 비정형 경로를 우선 추적하도록 탐색 지능을 개선한다.

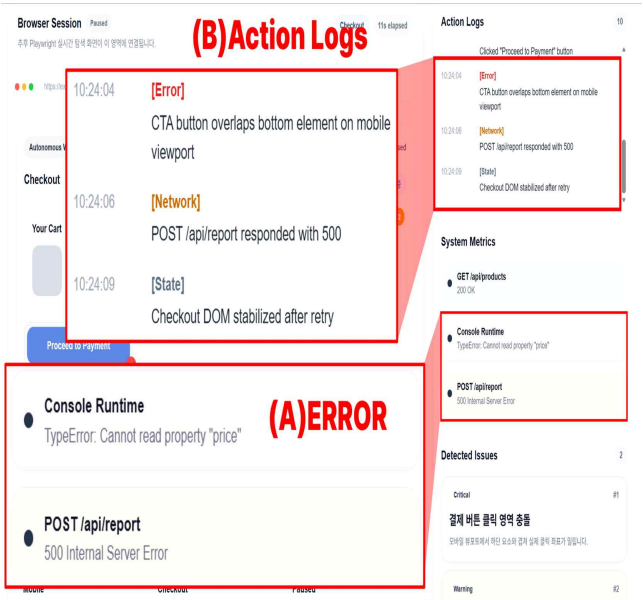
4. 적용 사례

우리는 시스템 실효성 검증을 위해 DOM 구조가 실시간 변이하는 현대적 웹 특성을 반영한 동적 퀴즈 앱 테스트베드를 구축하였다. 제안하는 방법은 학습 과정에 ReferenceError, TypeError 등 예외 상황과 Out-of-bounds 논리 결함을 주입하여 에이전트의 인지 능력을 평가한다. 특히 우리는 오류를 발견하지 못한 모든 정상 탐색 상태에 음의 보상을 부과하는 역발상적 전략을 통해 탐색 효율성을 극대화하였다. 이는 단순히 무의미한 중복 행동을 방지하는 차원을 넘어, 결함을 측정해내지 못한 탐색 실패

상황 자체에 패널티를 부여함으로써 에이전트가 결함 발견이라는 핵심 목적에만 압도적인 가중치를 두고 집중하게 설계한 것이다. 이러한 메커니즘은 에이전트가 특정 안전 경로에만 반복적으로 머무르는 조기 수렴 및 탐색 정체 현상을 원천적으로 극복하도록 탐색 지능을 개선하며, 반복 학습을 바탕으로 서비스 심층부의 엣지 케이스까지 자율적으로 도달함을 확인하였다.

4.1결함 측정 결과 및 학습 성과 분석

우리는 프로토타입 적용 결과 결함 유발 확률이 높은 행동 정책의 최적화를 확인하였다.



(그림 4) 테스트 베드 환경에서의 에이전트 자율탐색 및 실시간 런타임 오류 포착화면

그림 4의 (A) ERROR 영역을 통해 TypeError 등을 실시간 측정하고, (B) Action Logs의 5가지 이벤트를 시계열로 구조화하여 결함의 인과관계를 규명한다. 제안하는 방법은 Navigate(라우팅 및 상태 전이), Action(직접 조작), State(DOM 환경 변화), Error(UI 및 런타임 결함), Network(API 통신 오류)를 상세히 기록하여 상태 전이 지점을 정밀하게 역추적하는 분석 도구로 활용된다. 우리는 음의 보상 전략으로 탐색 정체를 회피하며 서비스 심층부의 엣지 케이스까지 자율적으로 도달하였다. 또한 측정된 정보를 템플릿에 자동 기록하여 관리 효율을 개선하였으며, 결론적으로 제안하는 방법은 복잡한 웹 환경 내 핵심 결함 식별 성능을 입증하였다.

5. 결론

우리는 RL의 탐색 지능과 LLM의 추론 능력을 결합해 복잡한 웹 환경에서 자율적으로 결함을 측정 및 분석하는 통합 시스템을 제안한다. 동적 테스트 베드 실험을 통해 ReferenceError, TypeError, SyntaxError 등 핵심 결함들을 성공적으로 식별하였다. 특히 결함 발견 시 고보상을 부여하고 중복 행동에 음의 보상을 적용하는 전략을 통해, 에이전트가 탐색 정체 문제를 극복하고 서비스 심층부의 엣지 케이스까지 도달함을 확인하였다.현재 시스템은 스크립트 생성 시 수동 작업이 수반되는 한계가 있으나, 우리는 이를 개선하기 위해 향후 LLM 기반의 자동 생성 체계를 구축할 계획이다. 제안하는 방법은 측정된 오류 데이터를 바탕으로 지능형 보고서를 자동 작성하는 기능을 통합하여 인적 개입을 최소화한 완전 자율형 QA 시스템을 지향한다. 나아가 음의 보상으로 정교화된 탐색 지능을 결합해 결함 탐지부터 보고까지의 전 과정을 지능화할 것이다.

Acknowledgment

본 연구는 홍익대학교 소프트웨어융합학과 학부생들의 종합설계 프로젝트 결과물이며, 홍익대학교 메타버스 융합SW아카데미(과제번호: 202301830004) 6기 교육생들의 프로젝트 결과물이다.

참 고 문 헌

[1] H. Jin, Y. Zhang, and L. Cheng, "From LLMs to LLM-based Agents for Software Engineering: A Survey," arXiv preprint arXiv:2408.02479, 2024.

[2] S. R. Doe and M. J. Lee, "Technical Debt and DevOps: Strategies for Managing Legacy Systems in a CI/CD World," Journal of Software Engineering Research, vol. 14, no. 2, pp. 112-128, 2025.

[3] A. H. Mughal, "An Autonomous RL Agent Methodology for Dynamic Web UI Testing in a BDD Framework," arXiv preprint arXiv:2503.08464, 2025.

[4] R. Almaghairbe and M. Roper, "An Empirical Study of Web Flaky Tests: Understanding and Unveiling DOM Event Interaction Challenges," in Proc. IEEE International Conference on Software Testing, Verification and Validation (ICST), 2025.

[5] Z. Gu, Y. Fan, and X. Tan, "Deep Reinforcement Learning for Automated Web GUI Testing," arXiv preprint arXiv:2504.19237, 2025.

[6] N. K. Le, T. H. Nguyen, and K. M. Lee, "Automated Web Application Testing: End-to-End Test Case Generation with LLMs and STG," arXiv preprint arXiv:2506.02529, 2026.