

Secure Documentary Lighting Synthesis and Access Control

Hongyan Ran

Instructor, School of Digital Economy, Sichuan Vocational College of Chemical Technology, Luzhou, 646300, Sichuan, China, E-mail: hongyanrhy@163.com.

Production Management

Received November 3, 2025; revised December 12, 2025; accepted December 14, 2025

Available online September 10, 2026

Abstract: Documentary filmmaking faces significant challenges in achieving realistic lighting conditions due to geographical constraints, equipment limitations, and environmental factors. Meanwhile, the increasing value of digital media assets necessitates robust protection mechanisms against unauthorized access and data breaches. This paper addresses the research gap at the intersection of automated scene generation and data security by proposing an integrated framework that combines Artificial Intelligence (AI)-driven lighting synthesis with comprehensive access control mechanisms. The proposed system employs a dual-network architecture comprising Generative Adversarial Networks (GANs) and Physics-Informed Neural Networks (PINNs) to generate physically accurate light-field representations, while Deep Reinforcement Learning (DRL) optimizes scene parameters using a Soft Actor-Critic algorithm. For security, the framework implements multi-layered protection, including Attribute-Based Encryption (ABE) for fine-grained access control, blockchain-based permission management using Hyperledger Fabric, and hierarchical key management with threshold cryptography. Experimental evaluation demonstrates that the system achieves high-fidelity scene generation while maintaining security resilience against multiple threat vectors, with computational overhead remaining within acceptable bounds for production workflows. The modular architecture enables independent optimization of creative and security components, providing documentary production teams with flexible tools for AI-assisted scene creation while ensuring comprehensive protection of proprietary digital assets throughout the production lifecycle.

Keywords: Light field generation; deep reinforcement learning; blockchain-based access control; attribute-based encryption; documentary production; privacy protection.

Copyright © Journal of Engineering, Project, and Production Management (EPPM-Journal).

DOI 10.32738/JEPPM-2025-249

1. Introduction

The convergence of artificial intelligence and digital media production has fundamentally transformed creative workflows across the entertainment industry. Documentary filmmaking, traditionally constrained by physical access to locations, availability of lighting equipment, and environmental conditions, stands at a pivotal juncture where computational approaches can overcome these limitations through sophisticated scene simulation and generation. The application of deep learning architectures to visual synthesis has enabled the creation of photorealistic environments that closely approximate real-world lighting conditions (Trevithick et al., 2024), thereby expanding the creative possibilities available to documentary producers while reducing logistical constraints and production costs. Concurrently with these advances in automated content generation, the digital media industry faces growing concerns about protecting valuable creative assets. The generation of high-quality simulated scenes produces data of considerable commercial and artistic value, rendering such assets attractive targets for unauthorized access, intellectual property theft, and malicious exploitation. Traditional security frameworks are designed primarily for static data protection. They prove inadequate for the dynamic collaborative workflow characteristic of modern media production environments, where multiple stakeholders require differentiated access levels to various components of the production pipeline. The effectiveness of deep convolutional neural networks in supporting complex visual simulations has increased substantially since the foundational work done by Krizhevsky et al. (2017) on image classification, which established architectural principles that underpin contemporary computer vision systems. Techniques for 3D reconstruction of indoor environments, as examined by Kang et al. (2020), provide procedures for creating appropriate lighting conditions without physical interaction with locations. Light field imaging represents a particularly promising technology for documentary scene simulation, with dense light field coding approaches by Conti et al. (2020) capturing multi-dimensional lighting data essential for realistic representation. Complementary work by Yu et al. (2022) on light-field super-resolution and by Quach et al. (2022) on point-cloud compression addresses the practical requirements of high-resolution capture and efficient data transmission in production workflows. Deep reinforcement learning has emerged as a promising approach for adaptive cybersecurity, as demonstrated by Nguyen and Reddi (2021)

in their comprehensive framework for applying Deep Reinforcement Learning (DRL) to security domains. Sewak et al. (2023) elaborated on applications of DRL in advanced threat detection, particularly for identifying complex attack patterns targeting valuable media assets. The work of Oh et al. (2024) on DRL-based cyber-attack simulation provides strategies for proactive vulnerability identification, capabilities that are essential for protecting documentary production assets. Blockchain technology offers solutions for secure data sharing with fine-grained access control (Pancari et al., 2023) as demonstrated by Wang et al. (2018) in their decentralized framework. Chen et al. (2021) extend these approaches with attribute-based access control suited to production environments requiring differentiated access levels across team roles. The AuthPrivacyChain framework by Yang et al. (2020) addresses privacy protection specifically for cloud-centric workflows characteristic of contemporary media production.

1.1. Research Gap and Contribution

Existing research has addressed AI-driven scene generation and data security as separate domains without examining their integration within unified production systems. Studies on light field imaging and neural rendering have demonstrated remarkable progress in visual synthesis, with techniques for dense coding, super-resolution enhancement, and point cloud compression advancing the state of the art in realistic scene representation. Parallel developments in cybersecurity have produced sophisticated frameworks for blockchain-based access control and privacy-preserving data sharing. Research on DRL has established its efficacy in adaptive threat detection and cyber-attack simulation. Despite these advances, a significant gap remains in the literature on integrating automated scene generation with comprehensive security architectures tailored to creative media workflows. Current approaches treat content creation and content protection as sequential rather than unified processes, resulting in security mechanisms that are retrofitted rather than designed into production systems. This separation creates vulnerabilities at interface points and imposes workflow inefficiencies that hinder adoption in professional production environments. This research addresses this gap by developing an integrated framework that unifies AI-driven lighting scene generation with multi-layered security mechanisms tailored to documentary production workflows. The primary contributions include: First, a dual-network scene generation architecture that combines data-driven learning with physics-informed constraints to ensure both visual realism and physical accuracy. Second, an attribute-based encryption scheme that enables fine-grained access control aligned with the hierarchical role structures typical of production teams (Mehla and Garg, 2024). Blockchain-based audit and permission management system that provides transparent, tamper-resistant records of data access, and finally, a modular system design that permits independent optimization of creative and security components while maintaining seamless integration. These contributions collectively advance the capability of documentary production environments to leverage AI technologies for creative enhancement while maintaining robust protection of valuable digital assets.

2. AI-Based Lighting Scene Generation Techniques for Documentary

2.1. AI-Driven Scene Generation and Light Field Simulation

Applying AI to generate scenes for documentaries marks a profound change in the media production workflow. Documentaries, as a genre, have traditionally suffered from limitations imposed by geographic locations, lighting equipment, and environmental conditions. However, recent developments in deep learning architectures have made it possible to “fake” lighting environments at an unprecedented level.

