AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

AN EVIDENTIARY TRUST FABRIC FOR LAW ENFORCEMENT WITH INTEGRITY ANCHORING AND OBSERVABLE CUSTODY STATE EVOLUTION

E. Sravanthi[1*], Pabbathi Laxmiprasanna[2], Mulukutla Jahnavi[2], Kancharla Kritika Reddy[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Kommuri Pratap Reddy Institute of Technology, Ghanpur, Ghatkesar, 501301, Telangana, India.

*Correspondence: E. Sravanthi (sravanthieega26@gmail.com)

ABSTRACT

The increasing reliance on digital systems in law enforcement has emphasized the need for secure, transparent, and reliable mechanisms to manage crime evidence. In existing systems, evidence management is typically handled through centralized databases and manual record-keeping, where crime reports, officer details, and evidentiary materials are stored in a single controlled environment. This approach introduces critical challenges such as data tampering, unauthorized access, loss of sensitive information, and lack of transparency, which can weaken trust and complicate legal proceedings. Furthermore, storing evidence in physical formats or unsecured digital systems makes it difficult to ensure authenticity and maintain a proper Chain of Custody (CoC). These limitations highlight the necessity for a system that ensures data integrity, traceability, and secure verification. To overcome these issues, the proposed framework adopts a decentralized architecture using Blockchain technology and Smart Contracts to provide immutability, transparency, and enhanced security of evidence records. The system leverages Ethereum for decentralized data storage, Web3 for enabling interaction between the application and the blockchain network, and Django as the web framework for managing the user interface, file handling, and administrative functionalities. Authorized officers can securely upload, access, and manage evidence, while administrators can monitor and verify transactions in real time. Each evidence record is assigned a unique identifier and permanently stored on the blockchain, preventing unauthorized modification and ensuring a verifiable audit trail. Although the system does not utilize Machine Learning (ML) or Deep Learning (DL), it effectively employs smart contracts-based automation for secure evidence tracking, thereby improving accountability, legal reliability, and operational efficiency.

Keywords: Digital Evidence Management, Blockchain, Access Control, Evidence Tracking, Digital Forensics

1. INTRODUCTION

Digital Evidence Management Systems (DEMSs) have become fundamental in contemporary criminal investigations, allowing Law Enforcement Agencies (LEAs) to systematically acquire, store, organize, and examine digital evidence in a secure manner. Such evidence includes information derived from computers, smartphones, cloud environments, and various modern digital devices, often serving as crucial proof in determining criminal activity or linking suspects to offenses. With the rapid growth in both the volume and complexity of digital data, DEMSs are now indispensable for maintaining data integrity and ensuring reliable access to information. These systems also play a key role in preserving the chain of custody, where every interaction with evidence must be logged to confirm that it remains unchanged [1]. Across different regions, LEAs have implemented DEMSs ranging from basic digital storage solutions to advanced forensic investigation platforms, supporting activities from crime scene evidence handling to detailed investigative analysis. Historically, LEAs have relied on centralized infrastructures for managing digital evidence, typically using centralized

databases that enable convenient storage, retrieval, and management from a single control point, as highlighted in [2].

These systems incorporate common security practices such as encryption and controlled access to safeguard sensitive information, while digital forensic methodologies follow structured procedures for identifying, collecting, analyzing, and preserving evidence. This process generally involves locating potential data sources, extracting information using specialized tools, and applying techniques like hashing to verify integrity and prevent unauthorized alterations. However, the rapid expansion of cybercrime, often spanning multiple digital platforms, has exposed the limitations of such centralized approaches. The increasing scale and diversity of digital evidence, particularly with the widespread adoption of interconnected digital devices, demand more advanced, scalable, and secure solutions for effective forensic data management while ensuring authenticity and reliability [3]. DEMSs remain critical for LEAs in guaranteeing that digital evidence is properly handled and preserved for legal proceedings, yet the growing data volume introduces significant scalability challenges, including storage limitations, computational demands, efficient data retrieval, and processing constraints. Failure to address these issues can jeopardize both the integrity and availability of evidence. Furthermore, reliance on third-party centralized storage introduces risks such as single points of failure, reduced transparency, and inconsistent governance policies [4].

