Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15825
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Web3-Based Cyber Incident Reporting System With Smart Contracts and Non-Fungible Token Rewards

Danang Juniar Permana[1)*], Wildan Mahmud[2)], Galuh Wilujeng Saraswati[3)]
[1,2,3)]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro PSDKU Kota Kediri, Indonesia.
[1)]djunee0@gmail.com, [2)]wildan.mahmud@dsn.dinus.ac.id, galuhwilujengs@dsn.dinus.ac.id

Submitted :Feb 12, 2026 | **Accepted** : Mar 2, 2026 | **Published** : Apr 2, 2026

Abstract: The rising frequency of cyber threats increases the need for incident reporting that is transparent, efficient, and privacy-preserving. This study designs and implements a hybrid Web2-Web3 cyber incident reporting prototype that anchors report references on a blockchain while storing full incident details off-chain, and explores non-fungible token (NFT) recognition incentives for reporters. Using an SDLC-based iterative prototyping approach, we built a React single-page application integrated with a Laravel REST API and MySQL for off-chain storage, and deployed Solidity smart contract modules on the Arbitrum Sepolia testnet to record report identifiers and UUID pointers (dataPointer) and to mint NFTs after administrative validation. We conducted black-box functional testing across core scenarios (submission, storage, pointer anchoring, validation, and minting) and a user acceptance study with 25 participants (15 cybersecurity students and 10 IT practitioners) using a 5-point Likert questionnaire. All tested scenarios executed as expected in the test environment, and on-chain events were traceable to corresponding backend records via transaction receipts and logged identifiers. The acceptance evaluation yielded an overall mean score of 3.4/5 (about 68%), indicating moderate acceptance and supporting the work as a prototype feasibility study rather than organizational-level generalization. The prototype demonstrates a practical workflow for hybrid incident reporting with transaction-level traceability and recognition incentives; future work should strengthen cryptographic binding (e.g., content hashing) and validate the approach with CSIRT stakeholders in operational settings.

Keywords: blockchain; cyber incident reporting; non-fungible token; smart contract; web3

INTRODUCTION

The frequency and sophistication of cyber incidents have increased significantly in recent years, placing considerable pressure on existing incident reporting mechanisms and response workflows. Recent reviews highlight an expanding attack surface and increasingly complex adversarial techniques that complicate detection, attribution, and mitigation processes (Ray, 2023; Saleh, 2024). As a result, effective and timely incident reporting has become a critical component of cybersecurity operations, particularly for Computer Security Incident Response Teams (CSIRTs).

Most incident reporting systems currently rely on conventional Web2 architectures. While these systems are generally familiar and easy to use, prior studies report several structural limitations, including centralized and tamperable logs, limited transparency, delayed feedback to reporters, and low participation rates due to the absence of clear recognition or incentive mechanisms (Marbouh et al., 2021; Diallo et al., 2024). Such limitations can reduce trust in reporting outcomes and discourage users from submitting complete or timely incident information, ultimately weakening incident response effectiveness.

Blockchain and Web3 technologies have been widely studied as potential solutions to these challenges because of inherent characteristics such as immutability, decentralization, and verifiable timestamping (Nasar, 2023). Several works demonstrate that blockchain-based approaches can enhance data integrity, provenance, and accountability by anchoring cryptographic proofs on-chain while keeping sensitive incident details off-chain

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

(Philip & Saravanaguru, 2022; Ma et al., 2024). Existing prototypes and frameworks further show that distributed ledgers improve transparency and traceability in incident reporting workflows (Putz et al., 2022; Banaeian Far & Rajabzadeh Asaar, 2024). In parallel, research into privacy-preserving and anonymous submission techniques suggests practical ways to protect reporter identity and reduce retaliation risk (Zhu et al., 2023). Studies on NFTs and token-based incentives also indicate that digital recognition mechanisms can increase engagement and the perceived value of contributions (Wu & Liu, 2023).

Despite these advances, most published systems are domain-specific (for example, healthcare or community mobilization) and often presented as isolated proofs of concept rather than operationally validated solutions for CSIRTs (Marbouh et al., 2021; Diallo et al., 2024). Moreover, few studies combine functional system validation with end-user acceptance testing to demonstrate early feasibility and adoption potential (Putz et al., 2022; Ray, 2023). Therefore, there is a need for a hybrid architecture that preserves the usability of Web2 interfaces while leveraging Web3 traceability and incentive mechanisms in a manner that is practical for security teams. In this paper, the contribution is positioned as a prototype feasibility study, and broader generalization requires validation with CSIRT stakeholders in real operational settings.

Compared with prior blockchain-based incident reporting prototypes that primarily emphasize traceability or decentralized participation (Putz et al., 2022; Diallo et al., 2024), this study contributes a CSIRT-oriented hybrid workflow that keeps full incident reports off-chain while anchoring minimal references on-chain through contract events. In contrast to domain-specific deployments (Marbouh et al., 2021) and anonymity-focused reporting protocols on public blockchains (Zhu et al., 2023), we prioritize prototype feasibility by reporting (i) an explicit Web2–Web3 integration stack (React SPA–Laravel REST API–MySQL), (ii) functional black-box validation of the end-to-end workflow, (iii) user acceptance results (n=25), and (iv) a CSIRT stakeholder walkthrough (n=5). Additionally, this work explores NFT-based recognition gated by administrative validation as an adoption-oriented mechanism rather than a monetary reward scheme.

