Solutions for enhancing the protection of digital evidence in judicial information systems

Ioan Vasile ȚICOVAN, Gheorghe SEBESTYEN

Faculty of Automation and Computer Science

Technical University of Cluj-Napoca

ticovan@gmail.com, Gheorghe.Sebestyen@cs.utcluj.ro

Abstract: In the digital era, the security, integrity, and authenticity of the digital forensic evidence are crucial in a judicial information system. In the paper a system that enables users to securely store the digital evidence used in legal proceedings within an architecture designed to withstand various types of attacks is proposed. It implements 12 security solutions that ensure the authenticity and protection of the stored data and prevent the interception of information within the digital evidence repository. The system integrates multiple solutions, including blockchain, data encryption techniques, communication encryption, customized solutions for immutable data storage, and access restriction through advanced filtering mechanisms. It also provides role-based access control to the digital content, ensuring the strict permission management. The implementation results demonstrate that the system is secure, robust, and capable of handling large files efficiently.

Keywords: cybercrime, electronic evidence, data integrity, security.

Soluții pentru îmbunătățirea protecției probelor digitale în sistemele informatice judiciare

Rezumat: În era digitală, securitatea, integritatea și autenticitatea probelor digitale sunt esențiale într-un sistem informațional judiciar. Lucrarea propune un sistem care permite utilizatorilor să stocheze în siguranță probele digitale utilizate în cadrul procedurilor legale sau judiciare, într-o arhitectură concepută să reziste la diverse tipuri de atacuri. Acesta implementează 12 soluții de securitate care asigură autenticitatea și protecția datelor stocate și previn interceptarea informațiilor din depozitul de probe digitale. Sistemul integrează multiple soluții, inclusiv blockchain, tehnici de criptare a datelor, criptarea comunicațiilor, soluții personalizate pentru stocarea imuabilă a datelor și restricționarea accesului prin mecanisme avansate de filtrare. De asemenea, oferă un control al accesului la conținutul digital, bazat pe roluri, asigurând o gestionare strictă a permisiunilor. Rezultatele implementării demonstrează că sistemul este sigur, robust și capabil să gestioneze eficient fișiere de dimensiuni mari.

Cuvinte-cheie: criminalitate informatică, probe digitale, integritatea datelor, securitate.

1. Introduction

Today, an efficient fight against criminality (including the ever-growing cyber-criminality) imposes the use of advanced information and communication technologies as well as artificial intelligence methods. A significant part of this activity is focused on collecting, preserving and processing the judicial evidence.

The proposed electronic digital evidence repository aims to address the diverse needs of the criminal investigation community by providing a unified platform for the acquisition, storage and management of the digital evidence. Simultaneously, the repository is designed to facilitate the collaboration among various agencies and experts in the field, enabling the secure storage and sharing of the digital information and resources essential for the criminal investigations.

The motivation for this approach was two-fold:

- Judicial investigation is becoming more and more an IT (related) activity; different IT devices, tools and methods may be used in the judicial investigation and criminality is moving to the cyber-space;
- In the near past too, many judicial cases were affected by improper handling of the evidences, that allowed the destruction or discrediting of valid evidences.

https://doi.org/10.33436/v35i2y202502

The goal of this paper is to address the different vulnerabilities of a traditional judicial repository, proposing a multi-layer security system. A key element in this proposal is the integration of blockchain technology to ensure the integrity and authenticity of the stored data. The system guarantees that the stored information is secure and can be utilized legally and ethically in the context of criminal investigations.

The content of the paper is organized as follows: Section 2 provides a brief survey of various techniques used to enhance the security and integrity of the stored data. Section 3 defines the main objectives and requirements. Section 4 describes the architecture of the proposed system, while Section 5 offers more details regarding the protective solutions included in the system. Section 6 presents some experimental results, and Section 7 contains the concluding remarks.

2. Related work

Various researchers have analyzed reliable access control mechanisms for the sensitive data in private environments, focusing on different approaches based on: blockchain, data encryption, write protection, and network security.

Easwaramoorthy et al. (2016) proposed storing data from criminal investigations in the cloud, highlighting its scalability and cost efficiency; however, the solution raises jurisdictional issues regarding data storage.

In their work, Singh et al. (2022) presented a secure storage model essential for enhancing the investigation process and safeguarding sensitive information. Their study introduces a process model designed to ensure the authenticity of evidence.