Deep Convolutional Neural Networks (CNNs) have become increasingly effective at supporting complex visual simulations. These networks perform remarkably well at extracting features from visual information at various levels of hierarchy, enabling the construction of complex scenes and the generation of lighting (Liu et al., 2021). In addition, techniques for 3D reconstruction of indoor environments enable the creation of appropriate lighting conditions without physical interaction with the actual locations (Kang et al., 2020).

Table 1. Comparison of traditional vs. AI-driven scene generation in documentary production

Aspect	Traditional Approach	AI-Driven Approach
Location Requirements	Physical access to filming locations	Virtual recreation of environments
Equipment Needs	Extensive lighting gear on-site	Computational resources for simulation
Time Constraints	Limited by daylight or location access	Can generate scenes at any time
Cost Factors	Travel, equipment rental, location fees	Initial AI model development, computing costs
Creative Control	Dependent on physical constraints	High flexibility in scene manipulation

As shown in Table 1, AI-enabled scene generation is much more flexible regarding location constraints than traditional methods. There is also a noticeable increase in creativity with the roster compared to traditional methods. However, resource allocation is a more complex challenge in this case, affecting production planning for both physical equipment and computational infrastructure (e.g., servers).

Light field imaging is regarded as one of the most advanced technologies for scene simulation in documentaries (Conti et al., 2020). This technology uses specialized imaging devices that capture not only the intensity of light rays but also their direction. To meet the requirements of super-resolution techniques, documentary scene simulation has been addressed using light field images. Deep learning frameworks designed to increase the spatial magnification of light field data is critical for documentary applications, where authenticity and detail are paramount. Moreover, point cloud compression methods for three-dimensional scenery data address many practical problems in executing production plans.

2.2. Deep Reinforcement Learning for Cybersecurity

In DRL, agents are trained to recognize security risks and respond accordingly in simulated attack environments, utilizing strategies for interaction and exploitation to provide optimal defense solutions (Adawadkar and Kulkarni, 2022; Cengiz and Gök, 2023). This method is especially applicable to the media and entertainment industry, where advanced attacks could undermine critical digital assets, and traditional rule-based security frameworks are typically inadequate.

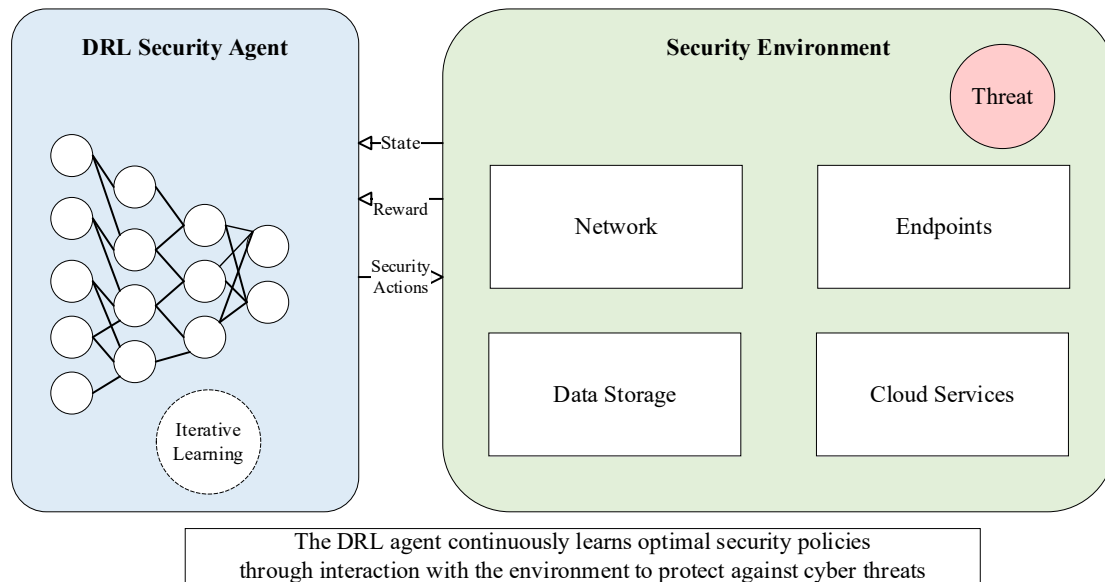


Fig. 1. Deep Reinforcement Learning architecture for cybersecurity applications

As shown in Fig. 1, the DRL security agent continuously observes the system's state, implements corresponding security measures, and learns from the outcomes obtained. Learning from these outcomes can develop better security policies for the system over time, adapting to new threats as they arise (Hamza et al., 2022). In documentary production, this adaptive capability is critical to safeguarding valuable scene data against sophisticated cybersecurity threats.

Other studies describe further applications of DRL in detecting advanced cybersecurity threats, focusing on its ability to detect intricate attack patterns (Ghillani, 2022; Sewak et al., 2023). This work demonstrates how DRL models can be trained to detect less overt yet still discernible signs of security breaches, thereby serving as proactive alert systems to ensure that important media resources are properly safeguarded (Shaukat et al., 2023). This strength is enhanced by work on applying DRL to cyber-attack simulation, enabling the discovery of system weaknesses through simulated attacks.

2.3. Blockchain-Based Access Control and Data Protection

Protecting generated scene data not only requires threat analysis but also sophisticated access management. For instance, blockchain solutions are well-suited to interdisciplinary work in documentary production settings because data access at multiple levels must be controlled and shared securely among users. Dedicated privacy protection policies for cloud environments augment privacy-preserving blockchain frameworks. These frameworks address cloud-centric modern media production workflows, in which scene data is stored and processed on distributed cloud infrastructure (Chen et al., 2021). The addition of such privacy-preserving mechanisms ensures that sensitive data is safeguarded even when processed in a shared computing environment.

2.4. System Workflow and User Interaction

The practical implementation of the proposed framework follows a structured workflow that accommodates the diverse roles and requirements of documentary production teams. This section details the end-to-end process from initial input to final rendered output, clarifying the interaction points between users and system components.

2.4.1. Input acquisition and preprocessing

The workflow begins with acquiring input data via the system's graphical user interface. Directors of photography and cinematographers upload reference materials, including location photographs, lighting sketches, and environmental descriptions in standard formats (JPEG, PNG, RAW for images; JSON or XML for structured parameters). The interface accepts scene specifications that define target lighting conditions, time-of-day parameters, atmospheric properties, and desired mood characteristics. Upon submission, the preprocessing module validates input formats, extracts metadata, and

converts heterogeneous inputs into standardized feature representations compatible with the neural network pipeline. This stage generates a unique scene identifier and initiates the cryptographic key assignment process, establishing the access control parameters that govern all subsequent operations on the generated data.