To address this gap, this study proposes and implements a Web3-based cyber incident reporting system that integrates a React-based Web2 interface with a Laravel REST API and MySQL for off-chain report storage, alongside Solidity smart contracts deployed on the Arbitrum Sepolia testnet for on-chain pointer anchoring (dataPointer UUIDs) and NFT-based recognition issuance. The prototype is developed using an SDLC-based iterative prototyping approach to structure requirements analysis, architecture design, implementation, and evaluation. We perform functional (black-box) validation across core scenarios and conduct a user acceptance survey to assess early feasibility and perceived benefits. Specifically, this study (1) designs and validates a hybrid Web2–Web3 reporting workflow that preserves data privacy while enabling transaction-level traceability between blockchain events and backend records, (2) explores whether NFT-based recognition incentives improve reporter motivation and perceived acknowledgment, and (3) identifies usability and deployment challenges relevant to future CSIRT adoption. By focusing on a reference architecture and limited-scope evaluation rather than a single institutional deployment, this study aims to provide early empirical insights for future Web3-enabled incident reporting efforts (Guan et al., 2023; Saleh, 2024).

LITERATURE REVIEW

Hybrid Web2–Web3 architectures have emerged as a pragmatic solution to balance privacy, cost, and verifiability in cyber incident reporting. Several studies recommend keeping sensitive incident details off-chain while anchoring minimal references or proofs on-chain to provide tamper-evident anchoring and provenance (Philip & Saravanaguru, 2022; Ma et al., 2024). Prototype work across related security and Web3 contexts indicates that anchoring can enhance transparency and stakeholder trust, while introducing engineering trade-offs such as transaction cost, confirmation latency, and integration complexity (Diallo et al., 2024; Ray, 2023). These findings motivate a hybrid workflow where Web2 components manage full reports and operational interactions, while the blockchain layer records minimal verifiable anchors.

Protecting reporter privacy while maintaining operational follow-up capability is a recurring requirement. Proposed approaches include cryptographic techniques and pseudonymous submission workflows that support anonymous reporting while still enabling verification of provenance (Zhu et al., 2023; Banaeian Far & Rajabzadeh Asaar, 2024). Evidence from sensitive domains such as healthcare suggests that auditability can be preserved by anchoring proofs on-chain while keeping detailed records in secure, access-controlled repositories (Marbouh et al., 2021). Human-centered security incident reporting also emphasizes that anonymity mechanisms should remain operationally aware; without a feasible follow-up path, triage and response quality may degrade (Putz et al., 2022). In parallel, research on AI-assisted validation highlights opportunities to support triage without exposing sensitive content, although governance and data partitioning are critical to prevent leakage (Khan et al., 2024; Saleh, 2024).

From a CSIRT and incident-management perspective, standards and operational frameworks emphasize structured phases for incident handling and clear reporting mechanisms. ISO/IEC 27035 outlines key concepts and phases for detecting, reporting, assessing, responding to incidents, and applying lessons learned, while NIST SP 800-61r3 details incident handling workflows and coordination practices. Operational guidance from FIRST also

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15825
e-ISSN : 2541-2019
p-ISSN : 2541-044X

recommends that CSIRTs provide secure reporting channels (e.g., portals/forms) and instructions for constituents, and RFC 2350 explicitly discusses incident reporting forms and expectations for CSIRT services (ISO/IEC, 2023; Nelson, 2025; FIRST, 2024; Brownlee & Guttman, 1998).

Digital incentives, particularly NFTs and tokenized credentials, have been studied as mechanisms to increase participation by providing verifiable and persistent recognition. Prior work suggests that immutable tokens can improve perceived legitimacy and motivate contributors, yet the design must address reward abuse prevention, equitable valuation, and usability for non-crypto users (Wu & Liu, 2023; Qurotul Aini et al., 2023; Widayanti et al., 2021). For incident reporting contexts, transparent contribution records may help strengthen trust and engagement, but incentive schemes require clear governance, transparent distribution rules, and alternative recognition paths for participants who do not use wallets (Diallo et al., 2024). Accordingly, many studies frame NFTs more reliably as recognition incentives rather than monetary rewards.

Prior studies provide important building blocks but often emphasize one dimension at a time. For example, BISCUIT focuses on blockchain-based incident reporting from human observations and highlights traceability considerations (Putz et al., 2022), while community-oriented decentralized reporting emphasizes participation and decentralization as the main driver (Diallo et al., 2024). Other works prioritize anonymity and covert reporting protocols on public blockchains (Zhu et al., 2023) or demonstrate incident reporting in domain-specific settings such as healthcare (Marbouh et al., 2021). In contrast, this study positions its contribution as an integrated CSIRT-oriented hybrid prototype that combines (i) off-chain storage with minimal on-chain anchoring, (ii) an explicit Web2–Web3 implementation stack (React SPA–Laravel REST API–MySQL), and (iii) NFT-based recognition gated by administrative validation, and reports functional validation and user acceptance as early feasibility evidence, rather than organizational-level generalization.

