Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

AI-Driven Security Threat Detection in Tokenized Real-World Assets: A Systematic Literature Review

Abisena Rais*✉, Aqsyal Hilmi Fadilla✉, Sarah Fajriah Rahmah✉
Faculty of Science and Technology, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Indonesia

Abstract: The tokenization of real-world assets (RWAs) introduces security challenges that extend beyond smart-contract vulnerabilities to include transaction manipulation, oracle-related risks, financial fraud, asset valuation, and regulatory governance. This study aims to systematically review security threats associated with tokenized RWAs, examine artificial intelligence (AI) and machine learning (ML) approaches proposed or applied to detect related threats, and identify research gaps that limit their application in RWA ecosystems. A systematic literature review was conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) as a reporting guide. Searches in Scopus and Google Scholar, with Publish or Perish used to retrieve Google Scholar records and publication years limited to 2021 through 2026, identified 1,322 records. Following duplicate removal, screening, full-text eligibility assessment, and quality assessment, 16 studies were retained for qualitative and descriptive synthesis. The findings were organized into four domains: RWA tokenization and market design (six studies; 37.50%), smart-contract vulnerability detection (six studies; 37.50%), smart-contract, decentralized finance, and oracle security (two studies; 12.50%), and blockchain anomaly and fraud detection (two studies; 12.50%). The reviewed literature indicates that ML-based vulnerability classification, large language model-assisted code analysis, explainable AI, transaction anomaly detection, and privacy-preserving learning may support complementary security functions. However, the evidence remains fragmented, and the review does not establish a single integrated detection system validated across RWA ecosystems. Future research should empirically evaluate layered approaches combining smart-contract analysis, transaction monitoring, external-data verification, and governance-led incident response.
Keywords: Real-world assets; Tokenization; Cybersecurity; Artificial intelligence; Systematic literature review;

1. INTRODUCTION

Tokenization of real-world assets (RWAs) enables asset-related rights, such as real-estate ownership and financial interests, to be represented and transferred through blockchain-based tokens. Although tokenization can improve transaction efficiency, traceability, and investment accessibility, its reliability depends on secure technology, accurate asset information, and effective governance. Research on regulated real-estate tokenization highlights the importance of security monitoring, privacy, interoperability, and institutional accountability.

Tokenized RWA ecosystems face security risks involving smart-contract vulnerabilities, suspicious transactions, unreliable external data, and inconsistencies between blockchain records and legal ownership. These risks can interact: even correctly executed smart

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

contracts may produce harmful outcomes when external information is inaccurate or governance responsibilities are unclear. Digital-asset research identifies cybersecurity, fraud, market manipulation, and regulatory uncertainty as interconnected challenges [1].

Previous studies have examined machine-learning-based smart-contract vulnerability detection, security design patterns, code representations, and AI-assisted detection methods [2], [3], [4], [5]. Research evaluating open-source detection tools also identifies differences in vulnerability coverage, usability, and maintenance [6]. These studies provide useful foundations for developing AI-driven security approaches, although their findings largely concern blockchain systems more broadly.

Existing reviews concentrate on one layer of the problem. Reviews of machine-learning-based vulnerability detection compare models, code representations, and datasets for smart contracts [2], [4], [5]. A review of security design patterns addresses how contracts should be written [3], and an evaluation of open-source tools compares their vulnerability coverage and usability [6]. None of these reviews takes tokenized RWAs as its object of analysis, and none considers how off-chain asset information, legal ownership, and regulatory requirements change what a detection system has to observe. Studies of tokenization, in turn, discuss valuation, market design, and regulation with limited attention to AI-based detection.

This study uses a systematic literature review guided by PRISMA to examine security threats affecting tokenized RWAs and the AI- and machine-learning-based approaches that could detect them. Its novelty lies in three points. First, it reads the tokenization literature and the blockchain-security literature together, so that code-level, transaction-level, external-data, and governance risks are mapped in one threat model for RWAs. Second, it labels each finding according to whether it comes from a study of tokenized assets or is transferred from general blockchain and DeFi research, which prevents general results from being presented as RWA evidence. Third, it compares AI techniques by the threat layer they can observe and derives a conceptual framework that links asset verification, smart-contract analysis, AI-driven detection, transaction monitoring, and governance-led incident response.

This study addresses three research questions: (1) What security threats and vulnerabilities affect tokenized RWAs? (2) Which AI and machine-learning techniques have been applied or proposed to detect these threats? (3) What research gaps remain? The study contributes a thematic synthesis of threats and detection methods, an assessment of their reported limitations, and directions for future research on integrated security detection for tokenized RWA ecosystems.

2. RESEARCH METHODOLOGY

This study adopted a systematic literature review approach and used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) as a guide for reporting the study-selection process. The methodology consisted of four stages: formulating the research questions, searching the literature, screening and assessing the eligibility of records, and extracting and synthesizing data from the selected studies. These stages were applied consistently so that the search scope, selection decisions, and final evidence base could be traced and reported transparently.

2.1 Research Questions (RQ)

Three research questions (RQs) were formulated to guide the review and define the information to be collected from the literature. The questions cover security threats associated with tokenized real-world assets (RWAs), the use of artificial intelligence (AI) and machine learning (ML) for security detection, and the remaining research gaps. The

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : https://doi.org/10.58602/itsecs.v5i1.478
Page 94-111

questions are listed in Table 1 and were used to guide the search, screening, and synthesis stages.

Table 1. Research Questions

ID	Questions
RQ1	What security threats and vulnerabilities related to tokenized real-world assets have been addressed in the existing literature?
RQ2	What artificial intelligence and machine learning techniques have been applied or proposed for detecting these security threats and vulnerabilities?
RQ3	What research gaps and challenges remain in applying AI-driven security threat detection to tokenized real-world asset ecosystems?

2.2 Search Strategy and Data Sources

The literature search was conducted in Scopus and Google Scholar. Scopus was searched directly, and Google Scholar records were retrieved with the Publish or Perish software because Google Scholar does not offer a bulk export of search results. Two search strings were used, and they are listed in Table 2. The first string targets literature that directly addresses real-world asset tokenization and security. The second targets related work on blockchain security, smart-contract vulnerabilities, fraud, and AI or ML techniques. Each string was run separately in each source, and the publication year was limited to 2021 through 2026 in both sources. The records returned by each source were recorded and counted before duplicate removal. The searches were run between 26 October 2026 and 2 November 2026. Table 2 presents the search strings and the number of records retrieved from each database.