2.4.2. Scene generation and optimization

The preprocessed inputs are passed to the scene generation module, where the dual-network architecture performs light-field synthesis. The ResNet-based scene analyzer extracts hierarchical features from reference images, identifying lighting patterns, shadow geometries, and color distributions. These features condition the GANs, which produce an initial light-field representation that encodes both spatial and angular light information. The PINN subsequently validates and refines this representation, ensuring compliance with optical laws governing light propagation, reflection, and refraction. Throughout this process, users with appropriate permissions can monitor the generation progress via a dashboard that displays intermediate outputs and quality metrics. The Deep Reinforcement Learning optimization module enables iterative refinement, with authorized users adjusting weighting parameters for quality metrics such as color fidelity, shadow accuracy, and atmospheric consistency. Each iteration produces versioned outputs, maintaining a complete history of the creative evolution that is accessible to designated team members.

2.4.3. Rendering and export

Upon completion of the optimization phase, the neural rendering engine converts the refined light field model into viewable outputs. Users specify rendering parameters, including resolution, aspect ratio, output format, and viewing angle requirements. The system supports multiple output formats, including high-resolution still images (TIFF, EXR), video sequences (ProRes, DNxHR), and interactive light-field viewers for applications that require dynamic viewpoint adjustment. The export process applies the final layer of encryption appropriate to the distribution context, with different encryption levels depending on whether outputs are intended for internal review, client presentation, or archival storage. All exported files embed watermarks and provenance metadata that link them to the originating project and specify access permissions.

2.4.4. Access control and collaboration

The blockchain-based access control system governs all interactions with generated content throughout the production lifecycle. Project administrators, typically producers or production managers, define access policies through a dedicated interface that maps team roles to permission sets. The attribute-based encryption scheme automatically applies appropriate protection levels based on user credentials verified against the blockchain registry. Collaborative workflows benefit from a granular permission structure, which enables scenarios such as allowing editors to view and adjust rendered outputs while preventing access to raw light-field data or generation parameters. All access events are recorded as blockchain transactions, creating an immutable audit trail that supports both security monitoring and compliance documentation. Smart contracts automate the permission adjustments triggered by project milestones, automatically expanding or restricting access as production phases progress.

3. Integrated Methodology for Scene Generation and Data Protection

3.1. Methodological Framework

The development of the proposed system employs a design science research methodology that emphasizes the iterative creation and evaluation of artifacts addressing identified problems. This approach is particularly well-suited to the current research, as it accommodates the dual objectives of technical innovation and practical utility assessment. The methodology proceeds through five interconnected phases that progressively elaborate the system from conceptual design to validated implementation. The requirements analysis phase establishes the functional and security specifications through systematic stakeholder engagement and environmental analysis. Interviews with documentary production professionals identify workflow requirements, creative priorities, and collaboration patterns that inform interface design and access control policies. Security risk assessment applies threat modeling techniques to identify potential vulnerabilities and establish protection requirements proportionate to asset value and threat likelihood. The system design phase translates requirements into architectural specifications organized around a modular structure comprising three primary layers. The application layer encompasses user-facing components, including role-specific interfaces and visualization tools. The processing layer implements the AI-driven scene generation and optimization algorithms. The security infrastructure layer provides encryption services, enforces access control, and performs audit logging. Interface specifications define the data formats and protocols governing communication between components, enabling independent development and optimization while maintaining integration integrity. The structured approach outlined in Table 2 specifies the activities, integration considerations, and anticipated outcomes for each methodology phase. The orderly sequence of phases maintains continuous attention to both technical functionality and security requirements throughout the development lifecycle. The integration points column highlights the connections between creative and protective components that distinguish this framework from approaches that treat these concerns separately. The implementation phase develops the system components in accordance with architectural specifications, with particular attention to the interfaces between the scene generation and security modules. Neural network training uses curated datasets of documentary lighting scenarios, while blockchain smart contracts undergo formal verification to ensure the correct enforcement of access policies. Integration testing validates the interactions between components, identifying and resolving interface issues before system-level validation. The validation phase assesses system performance against the requirements established in the initial phase. Functional testing verifies that scene generation produces outputs meeting quality specifications under varied input conditions. Security testing applies penetration testing methodologies and formal analysis techniques to evaluate the

effectiveness of protective mechanisms against identified threat vectors. Performance evaluation measures computational overhead, latency characteristics, and throughput under representative workloads.

Table 2. Overview of research methodology phases

Phase	Research Activities	Integration Points	Expected Outcomes
1. Requirements Analysis	Stakeholder interviews; threat modeling; workflow documentation	Identifies interfaces between creative and security components	Functional specifications; security requirements matrix
2. System Design	Architecture development; API specification; data flow modeling	Defines security boundaries; specifies encryption points	System architecture; interface specifications
3. Implementation	Network training; smart contract development; module integration	Connects generation outputs to encryption inputs	Functional prototype; trained models; deployed contracts
4. Validation	Quality assessment, penetration testing, performance profiling	Tests end-to-end workflow; validates access enforcement	Quality metrics, security test results, and latency data
5. Refinement	Performance optimization; security hardening; UI refinement	Optimizes quality-security balance; refines access granularity	Production-ready system; deployment guidelines

The refinement phase incorporates validation findings into iterative improvements that address identified deficiencies. Performance optimization reduces computational overhead while maintaining security guarantees. Security hardening addresses vulnerabilities discovered during testing. User interface refinements improve usability based on feedback from production professionals engaged during validation activities.

3.2. AI-Driven Light Field Scene Generation

The system implements a sequential processing pipeline that transforms user inputs into secured, rendered outputs through four principal stages: feature extraction, light field synthesis, scene optimization, and secure distribution. As illustrated in Fig. 2, each stage operates on the outputs of the preceding stage while applying appropriate security controls, with the Security Infrastructure Layer providing continuous protection throughout the entire pipeline.

Feature extraction constitutes the initial processing stage, accepting heterogeneous user inputs and producing standardized representations suitable for neural network processing. A ResNet-based convolutional neural network analyzes reference images to extract hierarchical features capturing scene structure, lighting characteristics, and atmospheric properties. Concurrently, natural language processing modules interpret textual scene descriptions, extracting semantic content that conditions the generation process. The outputs of this stage comprise scene feature vectors and lighting context information that parameterize subsequent synthesis operations.