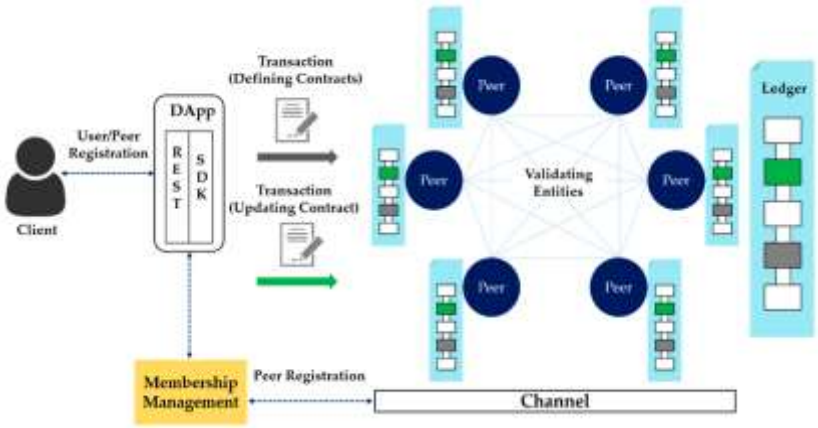

Fig. 1: Digital crime evidence management.

Limited scalability can also lead to operational inefficiencies, causing delays in accessing essential evidence and potentially affecting investigative outcomes. Additionally, digital images, which are widely used as forensic evidence from surveillance systems, mobile devices, and imaging tools, are inherently susceptible to manipulation and tampering, often without easy detection unless robust protective mechanisms are in place [5].

2. LITERATURE SURVEY

Rathod, et al. [6] presented a case study that integrates AI, blockchain, and 6G communication technologies to address data integrity attacks in public safety systems. Their approach utilizes blockchain to ensure secure and tamper-proof data storage, while AI models are used to detect anomalies and improve system intelligence. The inclusion of 6G networks enhances data transmission speed and reliability. The system was evaluated based on performance metrics such as scalability, packet drop ratio, and training accuracy, demonstrating its effectiveness in handling large-scale, real-time data in critical environments. Avelino, et al. [7] introduced BlockProof, a framework designed to verify the authenticity and integrity of web content by leveraging blockchain technology. The system allows content providers to register both static and dynamic web pages on the blockchain, ensuring that any modifications can be tracked and verified over time. It maintains a historical record of all

changes associated with a specific URL, enabling users to validate the originality of content. This approach is particularly useful in combating misinformation and ensuring compliance with data authenticity standards, making it applicable in domains such as journalism and digital evidence verification.

Shevchuk, et al. [8] conducted a comprehensive bibliometric analysis of blockchain applications in emergency management, examining research published between 2017 and 2024. By analyzing collaboration networks, citation patterns, and keyword trends across 248 research articles, the study identified key research clusters and emerging themes in the field. The findings highlight blockchain's growing role in improving transparency, coordination, and efficiency in emergency response systems, while also providing insights into future research directions. Alruwaili, et al. [9] highlighted the complexities involved in capturing and preserving digital evidence, emphasizing its highly volatile nature and the risks associated with improper handling. Their study explains that when systems are compromised, digital forensics becomes essential for identifying, extracting, analyzing, and preserving relevant evidence. The research underscores the importance of following structured forensic procedures to maintain evidence integrity and ensure its admissibility in court. It also points out that even minor mishandling can lead to data corruption or loss, making secure and standardized evidence acquisition methods critical in forensic investigations. Tageldin, et al. [10] discussed the major challenges faced in digital forensic investigations, particularly issues related to data heterogeneity, distributed data sources, and the massive volume of digital information generated in modern environments. These challenges often exceed the processing capabilities of human investigators, leading to delays and inefficiencies in forensic analysis. The study suggested that ML techniques can be leveraged to automate and enhance forensic processes, enabling faster and more accurate analysis of large-scale data.