Overall, the literature supports the feasibility of hybrid anchoring to improve traceability and tamper-evidence for report references while limiting on-chain exposure, privacy-preserving submission patterns that remain compatible with triage needs, and token-based recognition that can encourage participation when paired with robust governance and user-centered design. However, what remains underexplored is an integrated and empirically evaluated platform that simultaneously addresses (i) hybrid anchoring in a deployable workflow, (ii) anonymity that still supports triage and follow-up, and (iii) NFT-based recognition within a CSIRT-oriented reporting process. Many existing contributions are architectural proposals or domain pilots; fewer combine technical validation and end-user acceptance evaluation in a single study (Putz et al., 2022; Ray, 2023). This study aims to fill that gap by implementing a hybrid prototype and reporting functional validation and user acceptance results as a prototype feasibility study, while noting that broader generalization requires further CSIRT stakeholder validation.

METHOD

Method selection and justification

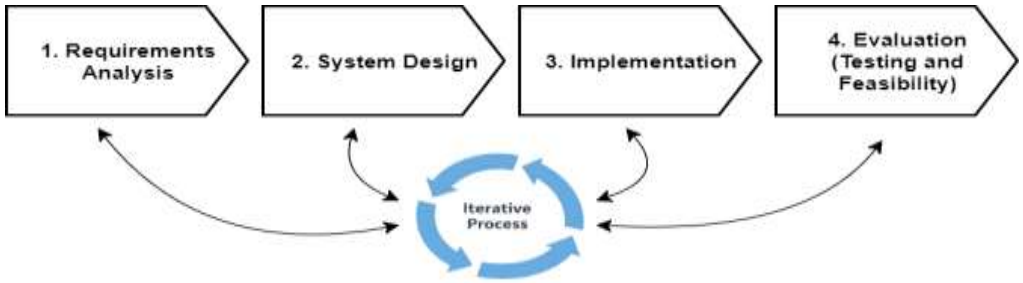

Fig. 1 SDLC-Based Iterative Prototyping Stages

This study adopts a software/system engineering approach using an SDLC-based iterative prototyping process to develop and evaluate a hybrid Web2–Web3 cyber incident reporting prototype (ISO/IEC/IEEE, 2017). This approach is suitable for applied prototype work because it structures engineering activities into staged steps, including requirements analysis, system design, implementation, and evaluation, while allowing iterative refinement based on testing outcomes and stakeholder feedback. The study is positioned as a prototype feasibility study, where findings are interpreted as early evidence of technical and user-level feasibility rather than organizational-level generalization.

Requirements analysis

We analyzed current incident reporting workflows with practitioner-like stakeholders to identify limitations and elicit requirements. Requirements elicitation was conducted through focused discussions and review of available operational practices to capture the expected reporting flow, validation steps, and user roles. This activity

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15825
e-ISSN : 2541-2019
p-ISSN : 2541-044X

produced a requirements specification covering functional needs (dual submission channels, validation workflow, status tracking, admin console) and nonfunctional requirements (privacy protection, traceability, usability, and minimal on-chain exposure). The specification served as acceptance criteria for subsequent design, implementation, and evaluation.