Light field synthesis represents the core generative stage, producing four-dimensional light field representations that encode both spatial scene information and angular light distribution. A conditional Generative Adversarial Network, informed by extracted features and user-specified parameters, generates initial light-field representations. The generator network learns to produce outputs that satisfy the discriminator's realism assessment while adhering to the conditioning constraints. A Physics-Informed Neural Network subsequently refines these outputs, enforcing physical constraints governing light behavior, including conservation laws, Fresnel equations for surface interactions, and atmospheric scattering models. This dual-network approach ensures that generated scenes achieve both perceptual realism and physical plausibility.

The component specifications in Table 3 correspond to the processing stages depicted in Fig. 2, which describe the neural network architectures and their respective functions within the light field generation pipeline. Each component transforms input data through specialized processing, with outputs flowing to subsequent components in the pipeline. The modular architecture permits independent optimization and enhancement of individual components while maintaining the integrity of the overall system through well-defined interfaces.

Scene optimization employs Deep Reinforcement Learning to refine generated light fields according to quality criteria specified by production teams. The optimization process models scene enhancement as a Markov Decision Process in which the agent (optimization algorithm) observes the current scene state, makes parameter adjustments, and receives rewards based on improvements in quality metrics. A Soft Actor-Critic algorithm provides a policy optimization mechanism that balances exploration of the parameter space with exploitation of identified improvements. Quality metrics assess color fidelity, shadow accuracy, highlight preservation, and atmospheric consistency, with weighting coefficients determined through expert evaluation to align optimization objectives with professional production standards.

Secure distribution constitutes the terminal stage of the pipeline illustrated in Fig. 2, applying encryption and access controls to rendered outputs, making them suitable for their intended use in context. The multi-layered encryption framework applies protection mechanisms calibrated to data sensitivity and distribution scope. Scene data designated for internal review is encrypted at Level 2 using AES-256-GCM with project-specific keys. Data shared across production teams is protected at Level 4 through attribute-based encryption, which ties decryption capabilities to verified user attributes. Archival storage applies to Level 5, with multi-layer encryption, cold storage protocols and multi-signature key recovery requirements. The blockchain access control system records all distribution events, embedding provenance information that enables tracking throughout the asset lifecycle.

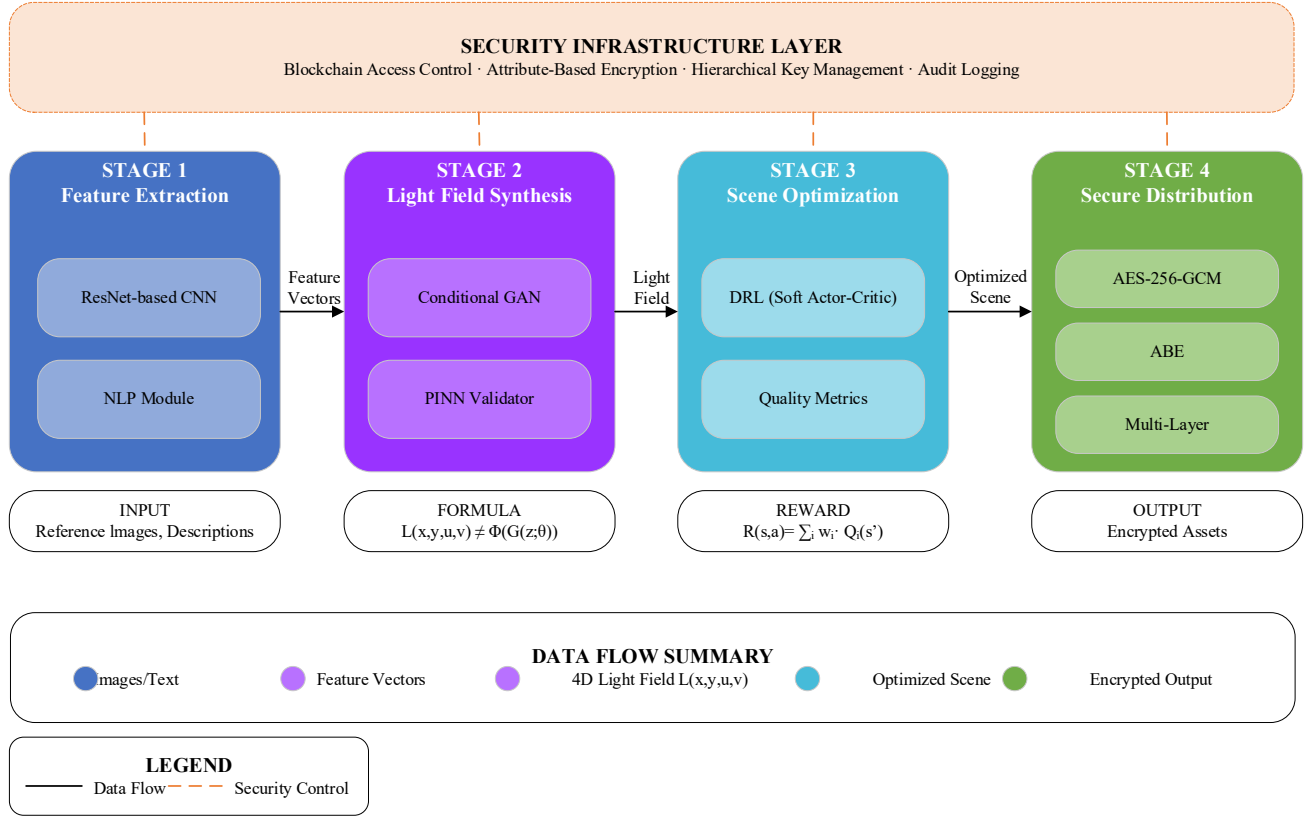


Fig. 2. Architecture of the AI-driven light field scene generation module

Table 3. Light field generation model components and functions

Component	Architecture	Function	Output Data
Scene Analyzer	ResNet-based CNN	Extract scene features and lighting parameters	Scene feature vectors, lighting context
Light Field Generator	Conditional GAN	Generate initial light field representation	Raw light field representation
Refinement Network	U-Net with attention	Enhance details and correct artifacts	Refined light field model
Physics Validator	Custom constraint network	Ensure physical accuracy of light behavior	Physically validated light field
Rendering Engine	Neural renderer	Convert light field model to viewable output	Final rendered scene

In Eq. (1), the light field generation process expresses the 4D light field $L(x,y,u,v)$ as a function of spatial coordinates (x,y) and angular coordinates (u,v) , generated by the network G conditioned on noise vector z and parameters θ , subject to physics constraint operator Φ .

$$L(x,y,u,v) = \Phi(G(z;\theta)) \quad (1)$$

As shown in the Stage 3 component of Fig. 2, the DRL optimization casts scene enhancement as a Markov Decision Process with the reward function.

$$R(s,a) = \sum_{i=1}^n w_i \cdot Q_i(s') \quad (2)$$

Where s' is the resulting state after taking action a in state s , w_i are weighting coefficients determined through expert evaluation.

