STRIDE Threat Modeling Identifies Risks in Secure Forensic Report Sharing

Risna Purwita Siwi[1*], Yudi Prayudi[2], Niken Dwi Wahyu Cahyani[1]

[1]School of Computing, Telkom University, Bandung, Indonesia

[2]Department of Informatics, Indonesian Islamic University, Yogyakarta, Indonesia

*Coressponding Author Email :purwitasiwi@student.telkomuniversity.ac.id

Abstract. General Background: Secure collaboration in digital forensic investigations requires mechanisms that ensure confidentiality, integrity, and traceability of shared reports. Specific Background: Existing approaches relying on centralized databases and manual verification are vulnerable to tampering and unauthorized disclosure, leading to the development of ShareBlock, a private blockchain-based system integrating Hyperledger Fabric and IPFS for decentralized forensic report sharing. Knowledge Gap: Despite prior evaluations focusing on confidentiality, integrity, and performance, the comprehensive security posture of ShareBlock has not been systematically assessed. Aims: This study aims to conduct a structured threat modeling analysis of ShareBlock using the STRIDE methodology to identify potential security risks. Results: Based on system architecture analysis, threats were identified across six STRIDE categories—spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege—and evaluated using likelihood and impact to construct a risk matrix and propose mitigation strategies. The findings show that while ShareBlock implements encryption before IPFS upload, role-based access control, and blockchain-backed integrity verification, vulnerabilities remain, particularly in on-chain signature verification and privilege isolation. Novelty: This study provides a comprehensive STRIDE-based threat modeling assessment of a blockchain-enabled forensic report sharing system. Implications: The results support the refinement of secure system design and demonstrate the role of structured threat modeling in developing more resilient blockchain-based digital forensic collaboration platforms.

Keywords: STRIDE threat modeling; Digital forensics security; Blockchain forensic sharing; Hyperledger Fabric IPFS; Risk analysis

1 Introduction

Advances in information technology have increased collaboration across many domains [1], [2], including digital forensic investigations that involve multiple stakeholders such as law enforcement investigators and forensic examiners [2]–[5]. The forensic process typically

R. Lomotey et al. (eds.), *Proceedings of the 1st International Conference on Communication and Digital Multimedia 2025 (ICCDM 2025)*, Advances in Social Science, Education and Humanities Research 1020,
https://doi.org/10.2991/978-2-38476-589-8_51

includes evidence handling, specialized analysis, and report generation, some of which may be presented in court [6].Given this diversity of roles, collaboration is essential to ensure accurate and comprehensive investigation outcomes. In practice, collaboration occurs through peer review and second-opinion discussions among examiners, consistent with the Reporting guidelines of NIST SP 800-86 [7], as well as joint interpretation of forensic reports by investigators in coordination with examiners, as recommended by the ACPO Good Practice Guide [8].Despite its importance, collaborative forensic work introduces challenges, including information leakage, unauthorized report modification, inconsistent standards, and trust issues, particularly when reports are exchanged through manual media or centralized systems. These conditions give rise to security threats that must be systematically identified and mitigated, making threat modeling a critical step in evaluating the security of collaborative forensic systems.

To address the limitations of traditional forensic report sharing, blockchain has been adopted as a foundation for secure data management due to its decentralized and immutable properties, which support verifiable records and resistance to tampering [9]–[11].When combined with distributed storage systems such as IPFS, content-based addressing further improves data availability and integrity without dependence on centralized infrastructure [12]. Building on this approach, this study introduces ShareBlock, a private blockchain-based platform using Hyperledger Fabric and IPFS to support secure forensic report sharing. The system employs a hybrid access control model, where Role-Based Access Control (RBAC) limits report creation and digital signing to examiners, and Case-Based Access Control (CBAC) restricts investigators to viewing and commenting on reports within their assigned cases. While prior evaluations have demonstrated that ShareBlock preserves confidentiality, integrity, and performance, its security posture has not been systematically examined. To address this gap, this study applies the STRIDE threat modeling framework to systematically identify possible vulnerabilities and propose suitable mitigation strategies.