Batista, et al. [11] carried out a comprehensive systematic literature review to investigate how blockchain technology can address challenges related to maintaining the chain of custody for both physical and digital evidence. By analyzing 26 selected studies, they identified key requirements and design considerations necessary for implementing blockchain-based custody solutions, such as traceability, immutability, and secure access control. Their findings emphasize that blockchain can significantly improve transparency and accountability in evidence handling by providing a decentralized and tamper-resistant record of all custody-related actions, making it suitable for diverse forensic and legal applications. Ellahi, et al. [12] examined the implementation of blockchain technology in food supply chain systems, focusing on its impact on data integrity, transparency, and operational efficiency. Their analysis demonstrated that blockchain's immutable ledger and smart contract capabilities can streamline transactions, reduce administrative overhead, and minimize fraud. The study highlighted how blockchain enhances trust among stakeholders by providing a secure and transparent record of supply chain activities, with potential applicability in digital evidence management systems. Abbas, et al. [13] proposed and implemented a hybrid system that combines blockchain and ML for drug supply chain management and recommendation. Their framework consists of two components: a blockchain-based module built on Hyperledger Fabric to monitor and track drug movement, ensuring transparency and traceability, and an ML-based recommendation module using models such as N-gram and LightGBM to suggest suitable medicines. This integration improves operational efficiency while ensuring secure and verifiable transactions. Shih, et al. [14] developed a blockchain-based reporting scheme designed to securely handle illegal activity reports from submission to reward issuance. The system ensures anonymity and safety for informants while maintaining non-repudiation, preventing denial or alteration of submitted reports. By leveraging blockchain, the framework guarantees data integrity and transparency while also incorporating mechanisms to filter false or malicious reports, ensuring system reliability.

3. PROPOSED METHODOLOGY

The proposed framework introduces an advanced approach to crime evidence management by combining blockchain technology with a web-based digital platform to enhance security, transparency, and reliability. In the existing system, evidence handling depends on centralized databases, which are highly susceptible to data tampering, unauthorized modifications, and potential loss of critical information. To address these challenges, the Evidence Integrity and Transparency Framework for Law utilize smart contract mechanisms within a decentralized blockchain network, ensuring that all records, including crime details and officer information, remain immutable, traceable, and securely verifiable. The system is developed using Django for the web interface and Ethereum integrated through Web3 as the decentralized backend. The Django interface enables administrators and police personnel to interact with the blockchain efficiently without requiring deep technical knowledge. Administrators are responsible for managing officer accounts and overseeing all stored evidence, while officers can securely upload, access, and review case-related information along with supporting images. Each piece of evidence is assigned a unique identifier and permanently recorded on the blockchain through smart contract execution, ensuring non-repudiation and full transparency as shown in Fig. 2.

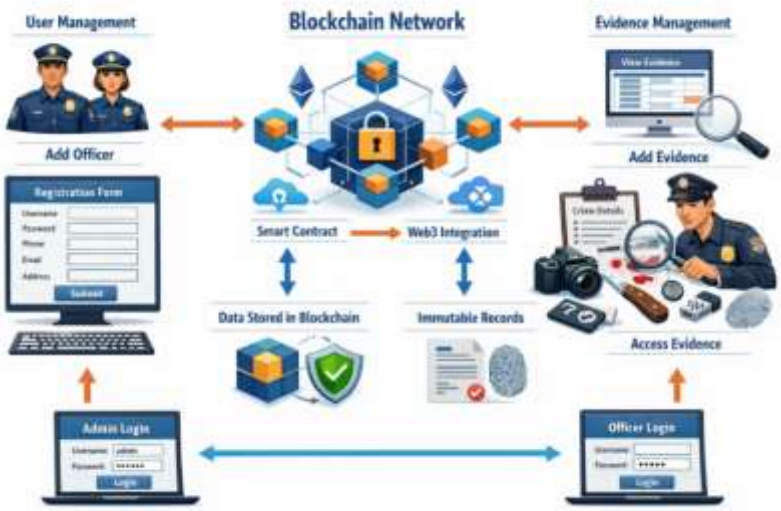

Fig. 2: system architecture for crime evidence.

When new evidence is submitted, the application initiates a blockchain transaction via the deployed Evidence smart contract, capturing key details such as officer identity, case description, witness information, and the incident date. Simultaneously, associated image files are securely stored within the server's file system. Each transaction generates a unique block hash and receipt, which act as verifiable proof of authenticity and data integrity within the blockchain network. Due to the distributed nature of blockchain, all nodes maintain a synchronized copy of the ledger, ensuring continuous data availability even in the event of system failures, thereby providing fault tolerance and reliable recovery. The system interface includes secure authentication modules for both administrators and officers, along with dedicated dashboards and blockchain-based data retrieval functionalities. Administrators can review and validate all records through dynamically generated tables, while officers can submit new evidence, search records using unique IDs, and access previously stored cases. The architecture ensures that once data is recorded, it cannot be altered by any central authority, thereby maintaining the credibility of evidence in legal proceedings. Overall, the framework delivers a tamper-resistant, transparent, and secure environment for handling sensitive crime evidence,

enhancing data authenticity, strengthening trust between investigative and judicial entities, and reducing delays associated with manual verification processes, thus representing a significant advancement in modern forensic data management.