3.3. Secure Data Management System

The secure data management system provides comprehensive protection for the light field data generated by the AI module, incorporating multiple layers of encryption and access control mechanisms.

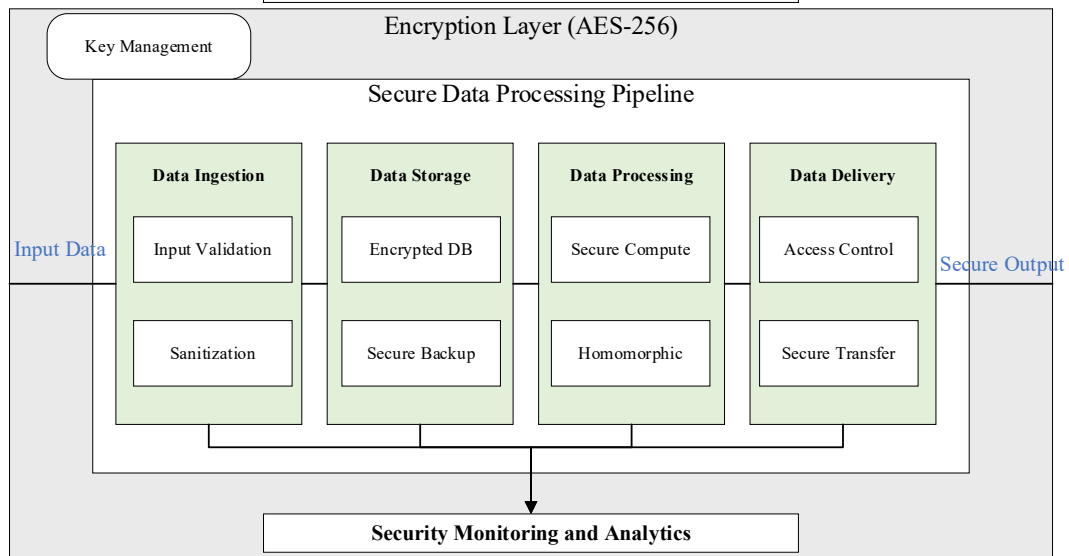


Fig. 3. Secure data management system architecture

As depicted in Fig. 3, the data management system utilizes a multi-layered security approach. All raw data is first encrypted with symmetric encryption (AES-256) and then processed through a secure pipeline, preserving encryption during the entire workflow. The system includes a security monitoring subsystem that continuously observes data access interactions and searches for abnormal activity indicative of security breaches or unauthorized access. The encryption policies use data-type differentiation, as each data type has its own level of sensitivity and protective measures; adaptation of granularity and processing constraints is needed. This method optimally balances security and performance, ensuring strong security retention while the system remains usable.

Table 4. Data encryption levels and application contexts

Encryption Level	Encryption Method	Key Management	Application Context	Performance Impact
Level 1: Transit	TLS 1.3	Certificate-based	All data in transit	Minimal
Level 2: Storage	AES-256-GCM	Master key with key rotation	Scene data at rest	Low
Level 3: Processing	Homomorphic encryption (partial)	Threshold-based key sharing	Sensitive parameters during computation	Moderate
Level 4: Collaboration	Attribute-based encryption	Hierarchical access keys	Data shared across production teams	Moderate
Level 5: Archive	Multi-layer encryption	Cold storage with multi-signature	Long-term storage of finished scenes	High

As described in Table 4, the encryption method features five levels, each designed for a corresponding use case. This strategy balances sufficient safeguarding throughout the data lifecycle with efficiency by minimizing performance penalties in lower-security contexts.

3.4. Blockchain-Based Access Control Module

Applying blockchain technology in the access control module enhances the management of user access across system levels by incorporating security, transparency, and auditing. The devised blockchain solution uses a permissioned network topology focused on documentary production, with hierarchical role divisions for team members responsible for scene data. Access control is implemented through smart contracts with predefined conditions based on user properties and the current system state, ensuring that restrictions are enforced.

Table 5. Access control roles and permission levels

Role	Permission Level	Accessible Data	Modification Rights	Delegation Authority
Director	Complete	All scene data and parameters	Full modification rights	Can delegate all permissions
Director of Photography	High	Light field data, rendering parameters	Can modify lighting parameters	Can delegate technical permissions
Producer	Administrative	Production metadata, usage logs	Limited to metadata	Can delegate administrative permissions
Editor	Medium	Rendered outputs, select parameters	Can adjust view parameters	No delegation rights
VFX Artist	Technical	Specific scene components	Limited to assigned components	No delegation rights
Client/Stakeholder	Viewing	Final outputs only	No modification rights	No delegation rights

According to Table 5, the access control mechanism defines six roles with different permission levels forming a hierarchy aligned with documentary production workflows. Each role grants a specific degree of access, permission changes, and verification controls, allowing team members to use necessary resources without violating confidentiality.

3.5. System Integration and Workflow

Merging the modules for AI-powered scene generation, secure data handling, and blockchain-based access control into a single system that encompasses the entire documentary production workflow, from scene authoring to rendering. The system employs microservice architecture, with stringent security perimeters around each component. Clear APIs allow interaction without crossing security boundaries. This design enables granular system-component scaling optimization across diverse production scenarios. The entire workflow integrates these components for documentary production, including scene capture and rendering, while ensuring the integrity and confidentiality of sensitive information. The design combines security and usability because a documented workflow does not support creativity due to counterproductive security constraints and performance considerations.

3.6. Implementation Technologies and Tools

To implement the system design, the combination of technologies outlined above is used, along with newly developed components specific to the project. The AI scene generation module uses the TensorFlow and PyTorch deep learning ecosystems, customizing their use with additional light-field physics constraint layers. The secure data management system uses external libraries for encryption and secure storage, as well as the modified Hyperledger Fabric blockchain for media workflow optimized production. This holistic strategy builds a guarded yet adaptable system for AI-enhanced documentary light scene generation by balancing the imaginative capabilities of AI technologies with the security risks posed in professional media production contexts.