Mincewicz (2020) explored the use of the blockchain technology for data management in the national security networks, highlighting its beneficial characteristics for the judicial information system. Cheng Lo & Lu (2024) designed a multi-authority system integrated with blockchain to facilitate secure data sharing in digital ecosystems; however, the configuration process for multiple authorities remains complex.

Sukhwani et al. (2018) examined the performance of the Hyperledger Fabric blockchain platform, noting that it operates efficiently in closed networks without internet access and that its scalability can be adjusted by modifying block sizes.

Roy & Ghosh (2024) introduced a decentralized security framework to ensure access control in communication networks without relying on cloud services, implementing their approach using Hyperledger Fabric, a permissioned blockchain platform.

Abdullah (2017) investigated the AES encryption and decryption standard, emphasizing its high level of security and its potential adaptation to the proposed secure judicial system.

Narayanamurthy, Muthyala & Makkar (2014) researched specialized storage systems such as WORMStore, underscoring their advantages in ensuring data immutability-an idea also integrated into the present solution.

Agrawal, Singhal & Sharma (2024) explored data access mechanisms in distributed storage and authentication using a hybrid encryption algorithm, concluding that implementing such a system requires significant computational resources.

Rana et al. (2023) proposed a decentralized model that eliminates the need for a centralized authority, thereby reducing the risk of data loss or manipulation. By leveraging a distributed ledger and smart contracts with programmable rules and automated enforcement mechanisms, the model ensures trust and accountability among the parties involved in the lifecycle of digital evidence. Their study examines the model's architecture, emphasizing key components such as the blockchain network, smart contracts, and decentralized storage. However, a notable drawback of this solution is the high data traffic required for replicating information within the blockchain.

Since no existing system was found to integrate all the necessary requirements, we designed and implemented a solution aimed at optimizing secure data storage while ensuring the authenticity of digital evidence. This solution employs a combination of techniques that significantly reduce the risk of compromising the integrity and authenticity of the stored evidence.

3. Main objectives

The existing models for secure data storage (Aleksieva, Valchanov & Huliyan, 2020) provide a foundation for safeguarding information. This solution intends to integrate some of these methods and models, offering a multi-level security system. The proposed solution aims to develop a system that fulfills the following objectives:

- Ensuring the secure storage of digital evidence;
- Guaranteeing the authenticity of stored files;
- Creating a system that employs multiple mechanisms to ensure that stored electronic documents are resilient to various types of attacks;
- Enabling access and controlled sharing of evidence based on assigned permissions;
- Monitoring and tracing access to the stored evidence;
- Assuring compliance with regulations and standards regarding preservation and manipulation of judicial evidence;
- Special handling of classified information.

4. The architecture of the proposed system

The paper introduces a novel system architecture for managing digital evidence, utilizing blockchain technology to ensure the integrity, traceability, and immutability of stored data. The proposed architecture also combines the immutable storage systems (WORM-Write Once, Read Many and WO-Write Once Immutable – which cannot be modified after it has been created.) with the file content encryption and the file name anonymization, offering a high level of security and protection against unauthorized access. The Hybrid logging of operations, achieved through blockchain and relational databases, merges traceability with fast data access, optimizing the system performance. Communication security solutions and network access restrictions strengthen the infrastructure's protection against external attacks.

An advanced system has been implemented that enables encrypted data to be stored in multiple locations, managed by trusted institutions. Additionally, a mechanism analogous to the black box used in aviation has been integrated, which ensures that data can only be written. This mechanism guarantees that, regardless of events affecting the storage systems, there are undeniable possibilities for investigating any incidents.

The data associated with evidence (e.g. metadata) is recorded in the blockchain, providing a high level of security and transparency. As for the evidence itself, it is stored in an encrypted form within specialized and separate systems located across multiple institutions involved in the justice system, such as courts, prosecutors' offices, and police departments. This approach ensures compliance with the jurisdiction of the location where the evidence is stored, in accordance with applicable legal regulations.

All the implemented methods were designed to integrate and combine multiple advanced protection techniques, aiming to eliminate any potential logical vulnerability in the secure storage process of digital evidence. These methods were focused on ensuring the authenticity and integrity of the stored digital evidence.

The following section presents the block diagram of the implemented solution, along with the twelve proposed protection methods. Additionally, the diagram (Figure 1) highlights the specific protection measures applied at each point.