The rest of the paper is organized as follows. Section II reviews related work on blockchain based forensic collaboration. Section III describes the system architecture and security design.Section IV presents the analysis results and discussion, and Section V concludes the paper with directions for future research.

2 Related Work

Blockchain has been widely investigated for digital forensics applications, particularly for ensuring the integrity, provenance, and auditability of digital evidence. Prior research indicates that blockchain can securely log evidence metadata, chain-of-custody records, and investigative actions within tamper-evident ledgers, thereby improving transparency and accountability among participating agencies [13], [14]. Several frameworks, including the IoT Forensic Chain (IoTFC) and other blockchain-based forensic models, emphasize the value of immutable logging and support for inter-agency collaboration [4].Nevertheless, despite these advantages, many proposed systems continue to face fundamental challenges.

These include ensuring confidentiality, achieving interoperability, and implementing fine-grained access control, all of which become increasingly complex in multi-organizational settings where examiners and investigators have clearly separated roles and responsibilities.

To address scalability limitations, hybrid designs that combine blockchain with distributed storage have been introduced. Integrations such as IPFSChain and other blockchain IPFS approaches improve availability, traceability, and auditability through off chain, content addressed storage [15]. Provenance oriented systems like ForensiBlock [16] and ForensiCross [17] also contribute by enabling role aware accountability and cross network data synchronization. Despite these advances, confidentiality remains a persistent concern, as sensitive forensic data are often stored unencrypted in IPFS or managed through public blockchains that are unsuitable for forensic workflows [3].In addition, strict enforcement of role separation and organizational privilege boundaries is still uncommon.

While much of the existing research emphasizes functionality, integrity, or performance [13]–[15], comprehensive security evaluations based on formal threat modeling remain limited. Studies from other domains indicate that STRIDE can effectively uncover attack vectors in blockchain enabled systems, as demonstrated in privacy focused health information exchange platforms such as MEXchange [18]. Comparable analyses are rare in digital forensics, even though collaborative investigations involve complex role hierarchies, cross organizational access, and interactions between blockchain and distributed storage. Addressing this gap, the present study conducts a STRIDE based security assessment of ShareBlock, a Hyperledger Fabric IPFS platform for forensic report sharing, and proposes measures to enhance the robustness of blockchain supported forensic collaboration.Unlike prior studies that focus primarily on evidence integrity or system performance, this work focuses on systematically identifying security threats across forensic workflows using the STRIDE framework.

3 System Overview

ShareBlock is designed to support secure and controlled sharing of forensic reports among authorized participants.The system combines a Django-based web application for role and case-aware access control with IPFS for encrypted off-chain report storage, while Hyperledger Fabric serves as the private blockchain to ensure data integrity and traceability. This integrated design provides the foundation for the STRIDE-based threat analysis conducted in this work.

Figure 1 presents the overall architecture of the ShareBlock system, which is designed as a multi layer structure consisting of the user interface, middleware services, blockchain network, and storage components. At the user facing level, the frontend provides a web application that accommodates different categories of users, namely Administrators, Examiners, and Investigators. Access rights are regulated through role based controls, where Administrators oversee account approval and system supervision, Examiners are granted permission to submit and digitally sign forensic reports, and Investigators are confined to viewing and providing comments on reports that belong to cases under their

responsibility. This arrangement supports collaboration while maintaining clear boundaries between roles. The middleware layer serves as an intermediary responsible for encryption, decryption, and digital signature verification, ensuring that access to forensic reports remains secure. Through this mechanism, only authenticated and authorized users are permitted to interact with validated forensic data. Hyperledger Fabric forms the blockchain layer, organizing three role aligned organizations within a single channel and enforcing core functions such as report submission, querying, and audit trail retrieval through smart contracts and endorsement policies. Smart contract logic governs essential operations, including report creation, record querying, and retrieval of immutable audit trails. For data storage, IPFS is used to store encrypted reports off chain, while only essential metadata is recorded on the blockchain to preserve integrity and minimize storage overhead.