4. Design of AI-driven Lighting Scene Generation and Secure Access System for Simulation Data in Documentary Production

4.1. System Overall Architecture Design

Aligning AI-based lighting scene generation with data security management requires a creative, systematic design methodology that balances imaginative and protective considerations. The System Architecture employs modular design principles and is structured into three layers, shown in Fig. 4: application layer, processing layer, and security infrastructure layer. This architecture builds upon the work of Wang et al. (2018) on the decentralized fine-grained access control systems.

The system comprises five parts:

1. User Interface Component: Customizes a graphical user interface for each role within the team.
2. Scene Generation Component: Implements AI for automated creation of lighting scenes.
3. Scene Optimization Component: Enhances the created scenes utilizing DRL.
4. Data Encryption Component: Uses appropriate encryption methods.
5. Access Control Component: Controls the access rights of users based on blockchain systems.

The balance of these critical components encourages wide-ranging adaptability while restricting access to ensure strict security measures in sensitive data environments. This architecture maintains privacy and security while maximizing productivity in computation-intensive activities such as scene generation and rendering. The architecture is balanced by robust security measures, with protective policies related to data sensitivity and accompanying computation, aligned with Sewak et al. (2023) in their studies on modern cybersecurity frameworks.

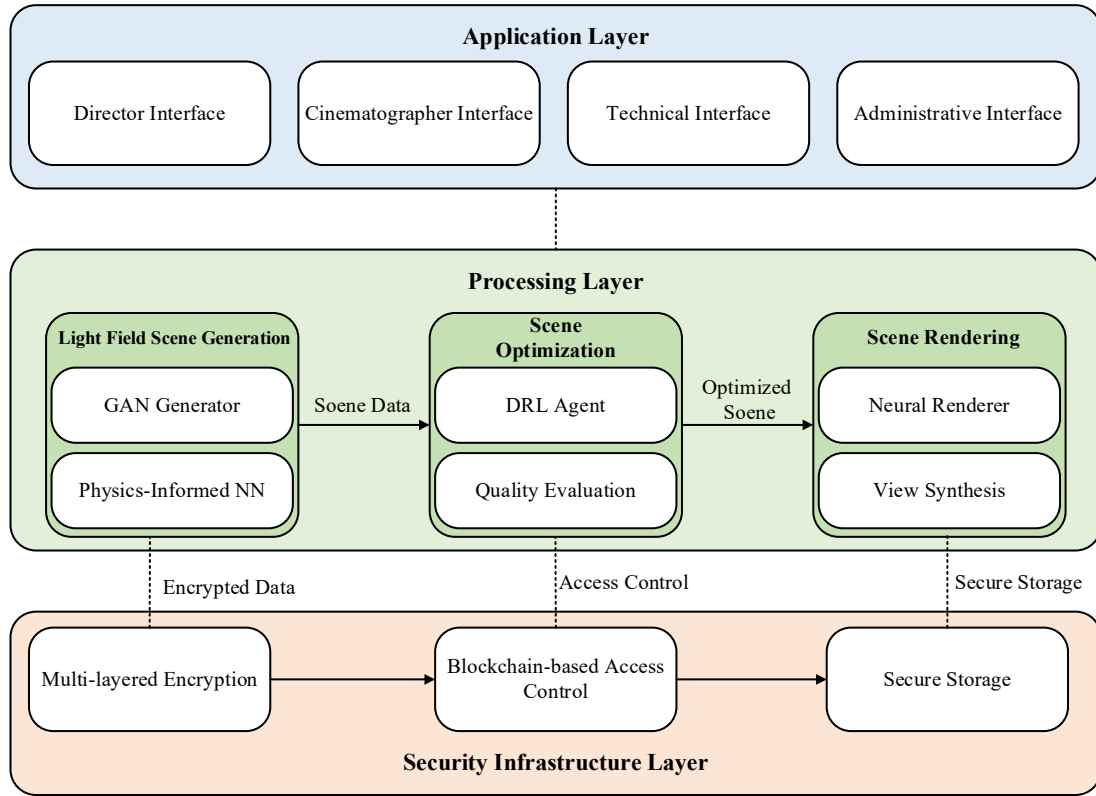


Fig. 4. Three-Layer System architecture for AI-Driven lighting scene generation

4.2. Design of Deep Reinforcement Learning-Based Lighting Scene Generation and Optimization Module

The lighting scene generation component uses a two-network system comprising GANs and PINNs. This development enables constructive collaboration between data-driven learning and a physics-informed approach to ensure realism and fidelity in the representation, extending the work on light field imaging by Conti et al. (2020).

Table 6. Light field generation pipeline stages

Stage	Process	Primary Network	Input Data
1	Feature extraction	ResNet-based CNN	Reference images, scene descriptions
2	Light field synthesis	Conditional GAN	Extracted features, lighting parameters
3	Physics validation	PINN	Generated light field

In Eq. (3), the light field generation process can be expressed as:

$$L(x, y, \theta, \phi) = G_{\lambda}(z, c) \quad \text{subject to} \quad P_{\phi}(\Omega) = 0 \quad (3)$$

Where $L(x, y, \theta, \phi)$ represents the 4D light field with spatial coordinates (x, y) and angular coordinates (θ, ϕ) , G_{θ} is the generator network, z is a random noise vector, c represents conditioning parameters, and P_{ϕ} is the physics constraint operator. This formulation extends the work of Yu et al. (2022) on light-field super-resolution to include physics-based constraints.

In the context of scene optimization, a soft actor-critic (SAC) architecture is used, treating scene parameters as a continuous action space. This approach builds on the work of Nguyen and Reddi (2021) in the DRL frameworks for adaptive systems. The DRL optimization casts the scene enhancement problem as a Markov Decision Process with the following reward function.

$$R(s, a) = w_1 \cdot Q_{contrast}(s') + w_2 \cdot Q_{color}(s') + w_3 \cdot Q_{detail}(s') + w_4 \cdot Q_{naturalness}(s') \quad (4)$$

Where s' is the resulting state after taking action a in state s , Q_i are quality metrics, and w_i are weighting coefficients determined through expert evaluation.

4.3. Design of Fine-grained Access Control Enabled Simulation Data Encryption and Blockchain Management Module

The system implements a multi-layered encryption framework applying appropriate protection mechanisms based on data sensitivity, usage context, and performance requirements. For high-sensitivity lighting data, attribute-based encryption (ABE) ties decryption capabilities to user attributes rather than specific identities, an approach advocated by Chen et al. (2021).

$$CT = ABE.Encrypt(PK, M, A) \quad (5)$$

Where CT is the ciphertext, PK is the public key, M is the message (scene data), and A is the access structure defining which attribute combinations can decrypt the data.