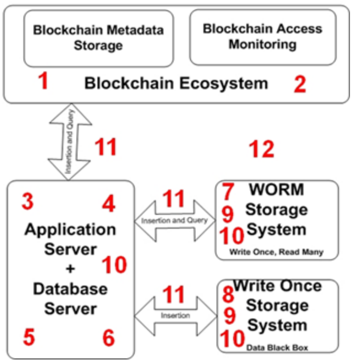


Figure 1. The specific points at which various protection solutions are applied (according to our own research)

The protection solutions integrated in the system are as follows:

1. Use of blockchain technology for storing metadata associated to digital evidence.

2. Encryption of communications between blockchain and the storage application.

3. Enabling shared and protected access to stored data.

4. File content and name encryption.

5. Hybrid logging of insert and query operations.

6. Storing operational data in a relational database with role-based access.

7. Hybrid WORM immutable storage for digital evidence.

8. Immutable storage of evidence with WO - Data Black Box.

9. Filtering of software ports and IP addresses.

10. Development of customized application servers for data transfer.

11. Securing network and communications.

12. Measures to protect access to the physical network.

The proposed system is designed to address the following categories of malicious actions (between brackets are the methods meant to mitigate the action):

- Attempt to intercept evidence (**2,4,9,10,11,12**);
- Attempt to modify evidence (**1,3,4,5,7,8**);
- Attempt to delete evidence (**3,5,7,8**).

Within the implemented solution, each identified type of attack is mitigated with a complex and diversified set of protection measures. These measures are designed to ensure a layered defense, thereby minimizing the risk of system corruption and enhancing the overall security of the data.

5. Protective solutions

5.1. Integration of blockchain technology for managing digital evidence

In the blockchain ecosystem, we store the metadata of the stored files/evidence. For efficiency reasons the blockchain itself will not store the files containing digital evidence but only their metadata. Files containing evidence will be stored on specialized storage platforms designed to provide an additional layer of safety and protection for the stored data.

For the blockchain implementation, we used Hyperledger Fabric, a platform specifically designed for permissioned blockchains. Only verified and authorized entities can become members of the network, adding an additional layer of security.

The reasons for choosing the Hyperledger Fabric blockchain solution are as follows:

- It operates in closed networks without internet access.
- Data stored on the blockchain is immutable.
- Communication between network nodes is encrypted.
- It delivers high performance in controlled intranet environments.
- Scalability is supported by the system's ability to easily expand as requirements grow, through the addition of new Peer nodes - which host the ledgers and execute smart contracts (chaincode) - or Orderer nodes, which are responsible for ordering transactions and ensuring their accurate delivery to the Peer nodes.

The implemented architecture consists of two "peer" nodes and one "orderer" node.

The information stored in the blockchain includes the following:

- Evidence index;
- Evidence name - The file name;
- Case identifier;
- Hash1 - A value generated using the SHA-256 algorithm;
- Hash2 - A value generated using the SHA-512 algorithm;
- MetadataHash - A hash generated by concatenating the metadata associated with the data;
- Evidence date - The date automatically generated at the moment the evidence is stored and uploaded;
- Name of investigation body - The name of the criminal investigation body.

To calculate the value of MetadataHash, the information provided by the STAT function applied to the evidence file was concatenated, specifically: the file size, the date and time of the last modification, and the date and time of file creation.

Data writing in the blockchain is performed by invoking the "CreateAsset" function from the smart contract within a chaincode implemented on the network. This operation involves using a dedicated write command, which is sent to one of the Peer nodes in the blockchain network.

Data reading from the blockchain is achieved through a similar mechanism, requiring the invocation of a specific function within the same chaincode.

As for the data deletion functionality, it has been disabled by removing the ability to call the deletion function in the chaincode. By eliminating the deletion functionality, the blockchain upholds the principle of immutability, ensuring that once recorded, data cannot be modified or deleted.

In conclusion, storing metadata associated with evidence in the blockchain ensures its distribution and replication across all entities participating in the network. The metadata includes information that certifies the integrity and originality of the stored evidence. Through its immutable and transparent nature, the blockchain prevents the substitution of authentic evidence with falsified versions that could favor a defendant.

5.2. Encryption of communications between blockchain systems

The encryption of communication between network nodes ensures the protection of transmitted data against interception. Even in scenarios where the traffic is captured by an attacker, the transmitted information remains inaccessible and unusable due to the applied encryption process. This measure eliminates the possibility of sensitive data being interpreted or exploited, thereby strengthening the overall security of the network.

Hyperledger uses the IP protocol as the foundation for communication between nodes, with additional mechanisms built on top of this layer to meet the blockchain requirements, such as encryption, synchronization, and transaction management (Tong & Qiu, 2023).