Table 2. Literature Search Results

Keywords	Scopus	Google Scholar	Total
"Real-world asset" AND tokenization AND security	18	530	548
Blockchain AND ("smart contract" OR vulnerability OR fraud) AND ("machine learning" OR AI)	53	721	774
Total	71	1,251	1,322

The searches returned 1,322 records in total: 71 from Scopus and 1,251 from Google Scholar. These figures represent the initial retrieval stage, before duplicate records and records outside the review scope were removed. The retrieved records were then consolidated and screened using the criteria described below.

2.3 Inclusion/Exclusion Criteria and Quality Assessment (QA)

The inclusion and exclusion criteria were applied to assess each record against the review scope. Studies were considered for inclusion when they were published between 2021 and 2026, were written in English, had accessible full text, and addressed security risks relevant to tokenized RWAs or related blockchain systems. Eligible publication types included primary research and scholarly review papers. Records were excluded when they did not meet the language, accessibility, publication-type, or topical requirements. The criteria are summarized in Table 3.

Table 3. Exclusion and Inclusion Criteria

Exclusion	Inclusion
Published before 2021 or after 2026	Published between 2021 and 2026
Written in languages other than English	Written in English
Full text unavailable for assessment	Full text accessible for assessment

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

Studies unrelated to tokenized RWA security or relevant blockchain security	Studies addressing RWA tokenization, blockchain security, smart contract vulnerabilities, fraud, or related security risks
Studies without sufficient relevance to the research questions	Primary studies and scholarly reviews relevant to the research questions

After eligibility screening, the remaining full-text articles were assessed using the three quality-assessment (QA) questions listed in Table 4. The assessment checked whether each publication was a peer-reviewed journal article or conference proceeding, whether it addressed security threats, vulnerabilities, or risks relevant to tokenized RWAs or related blockchain systems, and whether it presented a clear method, conceptual analysis, or verifiable findings relevant to the research questions. An article was retained only when it satisfied all three questions. Because of the number of records, the 110 full-text articles were divided among the three authors. Each author applied the three questions to the articles assigned to them, and the exclusions were then pooled and counted by criterion. No article was assessed independently by a second author, and inter-rater agreement was not calculated. The assessment supported consistent selection of studies with sufficient relevance and evidential clarity.

Table 4. Quality Assessment

ID	Descriptions
QA1	Is the article published in a peer-reviewed academic journal or conference proceeding?
QA2	Does the study explicitly address security threats, vulnerabilities, or risks relevant to tokenized RWA or related blockchain systems?
QA3	Does the research present a clear methodological framework, conceptual analysis, or verifiable findings relevant to the research questions?

The study-selection process began with 1,322 records. After 55 duplicate records were removed, 1,267 unique records remained for initial screening. Title and abstract screening excluded 1,145 records that did not meet the criteria in Table 3, leaving 122 reports sought for retrieval. The full text could not be obtained for 12 of these reports; therefore, 110 articles were assessed in full against the quality-assessment questions in Table 4. This stage excluded 94 articles under the three criteria. Twenty articles were excluded under QA1 because they were not published in a peer-reviewed journal or conference proceeding. Fifty-two articles were excluded under QA2 because they did not explicitly address security threats, vulnerabilities, or risks relevant to tokenized RWAs or related blockchain systems. Twenty-two articles were excluded under QA3 because they did not present a clear method, conceptual analysis, or verifiable findings relevant to the research questions. The remaining 16 studies were retained for the final synthesis. Figure 1 presents this flow of records through the review stages.

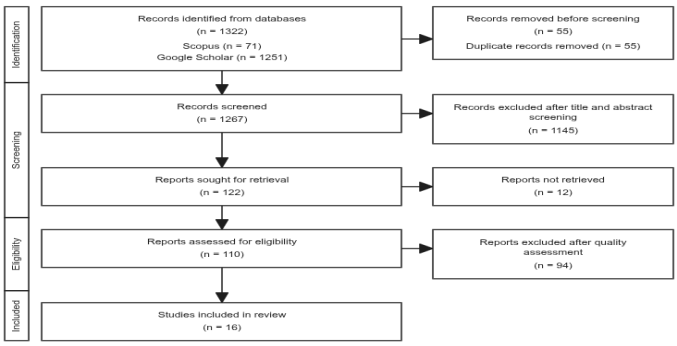


Figure 1. PRISMA Flow.

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : https://doi.org/10.58602/itsecs.v5i1.478
Page 94-111

2.4 Data Extraction and Synthesis

Following the selection process summarized above, the 16 retained studies formed the evidence base for data extraction and synthesis. Each study was examined in relation to the three research questions, with attention to the context of the security problem, the detection approach discussed, and the findings or limitations reported by the authors.

The 16 selected articles were organized into four thematic domains: (1) RWA tokenization and market design; (2) smart-contract vulnerability detection; (3) smart-contract, decentralized finance (DeFi), and oracle security; and (4) blockchain anomaly and fraud detection. Each study was assigned to one domain according to its principal contribution. Each study was also labelled as RWA-specific evidence when tokenized assets were its object of analysis, or as general blockchain evidence when it examined smart contracts, DeFi protocols, or blockchain transactions without an RWA setting. This thematic grouping allowed the review to distinguish findings directly concerning RWA tokenization from related blockchain-security research that may inform detection approaches in tokenized-asset ecosystems. The grouping also provided a consistent basis for comparing the threats studied, the techniques proposed or evaluated, and the limitations identified across the literature.

For each study, the review recorded bibliographic information, DOI when available, research domain, security threat or vulnerability addressed, AI or ML technique, research method, principal findings, and stated limitations. The extracted information was synthesized qualitatively and descriptively rather than pooled statistically. The synthesis compared which threats were addressed, how AI or ML was used or proposed for detection, and which methodological or application gaps remain for tokenized RWA environments. Where a study focused on blockchain security more broadly rather than tokenized RWAs specifically, its relevance was considered in relation to the research questions rather than treated as direct evidence about every RWA use case.

3. RESULT AND DISCUSSIONS

The synthesis of the 16 selected studies identified four connected domains: RWA tokenization and market design; smart-contract vulnerability detection; smart-contract, decentralized finance (DeFi), and oracle security; and blockchain anomaly and fraud detection. The findings were analyzed qualitatively and descriptively and organized around the three research questions. Because the studies use different methods and datasets, the results are synthesized thematically rather than pooled statistically.

