DID 식별자 검증의 구현 간 불일치 분석과 오류 분류 전처리 모듈에 관한 연구

김건민, 최민준, 정세연, 김경백
전남대학교 인공지능융합학과
E-mail: geonminkim@jnu.ac.kr, larrychoi@jnu.ac.kr,
320eyeon@naver.com, kyungbaekkim@jnu.ac.kr

요 약

분산식별자(DID)가 인증 서비스에 확산되면서 서비스 앞단의 입력 DID 검증이 중요해지고 있으나, 서로 다른 DID 처리 구현이 동일 비정상 입력을 일관되게 거부하는지는 충분히 검증되지 않았다. 본 논문은 차등 분석 방법론을 W3C DID Core의 기본 DID 식별자 검증에 적용하여, 실제 DID 처리 구현 2종을 166,000개 입력으로 측정하였다. 그 결과 구현 간 수용 결정 불일치가 관찰되었으며, 일부 입력은 검증 게이트 우회, DID URL 성분 혼입, 잘못된 퍼센트 인코딩 수용 등 보안 결정 불일치로 이어질 수 있음을 확인하였다. 이를 완화하기 위해 ABNF 기반 검증, 7종 오류 분류, 고정 우선순위, 길이 제한을 갖는 경량 전처리 모듈을 제안한다. 제안 모듈은 기본 DID 구문 기준 FAR/FRR 0을 달성하여 단일 입력 검증 게이트로 활용 가능함을 보인다.

Ⅰ. 서 론

분산식별자(DID)는 중앙 등록기관 없이 검증 가능한 식별자를 제공하는 W3C 표준으로[1], 신원·인증 서비스에 빠르게 도입되고 있다. 그러나 서비스 앞단에서 잘못된 prefix, 식별자 누락, 비허용 문자 등을 걸러내지 못하면 오류가 하위 단계로 전파되거나 컴포넌트별 오류 응답이 달라질 수 있다. 또한 SSL/TLS 인증서 검증[2], HTTP 구현[3]등에서 보고된 바와 같이, 서로 다른 구현이 동일 입력을 다르게 해석하면 상호운용성 및 보안 문제가 발생할 수 있다. 본 논문은 DID 식별자 검증에 차등 분석을 적용하여, 라이브러리 간 불일치를 166,000개 입력으로 정량화하고, 보안 결정 불일치 가능성을 실증하며, ABNF 기반 오류 분류 전처리 모듈을 제안한다.

Ⅱ. 선행 연구

SSL/TLS 인증서 검증[2]과 HTTP 구현[3]연구는 동일 입력에 대한 구현 간 해석 차이가 상호운용성 문제와 보안 취약점으로 이어질 수 있음을 보였다. 반면 기존 DID/VC 연구[4]는 해석 절차, method 분류, 자격증명·키 관리에 집중하며, 비정상 DID 입력의 구현 간 검증 일관성은 충분히 다루지 않았다.

Ⅲ. DID 검증 게이트와 오류 분류 체계

본 논문은 DID URL이 아닌 기본 DID 식별자 구문 검증만을 대상으로 한다. 따라서 /, ?, # 등을 포함한 입력의 거부는 DID URL 전체의 유효성 판단이 아니라, 서비스 앞단에서 기본 DID만 허용하는 입력 정책으로 해석한다. 제안 모듈은 기본 DID ABNF[1]와 운영용 길이 정책을 적용하고, 비적합 입력을 INVALID_PREFIX, INVALID_METHOD, EMPTY_IDENTIFIER, INVALID_PCT_ENCODING, INVALID_IDCHAR, MALFORMED_STRUCTURE, LENGTH_EXCEEDED의 7종으로 분류한다. 검사는 길이→구조→prefix→method→식별자→percent-encoding→idchar의 고정 우선순위로 동일 입력에 항상 동일 오류 코드를 반환한다.