TCP Ports used for communication in our Blockchain configuration are:

- gRPC for Peer Nodes: Port - 7051 for the main Peer node. Each Peer node exposes a gRPC service for communication with client applications and other Peer nodes.
- gRPC for Chaincode: Port - 7052 for executing smart contracts, where the peer interacts with containers running the chaincode.
- Orderer Nodes: Port - 7050 for "orderer" nodes, which use gRPC to receive transactions from Peer nodes and distribute blocks.
- Certificate Authority (CA): Port - 7054 for the Certificate Authority service, which uses this port to issue and validate certificates.
- Gossip Protocol: Port - 7051 for Peer nodes using the Gossip Protocol to distribute and synchronize blocks and transactions. This is usually the same port as the main Peer port but can be configured separately.

HTTP/REST APIs - The client in the browser connects to the Python application server on port 5000, while the Python server interacts with the blockchain through commands provided by the Hyperledger platform.

To enhance security, an additional measure has been implemented, namely the creation of VPNs (Virtual Private Networks), which encrypt the traffic between the systems running the blockchain. By encrypting the data transmitted between blockchain nodes, the risk of data interception through traffic captures is prevented.

5.3. Enabling shared access to stored data

Shared access to information is achieved through user authentication in the storage system, using classic identification mechanisms based on username and password. After authentication, each user is assigned specific access rights.

5.4. File encryption and anonymization of their names

A data encryption solution has been implemented to prevent the risks associated with storing information in an unencrypted format. If digital files, their data, and filenames were stored in plaintext, a corrupted system (hardware) could allow a potential attacker to identify and selectively delete specific information, including relevant evidence from a particular case.

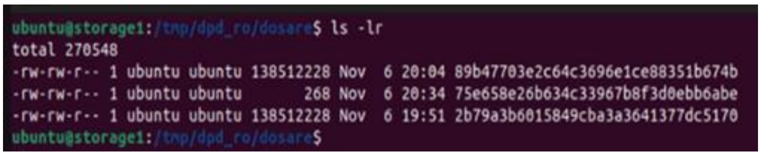
To ensure the integrity and confidentiality of the data, symmetric encryption using the Fernet cryptography method was implemented.

The choice of the Fernet encryption method over key rotation-based methods is justified by several significant advantages, both in terms of performance and encryption speed. The Fernet method is considerably faster in encrypting large files, such as those intended to be stored in repositories containing digital evidence. This feature facilitates optimization of the writing process by minimizing the time required for encryption.

Secondly, Fernet is a secure encryption method, as it uses the AES (Advanced Encryption Standard) algorithm in CBC mode, combined with an authentication mechanism based on HMAC-SHA256, ensuring both the confidentiality and integrity of the encrypted data. In contrast to key rotation-based methods, which require more complex key management and excessive use of computational resources, Fernet is easy to implement and manage, making it ideal for applications where performance and simplicity are critical.

The symmetric encryption used by Fernet is optimized for large volumes of data. Fernet encryption is widely recognized for its efficiency and simplicity, offering advantages over traditional key rotation methods in terms of both implementation and performance.

Another protection method involves anonymizing the filenames stored on the storage systems, as can be seen in the output of the `ls -lr` command in the provided image. Anonymizing the filenames ensures that files cannot be easily identified based on their names, thereby enhancing the security of the stored data. Figure 2 contains examples of stored file names.



```
ubuntu@storage1:/tmp/dpd_ro/dosare$ ls -lr
total 270548
-rw-rw-r-- 1 ubuntu ubuntu 138512228 Nov  6 20:04 89b47703e2c64c3696e1ce88351b674b
-rw-rw-r-- 1 ubuntu ubuntu       268 Nov  6 20:34 75e658e26b634c33967b8f3d0ebb6abe
-rw-rw-r-- 1 ubuntu ubuntu 138512228 Nov  6 19:51 2b79a3b6015849cba3a3641377dc5170
ubuntu@storage1:/tmp/dpd_ro/dosare$
```

Figure 2. Display of sample file names (according to our own research)

Due to the encryption of both the evidence filenames and the content of the files, if a malicious actor attempted to modify or delete an evidence file, they would be unable to identify the file, as both the name and the content are inaccessible and impossible to interpret. This encryption method adds an extra layer of security to the evidence files by concealing both visible identifiers (file names) and internal data (content), thereby further protecting the integrity and confidentiality of the evidence.

5.5. Hybrid logging of insert operations and query operations

To ensure the comprehensive logging of operations performed in the storage system, all executed commands are recorded both in the blockchain and in a traditional relational database.