3.1 Ethereum Blockchain

Ethereum is a decentralized blockchain platform that enables execution of smart contracts through the Ethereum Virtual Machine (EVM), as illustrated in Fig. 3. Users initiate transactions via wallets or decentralized applications (DApps), which are broadcast across a peer-to-peer (P2P) network. These transactions are validated and temporarily stored in a mempool before being selected by validators. Using the Proof of Stake (PoS) mechanism, validators propose and finalize blocks containing the transactions. The EVM executes contract logic and updates the global state, maintained as a Merkle-Patricia Trie. The finalized data is stored immutably on-chain and can be accessed via JavaScript Object Notation – Remote Procedure Call (JSON-RPC) or Web3 APIs.

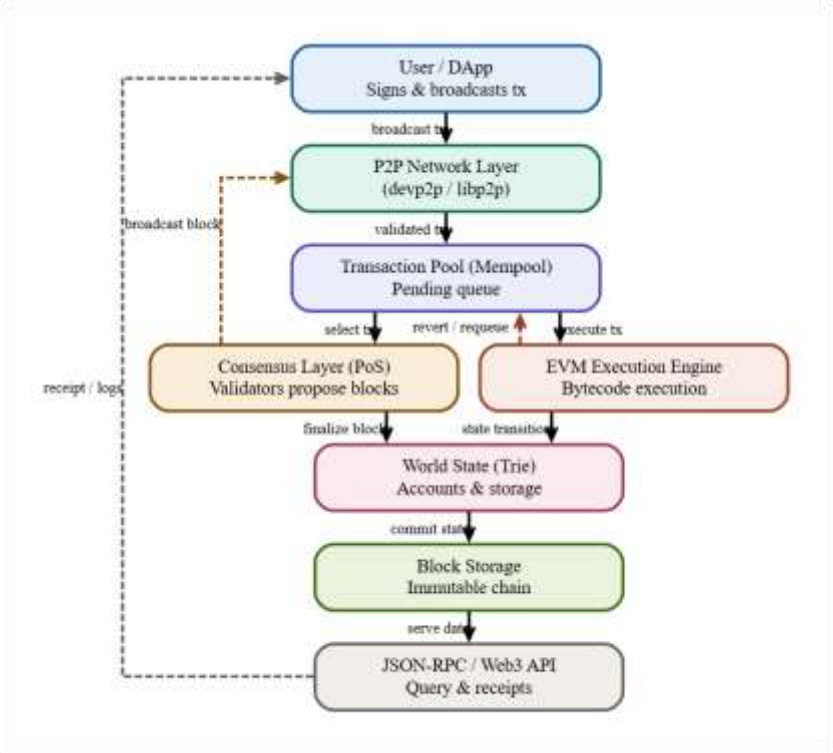

Fig. 3: Internal Workflow of Ethereum.

Transaction Creation & Broadcast: In this step, the user or decentralized application (DApp) initiates a transaction by specifying details such as recipient address, value, and optional smart contract data. The transaction is then digitally signed using the user's private key, ensuring authenticity and non-repudiation. Once signed, the transaction is broadcast to the Ethereum peer-to-peer network, where it becomes visible to multiple nodes for further processing.

2. Network Propagation & Mempool Entry: After broadcasting, the transaction is propagated across the P2P network using gossip protocols, allowing it to reach a large number of nodes efficiently. Each node performs basic validation checks such as verifying the digital signature, checking account balance, and ensuring correct nonce usage. If the transaction passes validation, it is stored in the mempool (transaction pool), where pending transactions are queued and often prioritized based on gas fees.

3. Transaction Selection & Execution: Validators select transactions from the mempool, typically prioritizing those with higher gas fees to maximize rewards. These selected transactions are included in a candidate block and executed within the Ethereum Virtual Machine (EVM). The EVM processes each instruction in the transaction or smart contract bytecode step-by-step, ensuring deterministic execution across all nodes and generating the resulting state changes.