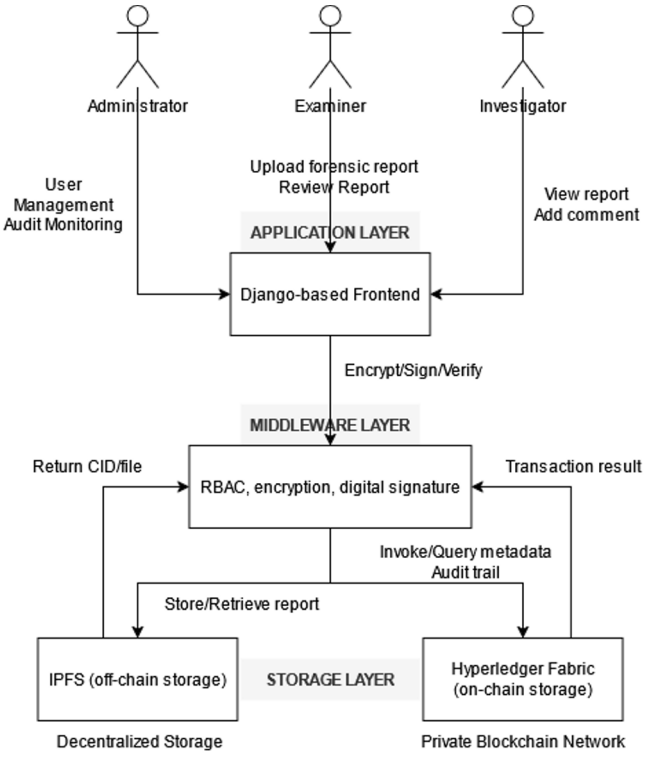

Fig. 1. System architecture of ShareBlock

These layers work together to create an integrated workflow that controls how ShareBlock handles, secures, and checks forensic reports.This architectural structure also

sets the trust boundaries and data flows that the STRIDE-based security analysis in the next section is based on

4 Methodology

This study applies the STRIDE threat modeling framework to systematically evaluate the security posture of the ShareBlock system.The STRIDE model categorizes threats into six types, namely Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.Using this framework, the analysis examines all major system components, including the user interface, the middleware that performs cryptographic operations, the blockchain network, and the IPFS storage layer, with the aim of identifying potential threats and assessing their impact on confidentiality, integrity, and availability.There were four main steps in the threat modeling process:

1. System Decomposition: The system architecture was performed by breaking down the architecture into its fundamental components and defining trust boundaries. It also mapping data flows between users, the Django based web service, the Hyperledger Fabric network, and the IPFS layer.
2. Threat Identification: Possible threat vectors were mapped to STRIDE categories for each component.For instance, spoofing risks were examined within the authentication process, tampering and repudiation were analyzed in relation to chaincode and ledger operations, and possible information disclosure was assessed at the IPFS gateway.
3. Risk Assessment: Each identified threat was assigned a Likelihood (L) and Impact (I) score using a qualitative scale (1 = Low, 2 = Medium, 3 = High). The overall Risk Level (R) was calculated as $R = L \times I$, which then formed the basis for the risk matrix.
4. Mitigation and Control: For threats classified as high risk, appropriate mitigation measures were defined, including the adoption of stronger authentication methods, cryptographic verification, more restrictive access controls, and improved logging to enhance auditability.

Before presenting the results, the identified threats were evaluated using the STRIDE criteria and mapped into a qualitative risk matrix.Table 1 provides an overview of the resulting risk evaluation across the key components of the ShareBlock system.