The blockchain is used to maintain an immutable and decentralized record of all operations, providing security and protection against unauthorized modifications.

The traditional relational database offers quick and easy access for querying and periodic reporting, making it suitable for the operational needs of the system.

The hybrid approach combines the advantages of a blockchain-based logging system, which ensures integrity and transparency, with the flexibility and performance of relational databases. The result is a robust monitoring and operation management system, tailored to meet both security requirements and administrative efficiency.

5.6. Storing data in a relational database

Storing information both in the blockchain and in a relational database has been implemented to ensure a redundant storage solution. This approach allows for quick access to the information stored in the blockchain without relying solely on blockchain queries. Additionally, the use of the relational database reduces the additional requests to the blockchain, thereby optimizing system performance.

This solution reduces the query management load on the blockchain system, allowing it to focus solely on validity aspects, while the relational database takes on the responsibility for data manipulation and processing.

5.7. Hybrid WORM immutable storage architecture

Systems capable of ensuring the immutable preservation of data across distributed infrastructures in distinct geographical locations have been developed. The evidence storage system is separated from the application server and consists of multiple independent systems, each with specific roles and functionalities. In the present implementation, two distinct systems were utilized to ensure redundancy and diversify functionalities. Figure 3 contains the block diagram of the storage system.

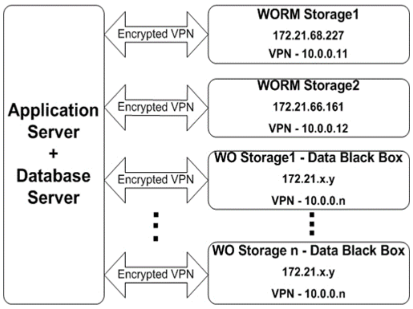


Figure 3. Block diagram of the specialized storage architecture (according to our own research)

Write Once, Read Many (WORM) is a storage technology that allows a dataset to be written only once, after which the data can be read but cannot be modified. This technology ensures data immutability, an essential feature for the protection of sensitive information (Hsu & Ong, 2007).

The WORM storage system, once it marks stored information as immutable, allows repeated access to it without any limitations. It is worth mentioning that both the content of the stored information and the filenames are encrypted. This additional security measure ensures data protection even in scenarios where the system is compromised. In such a case, an attacker attempting to delete specific data would be unable to identify the targeted files due to the encryption of the files and the anonymization of their names, thereby preventing any targeted deletion attempts.

5.8. Immutable storage architecture with WO

Write-Once (WO) is a technology that refers to a system where data can be written only once. Once written, the data cannot be queried, modified, or deleted, ensuring its integrity and immutability.

The second type of storage system differs from the first in that once the data is written, it can no longer be accessed. This system is designed to ensure a solution for sealing data and can be located in a different geographic location. Such placement offers significant benefits, including protection against natural disasters and ensuring a high level of physical security for the stored data.

Similar to the first system, both the content of the data and the file names are encrypted, providing an additional layer of security. The administrators of the two storage systems are distinct individuals or entities located in different locations and they do not have access to the "plaintext" data. Their role is limited to managing and ensuring the storage of the encrypted data, without being able to interpret or access the actual information. This separation reduces the risk of information compromise and enhances the overall security of the system.

5.9. Filtering of software ports and IP addresses

The firewall configuration serves the purpose of soft filtering software ports and defining the IP addresses allowed to communicate. The firewall is configured in an extremely restrictive manner regarding permitted traffic, with the default policy set to "DROP," meaning all connections are blocked unless explicitly allowed by defined rules.

To permit legitimate connections, strict rules must be established, authorizing only traffic between the application server and the storage service. In this setup, only IP addresses associated with the VPN network are allowed to access the application's specific port. Defining these rules involves specifying the source IP address, destination IP address, and communication port for permitted connections.

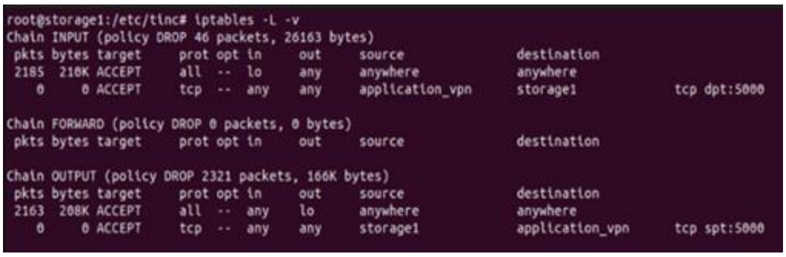
The firewall configuration is implemented using the iptables utility, which facilitates managing and enforcing these security rules.