System design

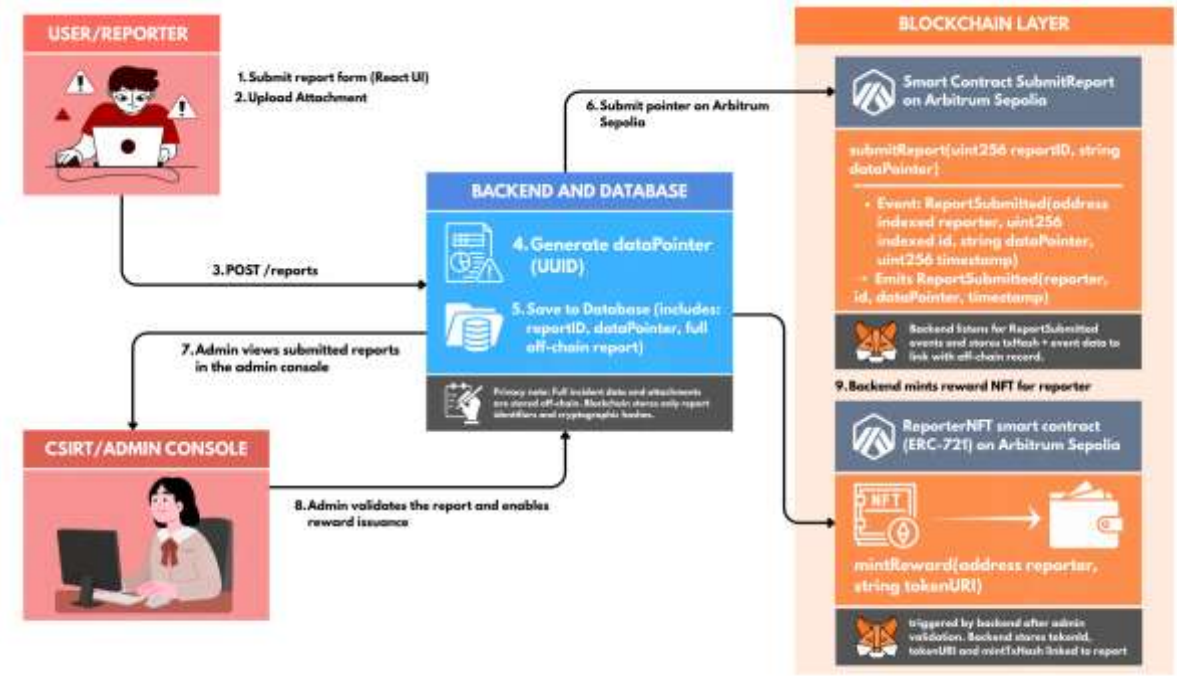

Fig. 2 Design Architecture System

Requirements were translated into a layered hybrid architecture that separates usability (Web2) from traceability anchoring (Web3). The Web2 layer uses a React single-page interface integrated with a Laravel REST API backend and MySQL for full report storage, user workflows, and administrative validation. The Web3 layer provides immutable anchoring and optional digital recognition using Solidity smart contracts deployed on the Arbitrum Sepolia testnet. To preserve privacy and reduce cost, only compact on-chain pointers (UUID dataPointer) and report identifiers are recorded on-chain; full report contents remain off-chain. Transaction receipts and contract event logs support traceability between on-chain records and off-chain database entries without exposing incident details. Event schemas, access roles, and minting controls are defined to prevent unauthorized token issuance (Philip & Saravanaguru, 2022; Ma et al., 2024).

Implementation

The implementation consists of two main smart-contract components: (1) a reporting contract for anchoring report references and emitting events, and (2) an ERC-721 contract for NFT-based recognition issuance after administrative validation. The prototype handles report submissions through the backend, which stores full records off-chain and generates a unique dataPointer UUID referencing each report. The backend then issues a blockchain transaction to the reporting smart contract, which emits a ReportSubmitted event containing the reporter address, report identifier, and pointer reference. The emitted event is linked to the corresponding MySQL record to preserve traceability. NFT issuance is performed through a secondary ERC-721 contract after administrative validation. The backend records the minting transaction hash and token metadata and links them to the validated report to preserve traceability between recognition issuance and reporting activity.

Evaluation (testing and feasibility assessment)

Evaluation comprises (i) functional (black-box) testing, (ii) user acceptance assessment, (iii) a CSIRT stakeholder walkthrough to strengthen external relevance, and (iv) descriptive measurement of transaction confirmation time in the testnet environment.

Functional (black-box) testing: Core scenarios were validated, including Web2 submission and off-chain storage, dataPointer generation, backend-to-contract pointer submission, event capture and linking to MySQL,

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15825
e-ISSN : 2541-2019
p-ISSN : 2541-044X

administrative validation flows, and NFT minting. Each test case recorded inputs, expected and actual outputs, transaction hashes, and screenshots, and was summarized as pass/fail.

User acceptance involved 25 participants (15 cybersecurity students and 10 IT practitioners) who performed scripted tasks and completed a 5-point Likert questionnaire. The acceptance score was computed as the overall mean Likert value (1–5) and normalized into a percentage using (mean/5) × 100%. Results are reported as descriptive statistics and interpreted as early feasibility evidence rather than broad generalization.

To improve relevance to CSIRT workflows, we conducted a structured walkthrough with five (5) CSIRT/incident response stakeholders from municipal cybersecurity teams. Participants reviewed the end-to-end workflow (report submission, administrative validation, on-chain anchoring, and NFT-based recognition issuance) using predefined scenarios and a checklist covering workflow fit, reporting fields, traceability needs, and confidentiality considerations. Feedback themes were summarized and are reported in the Results section to inform discussion of deployment considerations and limitations.

Transaction confirmation time measurement: Confirmation time was measured using blockchain transaction data in the testnet environment. For each observed transaction (report anchoring and/or NFT minting), we recorded the txHash and extracted receipt status and the mined block timestamp from the testnet explorer. The reported confirmation time is summarized descriptively as the average across ten (10) observed transactions on Arbitrum Sepolia. All blockchain activity used testnet transactions only. Ethical procedures included informed consent and anonymization. Key limitations (sample size, prototype/testnet setting, and pointer anchoring strength) are acknowledged and further discussed in the Discussion section.

RESULT

Functional Testing Results

Functional testing assessed whether the prototype executed the end-to-end reporting workflow as specified in the Method section. The defined black-box test cases produced the expected outputs, indicating that the web interface accepted incident submissions and stored report data and attachments in the off-chain database. Each submission generated a unique dataPointer identifier as a compact reference while keeping sensitive incident content off-chain. Before on-chain interaction, backend validation verified that the stored report record corresponded to the generated identifier and required fields.

