A Decentralized Framework for Digital Evidence Management in Open-Source Network Devices at the Transport Layer and Application Level to Ensure Data Integrity

***Abstract*—A decentralized technical framework for secure and efficient digital evidence management is proposed. The framework uses RSA-2048 encryption and IPFS decentralized storage to ensure the confidentiality, integrity, and availability of digital evidence. Smart contracts are used to automate the process of storing and managing digital evidence. The proposed framework has several advantages over traditional digital evidence management systems. First, the decentralized storage network ensures that digital evidence is stored on multiple nodes, making it more difficult for hostile actors to manipulate or damage. Second, the use of smart contracts automates the process of storing and managing digital evidence, which reduces the risk of human error. Third, the framework is transparent and auditable, which allows for accountability and provenance tracking. Fourth, the framework is scalable and can accommodate the growing volume of digital evidence. The proposed framework would be a valuable tool for organizations that need to manage digital evidence securely and efficiently. The framework would be particularly useful to manage digital evidence securely and efficiently investigative proceedings, as it would help to ensure the integrity of the evidence.**

Keywords—blockchain, digital evidence management, RSA-2048 encryption, IPFS, smart contracts, SMEs

I. Introduction

Digital evidence plays a critical role in modern investigative and legal proceedings. However, the availability of such evidence also introduces vulnerabilities that can be exploited by malicious actors, leading to network phishing and injection attacks. Evidence tampering, including modification or untraceable removal from centralized systems, can significantly impact the integrity of collected digital evidence. This issue is further compounded by the alarming increase in reported incidents, as evidenced by the Sri Lanka CERT annual report of 2020, which indicates a staggering 460% rise compared to the previous year [1].

In the context of small and medium-sized enterprises (SMEs), the vulnerability of network and transport layer devices in the TCP/IP Stack poses a significant risk. These enterprises often operate with limited L3/L4 devices, most of which are actively running. Consequently, gathering data from these devices in the event of an incident becomes challenging, as offline data collection is not feasible, and the dynamic nature of the network can result in temporary unavailability of critical data.

To address these challenges and ensure the integrity and security of digital evidence, blockchain technology emerges as a promising solution. Blockchain, as a shared and immutable ledger, offers end-to-end encryption, tamper-free data storage, transparency, and prevention of unauthorized activities. These inherent features make blockchain an ideal platform for supporting evidence management.

While blockchain-based applications and information system development have gained significant attention in recent years, research in the area of blockchain-based evidence management systems remains relatively limited. The primary focus has been on blockchain applications in finance and the Internet of Things (IoT). The scalability of cloud blockchain, its impact on hardware and network infrastructure, and addressing security threats such as 51% attacks, routing attacks, and phishing attacks are still open research challenges.

To ensure data confidentiality and integrity, the proposed framework utilizes RSA-2048 encryption combined with the InterPlanetary File System (IPFS) for decentralized storage. RSA-2048, a popular public key encryption scheme, enables the encryption of files, ensuring that only intended recipients with the corresponding private keys can access the original content. IPFS, on the other hand, provides a distributed storage solution by chunking encrypted files and distributing them across multiple network nodes. The content addressing mechanism in IPFS, based on cryptographic hashes, ensures the integrity of stored data.

The relationship between file size and encryption/upload times is analyzed, highlighting the impact of file size on the overall efficiency of the process. While download times remain consistent and efficient, the decryption and re-encryption processes become time-consuming, particularly for larger files. This emphasizes the importance of considering these factors when evaluating the overall efficiency of the proposed framework. This research also discusses approaches to mitigate bias and judgment in evidence gathering and analysis processes, ensuring accurate and comprehensive findings.

Overall, this research aims to address the challenges of managing digital evidence in the face of network phishing and injection attacks. The proposed framework, leveraging RSA-2048 encryption and IPFS decentralized storage, seeks to enhance the security, integrity, and availability of digital evidence, particularly from network and transport layer level devices. By providing a secure and efficient solution for evidence management, this framework has the potential to significantly benefit organizations, particularly those involved in legal or investigative proceedings, by safeguarding the integrity of digital evidence and preserving its chain of custody.