Table 1. STRIDE Risk Assesment

STRIDE	Component	Description	L	I	R	Mitigation
Spoofing	Auth Service / Fabric MSP	Impersonation using stolen fabric credentials or forged identity during enrollment / approval	2	3	6	MFA for admin approval, validate cert CN/OU, store examiner public key on-chain

Tampering	Chaincode / Ledger (CreateReport)	No on-chain signature check allows attacker (Org2 identity) to submit forged report signatures	3	3	9	Enforce on-chain signature verification, store examiner public key on-chain, validate MSP & user ID
Repudiation	Ledger Logs / Audit	User may deny uploading reports if signatures / timestamps aren't cryptographically validated	2	2	4	Immutable audit trail, enforce signature + timestamp validation
Information Disclosure	IPFS Node / Gateway	CID exposure could reveal content, though files are encrypted before upload	2	2	4	Encrypt files, secure key storage, restrict IPFS gateway, use private IPFS
Denial of Service	Peer Nodes / Orderer	Flooding peers / orderer may delay or block transactions	2	3	6	Rate limiting, resource quotas, monitoring, redundant peer / orderer
Privilege Escalation	Middleware API / Chaincode	Non-examiner tries to create reports; Django blocks it but chaincode lacks MSP attribute checks	1	3	3	Add MSP attribute checks, bind Django role and Fabric identity

5 Results and Discussion

The STRIDE analysis highlights the security posture of ShareBlock by linking potential threats to its system architecture and workflows.Tampering was identified as the paramount risk, as the lack of on-chain signature verification in the CreateReport function permitted an attacker possessing valid Org2 credentials to submit counterfeit signatures. Although the Django layer performs signature validation prior to transaction submission, relying solely on off chain checks limits trust at the blockchain level. Persisting examiner public keys on-chain would allow signature verification to be enforced within the blockchain network itself, thereby strengthening transaction authenticity.

A number of identified threats were evaluated as posing a moderate level of risk, with spoofing and denial-of-service being the most prominent. These risks are largely associated with limitations in off-chain identity management and insufficient redundancy within the network infrastructure. Spoofing may occur when compromised credentials are exploited during user enrollment, whereas denial of service attacks can take advantage of single points

of failure in peer or orderer components. The adoption of multi-factor authentication and the introduction of redundant network elements would significantly reduce both the likelihood and impact of these risks.

Threats evaluated at the lower to medium risk level, including repudiation, information disclosure, and privilege escalation, underscore the need for stronger attribute validation and more robust protection of IPFS gateways. Although encryption and immutable audit logs offer partial mitigation, authorization decisions still depend largely on off-chain mechanisms due to the absence of attribute-based enforcement in the chaincode. Overall, ShareBlock provides a solid security foundation through encryption, immutable ledger records, and role-based access control. Nevertheless, further improvements in identity assurance and transaction-level authentication are required to enhance the reliability and trustworthiness of the platform for collaborative forensic investigations.

6 Conclusion and Future Work

This study applied the STRIDE framework to evaluate ShareBlock, a blockchain–IPFS system for secure sharing of forensic report. The evaluation demonstrates that ShareBlock has a strong security base, supported by encryption mechanisms, immutable ledger storage, and role based access control. Nevertheless, tampering was identified as the most significant threat, while moderate and lower–medium risks point to areas that need additional safeguards, such as off-chain identity checks and IPFS gateway protections.Although the system is secure by design, establishing comprehensive end to end trust requires stronger identity assurance, enhanced transaction level authenticity, and more rigorous on chain authorization controls.

Future work will focus on adding key security controls to the blockchain layer.Some suggested changes are on-chain signature verification, enforcing access based on attributes through MSP attributes, and better identity provisioning through multi-factor authentication. Architectural upgrades, such as peer and orderer redundancy, broader endorsement policies, and hardened IPFS gateways, would further strengthen resilience. In addition, subsequent studies should investigate automated threat detection, real time audit logging, and performance evaluation in multi agency collaboration scenarios. These efforts aim to evolve ShareBlock into a more robust, reliable, and secure platform for digital forensic collaboration.

Acknowledgements. The author would like to express gratitude for the support provided through the Digital Talent Scholarship from the Ministry of Communications and Digital Affairs, Republic of Indonesia.