4. Consensus & Block Finalization: Once transactions are executed, validators participate in the Proof of Stake (PoS) consensus mechanism to agree on the validity of the proposed block. Validators attest to the correctness of the block, and through consensus protocols, the block is finalized. Finalization ensures that the block becomes immutable and cannot be altered, providing strong guarantees of data integrity and trust.

5. State Transition & Storage: The execution of transactions leads to updates in the global state, including account balances, contract storage, and other relevant data. These changes are represented using a Merkle-Patricia Trie, which allows efficient verification and storage of state data. The updated state root is committed to the blockchain and stored in block headers, ensuring consistency across all nodes in the network.

6. Data Access & Feedback: After block finalization and storage, the blockchain data becomes accessible through JSON-RPC or Web3 APIs. Users and applications can query transaction receipts, event logs, and current state information. This step completes the interaction cycle by providing feedback to the user, confirming transaction success or failure and enabling further interactions with the Ethereum network.

4. IMPLEMENTATION DESCRIPTION

The Blockchain-Based Evidence Management System has been implemented using Python (Django Framework) integrated with Ethereum Blockchain via Web3. The system allows administrators and police officers to securely manage crime evidence and officer records. All critical data is stored in the blockchain using smart contracts, while multimedia files (like images) are handled locally. The following section describes the key components and functionality of the provided Python code.

Blockchain Initialization and Smart Contract Integration

- **Web3 Connection:** The application uses Web3 to connect with a local Ethereum blockchain
- **Smart Contract Loading:** The smart contract's ABI and deployed address are loaded from Evidence.json, allowing the Python code to interact with Ethereum smart contracts.

Data Fetching from Blockchain

- **User Data (getUsersList()):** Fetches all officer details (username, password, phone, email, police station address) from the blockchain.
- **Evidence Data (getEvidenceList()):** Retrieves crime evidence details from the blockchain, such as evidence ID, officer name, crime details, area, witness name, and crime date.

Admin Functionalities

- **Admin Login:** Admin logs in using predefined credentials (admin/admin).
- **Add Officer (AddOfficerAction):** Admin can register new officers by invoking the createUser smart contract function. It prevents duplicate usernames.

- **View Officers (ViewOfficer):** Displays a table of registered officers by fetching data from the blockchain.
- **View All Evidence (ViewEvidence):** Shows a table of all submitted evidence along with associated images.

Officer Functionalities

- **Officer Login (OfficerLoginAction):** Verifies officer credentials against blockchain-stored data.
- **Add Evidence (AddEvidencesAction):**
  Officers can submit new evidence:
  - Metadata (crime type, witness info, etc.) is stored in the blockchain.
  - Images are stored locally in EvidenceApp/static/files/.
- **Access Evidence by ID (AccessEvidence and AccessEvidenceAction):** Officers can retrieve specific evidence using its unique ID and view details along with the image.

File Management

- **Evidence Image Storage:** Images are saved in the EvidenceApp/static/files/ directory with filenames matching the Evidence ID. Existing images with the same ID are overwritten.
- **File Upload Handling:** The code uses Django's FileSystemStorage to manage file uploads from the web interface.

Smart Contract Transactions

- **Transaction Execution:** Each time officer details or evidence is added, the corresponding smart contract function is invoked with transact ().
- **Transaction Receipt Handling:** The system waits for the blockchain to mine the transaction using web3.eth.waitForTransactionReceipt() to ensure data is committed.

Web Interface Rendering

- **Templates Used:**
  - AdminScreen.html
  - OfficerScreen.html
  - AddOfficer.html
  - AddEvidences.html
  - AccessEvidence.html
  - index.html
- **Dynamic Content:** HTML tables are generated dynamically using Python string concatenation and passed to Django templates via context dictionaries.

Security and Validation

- **Duplicate Checks:** Prevents duplicate officers and evidence entries by checking existing blockchain records.
- **Data Validation:** Basic input validations are performed before transactions are sent to the blockchain.
- **Role-Based Access:** Admin and Officer have different privileges in the system, implemented through role-based routing.