Ⅳ. DID 처리 구현 간 수용 결정 불일치 평가

1. 데이터셋 및 비교 대상

데이터셋은 정상 DID, 오류 주입 변형, 퍼징 입력, 경

표 1. 데이터셋 구성

세트	내용	규모(건)
D0	정상 DID	10,000
D1	변형 DID(오류 7종)	35,000
D2	퍼징/공격성 문자열	100,000
D3	경계값	1,000
D4	적대적/실세계	20,000

표 2. 기본 DID 입력 대비 구현 결과(이진 판정)

구현	정확도	FAR(기본 DID 정책 위반 수용)	비고
pydid 0.4.3	0.901	0.153	-
did-resolver 0.0.3	0.950	0.077	-
제안 모듈 (ABNF-only)	1.000	0.000	구문 적합성만 평가
제안 모듈 (ABNF+운영 정책)	**0.922**	0.000	길이 초과 입력 거부

표 3. 게이트-소비자 간 결정 불일치 유형

desync 유형	pydid	did-resolver
퍼센트 인코딩 오류 수용	5955	162
길이 미제한	5176	5176
제어문자(CRLF/log)	577	579
DID URL 파라미터 혼입	0	2431
기타 특수 문자	0	115
계	11,708	8,463

계값, 적대적/실세계 입력으로 총 166,000건이며, 구성은 표 1과 같다. 오류 분류 정확도는 결함 유형을 통제 주입한 D1 기준으로 평가하며, 비교 대상은 pydid 0.4.3과 did-resolver 0.0.3이다.

2. 구현 간 불일치

표 2는 기본 DID ABNF 오라클을 기준으로 각 구현의 수용/거부 결정을 비교한 결과이다. 세 판정자 간 Fleiss κ는 0.86이었고, pydid와 did-resolver의 쌍별 일치율은 0.948로 완전 일치하지 않았다. pydid는 잘못된 퍼센트 인코딩 입력을 수용하는 사례가 있었으며, did-resolver는 기본 DID 뒤의 DID URL 성분(/, ?, #)을 path·query·fragment로 분해하는 사례가 관찰되었다. 제안 모듈은 기본 DID 구문 기준 정확도 1.000, FAR/FRR 0을 달성하였고, 운영 정책 포함 모드의 정확도 0.922는 길이 초과 입력 5,176건을 정책적으로 거부한 결과이다. 이 입력이 게이트 거부·소비자 수용으로 이어진 보안 결정 불일치는 표 3에서 별도로 집계한다.

3. 보안 결정 불일치 유형 분석

전체 166,000개 입력 중 제안 모듈이 거부했으나 하나 이상의 소비자 구현이 수용한 입력은 14,418건(8.69%)이며, 유형별로는 표 3과 같이 pydid 11,708건, did-resolver 8,463건이었다. 예를 들어 잘못된 percent-encoding, 제어문자 포함 입력, DID URL 성분이 포함된 입력은 구현 조합에 따라 디코딩 혼동, 로그 오염, 파라미터 혼입 등으로 이어질 수 있다.

V. 결론 및 향후 연구

본 논문은 기본 DID 식별자 검증에 차등 분석을 적용하여, 실제 DID 처리 구현들이 동일 비정상 입력에 대해 서로 다른 수용 결정을 내리고 이로 인해 보안 결정 불일치가 발생할 수 있음을 확인하였다. 또한 ABNF 기반 검증, 7종 오류 분류 등을 갖는 경량 전처리 모듈을 제안하고 성능을 평가하였다. 향후 비교 구현을 확대하고 다양한 DID 처리 환경의 적용 가능성을 평가할 예정이다.

감사의 글

본 연구성과는 2025년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(RS-2025-25398164)(33%)이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임(IITP-2026-RS-2022-00156287)(34%)본 연구는 한국인터넷진흥원(KISA)-정보보안 특성화대학 지원사업의 지원을 받아 수행된 연구임.(33%)

References

[1] World Wide Web Consortium (W3C), "Decentralized identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022. [Online]. Available: https://www.w3.org/TR/did-core/

[2] C. Brubaker, S. Jana, B. Ray, S. Khurshid, and V. Shmatikov, "Using frankencerts for automated adversarial testing of certificate validation in SSL/TLS implementations," in Proc. *IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2014, pp. 114–129, doi: 10.1109/SP.2014.15.

[3] K. Shen, J. Lu, Y. Yang, J. Chen, M. Zhang, H. Duan, J. Zhang, and X. Zheng, "HDiff: A semi-automatic framework for discovering semantic gap attack in HTTP implementations," in Proc. *52nd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Baltimore, MD, USA, Jun. 2022, pp. 1–13, doi: 10.1109/DSN53405.2022.00014.

[4] C. Mazzocca, A. Acar, A. S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A survey on decentralized identifiers and verifiable credentials," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 6, pp. 3641–3671, 2025, doi: 10.1109/COMST.2025.3543197.