3.1. Characteristics and Thematic Clustering of the Selected Literature

The 16 selected studies cover an interdisciplinary research area involving real-world asset (RWA) tokenization, blockchain security, smart-contract vulnerability detection, transaction anomaly detection, and regulatory governance. The literature indicates that security in tokenized-asset ecosystems cannot be addressed exclusively through smart-contract auditing. Although contract-code vulnerabilities and transaction-protocol attacks remain important [7], [8], RWA applications also depend on reliable external information, asset valuation, institutional accountability, and regulatory compliance [7], [9], [10]. The selected studies were therefore characterized by publication year and principal research domain, while author-affiliation countries were considered for the geographical overview.

Table 5. Publication-Year Distribution of the Selected Studies

Publication year	Number of studies	Percentage
2021	1	6.25%

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : https://doi.org/10.58602/itsecs.v5i1.478
Page 94-111

2022	0	0.00%
2023	3	18.75%
2024	4	25.00%
2025	4	25.00%
2026	4	25.00%
Total	16	100.00%

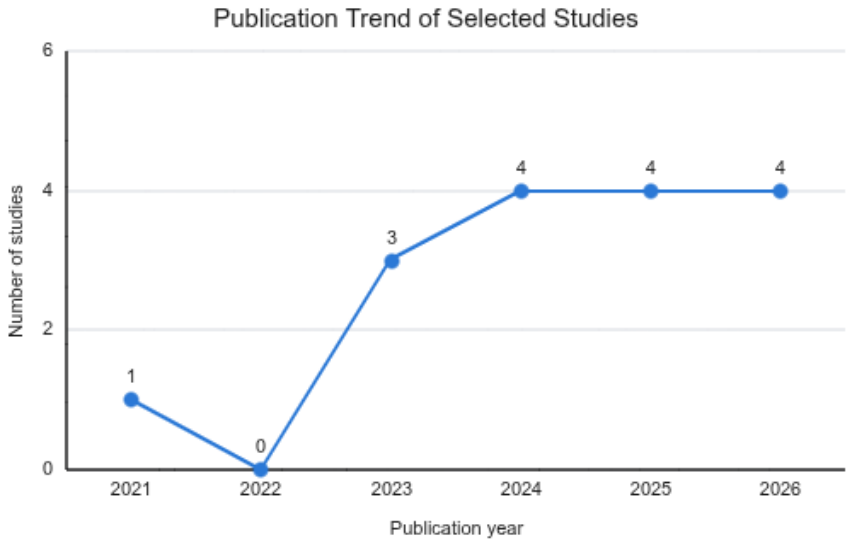


Figure 2. Publication Trend of the Selected Studies by Year.

The selected studies were published between 2021 and 2026 (Table 5 and Figure 2). One study dates from 2021, none from 2022, and three from 2023. The years 2024, 2025, and 2026 contribute four studies each, so 12 of the 16 studies (75.00%) were published in the last three years of the search period. Examples include LLM-assisted program analysis published in 2024 [11], a 2023 review of token creation and valuation [12], and 2025 studies of real-estate tokenization and blockchain anomaly detection [13], [14]. Studies dated 2026 address explainable machine-learning-based vulnerability detection, vulnerability benchmarks, and regulated real-estate tokenization [15], [16], [17]. This distribution describes only the selected evidence base and should not be interpreted as a complete bibliometric measure of the field's annual output.

Table 6. Thematic Classification of the Selected Literature

Research domain	Main scope	Representative studies
RWA tokenization and market design (n=6; 37.50%)	Asset tokenization, token valuation, real-estate investment, and regulatory arrangements	[9], [10], [12], [13], [17], [18]
Smart-contract, DeFi, and oracle security (n=2; 12.50%)	Oracle-related risks, DeFi attack mechanisms, and root causes of protocol-level losses	[7], [19]
Smart-contract vulnerability detection (n=6; 37.50%)	Vulnerability taxonomies, program analysis, AI-assisted code analysis, and vulnerability assessment	[8], [11], [15], [16], [20], [21]

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

Blockchain anomaly and fraud detection (n=2; 12.50%)	Blockchain anomaly detection, financial fraud, and broader security-oriented machine-learning approaches	[14], [22]

The thematic classification in Table 6 and Figure 3 shows that RWA tokenization and market design and smart-contract vulnerability detection each account for six studies (37.50% each). The first domain examines the economic, operational, and institutional conditions under which assets are represented digitally, whereas the second focuses on identifying weaknesses in the code governing blockchain transactions [8], [9], [12], [20]. These domains are complementary: secure tokenization requires both a reliable asset representation and sound technical implementation.

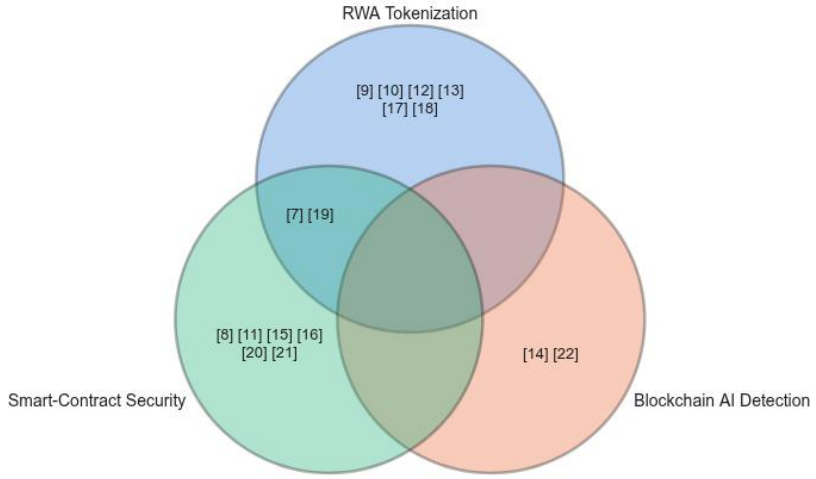


Figure 3. Distribution of the Selected Literature by Research Domain. Studies [7] and [19] form the smart-contract, DeFi, and oracle-security domain and are drawn at the intersection of RWA tokenization and smart-contract security.

The smart-contract, DeFi, and oracle-security domain comprises two studies (12.50%). These works highlight risks arising from interactions among contracts, transaction mechanisms, and external data sources. Oracle-related risks are particularly relevant to RWAs because a blockchain cannot independently guarantee the accuracy of off-chain information such as asset valuations or ownership records [7]. Research on DeFi attacks also demonstrates that vulnerabilities may emerge from interactions between contracts rather than from isolated programming defects [19]. Accordingly, code-level analysis alone may not identify every risk in a tokenized-asset ecosystem.