For the application server and the two storage systems, Storage1 WORM and Storage2 WO, a strict IP filtering policy has been implemented.

Storage systems only accept connections from the application server's IP address.

Only the necessary port for data transfer, port 5000, is open on the storage systems.

To meet these security requirements, the native Linux operating system firewall was configured on both the application server and the storage systems (Storage1 and Storage2), ensuring strict control of the network traffic. Figure 4 contains the firewall configurations of the Storage1 equipment.



```
root@storage1:/etc/tinc# iptables -L -v
Chain INPUT (policy DROP 46 packets, 26163 bytes)
 pkts bytes target     prot opt in     out     source               destination
 2185  210K ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     application_vpn      storage1             tcp dpt:5000

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 2321 packets, 166K bytes)
 pkts bytes target     prot opt in     out     source               destination
 2163  208K ACCEPT     all  --  any    lo      anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     storage1             application_vpn      tcp spt:5000
```

Figure 4. The iptables rules table for configuring the firewall for Storage1 (according to our own research)

By implementing these measures, the attack surface has been reduced, as the systems only accept connections from known IP addresses, and all unused communication ports are closed.

5.10. Development of customized application servers for data transfer

Within the system, custom application server services for data transfer have been created to handle both data writing and reading. These services are capable of managing both the writing and reading of data. The writing method ensures that data is written to multiple distinct storage locations.

Data storage is implemented on multiple immutable systems of WORM and WO types, following a method that adheres to the transactional principle—ensuring that data is either written to all systems or not written at all.

The transfer of data between the application server and the storage system is carried out via the HTTP protocol, using port 5000 for encrypted data transmission. Any other method of transfer between devices is restricted to ensure control and security of the communication process.

By employing servers that operate on ports specified by the system designer and avoiding the use of standard file transfer services—often vulnerable to cyberattacks exploiting weaknesses in default configurations—a higher level of protection is ensured. This approach contributes to reducing the system's attack surface, minimizing the risks of exploiting known vulnerabilities.

5.11. Securing network and communications

The network and communication security are ensured by encrypting the communications between the application server and the storage systems.

The encryption mechanism implemented between the application server and the two storage systems serves a dual purpose: ensuring the confidentiality of the transmitted data through an encrypted connection and restricting the access to the storage servers exclusively to the authorized devices.

By using encryption, the transmission of data becomes impervious to interception, effectively preventing any unauthorized access to sensitive or potentially exploitable information. This approach also contributes to reducing the attack surface by limiting the number of vulnerable points that could be exploited within the system. This measure significantly enhances the security of the infrastructure, protecting both the data and the integrity of the system.

Traffic encryption between storage systems is implemented through a Tinc VPN. One of the key advantages of using this type of VPN is its ability to place storage systems in geographically distinct locations without compromising the security of the communication between them.

RSA keys, with a length of 4096 bits, are used for node authentication. This makes direct decryption infeasible with current technology, while traffic is protected using AES encryption. The AES algorithm is renowned for its security and resistance to efficient cracking without the appropriate key (Smid & Branstad,2001).

5.12. Solutions to protect access to the physical network

A dedicated system has been implemented for monitoring and analyzing network traffic, aiming to detect and generate alerts in the case of identifying unauthorized MAC or IP addresses. This system contributes to preventing unauthorized access, enhancing network security.

Additionally, a closed WAN network has been established, allowing only authorized equipment to connect, defined by pre-approved MAC and IP addresses. The designed system is completely isolated from the internet, ensuring the highest level of protection against external attacks.

Within this infrastructure, devices are configured with static IP addresses, eliminating the use of dynamic configurations that could introduce vulnerabilities. Routes between various network locations are manually configured, providing greater control over traffic and ensuring strict segmentation of the network based on operational needs. This approach guarantees security and predictability in network behavior. In the production environment, security will be further enhanced by properly configuring communication equipment to permit communication only with specific, trusted device MAC addresses.

Port security will be enabled on communication equipment, a feature that allows access control based on MAC addresses at the switch port level. The switch ports are configured to block or disable traffic from unauthorized devices.

Private VLANs will be implemented, and the MAC filtering function at the VLAN level will be activated, limiting communication between devices within the same VLAN and allowing communication only with authorized devices.

