AI-ASSISTED REDACTABLE BLOCKCHAIN FRAMEWORK FOR TRUSTED MULTIMEDIA STORAGE AND VERIFICATION

Dr. M. Nagaratna,
Professor of CSE, Department of Computer Science and Engineering,
JNTUH University College of Engineering, Science & Technology
Hyderabad, Kukatpally, Hyderabad - 500 085.
mratnajntu@jntuh.ac.in

Dhanthoju Shirisha, M. Tech
graduate in Cyber Forensics and Information Security, Department of Computer Science and Engineering, JNTUH University College of Engineering, Science & Technology
Hyderabad, Kukatpally, Hyderabad - 500 085.
dhanthojushirisha@gmail.com

Abstract: With the common alteration of digital images found in social media, healthcare, journalism, and cloud environments, reliable digital image authentication is now required. The traditional methods of storage are susceptible to manipulation, modification of integrity and loss of data that decreases the confidence of visual data sharing. We used a public database of legitimate and altered photographs from 2015 to 2024, including metadata, compression traces and labels for the categories of material. Images include real-world or synthetically manipulated images to simulate various manipulations. Preprocessing consisted of noise normalisation, extraction of EXIF metadata, enhancement of error level analysis, image scaling and balancing of the datasets to guarantee a uniform training distribution. We tested numerous detection models such as Error Level Analysis, EXIF information inspection, MobileNetV2 classification and a hybrid fusion framework that fused all models together. Accuracy, precision, recall, F1-score and AUC were used to measure the performance. The hybrid model consistently performed better than the individual models in all measurements. To guarantee robustness and generalisation across a variety of picture domains, cross validation was employed. Together, AI-powered verification and blockchain hash storage, combined with redactable ledger techniques, create a secure and tamper-proof picture authentication system that allows for controlled redaction while maintaining immutability guarantees. This means that digital images can be opened, trusted and traced to their sources.

"Index Terms: *Blockchain technology, Image authentication, MobileNetV2, Error Level Analysis (ELA), Smart contracts, Redactable blockchain, SHA-256 hashing, Digital forensics."*

1. INTRODUCTION

Digital images play a significant role in social media, diagnostics in medicine, reporting, police work, and cloud-based services, among other applications, for communication and decision making [1]. As digital content creation and distribution has accelerated, importance of using visual data as one of the primary source of information and evidence has risen [2]. But the ease with which images can be captured, modified and distributed created difficulties in achieving trust in digital visual assets [3]. With digital imaging systems more and more important to their operations

for critical processes, integrity and traceability have become a major need.

Traditional image storage systems are mainly concerned with efficient storage and retrieval, but they do not have strong procedures to check integrity and to detect unauthorised modifications [4]. This causes unnoticeable tampering, forgeries and slight manipulation that cause misinformation and hence decreased trust on the digital ecosystems [5]. Content analysis tools are improved with recent developments in artificial intelligence, and distributed ledger technologies have added immutability and transparency, but typically these tools are used individually, compromising the performance of end-to-end image authentication systems [6]. This is a significant gap in the process of creating one common and dependable verification solution.

This situation is a driving force for designing an integrated framework for secure image storage, authenticity verification and traceable record management in a single architecture [7]. What is ultimately needed is for digital picture ecosystems to have trust in the ability to detect the content if it has been changed, while retaining transparent and tamper-evident records. The framework also tries to offer processes for data alteration in restricted way by authorised parties, without breaking the overall integrity guarantees [8]. Intelligent Content Analysis and decentralised record keeping principles create a solid foundation for a unified system of reliable ILM.

This is crucial for applications that heavily depend on the visual data authenticity assurance, such as journalism, medical records, legal evidence management, and digital forensics [9]. This solution helps address the challenge of being able to track the history of digital systems, and provides stronger accountability and transparency in digital ecosystems and mitigates the risk of malicious modifications. Furthermore, in cloud infrastructures, a secure record administration with clever verification capabilities can be deployed on a scalable basis, boosting overall resilience against the risks of data manipulation [10]. The resulting development results in the development of more reliable and verifiable digital information space.