II. Background

Blockchain technology is a decentralized digital ledger that securely records and verifies transactions. It has evolved beyond its initial application in Bitcoin and is now being used in various fields such as supply chain management, voting systems, and digital identity verification. Blockchain offers advantages like lower transaction costs, increased efficiency, and enhanced security by eliminating the need for intermediaries and reducing the risk of a single point of failure. Different consensus mechanisms, such as proof of work and proof of stake, govern how transactions are validated and recorded on the blockchain. However, there are

challenges regarding scalability and energy consumption that need to be addressed. Despite these challenges, blockchain has the potential to revolutionize transactions, data storage, and trust-building in digital environments.

Ethereum, a blockchain-based platform introduced in 2015, enables developers to create decentralized applications using smart contracts. Smart contracts are self-executing contracts with transaction conditions defined in code, eliminating the need for intermediaries. Ethereum's consensus mechanism, initially based on proof of work, is transitioning to proof of stake for improved energy efficiency and scalability. Ethereum finds significant use in decentralized finance, where individuals can engage in financial activities without relying on traditional institutions. It also has potential applications in supply chain management, digital identity verification, and decentralized autonomous organizations.

While Ethereum offers promising possibilities, it faces challenges related to scalability, security, and regulations. However, the Ethereum community is actively working on solutions, such as scaling techniques and security protocol upgrades. Overall, Ethereum has the potential to transform transactions and decentralize application development. Its unique properties and potential applications make it a subject of interest for further research and development in the blockchain space.

The InterPlanetary File System (IPFS) is a decentralized peer-to-peer system for sharing and storing files. Unlike traditional centralized servers, IPFS distributes files across a network of computers, enhancing security and resistance to censorship. It uses content addressing to efficiently store and retrieve files based on their content. IPFS can cache popular files on multiple computers, improving access speed and scalability. It can also integrate with other technologies like blockchain and distributed ledger technology (DLT), opening up possibilities for decentralized file storage and applications. While IPFS faces challenges in scalability and widespread adoption, the community is actively working on solutions. Overall, IPFS has the potential to revolutionize data storage and distribution on the internet, making it an exciting area of research and development in distributed systems and blockchain.

In the study referenced as [2], researchers have explored the utilization of deep learning and blockchain technology for evidence management in vehicular ad hoc networks. The framework consists of two main components. The first component leverages deep learning algorithms to analyze various safety conditions, including road conditions, traffic flow, past incidents, and speed limits. The second component focuses on storing the identified evidence in a blockchain network. To ensure the integrity and security of the blockchain, access control measures have been implemented to restrict unauthorized users from tampering with or accessing relevant forensic information. The researchers have introduced three types of blockchains: stakeholder chain, Roadside unit chain, and Evidence chain.

In the research study cited as [3], the author has proposed a digital forensic preservation mechanism utilizing blockchain technology and redundancy. The scholar has employed a redundant blockchain system to mitigate attacks targeting a single blockchain chain, thereby reducing the potential impact. Additionally, the researcher has successfully incorporated Hyperledger, a blockchain platform, and introduced dynamic node addition, a unique characteristic not commonly found in Hyperledger.

A research proposal mentioned as [4] focuses on Hyperledger-based evidence management with an emphasis on maintaining the chain of custody. The physical evidence gathered at a crime scene is added to the blockchain by an evidence collection unit referred to as a client. The primary objective of this research is to ensure integrity and maintain a reliable chain of custody using the features provided by the Hyperledger Fabric.

In [5], a framework for digital forensic investigation based on blockchain technology is proposed, specifically targeting the Internet of Things (IoT). This framework involves the collection of data from IoT devices physically. The digital evidence is identified and processed through a blockchain-based evidence management system for investigation and reporting purposes. The resulting information is then uploaded to the blockchain ledgers for access by verification parties. The authors have utilized existing examination tools during the evidence gathering process. However, the framework has yet to address the issue of the 51% majority gaining access power.