Layer 2 filtering on routers will be achieved using Ethernet Access Control Lists (ACLs).

SNMP alert monitoring and notification will be employed to immediately alert if an unauthorized device attempts to access the network.

Port Mirroring (SPAN) will be used to monitor and analyze suspicious traffic with dedicated IDS systems.

By utilizing an Intrusion Detection System (IDS), the network traffic can be monitored and analyzed in real-time, identifying potential unauthorized activities or anomalies. This functionality provides an additional layer of security, helping protect the system against cyberattacks or other malicious actions. Proactive monitoring through IDS enables early detection of threats and the adoption of appropriate measures to prevent system compromise.

By implementing these measures, the network infrastructure benefits from strict access control, isolation of sensitive segments, and continuous monitoring of the network activities. These strategies form a robust defense against both external and internal attacks, increasing the overall security of the IT system. By preventing unauthorized access and rapidly detecting threats, the risk of data and infrastructure compromise is significantly reduced.

6. Experimental results

The experimental part was conducted using virtual machines, all hosted on a single physical computer with the following specifications: Intel i7 processor, 16GB of RAM, and SSD storage. In the second phase, the system was distributed across multiple distinct devices interconnected through communication networks with varying speeds.

Table 1. Duration of specific operations on a single physical computer in seconds (according to our own research)

Evidence size	Local storage	Data Encryption	Transfer Storage 1	Transfer Storage 2	Writing B-Chain	Immutability 1	Immutability 2	Total time (sec)
1 MB	0,001	0,07	0,08	0,1	0,25	0,09	0,02	0,585
10 MB	0,01	0,23	0,97	0,9	0,08	0,01	0,04	2,397
50 MB	0,09	2,16	4,39	3,24	0,08	0,05	0,04	10,629
100 MB	0,14	3,55	8,56	8,73	0,13	0,02	0,03	22,697
200 MB	0,35	3,35	16,29	13,55	0,31	0,06	0,03	36151

Table 1 contains the duration of the specific operations throughout the lifecycle of the storage and process execution in different experimental scenarios.

Based on the conducted experiments, it was observed that the most significant time-consuming processes are the specialized storage and encryption.

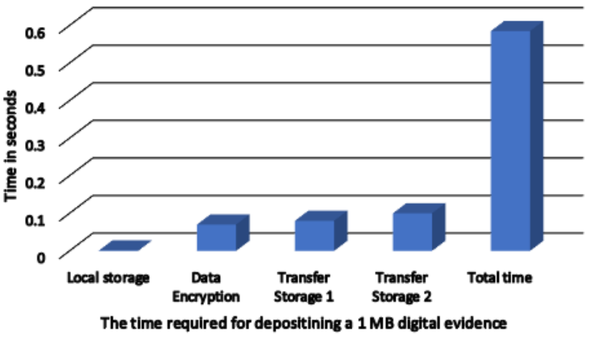


Figure 5. Identifying the Dominant Components in Time Consumption (according to our own research)

Figure 5 presents the times identified as dominant in the process of storing evidence in the digital evidence repository. The sum of these times is lower than the total time, as there are additional time components not included in the graphical representation (e.g., blockchain writing, time required for achieving immutability, etc.).

The main parameters that define a given scenario are the amount of stored data and the network speed. Table 2 contains the duration of the specific operations on a distributed system across multiple computers.

Table 2. Duration of specific operations on a distributed system in seconds (according to our own research)

Network Speed Evidence size	local storage	encryp tion	Transfer WORM	Transfer WO	write B-hain	Immut. WORM	Immut. WO	Total time(s)
Net 10Mbps-1MB	0,010	0,030	1,287	1,247	0,147	0,027	0,030	2,802
Net 10Mbps-10MB	0,03	0,307	12,377	12,363	0,087	0,037	0,04	25,313
Net 10Mbps-50MB	0,133	1,493	60,61	60,627	0,09	0,027	0,063	123,428
Net10Mbps-100MB	0,12	2,693	123,99	123,553	0,093	0,027	0,05	251,33
Net10Mbps-200MB	0,277	3,493	244,093	244,673	0,127	0,027	0,107	494,643
Net100Mbps-1MB	0,01	0,03	0,143	0,143	0,117	0,027	0,03	0,506
Net100Mbps-10MB	0,1	0,12	1,257	1,257	0,87	0,037	0,037	2,881
Net100Mbps-50MB	0,053	0,67	6,147	6,13	0,087	0,023	0,05	13,583
Net100Mbps-100MB	0,083	1,86	12,517	12,467	0,14	0,023	0,87	28,152
Net100Mbps-200MB	0,23	3,707	24,723	24,657	0,15	0,023	0,107	55,553
Net1Gbps-1MB	0,01	0,01	0,09	0,097	0,077	0,03	0,027	0,341
Net1Gbps-10MB	0,01	0,127	0,643	0,637	0,08	0,04	0,04	1,649
Net1Gbps-50MB	0,047	0,637	4,14	4,227	0,08	0,033	0,03	9,536
Net1Gbps-100MB	0,09	1,277	6,97	8,053	0,08	0,023	0,047	17,296
Net1Gbps-200MB	0,247	3,37	14,217	12,923	0,113	0,027	0,107	32,883