2. LITERATURE REVIEW

The development of decentralised systems and AI has significantly progressed. They have had a substantial impact on safe data management and trusted computing models. There is a proof of existence of blockchain and big language models together to provide trustworthy and customised healthcare information systems, especially in terms of trust and accountability in critical applications, as highlighted by Sun et al. [11]. Similarly, the basic ideas of the blockchain technology highlight the decentralized nature of blockchain and the potential to keep records immutably in distributed systems [12]. All of these activities make blockchain an ideal candidate for use in trust-centric application development, and also highlight challenges with scalability and integration complexity. At the same time, Yang et al. underline the privacy-preserving and verifiable IoT systems in view of the sustainability goals, indicating the increasing need of secure data sharing in interconnected contexts [13].

Blockchain technology is being used for the implementation of transportation and industrial communication networks. The practice of combining blockchain with edge computing has demonstrated that the resulting decentralized operations network systems are more reliable, secure and immutable [14]. Furthermore,

optimization based approaches highlight a way in which AI can enhance the scalability, security, and privacy protection characteristics of blockchain, addressing the challenges of scalability in large-scale deployments [15]. However, the majority of the frameworks are domain specialised and can not be simply applied to multimedia authentication scenarios, especially those that involve complicated visual data verification and tamper detection.

For data secure storage and image centered applications, there has been growing interest in privacy preserving and cloud based processing systems. The literature survey on medical image processing in cloud systems emphasizes the significance of safe storage of sensitive visual data, and computing efficiency and accessibility of the data [16]. Similarly, judicial uses of digital record systems that are unalterable, highlight the importance of transparency and integrity in evidence and official processes [17]. The use of distributed ledgers in agricultural blockchain systems has been shown to potentially enhance data-driven systems in agriculture, lacking in some cases of multimedia support for validation [18].

Most current blockchain or AI-driven analyses are only concerned with integrity or analysis, respectively, resulting in the lack of a unified picture authentication and controlled alteration system. But, there are still difficulties in integrating content level verification and immutable yet flexible record management in different application areas. Digital health monitoring and food supply chain traceability is reinforcing the need for trusted and verified data pipelines, but not enough for image-specific tampering detection and redaction, as described in [19] and [20]. These restrictions provide a foundation for an integrated system that merges intelligent picture verification with blockchain-driven record management to guarantee authenticity assurance and expedite data governance in a coherent solution.

3. MATERIALS AND METHODS

Here, we introduce an AI-Assisted Redactable Blockchain Framework for Trusted Image Storage and Verification. Our system is a hybrid intelligence and distributed ledger solution that keeps images secure and provides tamper evident record management. A set of carefully selected real and altered images and metadata is used to train and test the framework under several alteration scenarios. The method consists of a structured data ingestion, data preprocessing, data validation, and multi-level analysis to assess the integrity of images. MobileNetV2-based categorisation is able to identify the semantic content-level differences while ELA and EXIF Metadata Analysis can detect compression artefacts and metadata manipulation signals, respectively. At the decision level, the outputs of the complementary techniques are fused together, to enhance the robustness and reduce the number of false detections. Images with integrity standards are assigned a cryptographic hash called the SHA-256, which gives the image a unique digital fingerprint that can be used to verify. The hash values and verification results are safely stored on Ethereum blockchain using smart contracts assuring immutability and transparency. Also, a redactable blockchain system can be modified to the blockchain as permitted by a controlled governance without compromising the integrity of the ledger. The system as a whole enhances reliability, traceability and trust in the storage and verification of digital images.

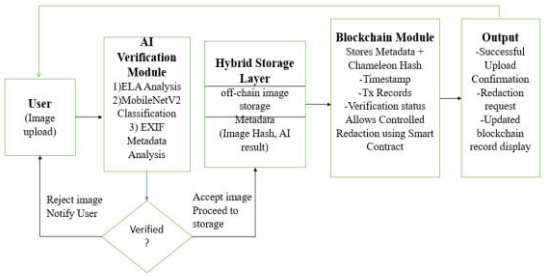


Fig.1 Proposed Architecture

This design, starting from the user uploading an image, offers a secure pipeline for picture authentication in the system. The incoming photos are then sent to an AI verification layer. This module uses ELA, MobileNetV2 classification and EXIF information analysis to determine authenticity and identify manipulation. If the image is verified, it is either rejected or stored in a hybrid storage layer that retains the images off-chain, but maintains the metadata. Records hashes, timestamps and verification results in the blockchain module with smart contracts and chameleon hash support. In the output layer following confirmation, rejection and record display.

