



Development of a Cryptographic Proof of Creation: A Secure Middleware Approach to Intellectual Property Protection

Okechi Onyedimekwu^{*1}, Moses O. Onyesolu²

^{*1}Department of Computer and Robotics Education,
Federal College of Education (Technical), Omoku, Nigeria
E-mail: okechi@fctomoku.edu.ng
ORCID iD: <https://orcid.org/0000-0001-7663-784X>

²Department of Computer Science,
Nnamdi Azikiwe University, Awka, Nigeria
E-mail: mo.onyesolu@unizik.edu.ng
ORCID iD: <https://orcid.org/0000-0003-3357-4847>

ABSTRACT

Protection of intellectual property (IP) in the digital era has become increasingly challenging due to ease of duplication, rapid dissemination, and weak technical evidence of authorship. Existing approaches such as copyright registration, blockchain timestamping, and watermarking provide partial solutions but fail to simultaneously guarantee confidentiality, authorship binding, and non-repudiation. This paper proposes **SecureCipher-IP**, a cryptographic middleware that provides proof-of-creation and authorship assurance for intellectual property using a dual-signature trust model. SecureCipher-IP is developed using the Secure Software Development Life Cycle and Object-Oriented Analysis and Design Methodology. It integrates cryptographic hashing (SHA-384), authenticated encryption (AES-256-GCM), and elliptic curve digital signatures (ECDSA-P384) to generate verifiable, privacy-preserving evidence of IP ownership, in line with NIST recommendations. The system is designed as an interoperable middleware that integrates with existing legal, academic, and industrial workflows. Analytical evaluation demonstrates that SecureCipher-IP offers stronger security guarantees than registry-based, blockchain-only, and watermarking approaches.

Keywords: SecureCipher, Intellectual Property Protection, Cryptographic Middleware, Digital Signatures, ECDSA, Proof of Creation, AES-GCM, Privacy-Preserving.

1.0 INTRODUCTION

The digital transformation of creative and scientific works has intensified concerns surrounding intellectual property (IP) protection. Digital artifacts such as software, research manuscripts, multimedia content, and engineering designs can be copied, modified, and redistributed at negligible cost. While copyright and patent laws provide legal protection, enforcement typically depends on technical evidence establishing authorship, originality, and time of creation (World Intellectual Property Organization [WIPO], 2020).

Traditional IP protection mechanisms rely on centralized registries and administrative documentation. Although authoritative, such systems are often slow, jurisdiction-dependent, and ill-suited for fast-paced digital innovation (Rose, 2020). To address these limitations, technical approaches including blockchain timestamping, cryptographic hashing services, and digital watermarking have been proposed (Hamza & Pradana, 2022; Chu et al., 2024). However, many of these approaches focus on immutability or traceability while neglecting confidentiality, strong identity binding, and non-repudiation.

This paper introduces **SecureCipher-IP**, a cryptographic middleware designed to provide verifiable proof of creation and authorship for digital IP. Unlike blockchain-centric approaches, SecureCipher-IP emphasizes privacy, cryptographic rigor, and efficiency through a dual-signature trust model, ensuring that both the creator and an independent middleware attest to the existence and ownership of an IP artifact (Al-Zubaidie et al., 2019).

2.0 REVIEW OF RELATED LITERATURE

2.1 Legal and Registry-Based IP Protection

Legal frameworks such as copyright and patent law grant automatic rights to creators, but enforcement often requires external proof of originality and creation time. Institutions such as WIPO provide registration and documentation services that establish priority and ownership (WIPO, 2020). However, these mechanisms are primarily administrative and do not inherently provide cryptographic guarantees of integrity or authorship.

WIPO PROOF introduces a digital evidence service based on cryptographic hashing and timestamping to prove existence at a specific time (WIPO, 2020). While effective for existence verification, it does not cryptographically bind the creator's identity to the artifact, limiting its usefulness in authorship disputes.

2.2 Blockchain-Based IP Protection Systems

Blockchain-based IP systems leverage immutability and decentralized consensus to establish proof of existence and priority (Rose, 2020; Al-Humaimedy, 2025). Several studies propose storing cryptographic hashes of IP artifacts on public or permissioned blockchains to provide tamper-evident records (Chu et al., 2024).

Despite these advantages, blockchain systems introduce challenges related to scalability, transaction cost, latency, and metadata exposure. Moreover, immutability alone does not guarantee authorship unless combined with cryptographic identity verification (Ullah et al., 2023). Public blockchains may also conflict with confidentiality requirements in academic and industrial contexts.

2.3 Hash-Based Fingerprinting and Timestamping

Cryptographic hash functions generate fixed-length digests that uniquely represent digital content, enabling integrity verification without revealing the original data (ScoreDetect, 2023). Hash-based timestamping systems are widely used to establish proof of existence.

However, hashing alone cannot establish ownership or prevent repudiation, as any party with access to the content can generate the same hash (Li et al., 2022). This limitation necessitates additional mechanisms for identity binding and non-repudiation.