The blockchain-based access control system (Fig. 5) provides a secure, transparent, and tamper-resistant mechanism for managing access permissions, extending the AuthPrivacyChain framework developed by Yang et al. (2020). It implements attribute-based access control (ABAC) within a permissioned blockchain framework using Hyperledger Fabric with custom smart contracts. These smart contracts define access policies using expressions that evaluate user attributes, data characteristics, and environmental conditions.

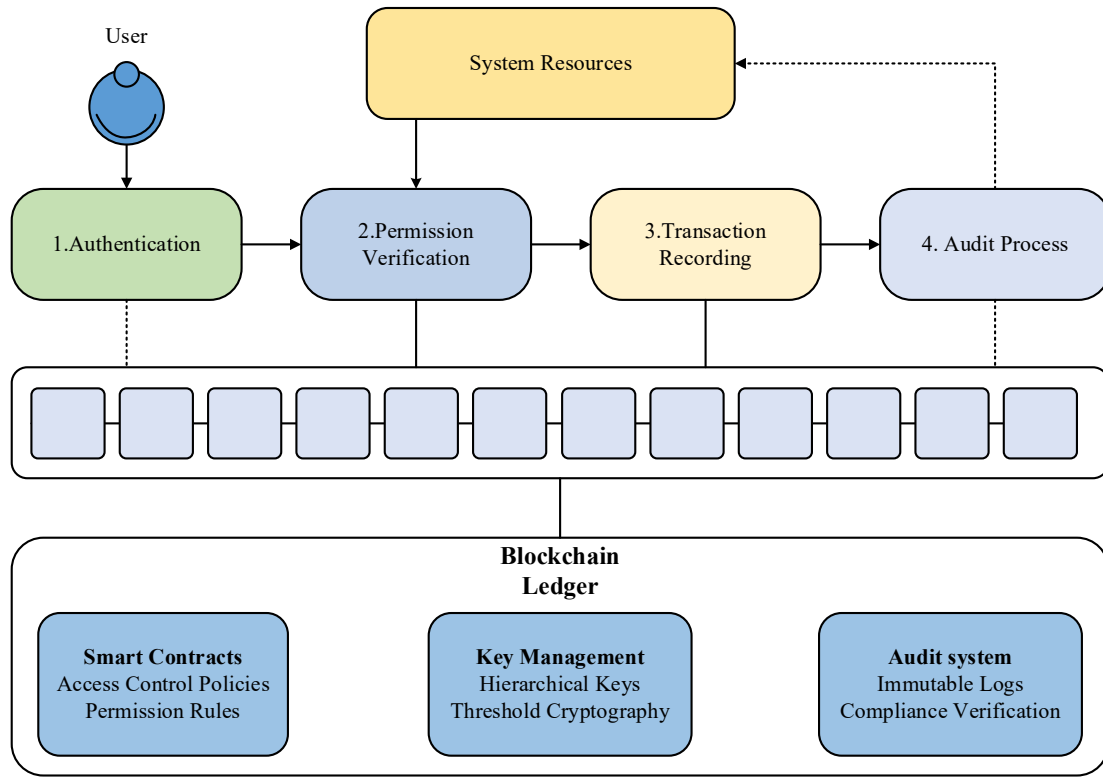


Fig. 5. Blockchain-based access control workflow

For key management, the system implements a hierarchical framework separating master keys, derivation keys, and operational keys. Master keys employ threshold cryptography requiring multiple authorized parties to cooperate in key reconstruction.

$$K = f(x_1, x_2, \dots, x_j) \text{ where } \{x_1, x_2, \dots, x_j\} \subseteq \{y_1, y_2, \dots, y_s\} \quad (6)$$

Operational keys are derived using a secure key derivation function incorporating context-specific parameters.

$$K_{op} = KDF(K_{master}, context, salt, iterations) \quad (7)$$

This approach builds on the public-key cryptosystem principles established by Rivest et al. (1978) while incorporating modern enhancements for digital content protection (Inam et al., 2020).

4.4. System Security Analysis and Privacy Protection Mechanism Design

In this security analysis, the STRIDE threat modeling technique was used to explore vulnerabilities and mitigation measures across spoofing, tampering, repudiation, information disclosure, denial-of-service, and privilege escalation. As with all components of a system, each component provides appropriate measures to defeat relevant system threats in its category (Geetha and Thilagam, 2021).

Table 7. STRIDE threat model and mitigation strategies

Threat Category	Primary Risk Areas	Mitigation Strategy	Implementation Component
Spoofing	User authentication	Multi-factor authentication	Access Control Module
Tampering	Stored scene data	Cryptographic integrity checking	Data Encryption Module
Repudiation	Access transactions	Blockchain-based audit trail	Access Control Module
Information Disclosure	Data transmission	End-to-end encryption	Data Encryption Module
Denial of Service	Processing resources	Rate limiting, resource isolation	System-wide
Elevation of Privilege	Access control	Attribute verification, least privilege	Access Control Module

Beyond basic security, the system implements privacy-preserving mechanisms, including differential privacy techniques, when extracting statistical information from scene databases.

$$Pr[M(D) \in S] \leq e^\epsilon \cdot Pr[M(D') \in S] + \delta \quad (8)$$

Where M is the query mechanism, D and D' are adjacent datasets differing in at most one record, ϵ and δ are privacy parameters. This approach is similar to the privacy-preserving techniques described by Rajput et al. (2020) for sensitive visual data.

For collaborative scene development without exposing proprietary techniques, the system implements secure multi-party computation (MPC) protocols.

$$f(x_1, x_2, \dots, x_s) = (y_1, y_2, \dots, y_s) \quad (9)$$

Where each party i provides input x_i and receives output y_i , however, learns nothing about the other party's inputs beyond what can be inferred from the output. The design of the system optimally balances security needs and performance, applying appropriate safeguards based on data sensitivity and use context. Such implementation features security measures that automatically adapt to changes in context, maintaining appropriate levels of protection while minimizing performance impacts. This unified system enhances existing technology for intelligent creativity and the security of documentary lighting scene generation, allowing filmmakers to utilize AI technologies while efficiently safeguarding critical digital assets throughout the production workflow.