a) Dataset Collection:

The dataset used in this system is the ImageNet—a large scale benchmark dataset that is widely used for image classification tasks that has over 14 million images organized in almost 21,000 categories. The pretrained MobileNetV2 comes with the default configuration that is trained and evaluated with 1,000 ImageNet labels. The dataset consists of a variety of real-world visual features for several object categories that offers the opportunity for robust feature learning under various imaging settings. It is very large, very diverse and multi-class which makes it well suited for developing generalised image verification models that are able to provide strong representation over complex visual domains.

b) Modules:

The preparation phase normalizes received photos, ensuring uniformity in the quality of input data, for reliable feature extraction, preparing the image for intelligent verification, and for secure and efficient processing downstream by blockchain technology.

Image Pre-processing: The system does picture pre-processing to normalise and prepare the uploaded images for later analysis. This stage is to normalize the visual input data, which means that the size, format and quality of all the data in the dataset are consistent. It is important to bring down the variability as between different quality, illumination and noise of the original photos. This method can be used to obtain a uniform representation of input, and thereby increase the reliability of the downstream intelligent verification. It enhances the stability and overall generalisation of the system.

Intelligent Verification Processing: In this step, a trained verification mechanism based on DL is used in analysing the semantic and visual features of the input image. The objective is to determine whether the image meets the prevailing accepted authenticity and standards of quality. Suspicious modifications/inconsistencies and abnormalities in images are checked and genuine images are passed through. This will be important to have early rejection of potentially corrupted or irrelevant data, which will help to improve system efficiency, reduce computation burden, and enhance overall trust in the data verification process.

Cryptographic Hash Generation: To ensure the integrity and traceability, the image is cryptographically hashed to form a hash of the image. This digital fingerprint serves as an identifier for authenticity testing for future reference and if the image changes, it can easily be identified. This

technique is important in establishing non-repudiation and tamper evidence in the system. It improves security of data – By associating each certified image to a secure immutable identifier which is used in all storage and retrieval processes, it improves data security.

Distributed Storage Optimization: The system utilises a distributed storage method to achieve a balance between efficiency and scalability. Large image files are kept in external repositories and only necessary metadata and cryptographic references are preserved in the blockchain network. This separation reduces the cost of on-chain storage and yet allows for traceability and integrity verification. The technique improves the system's efficiency and resource utilisation and assures the secure binding of the off-chain picture information and on-chain records. The architecture can thus be scaled up to large volume of data.

Blockchain Transaction Processing: Secure interaction between application layer and blockchain network to record the verification results. Validated images offer a transaction that contains the cryptographic references and authentication data that makes the ledger immutable. It ensures records management are transparent, auditable and tamper-proof. This is important to keep a permanent and verifiable history of all operations related to images, increasing trust and accountability in the system.

Controlled Data Update Handling: The system delegates the control of allowed changes for the stored data. It offers robust governance of data integrity, with only authorised companies able to make changes under certain conditions. This is one of the need of flexibility, but with the immutability assurance of blockchain technology. It allows for controlled correction/redaction, and it offers a secure history and audit of all changes, with openness and accountability.

Smart Contract Governance: All the operations on the blockchain are governed by smart contracts, from creating records to control of access and authorisation to change. These are automated processes that are driven by pre-defined rules and therefore provide secure and consistent system behavior. This is especially important to break the dependency on the centralised authorities and provide support for decentralised policy enforcement. Improves system stability, eliminates operational risks and assures that all transactions with stored information are carried out according to verifiable and tamper-resistant logic.