2.4 Digital Watermarking Techniques

Digital watermarking embeds ownership information directly into media files such as images, audio, or video. While watermarking enables persistent ownership identification, it alters the original content and may degrade quality (Hamza & Pradana, 2022). Watermarks are also vulnerable to removal, distortion, or re-watermarking attacks.

Hybrid watermarking-blockchain approaches improve traceability but increase system complexity and still rely on trusted intermediaries (Chu et al., 2024).

2.5 Cryptographic Signatures and Secure Middleware

Digital signature schemes such as ECDSA provide authentication, integrity, and non-repudiation. Elliptic curve cryptography offers strong security with lower computational overhead compared to RSA (Al-Zubaidie et al., 2019; Genc & Afacan, 2021). Secure middleware architectures have successfully enforced cryptographic trust in domains such as financial systems and secure communications.

However, existing IP protection systems rarely integrate encryption, hashing, and independent cryptographic attestation into a unified middleware framework (Al-Humaimedy, 2025).

2.6 Research Gap

The literature shows that current IP protection mechanisms address isolated properties such as immutability, integrity, or traceability. None simultaneously ensure confidentiality, authorship binding, non-repudiation, and interoperability. This gap motivates the SecureCipher-IP framework.

3.0 METHODOLOGY

3.1 Design Objectives

SecureCipher-IP is designed to (i) provide cryptographic proof of creation, (ii) bind authorship to IP artifacts, (iii) preserve confidentiality, (iv) enable independent verification, and (v) integrate with existing workflows, consistent with NIST cryptographic guidance (Barker, 2020a).

3.2 System Model and Architecture

The system comprises three entities: the creator, the SecureCipher middleware, and an immutable audit verifier. The creator generates the IP artifact and initiates proof generation. The middleware validates creator claims and issues independent attestation. Verifiers validate proofs without accessing plaintext content.



Fig. 1.1: SecureCipher IP Architectural Flow

The SecureCipher-IP system operates as a middleware framework that cryptographically binds authorship to digital artifacts while preserving confidentiality and integrity. When a creator produces an IP artifact, a SHA-384 hash of the content is computed to serve as a unique fingerprint. This hash is signed with the creator’s ECDSA-P384 private key, generating a signature (Sig_P) that proves authorship and ensures tamper-evidence. For additional privacy, the artifact or its hash may be encrypted using AES-256-GCM, which simultaneously provides confidentiality and an internal integrity check. The signed and encrypted package is then transmitted to the SecureCipher middleware for further processing.

Upon receiving the creator's package, the middleware verifies Sig_P to confirm the artifact's authenticity and integrity. Once validated, the middleware applies its own ECDSA-P384 signature (Sig_S) to produce a dual-signed record, which is stored in an append-only audit log and optionally returned to the creator as a proof-of-creation receipt. This dual-signature model ensures that neither the creator nor the middleware can unilaterally forge or alter the record, providing non-repudiation. Third parties can independently verify ownership by recomputing the SHA-384 hash of the artifact and validating both signatures, enabling secure, tamper-evident, and privacy-preserving verification without reliance on centralized registries or public blockchains. Through this workflow, SecureCipher-IP integrates hashing, authenticated encryption, and dual digital signatures into a cohesive system for robust intellectual property protection.

3.3 Cryptographic Primitives

SecureCipher-IP employs SHA-384 for hashing, AES-256-GCM for authenticated encryption, and ECDSA-P384 for digital signatures. These primitives are recommended for long-term security and efficient implementation (Barker, 2020a, 2020b).

3.4 Protocol Workflow

The creator computes a SHA-384 hash of the artifact and signs it using an ECDSA-P384 private key. The signed hash is transmitted to the middleware, which verifies the signature and appends its own ECDSA signature with a timestamp. The resulting dual-signed record is stored in an append-only audit log and returned as proof of creation.

3.5 Security Assumptions

Security relies on proper key management, collision resistance of SHA-384, and the unforgeability of ECDSA under standard cryptographic assumptions (Al-Zubaidie et al., 2019).

4.0 IMPLEMENTATION AND EVALUATION

SecureCipher-IP is implemented using standard cryptographic libraries and deployed as a modular middleware service. Performance analysis indicates that ECDSA signing and AES-GCM encryption incur minimal overhead, making the system suitable for real-time applications (Genc & Afacan, 2021; Gour et al., 2024).

5.0 COMPARATIVE ANALYSIS AND DISCUSSION

Compared with registry-based systems, SecureCipher-IP provides cryptographic non-repudiation rather than administrative evidence (WIPO, 2020). Relative to blockchain-based solutions, it avoids transaction cost and metadata exposure while maintaining verifiability (Rose, 2020; Chu et al., 2024). Unlike watermarking, SecureCipher-IP preserves content integrity and quality (Hamza & Pradana, 2022).

The dual-signature model ensures that neither the creator nor the middleware can unilaterally forge or alter records, strengthening trust and auditability.