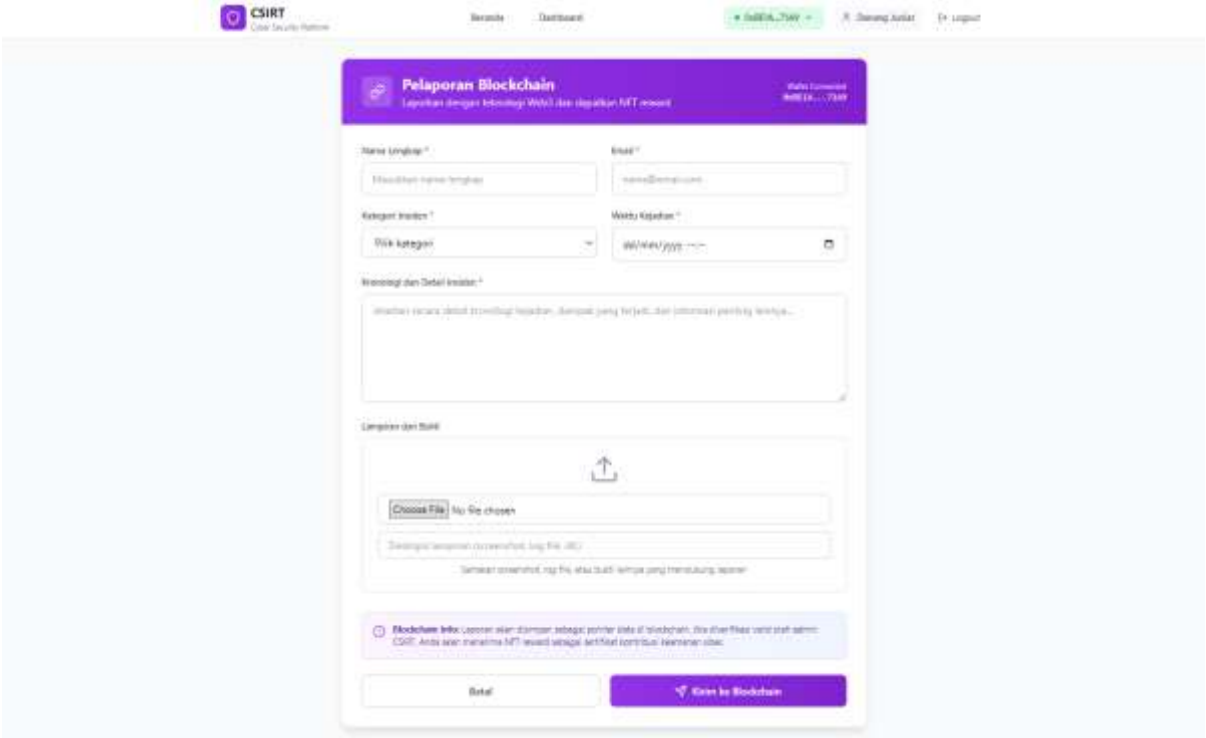

Fig. 3 Submission Interface

After submission, the backend initiated a smart-contract transaction on the Arbitrum Sepolia testnet and emitted a ReportSubmitted event. The event payload contained the reporter wallet address, report identifier, and pointer reference. The emitted event data were captured and linked to the corresponding off-chain database record. These results indicate that pointer-based anchoring can support transaction-level traceability between off-chain reports and on-chain evidence while minimizing on-chain exposure.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15825
e-ISSN : 2541-2019
p-ISSN : 2541-044X

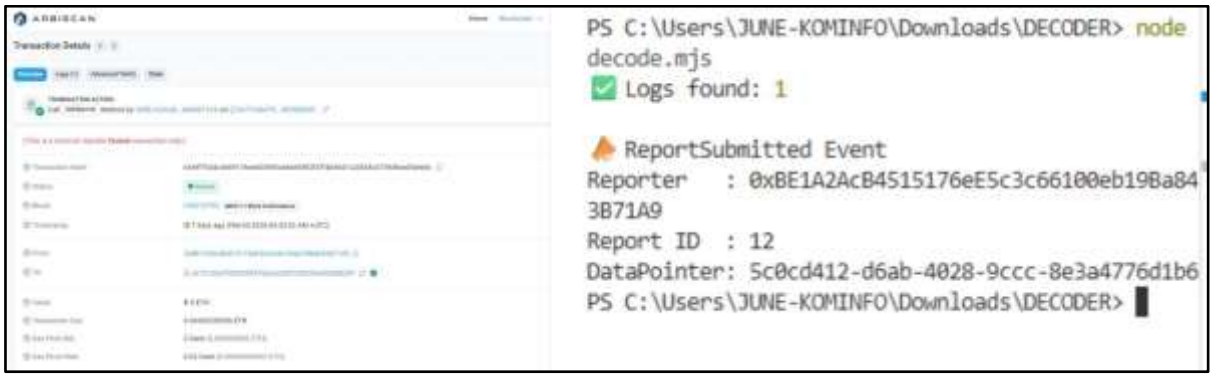

Fig. 4 Blockchain Transaction and Decoded Event Log

Functional tests also validated the administrative workflow and ensured that NFT-based recognition issuance was gated by the validation step. After a report was verified by the administrator, the backend triggered the ERC-721 contract to mint an NFT associated with the reporter's wallet address. The minting transaction was confirmed on the testnet, and the resulting transaction hash and token metadata were stored and linked to the validated report record. This confirms that NFT-based recognition can be integrated with the reporting lifecycle and linked back to the corresponding validation decision.