In [6], the researcher has designed a two-level blockchain system for digital evidence management. The first blockchain, referred to as the "hot" blockchain, is used to store frequently changing information during an ongoing investigation. The second blockchain, known as the "cold" blockchain, is utilized for storing digital evidence that requires a significant amount of disk space and is not frequently modified. The proposed framework has been implemented using a software virtualization framework called Docker. During experimental testing, the researchers observed a reduction in transaction speed during the storage and retrieval of data.

III. Methodology

A. *Proposed System Architecture*

The proposed system architecture consists of five key components that work together to ensure the integrity and security of data. These components include the user, agent, reporting server, IPFS node, and blockchain network. The user initiates requests for accessing evidence, while the agent collects and uploads the data to the IPFS and blockchain networks. The reporting server serves as an intermediary for agents and generates anomaly and behavior-based detection reports. The IPFS node provides decentralized storage for uploaded files, and the blockchain network acts as a tamper-proof ledger for storing cryptographic keys and validating data integrity. Together, these components form a robust system for secure and transparent data management.

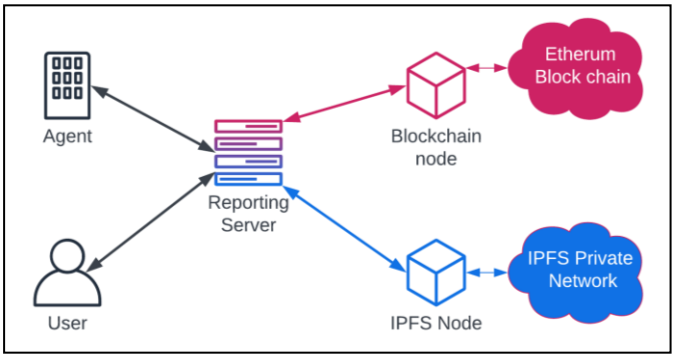


Fig.1. System Diagram

B. System Workflow

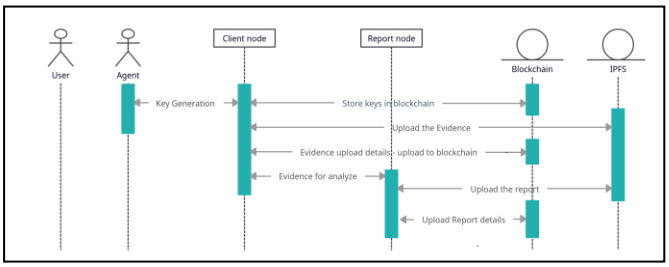


Fig.2. Upload Workflow Diagram

The system architecture ensures a secure and reliable process for accessing and analyzing evidence. The user requests specific evidence, and the reporting server analyzes the data to generate reports. The IPFS node securely stores the files, while the blockchain network maintains keys and records for data integrity and traceability. The agent generates private and public keys, which are stored in the blockchain for secure access. Relevant evidence is uploaded to IPFS and the Report Node, and the Report Node generates a final report, which is also uploaded to IPFS. The blockchain records report details and uploads them to the Report Node, enhancing traceability and transparency. When a user requests files, the report node retrieves the IPFS URL from the blockchain and downloads the encrypted evidence file. The report node then encrypts the file using the user and agent's public keys, ensuring confidentiality.