6.0 CONCLUSION AND FUTURE WORK

This paper presented SecureCipher-IP, a cryptographic middleware for intellectual property protection. By integrating hashing, authenticated encryption, and dual digital signatures, SecureCipher-IP provides strong proof of creation, authorship binding, and non-repudiation while preserving confidentiality. The framework addresses critical gaps in existing IP protection mechanisms and is suitable for engineering-focused deployment. Future work will explore post-quantum cryptographic integration and decentralized audit anchoring (Gidney & Ekerå, 2021).

REFERENCES

Ahmad, S. A., & Garko, A. B. (2020). A hybrid cryptographic algorithm for data security in the cloud. *African Journal of Management Information System*, 2(2), 35–58. <https://afrijmis.net/wp-content/uploads/2020/07/jmisvol22paper4pagenumb.pdf>

- Al-Humaimedy, A. S. (2025). Intellectual property protection through blockchain: Introducing the SmartRegistry-IP for secure digital ownership. *Future Internet*, 17(10), 444. <https://doi.org/10.3390/fi17100444>
- Al-Zubaidie, M., Zhang, Z., & Zhang, J. (2019). Efficient and secure ECDSA algorithm and its applications: A survey. *International Journal of Communication Networks and Information Security*, 11(1), 7–35. https://research.usq.edu.au/download/fc0a146c1dd9d6da09882b6ccfc134e6c84d5402d9b21d404e1fd291d0afc439/615211/ECDSA_survey.pdf
- Barker, E. (2020a). *Recommendation for key management: Part 1 – General* (NIST SP 800-57 Rev. 5). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-57pt1r5>
- Barker, E. (2020b). *Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms* (NIST SP 800-175B Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-175Br1>
- Chu, Y., Li, J., Zhang, H., & Wang, Z. (2024). A blockchain-based privacy-preserving intellectual property authentication method. *Symmetry*, 16(5), 622. <https://doi.org/10.3390/sym16050622>
- Genc, Y., & Afacan, E. (2021). Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. <https://doi.org/10.1109/IEMTRONICS52119.2021.9422589>
- Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5, 433. <https://doi.org/10.22331/q-2021-04-15-433>
- Gour, A., Singh Malhi, S., Singh, G., & Kaur, G. (2024). Hybrid cryptographic approach for secure data communication using block cipher techniques. *E3S Web of Conferences*, 556, 01048. <https://doi.org/10.1051/e3sconf/202455601048>
- Hamza, R., & Pradana, H. (2022). A survey of intellectual property rights protection in big data applications. *Algorithms*, 15(11), 418. <https://doi.org/10.3390/a15110418>
- Li, M., Zhang, Y., Chen, X., & Wang, H. (2022). Information-theoretically secure quantum timestamping with one-time universal hashing. *Algorithms*, 15(11), 418. <https://doi.org/10.3390/a15110418>
- Rose, A. (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. *WIPO Magazine*. World Intellectual Property Organization. <https://www.wipo.int/en/web/wipo-magazine/articles/blockchain-transforming-the-registration-of-ip-rights-and-strengthening-the-protection-of-unregistered-ip-rights-55817>
- ScoreDetect. (2023). Securing digital assets with cryptographic hashing explained. *ScoreDetect Blog*. <https://www.scoredetect.com/blog/posts/securing-digital-assets-with-cryptographic-hashing-explained>
- Ullah, S., Bazai, S. U., Zaland, Z., Ghafoor, M. I., Haider, A., & Hussain, L. (2023). Ownership verification for digital art using smart contract and blockchain technology. In *Proceedings of the 17th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICOSST60641.2023.10414236>
- World Intellectual Property Organization. (2020). *WIPO PROOF: A newly introduced and trusted digital fingerprint*. <https://www.totalserve.eu/en/media-centre/news/wipo-proof-a-newly-introduced-and-trusted-digital-fingerprint/>

Authors' Profiles



Okechi Onyedimekwu is a Computer Science Lecturer and Examination Officer at the Federal College of Education (Technical), Omoku, Nigeria. He holds a B.Eng. in Elect/Elect Engineering (IT Options) from ABU, Zaria, PGDE, M.Sc. in Information Technology, and is about concluding his Ph.D. in Computer Science (Software Engineering) at Nnamdi Azikiwe University, Awka, Nigeria. A member of Computer Professionals Registration Council of Nigeria (CPN) and Teachers Registration Council of Nigeria (TRCN). His expertise is in Software Engineering Design & Modeling, Data Analytics and Applied Cryptography.



Moses Okechukwu Onyesolu, Professor, Department of Computer Science, Nnamdi Azikiwe University, Awka-Nigeria. His research interest is mainly in software engineering which revolves around modeling/simulation, computer security, and artificial intelligence. He is a member Nigerian Computer Society (NCS), Computer Professionals (Registration Council of Nigeria) (CPN), and International Association of Engineers (IAENG), International Association of Computer Science and Information Technology (IACSIT) and European Association for Programming Languages and Systems (EAPLS).