The blockchain anomaly and fraud-detection domain also comprises two studies (12.50%). Unlike code-level vulnerability analysis, this research focuses on suspicious behavior and unusual transaction or financial-activity patterns [14], [22]. Such monitoring may complement code analysis because an application can experience suspicious activity even when no immediately identifiable software defect has been established. The usefulness of integrating these approaches for RWA settings, however, requires empirical validation.

The geographical distribution (Figure 4) was derived from the institutional affiliations of all authors of the 16 studies. A study was counted once for every region in which at least one of its authors is affiliated, so the regional counts sum to more than 16. Europe is represented in 11 studies, with affiliations in Italy [7], [16], [21], Malta [7], Portugal [8],

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : https://doi.org/10.58602/itsecs.v5i1.478
Page 94-111

the United Kingdom [9], [13], [14], [18], [19], Latvia [10], Romania [12], Lithuania [13], Poland and Ukraine [14], and Germany and Switzerland [19]. Asia is represented in seven studies, with affiliations in Vietnam [9], Singapore [11], China [11], [18], [19], India [13], [15], and Saudi Arabia [17]. North America is represented in three studies, with affiliations in the United States [19], [20] and Canada [22]. Africa is represented in one study, with an affiliation in Morocco [13]. European and Asian institutions therefore account for most of the selected literature, and no selected study has an author affiliated with an institution in South America or Oceania.

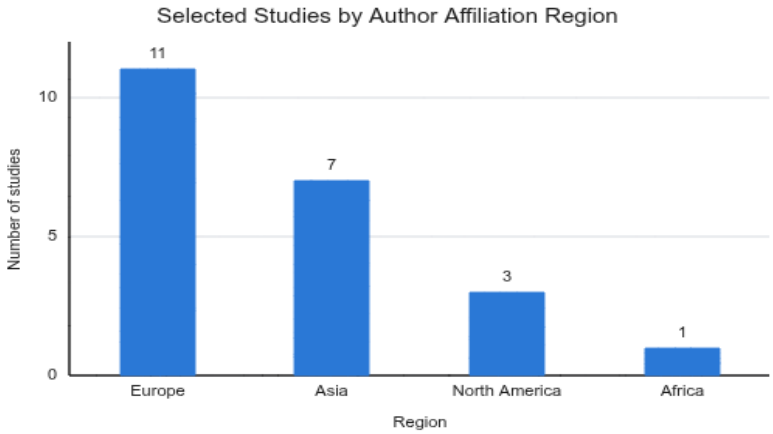


Figure 4. Geographical Distribution of the Selected Literature by Author Affiliation.

Overall, the selected literature addresses connected but distinct security dimensions: smart-contract and protocol vulnerabilities, transaction-level anomaly detection, and the economic, legal, and institutional conditions under which tokenized assets operate. These dimensions suggest the need for security approaches that connect technical detection with asset-level verification and governance controls. The categories in Table 6 represent each study's principal thematic contribution; they do not imply that the research domains are mutually exclusive.

3.2. RQ1: Security Threats and Vulnerabilities Affecting Tokenized RWAs

The reviewed studies indicate that security threats relevant to tokenized RWAs arise at several levels: smart-contract code and business logic, transaction and protocol interactions, external data and oracle dependencies, and governance or regulatory arrangements. A single incident may cross these levels, for example when an attacker exploits a contract weakness through transaction ordering or unreliable external inputs.

Table 7. Security Threat Mapping in Tokenized RWA Ecosystems

Threat dimension	Threats identified	Supporting studies	Evidence base
Smart-contract vulnerabilities	Programming defects, business-logic bugs, and incomplete coverage of vulnerability categories	[8], [11], [16], [20], [21]	General blockchain: Ethereum smart-contract studies
Transaction and protocol attacks	Flash loans, front-running, DeFi exploits, and interacting vulnerabilities across contracts	[7], [19]	General blockchain: DeFi incident and oracle studies

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

Oracle and external-data risks	Manipulated or unreliable inputs and discrepancies between on-chain execution and off-chain information	[7], [19]	General blockchain: DeFi studies, transferred to RWAs by inference
Tokenization and economic-design risks	Token standards, valuation, transaction costs, and design of tokenized markets	[9], [12], [13]	RWA-specific: tokenization studies
Governance and regulatory risks	Legal friction, fragmented institutional responsibilities, and regulated-market controls	[10], [17], [18]	RWA-specific: regulation and governance studies

Smart-contract security is a foundational concern, but it does not exhaust the risk profile of tokenized RWAs. A review that maps detection techniques against the DASP and SWC vulnerability classifications identifies research gaps in each technique [8]. Combining large language models with program analysis can help identify business-logic bugs that may be missed by pattern matching alone; the GPTScan study reports nine previously unknown logic bugs [11]. These findings highlight the value of contextual reasoning while also indicating that detection coverage remains incomplete.

Transaction- and protocol-level threats require analysis beyond individual functions. Oracle-related risks and DeFi attack mechanisms include flash loans and front-running [7]. A systematization of 77 academic papers, 30 audit reports, and 181 real-world DeFi incidents further shows how multiple vulnerabilities can interact across contracts [19]. Taken together, these findings indicate that contract interactions, transaction ordering, and protocol assumptions can combine to create attack paths.

Oracle and external-data risks are documented in DeFi research, not in RWA deployments. Price-oracle attacks are the most frequent incident type among the DeFi incidents analyzed in [19], and the oracle problem is described as a structural weakness of DeFi protocols that rely on external data [7]. These findings are relevant to RWAs because tokenized assets depend on information maintained outside the blockchain, including valuation inputs and asset records. A contract may execute as programmed yet still produce an undesirable outcome when the information supplied to it is inaccurate or manipulated. Secure tokenization therefore requires controls for both contract logic and the provenance and reliability of external data, although this conclusion is an inference from DeFi evidence and has not been measured in RWA systems.

Governance is another material part of the risk profile. The relationship between the Markets in Crypto-Assets Regulation (MiCA) and land registration in Latvia illustrates potential friction between deterministic on-chain execution and legal processes maintained by external registries [10]. Institutional centralization in the use of decentralized technology and governance arrangements for regulated real-estate tokenization raise related questions about responsibilities and oversight [17], [18]. Technical security must therefore be complemented by asset verification, clearly assigned responsibilities, and legally appropriate response procedures.