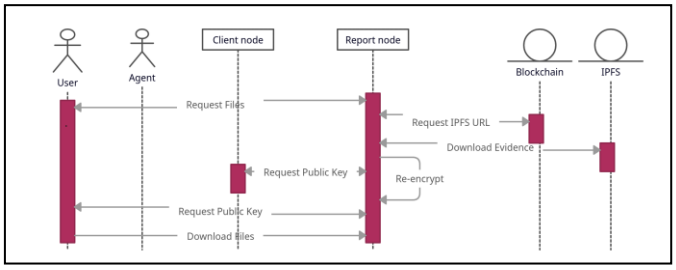


Fig.3. Download Workflow Diagram

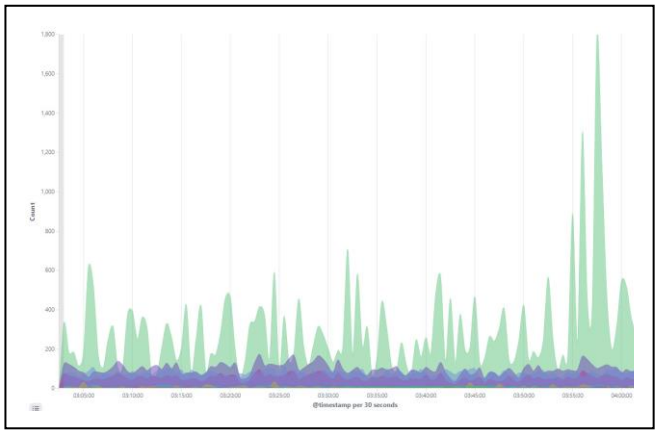
The user can securely download the encrypted file from the report node, protecting sensitive information.

In system workflow, the agent installation and registration procedure are critical. It generates a unique public key for each agent and registers them on the blockchain as genuine agents. This guarantees that any evidence or information gathered by the agent can be tracked back to its source and authenticated. When the agent is registered, it begins gathering data from each system. This data is encrypted using the agent's public key and stored in the InterPlanetary File System (IPFS).

Simultaneously, the acquired data is sent to forensic analysis for decoding and visualization. The forensic analysis graphical reports are then encrypted and saved on IPFS with the original encrypted data. When the first data is published to IPFS, it is issued with a unique hash value, which is then saved on the blockchain for future reference. Likewise, the hash value for the visualized report is generated and uploaded to the blockchain. During information retrieval, the user requests the information from the IPFS, which is then decrypted and re-encrypted with the user's public key. This technique protects the information's integrity throughout data transfer.

IV. RESULTS

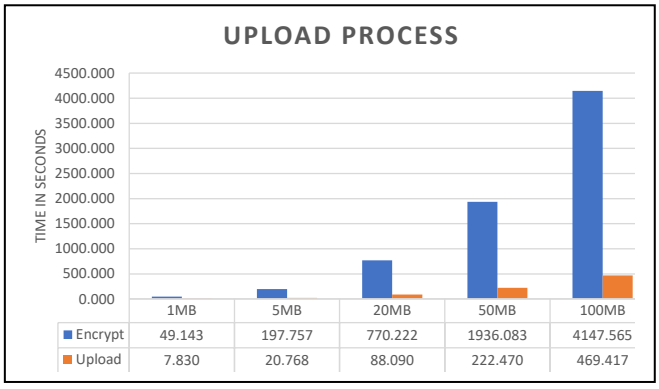
The research focused on classifying evidence obtained from network devices, specifically logs and packet captures, which are valuable for digital forensic investigations. Logs contain recorded system events, security events, network traffic events, and device-specific events, providing a chain of events and detecting various attack patterns and network flaws. Packet captures record network traffic, allowing the analysis of source and destination, protocols used, and identifying network-based threats and anomalies. The researcher used two sampling methods: time sampling, collecting data over four consecutive weeks to identify trends and changes in network behavior, and purposive sampling, selecting evidence known to have undergone security events or breaches to assess logs and packet captures more



effectively. Purposive sampling ensures the sample represents the population of interest and allows researchers to focus on relevant data while avoiding irrelevant devices.

Fig.4. Anomaly detected via report service engine – Sample Incident

The research employs a detailed processing and visualization approach to create a graph that provides a comprehensive view of open incidents. The approach focuses on analyzing previously identified information to generate a graph that simplifies the recognition and interpretation of the incidents. The graph serves as an intuitive visual



representation, allowing users to easily grasp the nature and importance of the incidents. In particular, the graph demonstrates a noticeable increase in the off-threshold value at a specific time, which effectively highlights the incident. The professional presentation of the graph enables users to quickly identify the significant deviation from the expected pattern, facilitating a thorough understanding of the incident.