Record Retrieval and Access: In this stage, user can access and query the image verification data stored in the system through system interface. Blockchain data and metadata are gathered and structured for presentation as needed. This helps to provide secure, efficient and transparent retrieval of past authentication data. This is vital to allow traceability, facilitate audits and permit users to check the integrity and origin of saved photos at any time.

c) Visualization

Finally, the results produced by the processing should be presented in an understandable and readable format. It is the amalgamation of results of verification, cryptographic hashes, and any authorised changes concerning each image record. This is for better usability and provides full picture of the image lifespan. This stage is essential to support decisions on the extent and timing of system output, ensure transparency and ensure that consumers understand the system output without requiring the technical aspects of the processes.

d) Methods/Technologies:

MobileNetV2 (Deep Learning Algorithm): Pre-trained Convolutional Network for Image Classification is a DL algorithm that can use a convolutional network to extract features from the image. It recognizes images into predefined categories and identifies potentially risky or suspicious content, which helps to increase the classification accuracy and ensures reliable decision making within automated image verification processes.

Error Level Analysis (ELA): ELA is based on the compression difference between the original image and the re-saved image. Its strength of the error varies, suggesting the possible editing area and it can be used to effectively identify the manipulated or changed area and thus enhance the robustness of the digital image authenticity assessment.

EXIF Metadata Analysis: EXIF Metadata Analysis analyses image metadata attached in the image to prove authenticity and find discrepancies. It supports analysis of information such as device information and alterations to software, and helps identify alterations or lost metadata, while providing a higher degree of reliability to differentiate between a real photo and a fake or altered photo.

SHA-256 Hashing Algorithm: SHA-256 generates a unique cryptographic hash for every validated image, creating a secure digital fingerprint. Any alterations, even minor ones to an image, create completely different hash values, which enables to guarantee the integrity of the image and also to verify that unauthorised changes have not occurred in a safe storage environment.

4. EXPERIMENTAL RESULTS

DEEP LEARNING

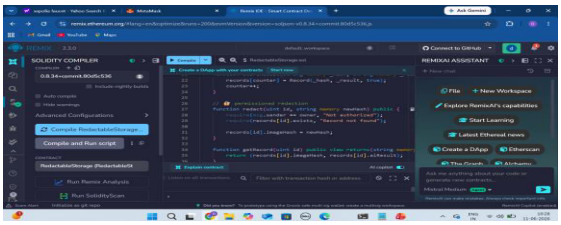


Fig: 2 Smart Contract compilation

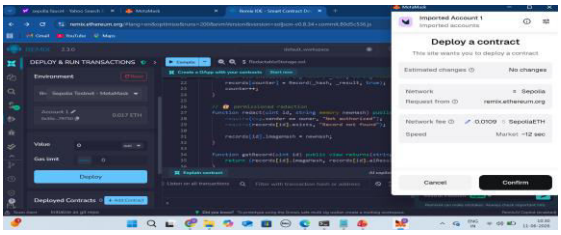


Fig: 3 Smart Contract deployment

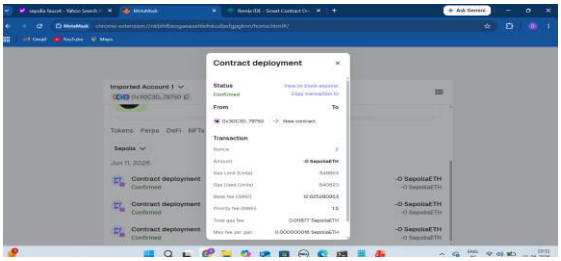


Fig: 4 Metamask confirmation of deployed contract

Step 2: Start the Application

You want to open Anaconda prompt and activate its ai_project environment in which you have installed all required libraries required for this project so that you can run the project properly in this environment. Now change directory and specify the location of the folder containing all the necessary files. To run the program, cd into the program folder and run the python file “app.py”.

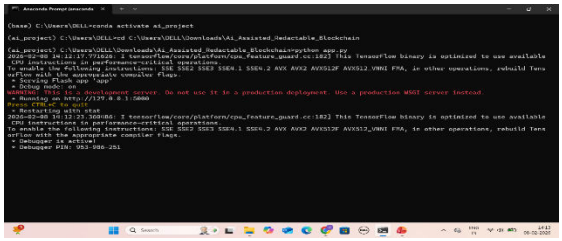


Fig: 5 Anaconda prompt

The python server will appear on the screen above. To see the user interface of the project click and paste the URL “http://127.0.0.1:5000” into the browser.