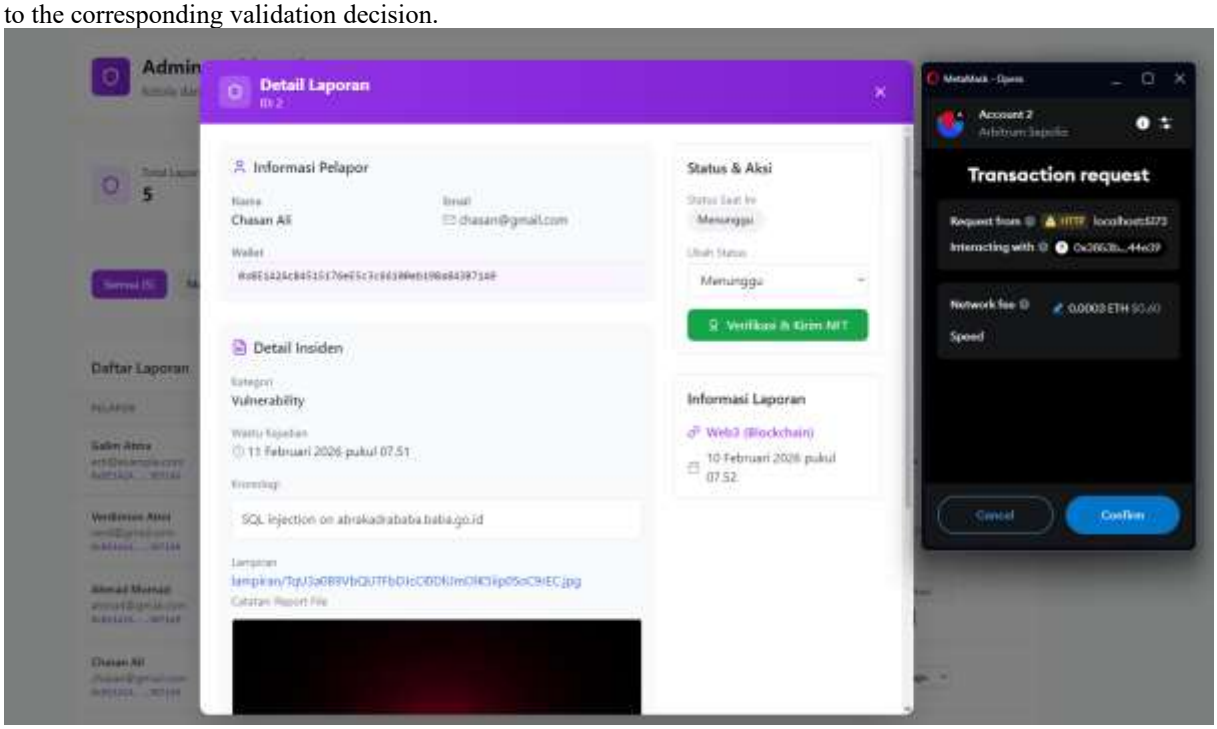

Fig. 5 NFT minting confirmation after administrative validation

User Acceptance Testing

User acceptance testing evaluated perceived usability and usefulness of the prototype. A total of 25 participants completed scripted tasks and responded to a 5-point Likert questionnaire covering ease of use, perceived usefulness, trust in the reporting process, perceived value of NFT-based recognition, and intention to use. Participants were able to complete the reporting workflow and follow the validation process with brief guidance.

Table 1
User Acceptance Summary

Evaluation Aspect	Mean Score (1–5)
Ease of Use	3.4
Perceived Usefulness	3.5
Trust in Reporting Process	3.3
NFT Recognition Value	3.7

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 2, April 2026
DOI : https://doi.org/10.33395/sinkron.v10i2.15825
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Intention to Use	3.4
Overall Acceptance	3.4 (≈68%)

Overall, the mean scores were above the neutral midpoint (3) across all aspects, with the highest score observed for the perceived value of NFT-based recognition (3.7). The overall acceptance score (3.4/5 ≈ 68%) indicates moderate acceptance within the limited evaluation scope and supports the positioning of this work as a prototype feasibility study.

To improve relevance to CSIRT workflows, five CSIRT/incident response stakeholders reviewed the end-to-end prototype using predefined scenarios. Overall, stakeholders considered the workflow directionally suitable for CSIRT-style reporting and validation at the prototype level, while highlighting several refinements needed for operational use. Feedback converged on three themes. First, regarding workflow fit, stakeholders noted that the submission and validation flow was aligned with incident triage stages, but they requested clearer escalation and status categories for operational use. Second, in terms of usability and onboarding, wallet interaction and blockchain terminology created friction, suggesting the need for guided onboarding and confirmation progress indicators. Third, for evidence binding, participants valued transaction-level traceability but recommended stronger cryptographic binding (e.g., content hashing or selective disclosure) to strengthen verification while preserving confidentiality. These inputs were used to refine the discussion of deployment considerations and limitations.

Performance Observation

Performance observations were recorded during report anchoring and NFT minting transactions on the Arbitrum Sepolia testnet. Across ten (10) observed transactions, confirmation times were approximately within a 5–10 second range under the evaluation setting. These timing results are reported as descriptive observations under testnet conditions and are not intended as production performance benchmarks.