Fig.5. Upload Process time for each subsection

The graph illustrates how file size affects both encryption and upload times. It consists of five lines, each representing a different scenario of encryption and upload. The graph reveals that as the file size increases, the time required for encryption also increases. This relationship is evident in the upward trend of the first line, indicating that as the file size doubles, the encryption time approximately doubles as well. Similarly, the remaining four lines represent different file sizes and demonstrate that upload time also increases as file size doubles. The graph highlights the consistent trend of upload time closely mirroring the pattern of encryption time, with both exhibiting a doubling effect as the file size doubles.

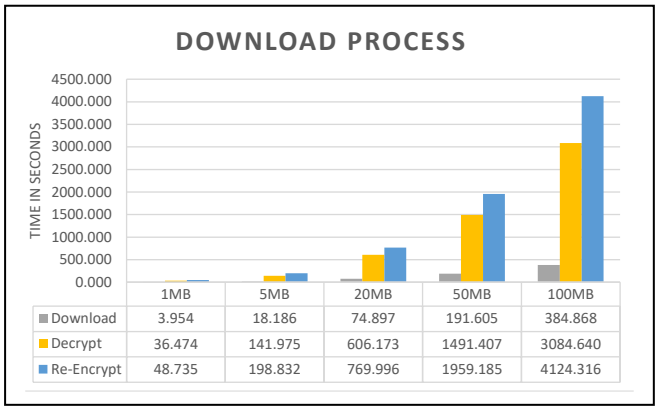


Fig.6. Download Process overall time for each subsection

The graph highlights an important finding regarding the time required for decryption and re-encryption compared to download time. It shows that the download time remains consistent and efficient regardless of file size. However, the decryption and re-encryption processes take up a significant amount of time, especially for larger file sizes. This finding emphasizes the need to consider these additional time-consuming steps when evaluating the overall efficiency of the process. It suggests that optimizing the decryption and re-encryption processes could lead to improved efficiency in handling larger files.

V. CONCLUTION

The research presents a decentralized digital evidence management framework that prioritizes security and utilizes blockchain, IPFS, and encryption techniques. The system demonstrates improved security measures through transport and content encryption, resulting in doubled effectiveness.

The research identifies several limitations and considerations regarding the processing power, memory requirements, and storage capacity of IPFS and Ethereum projects. Insufficient processing power can lead to slower transaction processing and system slowdown, while inadequate memory capacity may result in performance issues and system crashes. Additionally, the decentralized storage mechanisms utilized by IPFS and Ethereum require sufficient storage capacity to accommodate the growing volume of data. These limitations should be considered when implementing and scaling IPFS and Ethereum-based systems. However, there is a trade-off as the system experienced a 350% reduction in overall efficiency. Despite this limitation, the framework holds potential for law enforcement and investigative agencies by offering secure storage, management, and sharing of digital evidence while ensuring its integrity and provenance

REFERENCES

[1] Cert.gov.lk. 2021. Annual Activity Report 2020 Sri Lanka CERT|CC. [online] Available at: <https://cert.gov.lk/documents/Sri_Lanka_CERT_Annual_Activity_Report_2020.pdf> [Accessed 15 August 2022].

[2] A. Philip and R. Saravanaguru, "Secure Incident & Evidence Management Framework (SIEMF) for Internet of Vehicles using Deep Learning and Blockchain", Open Computer Science, vol. 10, no. 1, pp. 408-421, 2020. Available: 10.1515/comp-2019-0022 [Accessed 05 September 2022].

[3] G. Liu, J. He and X. Xuan, "A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics", Complexity, vol. 2021, pp. 1-12, 2021. Available: 10.1155/2021/5536326 [Accessed 10 August 2022].

[4] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip and N. Singh, "An Implementation of Blockchain Technology in Forensic Evidence Management", 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021. Available: 10.1109/iccike51210.2021.9410791 [Accessed 15 August 2022].

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

[6] D. Kim, S. Ihm and Y. Son, "Two-Level Blockchain System for Digital Crime Evidence Management", Sensors, vol. 21, no. 9, p. 3051, 2021. Available: 10.3390/s21093051 [Accessed 10 August 2022].