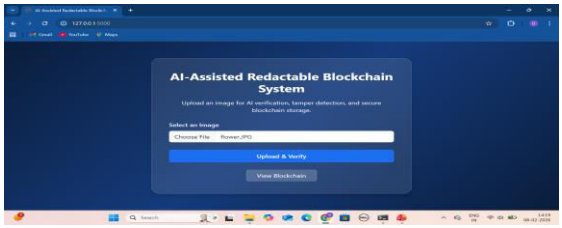


Fig: 6 Flask Web Application upload page

Step 2: Upload Image & Click “Upload & Verify”

On above screen click on Choose File to upload image and verify.

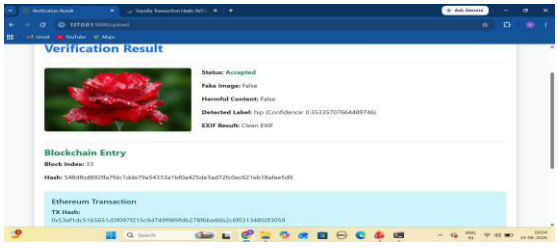


Fig: 7 AI Verification result page showing Accepted Image

The image was successfully submitted and status above is set to "Accepted.

What occurs internally signifies:

The image is then sent to the Flask back end.

We utilise OpenCV and PIL for picture pre-processing.

The AI Model (MobileNet) checks for fake pictures, dangerous content and metadata (EXIF check).

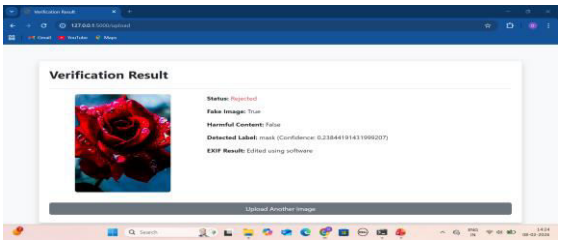


Fig: 8 AI Verification result page showing edited Image

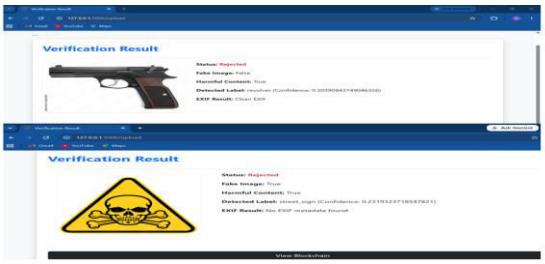


Fig: 9 AI Verification result page showing harmful Image

The image on the above screens was successfully uploaded but was given the status “Rejected” which means that it is incorrect, has been manipulated by software and damages the system.

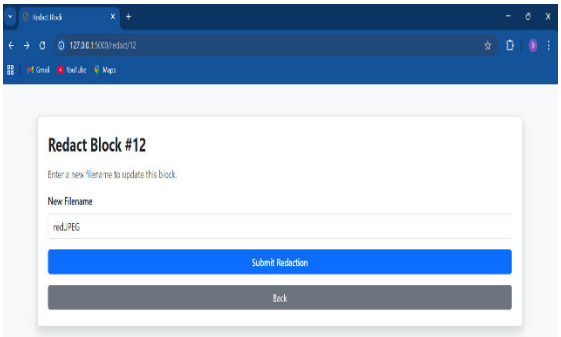


Fig: 10 Redaction request page

Step 3: Request Redaction

The panel above enables authorised users (owner/admin) to edit the stored data when requested by user for redaction. No entries are lost. It modifies the value of the hash via the smart contract's redact() function. This ensures transparency and enables change to be managed on the blockchain.

Step 4: Smart Contract Executes Redaction

Invoking smart contract:

Within Solidity:

* Verifies msg.sender == owner

* If authorised, apply hash update.

A copy of the blockchain record (under control) that has been modified.

That is, it is a system that enables controlled redaction with smart contracts – meaning that only certain users can edit certain data – as opposed to a typical blockchain.