The evidence behind Table 7 is of two kinds, and the distinction matters for how the findings should be read. Six of the 16 studies take tokenized assets as their object of analysis [9], [10], [12], [13], [17], [18]. They document risks in tokenization and economic design and in governance and regulation, including valuation uncertainty, regulatory fragmentation, and gaps between token transfers and land registration. In these studies, technical security appears mainly as a requirement or an adoption barrier and is not supported by measured attack data. The other ten studies examine smart contracts,

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : https://doi.org/10.58602/itsecs.v5i1.478
Page 94-111

DeFi protocols, or blockchain transactions in general [7], [8], [11], [14], [15], [16], [19], [20], [21], [22]. The first three rows of Table 7 rest on this second group. Their application to RWAs is a reasoned transfer, justified because RWA tokens are issued and moved by the same kinds of contracts and depend on the same kinds of oracles. It should not be read as evidence that these attacks have been observed with the same frequency or impact in RWA ecosystems.

3.3. RQ2: AI and Machine Learning for Security Threat Detection

The selected literature describes several AI-enabled approaches, including ML-based vulnerability classification, LLM-assisted code analysis, explainable AI, transaction anomaly detection, and privacy-preserving collaborative learning. The approaches address different detection objectives and should not be treated as direct substitutes. The synthesis does not establish a single system validated across all components of an RWA ecosystem.

Table 8. AI-Driven Approaches for Security Detection

Approach	Detection capability (threat layer)	Strengths	Limitations and considerations	Supporting studies
Machine learning vulnerability detection	Classify smart contracts according to known vulnerability patterns (smart-contract code)	Screens large contract sets automatically for known vulnerability classes	Class imbalance, duplicated contracts, and inconsistent labels can distort reported performance; detection is limited to labelled vulnerability classes	[8], [15], [20], [21]
LLM-assisted program analysis	Identify contextual and business-logic bugs in contract code (smart-contract code)	Reasons about intended behavior; found logic bugs missed by human auditors	Performance depends on the analysis design, code context, and independent validation	[11]
Explainable AI	Provide interpretable evidence for model predictions (smart-contract code and alert review)	Gives auditors and regulators evidence they can inspect	An explanation does not itself establish that a prediction is correct	[15]
Blockchain anomaly detection	Identify suspicious transaction or financial-activity patterns (transactions and protocol interactions)	Works after deployment; can flag attacks that have no known code defect	Requires representative data, suitable labels or anomaly assumptions, and careful evaluation	[14]
Federated and privacy-preserving learning	Support collaborative anomaly detection without centralizing raw data (transactions across institutions)	Lets institutions collaborate without sharing raw data	Identified as a research direction; cost and accuracy in multi-institution settings have not been evaluated	[14], [22]

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

Blockchain-supported AI integrity	Use blockchain to protect the integrity of AI training and model outputs (detection infrastructure)	Tamper-resistant record of training data and model outputs	Conceptual synergy does not demonstrate improved detection performance without empirical testing	[15], [22]

The approaches summarized in Table 8 provide complementary functions and do not form a unified benchmark. Class imbalance has been neglected by most machine-learning-based detectors, and algorithm-level remedies are considered more promising than data-level resampling [20]. Dataset construction is a second weakness: many contracts in commonly used datasets are identical, labeling methods differ between studies, and results are often reported as an average instead of per vulnerability class [21]. For this review, the implication is that duplicated contracts should be removed before data are split, because identical samples in the training and test sets would overstate performance, and that F1-scores should be reported for each vulnerability class.

Combining a large language model with program analysis can help detect business-logic bugs in smart contracts [11]. In RWA applications, similar techniques could be investigated for reviewing authorization conditions, asset-transfer rules, and token issuance or redemption logic. These are plausible extensions of the method, not results demonstrated directly for every RWA implementation.

A machine-learning framework that combines ensemble classifiers, SHAP-based explainability, and an on-chain registry for recording model predictions reports 87.67% accuracy for a Random Forest classifier on the 143-contract SmartBugs-Curated dataset and was then extended to the 47,398 contracts of SmartBugs-Wild [15]. On the larger dataset the classifiers predict cluster labels obtained from unsupervised clustering, not verified vulnerability labels, so the reported 99% accuracy indicates that the approach scales and does not measure detection accuracy. SHAP can help interpret feature contributions; independent validation is still necessary to establish predictive reliability, and both datasets contain general Ethereum contracts, not RWA-specific ones.

At the transaction level, a bibliometric analysis of 363 publications indexed in the Web of Science Core Collection from 2017 to 2024 identifies a shift from rule-based detection toward unsupervised learning, graph neural networks, and federated learning for blockchain anomaly detection, and it names privacy-preserving and explainable techniques as open research directions [14]. Bibliometric findings indicate research directions and do not compare algorithmic performance. A critical review of machine learning and blockchain security likewise identifies federated learning and zero-knowledge proofs as important advances and discusses how the tamper resistance of blockchain can protect AI training in trustless environments [22]. Neither study evaluates a privacy-preserving detector on RWA transactions, so these contributions remain subject to implementation-specific validation.

Comparing the techniques by what they can observe clarifies their suitability for different RWA threats. Supervised ML classifiers can screen large numbers of contracts automatically, but they detect only the vulnerability classes present in their training labels. This makes them suitable for known code-level defects and unsuitable for business-logic errors or off-chain discrepancies [20], [21]. LLM-assisted program analysis addresses that weakness because it reasons about the intended behavior of code; GPTScan identified nine vulnerabilities that human auditors had missed [11]. Its limits are its dependence on predefined vulnerability scenarios and the need to confirm candidate findings with static analysis, so it fits pre-deployment audits of issuance, redemption, and transfer logic better than continuous monitoring. Explainable models add evidence that an auditor or regulator can inspect, which is valuable in regulated RWA markets, although an explanation does

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : https://doi.org/10.58602/itsecs.v5i1.478
Page 94-111

not make a prediction correct [15]. Transaction anomaly detection is the reviewed approach that works on live activity after deployment. It can therefore flag attacks that exploit contract interactions, oracle inputs, or abnormal transfers without a known code defect, but it depends on representative transaction data and produces alerts that require human interpretation [14]. Federated and other privacy-preserving learning would let issuers, custodians, and exchanges train shared detectors without disclosing customer data, yet in the reviewed literature it remains a research direction without RWA evaluation [14], [22]. No reviewed technique observes off-chain asset records or legal status directly. Valuation fraud and mismatches between tokens and registries therefore remain outside the reach of current AI-based detection and must be handled through external-data validation and governance controls.