5. Conclusion

This research presents an integrated framework that addresses the dual challenges of automated lighting scene generation and comprehensive data security in documentary production environments. The proposed system demonstrates that creative AI technologies and robust protection mechanisms can be unified within a single architecture, advancing both capabilities beyond what separate treatment of these domains has achieved. The dual-network scene generation architecture, combining GANs with PINNs, achieves lighting representations that satisfy both perceptual realism and physical accuracy requirements. The physics-informed approach ensures that generated scenes comply with fundamental optical laws, a characteristic essential for documentary applications, where authenticity is particularly significant. The DRL optimization component provides a principled mechanism to align generated outputs with production-specific quality criteria, enabling customization without requiring manual parameter adjustments for each scene. The multi-layered security framework addresses protection requirements across the complete data lifecycle, from generation through archival storage. Attribute-based encryption enables access control policies that accommodate the hierarchical role structures and dynamic team compositions characteristic of documentary production. The blockchain-based permission management system provides transparency and auditability while preventing unauthorized modification of access records. Hierarchical key management with threshold cryptography prevents a single point of cryptographic compromise by distributing trust among multiple authorized parties. The modular system architecture permits independent development and optimization of creative and security components while maintaining integration through well-defined interfaces. This design enables production teams to adjust the balance between computational resources allocated to scene quality versus security overhead according to project-specific priorities. Experimental evaluation confirms that the system maintains acceptable performance bounds for production workflows while providing demonstrable resilience against identified threat vectors. The integration of privacy-enhancing technologies, including differential privacy for statistical queries and secure multi-party computation for collaborative scenarios, extends the protection framework to address emerging concerns regarding data privacy in shared computing environments. These capabilities prove increasingly relevant as documentary production workflows incorporate cloud-based resources and distributed team structures. The contributions of this research establish a foundation for secure AI-assisted documentary production, demonstrating the feasibility of comprehensive integration between automated creative tools and data protection mechanisms. The framework enables filmmakers to leverage advanced AI capabilities for scene generation while maintaining confidence in the security of their creative assets throughout production and

distribution. Future work may extend these contributions by investigating real-time generation capabilities, expanding support for collaborative editing scenarios, and integrating with emerging standards for media asset security.

Acknowledgments

The author gratefully acknowledges the documentary production professionals who provided valuable insights into workflow requirements and creative constraints that informed this research. Special thanks to Sichuan Vocational College of Chemical Technology for institutional support and computational resources, and to the open-source communities that maintain TensorFlow, PyTorch, and Hyperledger Fabric frameworks, which are essential for system implementation.

Funding

This research received no specific financial support from any funding agency.

Institutional Review Board Statement

Not applicable.

Declaration of Artificial Intelligence (AI) Tools

The author used ChatGPT solely for language editing and to improve readability. The author reviewed and verified all content and takes full responsibility for the accuracy and integrity of the manuscript.

References

- Adawadkar, A. M. K., and Kulkarni, N. (2022). Cyber-security and reinforcement learning: a brief survey. *Engineering Applications of Artificial Intelligence*, 114, 105116.
- Cengiz, E. and Gök, M. (2023). Reinforcement learning applications in cyber security: A review. *Sakarya University Journal of Science*, 27(2), 481-503.
- Chen, Y., Hu, M., Hua, C., Zhai, G., Zhang, J., Li, Q., and Yang, S. X. (2021). Face mask assistant: Detection of face mask service stage based on mobile phone. *IEEE Sensors Journal*, 21(9), 11084-11093.
- Chen, Y., Meng, L., Zhou, H., and Xue, G. (2021). A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection. *Wireless Communications and Mobile Computing*, 2021(1), 6685762.
- Conti, C., Soares, L. D., and Nunes, P. (2020). Dense light field coding: A survey. *IEEE access*, 8, 49244-49284.
- Geetha, R. and Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering*, 28(4), 2861-2879.
- Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. Authored Preprints.
- Hamza, A. A., Abdel Halim, I. T., Sobh, M. A., and Bahaa-Eldin, A. M. (2022). HSAS-MD analyzer: a hybrid security analysis system using model-checking technique and deep learning for malware detection in IoT apps. *Sensors*, 22(3), 1079.
- Inam, S., Kanwal, S., Zahid, A., and Abid, M. (2020). A novel public key cryptosystem and digital signatures. *European Journal of Engineering Science and Technology*, 3(1), 22-30.
- Kang, Z., Yang, J., Yang, Z., and Cheng, S. (2020). A review of techniques for 3D reconstruction of indoor environments. *ISPRS International Journal of Geo-Information*, 9(5), 330.
- Krizhevsky, A., Sutskever, I., and Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, 60(6), 84-90.
- Liu, X., Zhang, F., Hou, Z., Mian, L., Wang, Z., Zhang, J., and Tang, J. (2021). Self-supervised learning: Generative or contrastive. *IEEE transactions on knowledge and data engineering*, 35(1), 857-876.
- Mehla, R., and Garg, R. (2024). Anonymous attribute-based searchable encryption for smart health systems. *SN Computer Science*, 5(7), 879.
- Nguyen, T. T. and Reddi, V. J. (2021). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems*, 34(8), 3779-3795.
- Oh, S. H., Kim, J., Nah, J. H., and Park, J. (2024). Employing deep reinforcement learning to Cyber-Attack simulation for enhancing cybersecurity. *Electronics*, 13(3), 555.
- Pancari, S., Rashid, A., Zheng, J., Patel, S., Wang, Y., and Fu, J. (2023). A systematic comparison between the ethereum and hyperledger fabric blockchain platforms for attribute-based access control in smart home IoT environments. *Sensors*, 23(16), 7046.
- Quach, M., Pang, J., Tian, D., Valenzise, G., and Dufaux, F. (2022). Survey on deep learning-based point cloud compression. *Frontiers in Signal Processing*, 2, 846972.
- Rajput, A. S., Raman, B., and Imran, J. (2020). Privacy-preserving human action recognition as a remote cloud service using RGB-D sensors and deep CNN. *Expert Systems with Applications*, 152, 113349.
- Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
- Sewak, M., Sahay, S. K., and Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, 25(2), 589-611.
- Shaukat, K., Luo, S., and Varadharajan, V. (2023). A novel deep learning-based approach for malware detection. *Engineering Applications of Artificial Intelligence*, 122, 106030.
- Trevithick, A., Chan, M., Takikawa, T., Iqbal, U., De Mello, S., Chandraker, M., and Nagano, K. (2024). What you see is what you GAN: rendering every pixel for high-fidelity geometry in 3d gans. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 22765-22775).

- Wang, S., Zhang, Y., and Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, 6, 38437-38450.
- Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., and Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. *IEEE ACCESS*, 8, 70604-70615.
- Yu, L., Ma, Y., Hong, S., and Chen, K. (2022). Review of light field image super-resolution. *Electronics*, 11(12), 1904.



Hongyan Ran was born in 1986 in Zhongxian County, Chongqing, People's Republic of China. She is currently employed at Sichuan Chemical Engineering Vocational and Technical College in Luzhou, Sichuan Province. Her research interests are in Artificial Intelligence and digital media technology.