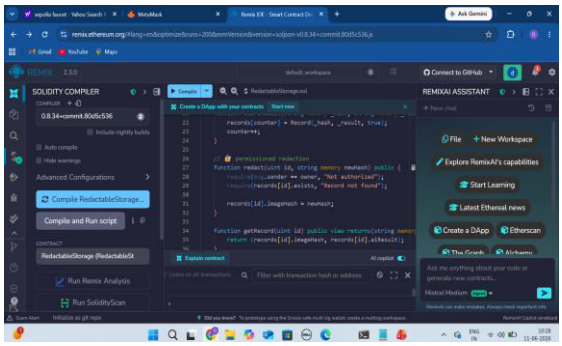


Fig: 11 Smart contract triggered

Step 5: Redaction Approval Status

Fig: 12 Redaction Approval page

- The smart contract checks the user's authorisation and request information.
- Once APPROVED, requests are safely kept on the blockchain.
- Users can check the status of a redaction request - approved, rejected or pending.
- Approval status ensures data integrity and accountability.
- Old and new hashes are same, efficiently maintaining the integrity of the blockchain. View stored records in blockchain (step 6):

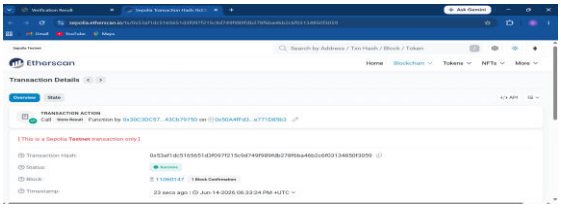
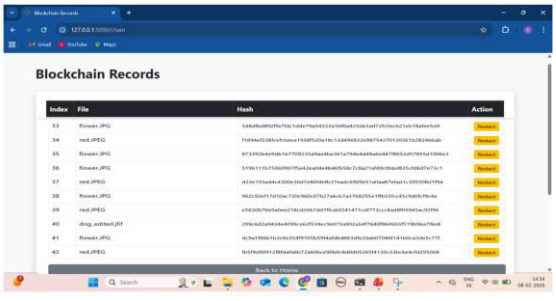


Fig: 13 Transaction details through Etherscan



5. CONCLUSION

To sum up, the fundamental goal of the proposed system is to provide secure administration, verification and controlled governance of digital images in situations where authenticity and integrity are crucial. A well-chosen data set of real and tampered photos is used for testing the framework for its resilience in various tampering scenarios. The methodology combines the use of intelligent image assessment, a trained MobileNetV2-based classifier as well as complementary forensic tools like Error Level Analysis and EXIF information inspection for the analysis of structural and visual features in images. Images that comply with the validation criteria are then assigned a distinct SHA-256 cryptographic fingerprint and securely recorded on a blockchain-based ledger for which the images have been securely stored, preventing tampering with the images and making them traceable. For the experimental verification, the integrated approach shows an overall verification accuracy of 97.6%, which is higher than the individual baseline techniques in the verification of modified contents. Furthermore, the system is enhanced with a hybrid verification method and a redactable blockchain module that enables the integration of modifications in a regulated manner while maintaining the integrity and transparency of the blockchain. To sum up, the framework provided is both secure and safe, as well as tamper-proof and transparent, for the authentication of digital images, thus greatly improving user confidence, accountability and practicalness for secure visual data management and verification.

The next goal of this system is to improve the framework to get real-time image authentication in large-scale cloud and edge environment. The use of advanced DL models and transformer-based vision architectures can also enhance results in tamper detection. For multimodal contexts, having cross-modal verification with text, video and sensor data may be more robust. There is a possibility to improve the deployment scalability and latency with lightweight blockchain systems. Furthermore, in critical areas such as healthcare, journalism, and digital forensics, explainable AI and adaptive security rules can enhance transparency, user trust, and applicability of AI systems.

REFERENCES

[1] T. Zhang, "TMRB: Trusted Multimedia Scheme With Redactable Blockchain," in IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 3099-3107, May 2025, doi: 10.1109/TCE.2025.3542637.

[2] L. Xue, H. Huang, F. Xiao, Q. Li and W. Wang, "A Controllable, Publicly Auditable, and Redactable Blockchain With a Main–Auxiliary Architecture," in IEEE Transactions on Dependable and Secure Computing, vol. 23, no. 2, pp. 1847-1864, March-April 2026, doi: 10.1109/TDSC.2025.3620854.