Table 2
Blockchain Transaction Performance Observation (Testnet, n=10)

Operation	Observed Confirmation Time (Approx. Range)	Status
Report submission anchoring	~5–10 seconds	Confirmed
NFT minting	~5–10 seconds	Confirmed

Gas usage was observed to be low in the testnet setting; however, gas cost and confirmation behavior may differ under production/mainnet conditions. Across the evaluated transactions, the system consistently linked off-chain records with the corresponding on-chain events during report anchoring and NFT-based recognition issuance, supporting transaction-level traceability in a prototyping environment.

DISCUSSIONS

The results indicate that integrating a hybrid Web2–Web3 architecture into a cyber incident reporting workflow is technically feasible as a prototype feasibility study. Functional testing showed that the core workflow steps operated as intended, including report submission, off-chain storage, on-chain anchoring through contract events, and NFT-based recognition issuance after administrative validation. This supports the architectural rationale that sensitive incident narratives and attachments can remain off-chain, while on-chain evidence such as pointer references and transaction receipts can provide transaction-level traceability and tamper-evident logging without disclosing confidential content.

The hybrid design in this study aligns with prior recommendations to keep sensitive incident information off-chain while using blockchain to anchor verifiable references and strengthen traceability (Marbouh et al., 2021; Philip & Saravanaguru, 2022). Compared with BISCUIT, which emphasizes blockchain-based incident reporting from human observations and highlights traceability considerations (Putz et al., 2022), our work contributes an explicit Web2–Web3 implementation stack (React SPA–Laravel REST API–MySQL) and demonstrates end-to-end linkage between off-chain records and on-chain events via pointer anchoring. In contrast to decentralized/community-oriented reporting approaches that focus on participation and decentralization as the primary driver (Diallo et al., 2024), this prototype adopts a CSIRT-oriented workflow with administrative validation before issuing NFT-based recognition. Moreover, while anonymity and covert reporting protocols have been studied on public blockchains (Zhu et al., 2023), this study focuses on feasibility and adoption considerations, and discusses stronger cryptographic binding (e.g., content hashing) as future work.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

User acceptance outcomes suggest that the prototype can be used after brief onboarding and that participants perceived benefits related to transparency and recognition. NFT-based acknowledgment was viewed positively, indicating that digital recognition may increase perceived contribution value without substantially changing the reporting flow. However, overall acceptance remains moderate, which may reflect the need for clearer onboarding and may also be influenced by participant background, given that the sample consisted of cybersecurity students and IT practitioners rather than a full range of potential reporters or CSIRT constituencies.

Performance observations on the Arbitrum Sepolia layer-2 testnet suggest that report anchoring and NFT minting transactions can be confirmed within a short time window during evaluation sessions. These results are reported as descriptive testnet observations, not production performance benchmarks, because congestion, wallet behavior, RPC reliability, and infrastructure conditions may differ substantially in operational deployments. Nevertheless, the observations indicate that a layer-2 environment can be a practical option for prototyping due to relatively low latency and cost characteristics under controlled evaluation conditions.

Several practical considerations relevant to adoption emerged. Participants reported onboarding friction related to wallet interaction, transaction confirmation steps, and blockchain terminology. This indicates that future work should prioritize simpler onboarding, clearer interface feedback (e.g., confirmation progress indicators and explicit success/failure messages), and alternative interaction paths for users who are unfamiliar with crypto wallets. In addition, the current system relies on pointer-based anchoring (UUID dataPointer). While this supports traceability through immutable timestamps and event logs, it provides weaker cryptographic binding than anchoring a content hash on-chain. This reflects a trade-off between privacy exposure and verification strength; future work should evaluate stronger binding strategies (e.g., hashing selected report fields or attachments) while maintaining confidentiality.

Threats to validity should be acknowledged. First, the sample size was limited and purposive, and it may not represent broader CSIRT constituencies or non-technical reporters. Second, the evaluation used a testnet and prototype infrastructure, so observed confirmation behavior and cost characteristics may not generalize to production networks. Third, acceptance results may be influenced by scripted tasks and short-term exposure, whereas real adoption depends on long-term usability, governance, and institutional processes. These limitations motivate broader trials with more diverse participants, along with deployment-oriented evaluation and CSIRT stakeholder validation.

Overall, the findings support the view that Web3 components can strengthen traceability and accountability in incident reporting when integrated carefully with familiar Web2 workflows. The prototype demonstrates early feasibility while highlighting that adoption will depend on usability refinement, incentive governance, and stronger privacy-preserving verification mechanisms.

CONCLUSION

This study developed a hybrid Web2–Web3 cyber incident reporting prototype integrating conventional backend workflows with blockchain anchoring and NFT-based recognition. Functional validation confirmed that the end-to-end process—report submission, off-chain storage, smart contract interaction, event recording, and token issuance—operated as intended. User acceptance results (mean 3.4/5; ~68%) indicate moderate acceptance and suggest that NFT-based recognition may enhance perceived reporting value.

The system demonstrates that on-chain anchoring enables traceability and tamper-evident linkage to off-chain data while preserving privacy. Performance observations on the Arbitrum Sepolia testnet show that transactions can be confirmed within a short time; however, these results are indicative and not representative of production environments. Adoption challenges remain, particularly onboarding friction related to wallet usage and transaction processes.