Overall, the studies suggest that an AI-based security approach should be layered: code analysis can assess vulnerabilities before or during audits, transaction monitoring can flag suspicious activity, and explainability and privacy mechanisms can support review and data-sharing requirements. The practical effectiveness of such a combined architecture for tokenized RWAs remains to be empirically established.

3.4. RQ3: Research Gaps and Future Directions

The synthesis identifies gaps in vulnerability coverage, dataset quality, cross-study comparability, lifecycle integration, and alignment between technical controls and institutional governance. These limitations restrict the extent to which individual AI methods can be translated into reliable end-to-end security for tokenized RWAs.

Table 9. Research Gaps and Future Directions

Research gap	Evidence from the synthesis	Future direction
Incomplete vulnerability coverage	Limits in existing tools and the importance of business-logic bugs	Combine known vulnerability analysis with contextual reasoning and program analysis
Dataset imbalance and duplication	Class imbalance and duplicated contract code can distort evaluation	Deduplicate contracts before splitting data; treat class imbalance; report per-class F1-scores and results on unseen contracts
Limited comparability	Studies use different datasets, methods, and evaluation settings	Develop a public RWA security benchmark with fixed data splits, threat labels, and transparent evaluation protocols
Fragmented lifecycle monitoring	Code, transaction, oracle, tokenization, and governance risks are examined separately	Build and test integrated monitoring across contracts, transactions, external data, and asset processes, measuring threat coverage, false alarms, and response time
Technical-legal alignment	Smart-contract execution may not align automatically with registries and legal procedures	Connect alerts with asset verification, defined responsibilities, and escalation processes
Privacy and interoperability	Collaborative learning and regulated-market controls are explored separately	Evaluate federated and other privacy-preserving detection across issuers, custodians, and exchanges, including accuracy, cost, and privacy guarantees
Limited RWA-specific validation	Many methods are evaluated in general	Build labelled datasets of RWA token contracts, transactions, and oracle feeds, and test detectors on them

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : https://doi.org/10.58602/itsecs.v5i1.478
Page 94-111

	blockchain or DeFi contexts	
Single-platform evaluation	Detection studies are evaluated on Ethereum smart contracts	Validate detectors across the blockchains and token standards used for RWAs, including permissioned ledgers
Explanations not validated with users	Explanations are generated, but their usefulness to auditors and regulators is not tested	Evaluate explanations with auditors and compliance staff and link them to audit evidence

Table 9 shows that progress requires more than increasing predictive performance. Researchers must establish the reliability of the datasets, define the threats a system is designed to detect, and assess whether alerts can be incorporated into real operational workflows. General smart-contract benchmarks may provide a starting point, but they do not necessarily represent asset valuation, external ownership records, or legally constrained transfer conditions.

Six research opportunities follow from these gaps. The first is an RWA-specific dataset. Current detectors are trained on general Ethereum collections such as SmartBugs [15], [21], and the reviewed literature offers no public corpus that pairs RWA token contracts with their transactions, oracle feeds, and incident labels. The second is a benchmark built on such data, with fixed training and test splits, deduplicated contracts, and per-class metrics, so that results from different studies can be compared [16], [21]. The third is cross-platform validation. The detection studies reviewed here are evaluated on Ethereum smart contracts, whereas regulated tokenization may run on other public blockchains or on permissioned ledgers, and whether detectors transfer between platforms is untested. The fourth is explainable AI evaluated with its intended users: explanations should be tested with auditors and compliance staff and tied to the evidence that regulated markets require [15], [17]. The fifth is privacy-preserving detection, in which federated learning and related techniques are evaluated across institutions with measured accuracy, communication cost, and privacy guarantees [14], [22]. The sixth is empirical evaluation of integrated frameworks such as the one proposed in Section 3.5, measuring threat coverage, false-positive and false-negative rates, and the time from alert to response in a realistic RWA environment. Across all six, evaluations should state which RWA threats a dataset represents, which threats lie outside the detector's scope, and what false positives and false negatives would cost.

3.5. Integrated Discussion

Across the three research questions, a consistent pattern emerges: threats affecting tokenized RWAs span technical, transactional, data, and governance layers, while many reviewed detection methods focus on only one or two layers. A conceptual architecture should therefore connect asset and external-data verification, blockchain and smart-contract analysis, AI-driven detection, and governance-led response.

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

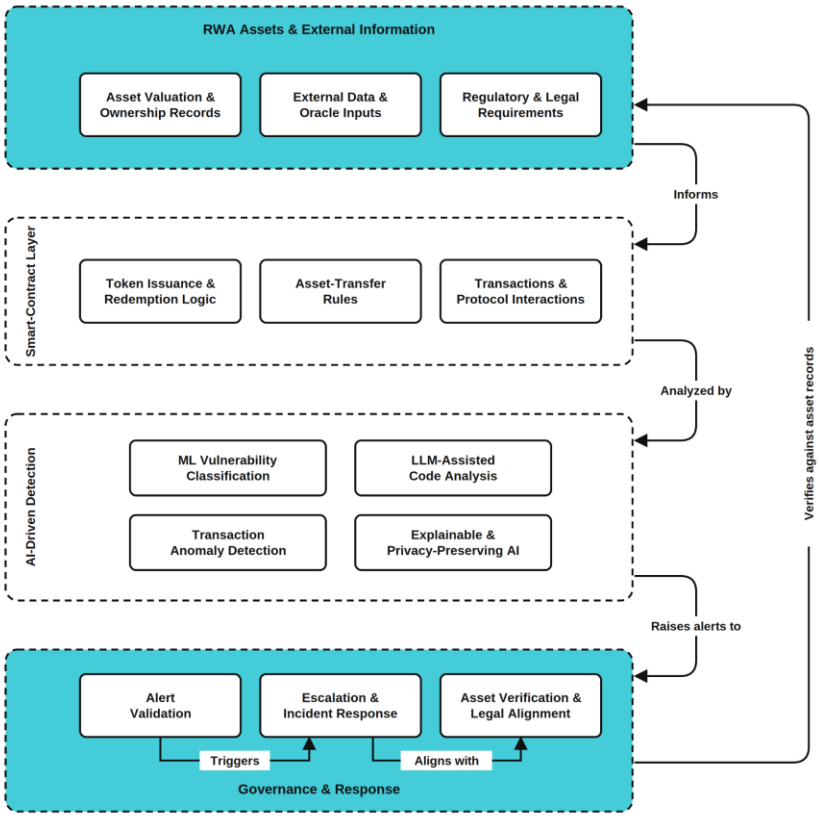


Figure 5. Conceptual Framework for AI-Driven Security Threat Detection in Tokenized RWAs.