References

[1] V. Jackson, A. van der Hoek and R. Prikladnicki, "Collaboration Tool Choices and Use in Remote Software Teams: Emerging Results from an Ongoing Study," 2022 IEEE/ACM 15th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE), Pittsburgh, PA, USA, 2022, pp. 76-80, https://doi.org/10.1145/3528579.3529171

[2] Y. Al-Husaini, H. Al-Khateeb, M. Warren, L. Pan, and G. Epiphaniou "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", in Security and Organization within IoT and Smart Cities, K. Ghafoor et al., Ed. Boca Raton: CRC Press, Taylor & Francis Ltd, 2021, pp. 157-180, ISBN: 9780367893330, https://doi.org/10.1201/9781003018636

[3] M. M. Khubrani, "Mobile Device Forensics, challenges and Blockchain-based Solution," 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon), Singapore, Singapore, 2023, pp. 1504-1509, https://doi.org/10.1109/SmartTechCon57526.2023.10391719

[4] S. Li, T. Qin and G. Min, "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems," in IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1433-1441, Dec. 2019, https://doi.org/10.1109/TCSS.2019.2927431

[5] V. R. Silvarajoo, S. Yun Lim and P. Daud, "Digital Evidence Case Management Tool for Collaborative Digital Forensics Investigation," 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 2021, pp. 1-4, https://doi.org/10.1109/CRC50527.2021.9392497

[6] G. A. Kaya and A. Badwan, "Selecting the Best Forensic Report by Using a Group Decision Making Method: A case study on three forensic reports," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 2021, pp. 1-5, https://doi.org/10.1109/ISDFS52919.2021.9486380

[7] K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2006, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

[8] Association of Chief Police Officers (ACPO), *ACPO Good Practice Guide for Digital Evidence*, London, UK: ACPO, 2012, https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[9] Howard E. Poston III, "Blockchain Security from the Bottom Up Securing and Preventing Attacks on Cryptocurrencies, Decentralized Applications, NFTs, and Smart Contracts", John Wiley & Sons, Inc., Hoboken, New Jersey, 2022, 1, Introduction to Blockchain Security, p. 24-25.

[10] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions", Electronics, 13(17), 3568, 2024, https://doi.org/10.3390/electronics13173568

[11] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A blockchain-based chain of custody for evidences management in digital forensics," OpenAccess Series in Informatics, 71, 2020, https://doi.org/10.4230/OASIcs.Tokenomics.2019.12

[12] J. Benet, IPFS - Content Addressed, Versioned, P2P File System. ArXiv, 2014, https://doi.org/10.48550/arXiv.1407.3561

[13] E. Yunianto, Y. Prayudi, and B. Sugiantoro, "B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management", International Journal of Computer Applications. 181, 45, 22-29, 2019, https://doi.org/10.5120/ijca2019918580
[14] E. Nyaletey, R. M. Parizi, Q. Zhang and K. -K. R. Choo, "BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 18-25, https://doi.org/10.1109/Blockchain.2019.00012
[15] J. Hanafi, Y. Prayudi, and A. Luthfi, IPFSChain: Interplanetary File System and Hyperledger Fabric Collaboration for Chain of Custody and Digital Evidence Management, International Journal of Computer Applications 183(41):24-31, 2021, https://ijcaonline.org/archives/volume183/number41/32203-2021921808
[16] A. J. Akbarfam, M. Heidaripour, H. Maleki, G. Dorai, G. Agrawal, "ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability", 2023, https://doi.org/10.48550/arXiv.2308.03927
[17] A. J. Akbarfam, G. Dorai, H. Maleki, "Secure Cross-Chain Provenance for Digital Forensics Collaboration", 2024, https://doi.org/10.48550/arXiv.2406.11729
[18] D. Lee and M. Song, "MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address," in IEEE Access, vol. 9, pp. 158122-158139, 2021, https://doi.org/10.1109/ACCESS.2021.3130552