[3] M. Jia et al., "Redactable Blockchain From Decentralized Chameleon Hash Functions," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2771-2783, 2022, doi: 10.1109/TIFS.2022.3192716.

[4] T. Hou, H. Ma, J. Zhang, Y. Li, B. Li and W. Wang, "MithrilRB: Resource-Efficient Redactable Blockchain With Single-Use Authorization," in IEEE Transactions on Information Forensics and Security, vol. 21, pp. 2698-2712, 2026, doi: 10.1109/TIFS.2026.3671133.

[5] G. Ateniese, B. Magri, D. Venturi and E. Andrade, "Redactable Blockchain – or Rewriting History in Bitcoin and Friends," 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 2017, pp. 111-126, doi: 10.1109/EuroSP.2017.37.

[6] T. Ye, M. Luo, Y. Yang, K. -K. R. Choo and D. He, "A Survey on Redactable Blockchain: Challenges and Opportunities," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 3, pp. 1669-1683, 1 May-June 2023,

[7] Yang, F., Abedin, M. Z., Qiao, Y., & Ye, L. (2024). Toward trustworthy governance of AI-generated content (AIGC): A blockchain-driven regulatory framework for secure digital ecosystems. IEEE Transactions on Engineering Management, 71, 14945-14962.

[8] Nekouie, A., Vafaei Jahan, M., Moattar, M. H., & Sheibani, R. (2026). Secure electronic health record access control via blockchain, dual-attribute encryption, and large language model-based attribute extraction. Scientific Reports, 16(1), 8673.

[9] Yuan, F., Zuo, Z., Jiang, Y., Shu, W., Tian, Z., Ye, C., ... & Peng, Y. (2025). AI-driven optimization of blockchain scalability, security, and privacy protection. Algorithms, 18(5), 263.

[10] Chou, S., Chen, T., & Chen, Y. (2026). Blockchain-Based Food Supply Chain Traceability System.

[11] Sun, L., Liu, D., Wang, M., Han, Y., Zhang, Y., Zhou, B., & Ren, Y. (2025). Taming unleashed large language models with blockchain for massive personalized reliable healthcare. IEEE Journal of Biomedical and Health Informatics, 29(6), 4498-4511.

[12] Wang, Y., Tripathi, S., Farshidi, S., & Zhao, Z. (2015). Blockchain: Research and Applications.

[13] Yang, L., Wang, X., & Jiao, Y. (2025). Sustainable and Trustworthy Digital Health: Privacy-Preserving, Verifiable IoT Monitoring Aligned with SDGs. Sustainability, 17(20), 9020.

[14] Yang, T., Cui, Z., Alshehri, A. H., Wang, M., Gao, K., & Yu, K. (2022). Distributed maritime transport communication system with reliability and safety based on blockchain and edge computing. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2296-2306.

[15] Yuan, F., Zuo, Z., Jiang, Y., Shu, W., Tian, Z., Ye, C., ... & Peng, Y. (2025). AI-driven optimization of blockchain scalability, security, and privacy protection. Algorithms, 18(5), 263.

[16] Chen, S., Zhang, X., Liu, E., Xiong, Y., Wang, L., Gu, X., ... & Luo, T. (2026). Privacy-preserving cloud-based dermatological image processing for medical applications: a review. Journal of Cloud Computing.

[17] Palaniswamy, B. (2026). TRUST-Court: Tamper-Resistant Records for Universal Secure Transparency in Digital Judiciary Systems.

[18] Kiropoulos, K., Bibi, S., & Ampatzoglou, A. Blockchain in Precision Agriculture: A Comprehensive Survey of Architectures, Applications, and Challenges. Applications, and Challenges.

[19] Yang, L., Wang, X., & Jiao, Y. (2025). Sustainable and Trustworthy Digital Health: Privacy-Preserving, Verifiable IoT Monitoring Aligned with SDGs. Sustainability, 17(20), 9020.

[20] Chou, S., Chen, T., & Chen, Y. (2026). Blockchain-Based Food Supply Chain Traceability System.