Figure 5 presents a synthesis-derived conceptual model, not an experimentally validated architecture. It contains four components connected by four data flows. The first component, RWA assets and external information, holds asset valuation and ownership records, external data and oracle inputs, and regulatory and legal requirements. Asset verification takes place here: the off-chain facts about an asset are established before tokenization and kept current afterwards. This component informs the smart-contract layer, which means that valuations, ownership data, and compliance rules enter the blockchain through oracles and contract configuration and set the conditions for token issuance and redemption logic, asset-transfer rules, and transactions and protocol interactions.

The smart-contract layer is analyzed by the AI-driven detection component, and two kinds of data move along this flow. Contract source code and bytecode feed ML vulnerability classification and LLM-assisted code analysis, mainly before deployment and at each contract upgrade. Transaction records, event logs, and oracle updates produced while the contracts run feed transaction anomaly detection, which is how transaction monitoring enters the framework. Explainable and privacy-preserving AI is not a separate detector. It conditions the other three by attaching an explanation to each alert and by allowing models to be trained across institutions without pooling raw data.

Detection raises alerts to the governance and response component. An alert identifies the affected contract or transaction, the suspected threat type, and the explanation produced by the model. Alert validation is a human review that confirms or dismisses the alert. A confirmed alert triggers escalation and incident response, and the response is

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

aligned with asset verification and legal requirements so that any action taken on-chain can be enforced off-chain. The final flow closes the loop: governance verifies the incident against the asset records in the first component and corrects valuations, ownership entries, or oracle sources where needed, and the corrected information again informs the smart-contract layer. The framework is therefore a cycle in which off-chain verification, on-chain analysis, monitoring, and institutional response depend on one another, and a weakness in one component limits the others.

AI should not be treated as a substitute for secure engineering or legal verification. A model may flag suspicious code or transactions, but the meaning of an alert depends on contract rules, external data reliability, and the operating context. Likewise, explainability can help reviewers understand a model output but cannot independently prove that the output is correct. The central research direction is therefore to develop and empirically evaluate a layered architecture connecting smart-contract analysis, transaction monitoring, external-data validation, and governance controls for tokenized RWAs.

4. CONCLUSION

This systematic literature review synthesized 16 selected studies to examine security threats affecting tokenized real-world assets (RWAs), AI-driven detection approaches, and remaining research gaps. The findings identify four interconnected research domains: RWA tokenization and market design, smart-contract vulnerability detection, smart-contract, decentralized finance (DeFi), and oracle security, and blockchain anomaly and fraud detection. Across these domains, security risks extend beyond smart-contract code to include suspicious transactions, unreliable external data, asset verification, privacy, interoperability, and regulatory governance. AI and machine learning offer complementary capabilities for identifying code vulnerabilities and anomalous activities, while explainability and privacy-preserving mechanisms may support security analysis and responsible information sharing. However, the reviewed evidence indicates that these capabilities are often studied separately. Therefore, effective security for tokenized RWAs requires a layered approach that connects smart-contract analysis, transaction monitoring, external-data validation, asset-related processes, and governance-led incident response. The principal contribution of this review is to integrate these research areas into a unified conceptual perspective while distinguishing evidence directly related to RWAs from findings derived from broader blockchain-security research.

Several limitations should be considered when interpreting these findings. First, the review is based on 16 studies selected according to the defined search, accessibility, language, and topical eligibility criteria; therefore, relevant research outside the selection scope may not be represented. Second, the selected studies differ in research objectives, datasets, detection techniques, evaluation metrics, and experimental settings, which limits direct comparisons of their reported performance. Third, a substantial portion of the AI-based security literature examines general blockchain, smart-contract, or DeFi environments rather than tokenized RWA applications specifically. Consequently, the effectiveness of these techniques in addressing RWA-specific risks, including discrepancies between on-chain records and off-chain asset information, cannot be assumed from their performance in other contexts. Fourth, this study employs qualitative and descriptive synthesis rather than statistical meta-analysis or independent experimental validation. Fifth, the quality assessment was divided among the three authors and was not repeated independently, so assessment bias cannot be excluded. The proposed layered security perspective should therefore be understood as a synthesis-derived conceptual direction, not as a deployed or empirically validated detection system. These limitations indicate that the conclusions identify promising approaches and unresolved challenges but do not

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

establish the operational effectiveness of an integrated AI-driven security solution for tokenized RWAs.

Future research should prioritize the development and empirical evaluation of integrated security frameworks tailored to tokenized RWA ecosystems. Such frameworks should combine smart-contract vulnerability analysis, transaction anomaly detection, oracle and external-data validation, and asset-related verification with clearly defined governance and incident-response procedures. Researchers should also develop representative RWA-specific datasets and reproducible benchmarks that cover realistic contracts, transaction patterns, external-data dependencies, and relevant threat scenarios. Evaluation should address duplicated contract code, class imbalance, data leakage, generalization to unseen contracts, and consistent reporting of per-class F1-scores alongside false-positive and false-negative rates. Further work should examine cross-platform validation, explainability, computational cost, privacy-preserving collaboration, interoperability, and the practical usefulness of alerts for human reviewers and institutional decision-makers. In addition, technical detection results should be connected to asset records, legal ownership verification, regulatory requirements, and clearly assigned responsibilities for validating and escalating security alerts. Ultimately, future studies should move beyond isolated detection tasks toward end-to-end evaluations in representative RWA environments to determine whether integrated AI-driven approaches can improve threat coverage, reliability, and operational decision-making while preserving privacy and accountability.

CRediT AUTHORSHIP CONTRIBUTION STATEMENT

Abisena Rais: Conceptualization, Methodology, Formal analysis, Visualization, Writing – original draft. **Aqsyal Hilmi Fadilla:** Investigation, Data curation, Writing – original draft, Writing – review & editing. **Sarah Fajriah Rahmah:** Validation, Investigation, Writing – review & editing.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENTS

The author(s) received no financial support for the research, authorship, and/or publication of this article.

DECLARATION OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

Generative AI tools, including ChatGPT (GPT-5.6) by OpenAI and Claude Sonnet 5.5 by Anthropic, were used to assist with language refinement, manuscript organization, and improvement of writing clarity. The authors critically reviewed and edited all AI-assisted content and take full responsibility for the accuracy, integrity, and final content of the manuscript. The AI tools were not listed as authors.