5. CONCLUSION

The research is designed to overcome critical limitations in conventional crime evidence handling, such as data tampering, inefficiencies, and lack of transparency. By utilizing blockchain technology, the system ensures that all evidence records are stored in an immutable and secure manner, enabling complete traceability throughout their lifecycle. It incorporates essential functionalities including officer registration, evidence submission, secure storage of multimedia files, and transparent retrieval mechanisms, thereby establishing a dependable framework for law enforcement operations. The use of smart contracts enables automated and consistent execution of processes without manual intervention, reducing the risk of human error or manipulation. Each evidence record is assigned a unique identifier and permanently recorded on the blockchain, preventing duplication, loss, or unauthorized alterations. In comparison to traditional approaches, the proposed evidence integrity and transparency framework for law enhances accountability, operational efficiency, and overall trust in the criminal investigation process.

REFERENCES

[1] Mifsud Bonnici, J.P.; Tudorica, M.; Cannataci, J.A. The European legal framework on electronic evidence: Complex and in need of reform. In Handling and Exchanging Electronic Evidence Across Europe; Springer: Cham, Switzerland, 2018; pp. 189–234.

[2] Widodo, A.M.; Biyanto, T.R.; Pappachan, P.; Colace, F. Recent Advances in Digital Forensics and Cybercrime Investigation. In Digital Forensics and Cyber Crime Investigation; CRC Press: Boca Raton, FL, USA, 2024; pp. 42–69.

[3] Atlam, H.F.; Ekuri, N.; Azad, M.A.; Lallie, H.S. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. Electronics 2024, 13, 3568.

[4] Klasén, L.; Fock, N.; Forchheimer, R. The invisible evidence: Digital forensics as key to solving crimes in the digital age. Forensic Sci. Int. 2024, 362, 112133.

[5] Kazaure, A.A.; Yusoff, M.N.; Jantan, A. Digital Forensics Investigation Approaches in Mitigating Cybercrimes: A Review. J. Inf. Sci. Theory Pract. (JIStaP) 2023, 11, 14.

[6] Rathod, T.; Jadav, N.K.; Tanwar, S.; Sharma, R.; Tolba, A.; Raboaca, M.S.; Marina, V.; Said, W. Blockchain-Driven Intelligent Scheme for IoT-Based Public Safety System beyond 5G Networks. Sensors 2023, 23, 969. https://doi.org/10.3390/s23020969

[7] Avelino, M.; Rocha, A.A.d.A. BlockProof: A Framework for Verifying Authenticity and Integrity of Web Content. Sensors 2022, 22, 1165. https://doi.org/10.3390/s22031165

[8] Shevchuk, R.; Lishchynskyy, I.; Ciura, M.; Lyzun, M.; Kozak, R.; Kasianchuk, M. Application of Blockchain Technology in Emergency Management Systems: A Bibliometric Analysis. Appl. Sci. 2025, 15, 5405. https://doi.org/10.3390/app15105405

[9] Alruwaili, F.F. CustodyBlock: A Distributed Chain of Custody Evidence Framework. Information 2021, 12, 88. https://doi.org/10.3390/info12020088

[10] Tageldin, L.; Venter, H. Machine-Learning Forensics: State of the Art in the Use of Machine-Learning Techniques for Digital Forensic Investigations within Smart Environments. Appl. Sci. 2023, 13, 10169. https://doi.org/10.3390/app131810169

[11] Batista, D.; Mangeth, A.L.; Frajhof, I.; Alves, P.H.; Nasser, R.; Robichez, G.; Silva, G.M.; Miranda, F.P.d. Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. J. Risk Financial Manag. 2023, 16, 360. https://doi.org/10.3390/jrfm16080360

[12] Ellahi, R.M.; Wood, L.C.; Bekhit, A.E.-D.A. Blockchain-Driven Food Supply Chains: A Systematic Review for Unexplored Opportunities. Appl. Sci. 2024, 14, 8944. https://doi.org/10.3390/app14198944

[13] Abbas, K.; Afaq, M.; Ahmed Khan, T.; Song, W.-C. A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry. Electronics 2020, 9, 852. https://doi.org/10.3390/electronics9050852

[14] Shih, T.-F.; Chen, C.-L.; Syu, B.-Y.; Deng, Y.-Y. A Cloud-Based Crime Reporting System with Identity Protection. Symmetry 2019, 11, 255. https://doi.org/10.3390/sym11020255