The novelty of this study lies in presenting an integrated CSIRT-oriented prototype combining (i) a Web2–Web3 stack (React, Laravel, MySQL), (ii) event-based on-chain anchoring linked to off-chain records, and (iii) NFT-based recognition with administrative validation. This is supported by functional validation, user testing (n=25), and stakeholder walkthroughs (n=5), distinguishing it from prior studies that focus mainly on traceability, decentralization, or anonymity without full system evaluation.

Limitations include the prototype-scale implementation, testnet dependency, purposive sampling, and the use of pointer-based anchoring rather than stronger cryptographic binding. Future work should involve real-world CSIRT deployment, improved usability for non-crypto users, stronger privacy-preserving mechanisms (e.g., content hashing), and broader user evaluations. Overall, the study provides early evidence that hybrid Web2–Web3 architectures can enhance traceability and recognition in cyber incident reporting systems.

*name of corresponding author

REFERENCES

Banaeian Far, S., & Rajabzadeh Asaar, M. (2024). A blockchain-based anonymous reporting system with no central authority: Architecture and protocol. (2023). *Cyber Security and Applications, 2*, 100032. https://doi.org/10.1016/j.csa.2023.100032

Brownlee, N., & Guttman, E. (1998). *Expectations for computer security incident response (RFC 2350)*. Internet Engineering Task Force (IETF). https://doi.org/10.17487/RFC2350

Diallo, E.-H., Abdallah, R., Dib, M., & Dib, O. (2024). Decentralized incident reporting: Mobilizing urban communities with blockchain. *Smart Cities, 7*(4), 2283–2317. https://doi.org/10.3390/smartcities7040090

Forum of Incident Response and Security Teams (FIRST). (2024). *CSIRT services framework (Version 2.1)*. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Guan, C., Ding, D., Guo, J., & Teng, Y. (2023). An ecosystem approach to Web3.0: A systematic review and research agenda. *Journal of Electronic Business & Digital Economics, 2*(1), 139–156. https://doi.org/10.1108/JEBDE-10-2022-0039

International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023 Information security, cybersecurity and privacy protection—Information security incident management—Part 1: Principles of incident management*. https://www.iso.org/standard/78973.html

International Organization for Standardization. (2017). *ISO/IEC/IEEE 12207:2017 Systems and software engineering—Software life cycle processes*. https://www.iso.org/standard/63712.html

Khan, B. U. I., Goh, K. W., Khan, A. R., Zuhairi, M. F., & Chaimanee, M. (2024). Integrating AI and blockchain for enhanced data security in IoT-driven smart cities. *Processes, 12*(9), 1825. https://doi.org/10.3390/pr12091825

Ma, W., Wei, X., & Wang, L. (2024). A security-oriented data-sharing scheme based on blockchain. *Applied Sciences, 14*(16), 6940. https://doi.org/10.3390/app14166940

Marbouh, D., Simsekler, M. C. E., Salah, K., Jayaraman, R., & Ellahham, S. (2021). Blockchain-based incident reporting system for patient safety and quality in healthcare. In M. H. ur Rehman (Ed.), *Trust models for next-generation blockchain ecosystems* (pp. 167–186). Springer. https://doi.org/10.1007/978-3-030-75107-4_7

Nasar, M. (2023). Web 3.0: A review and its future. *International Journal of Computer Applications, 185*(10), 41–46. https://doi.org/10.5120/ijca2023922776

Nelson, A. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST SP 800-61r3)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Philip, A. O., & Saravanaguru, R. A. K. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences, 34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Putz, B., Vielberth, M., & Pernul, G. (2022). BISCUIT: Blockchain security incident reporting based on human observations. In *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES 2022)*. ACM. https://doi.org/10.1145/3538969.3538984

Qurotul Aini, N. A. Y., Rahardja, U., & Santoso, N. P. L. (2023). Skema kredibilitas sertifikat berbasis iLearning gamifikasi blockchain pada Kampus Merdeka. *Jurnal Teknologi Informasi dan Ilmu Komputer, 10*(1), 203–214. https://doi.org/10.25126/jtiik.2023106164

Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems, 3*, 213–248. https://doi.org/10.1016/j.iotcps.2023.05.003

Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications, 5*, 100193. https://doi.org/10.1016/j.bcra.2024.100193

Widayanti, R., Purnama Harahap, E., Lutfiani, N., Oganda, F. P., & Manik, I. S. P. (2021). The impact of blockchain technology in higher education quality improvement. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI), 7*(2), 207–216. https://doi.org/10.26555/jiteki.v7i2.20677

Wu, C.-H., & Liu, C.-Y. (2023). Educational applications of non-fungible token (NFT). *Sustainability, 15*(1), 7. https://doi.org/10.3390/su15010007

Zhu, L., Zhang, J., Zhang, C., Gao, F., Chen, Z., & Li, Z. (2023). Achieving anonymous and covert reporting on public blockchain networks. *Mathematics, 11*(7), 1621. https://doi.org/10.3390/math11071621

*name of corresponding author