REFERENCES

[1] H.-W. Teng *et al.*, "Digital assets: risks, regulations, mitigation," *Financ. Innov.*, vol. 12, no. 1, p. 65, 2026, doi: 10.1186/s40854-025-00848-y.
[2] J. Crisostomo, F. Bacao, and V. Lobo, "Machine learning methods for detecting smart contracts vulnerabilities within Ethereum blockchain - A review," *Expert Syst. Appl.*, vol. 268, p. 126353, 2025, doi: 10.1016/j.eswa.2024.126353.

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

[3] S. Azimi, A. Golzari, N. Ivaki, and N. Laranjeiro, "A systematic review on smart contracts security design patterns," *Empir. Softw. Eng.*, vol. 30, no. 4, p. 95, 2025, doi: 10.1007/s10664-025-10646-w.
[4] B. Wang, Y. Tong, S. Ji, H. Dong, X. Luo, and P. Zhang, "A Review of Learning-based Smart Contract Vulnerability Detection: A Perspective on Code Representation," *ACM Trans. Softw. Eng. Methodol.*, vol. 35, no. 6, p. 167, 2026, doi: 10.1145/3750042.
[5] S. J. Alsunaidi, H. Aljamaan, and M. Hammoudeh, "Leveraging Machine Learning Models to Improve Smart Contract Security: A Survey of Vulnerabilities and Detection Methods," *ACM Comput. Surv.*, vol. 58, no. 6, p. 151, 2026, doi: 10.1145/3772367.
[6] Y. He, J. Fan, and H. Wu, "A Systematic Review and Performance Evaluation of Open-Source Tools for Smart Contract Vulnerability Detection," *Comput. Mater. Contin.*, vol. 80, no. 1, pp. 995–1032, 2024, doi: 10.32604/cmc.2024.052887.
[7] G. Caldarelli and J. Ellul, "The Blockchain Oracle Problem in Decentralized Finance: A Multivocal Approach," *Appl. Sci.*, vol. 11, no. 16, p. 7572, 2021, doi: 10.3390/app11167572.
[8] F. R. Vidal, N. Ivaki, and N. Laranjeiro, "Vulnerability detection techniques for smart contracts: A systematic literature review," *J. Syst. Softw.*, vol. 217, p. 112160, 2024, doi: 10.1016/j.jss.2024.112160.
[9] U. Tanveer, S. Ishaq, and T. G. Hoang, "Tokenized assets in a decentralized economy: Balancing efficiency, value, and risks," *Int. J. Prod. Econ.*, vol. 282, p. 109554, 2025, doi: 10.1016/j.ijpe.2025.109554.
[10] N. Jūrmalis, A. Berķe-Berga, and M. Urbāne, "Advancing Asset Tokenization in the European Union and Latvia: A Regulatory and Policy Perspective," *Laws*, vol. 14, no. 1, p. 7, 2025, doi: 10.3390/laws14010007.
[11] Y. Sun *et al.*, "GPTScan: Detecting Logic Vulnerabilities in Smart Contracts by Combining GPT with Program Analysis," in *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, Lisbon, Portugal, 2024, pp. 2048–2060. doi: 10.1145/3597503.3639117.
[12] O. Marin, T. Cioara, L. Toderean, D. Mitrea, and I. Anghel, "Review of Blockchain Tokens Creation and Valuation," *Future Internet*, vol. 15, no. 12, p. 382, 2023, doi: 10.3390/fi15120382.
[13] A. El Jaouhari, A. Samadhiya, A. Kumar, H. Chokshi, A. Šešplaukis, and S. Raslanas, "Tokenization and the future of property investment: A new paradigm for real estate," *Int. J. Strateg. Prop. Manag.*, vol. 29, no. 4, pp. 297–315, 2025, doi: 10.3846/ijspm.2025.24814.
[14] R. Shevchuk, V. Martsenyuk, B. Adamyk, V. Benson, and A. Melnyk, "Anomaly Detection in Blockchain: A Systematic Review of Trends, Challenges, and Future Directions," *Appl. Sci.*, vol. 15, no. 15, p. 8330, 2025, doi: 10.3390/app15158330.
[15] A. Vishnoi, V. Sapra, L. Sapra, P. Narooka, and D. Panwar, "Blockchain-integrated machine learning framework for transparent smart contract vulnerability detection," *Front. Blockchain*, vol. 9, p. 1735510, 2026, doi: 10.3389/fbloc.2026.1735510.
[16] G. Iuliano and D. Di Nucci, "Smart contract vulnerabilities, tools, and benchmarks: An updated systematic literature review," *J. Syst. Softw.*, vol. 236, p. 112788, 2026, doi: 10.1016/j.jss.2026.112788.
[17] A. S. Al-Humaimeedy and R. Al-Hammadi, "Blockchain-based real-estate tokenization in regulated markets: A systematic review and socio-technical governance framework," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 38, no. 8, p. 855, 2026, doi: 10.1007/s44443-026-01255-8.
[18] Y. Zhang, B. Gong, and P. Zhou, "Centralized use of decentralized technology: Tokenization of currencies and assets," *Struct. Change Econ. Dyn.*, vol. 71, pp. 15–25, 2024, doi: 10.1016/j.strueco.2024.06.006.
[19] L. Zhou *et al.*, "SoK: Decentralized Finance (DeFi) Attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2023, pp. 2444–2461. doi: 10.1109/SP46215.2023.10179435.
[20] R. Kiani and V. S. Sheng, "Ethereum Smart Contract Vulnerability Detection and Machine Learning-Driven Solutions: A Systematic Literature Review," *Electronics*, vol. 13, no. 12, p. 2295, 2024, doi: 10.3390/electronics13122295.

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 5, Number 1, January 2027
DOI : **https://doi.org/10.58602/itsecs.v5i1.478**
Page 94-111

[21] D. Ressi, A. Spanò, L. Benetollo, M. Bugliesi, C. Piazza, and S. Rossi, "Vulnerability Detection in Solidity Smart Contracts via Machine Learning: A Qualitative Analysis," *Blockchain Res. Appl.*, vol. 7, no. 6, p. 100390, 2026, doi: 10.1016/j.bcra.2025.100390.
[22] H. Taherdoost, "Blockchain and Machine Learning: A Critical Review on Security," *Information*, vol. 14, no. 5, p. 295, 2023, doi: 10.3390/info14050295.

Abisena Rais: *Corresponding Author
Copyright © 2027, Abisena Rais, Aqsyal Hilmi Fadilla, Sarah Fajriah Rahmah.