The test was conducted over communication networks with speeds of 10 Mbps, 100 Mbps, and 1 Gbps. Networks with these speeds are commonly available from the communication service providers. Figure 6 presents the insertion time of samples using networks of different speeds.

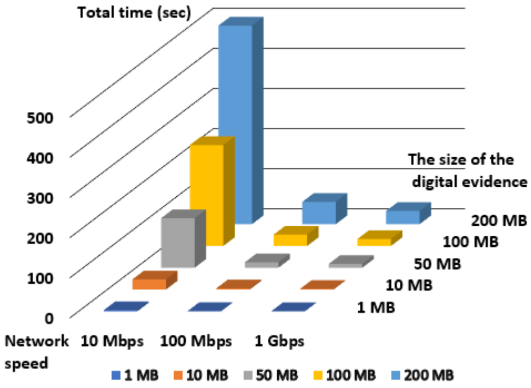


Figure 6. Insertion time of files influenced by the network speed on a distributed system (according to our own research)

Furthermore, the experiments revealed a lack of linearity in performance; specifically, increasing the transfer speed by a factor of 10 does not result in storing a sample 10 times faster.

Table 3. Write time comparison: with vs. without protection (200MB) (according to our own research)

Delay vs. network speed and storage time	Net 10Mbps	Net 100Mbps	Net 1Gbps
Storage with data protection	494.643 sec	55.553 sec	32.883 sec
Simple storage	498.043 sec	49.61 sec	27.387 sec
Ratio of protected / simple storage times	1.103	1.119	1.2

Table 3 shows a comparison of write times with and without the protection method applied to a 200MB digital evidence file. This discrepancy is explained by the fact that the operating system performs additional background operations that are not directly controlled by the storage system. Consequently, the system can maintain its efficiency only if the subsystems comprising the secure storage architecture are deployed within a network offering a speed of at least 1 Gbps.

7. Conclusions

The paper introduces a novel approach to managing digital evidence by utilizing blockchain technology to ensure the certification of data integrity. The proposed specialized architecture combines immutable storage systems (WORM and WO) with file encryption and anonymization of file names, providing a high level of security and protection against unauthorized access. The separate storage of metadata in the blockchain, alongside the distinct storage of evidence files, ensure a secure storage solution regarding their authenticity. The hybrid journaling of the operations, implemented through blockchain and relational databases, merges traceability with fast data access. The encryption of the communication channels ensures the confidentiality of the transferred data. The solution integrates multiple information security techniques. The measures for securing the communications and the restricting network access further reinforce the protection of the infrastructure against external attacks.

As future research directions, it is intended to evaluate the performance of the proposed system under conditions of managing large data volumes, with the aim of identifying the potential limitations and improving its scalability.

A second research direction focuses on integrating the immutable data storage system with the previous research, namely: Techniques for filtering, analyzing, and interpreting network traffic for legal purposes (Țicovan, & Sebestyen 2022) and Methods for legal investigation of data storage systems using artificial intelligence (Țicovan, & Sebestyen 2024).

REFERENCES

Abdullah, A. M. (2017) Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network. *Security*. 16, 1-11.

Agrawal, R., Singhal, S. & Sharma, A. (2024) Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. *Cluster Computing*. 27(6), 8015–8030. doi:10.1007/s10586-024-04411-9.

Aleksieva, V., Valchanov, H. & Huliyan, A. (2020) Implementation of Smart-Contract, Based on Hyperledger Fabric Blockchain. In *2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), 3-6 June 2020, Bourgas, Bulgaria*. IEEE. pp. 1-4. doi:10.1109/SIELA49118.2020.9167043.

Cheng, H., Lo, S.-L. & Lu, J. (2024) A blockchain-enabled decentralized access control scheme using multi-authority attribute-based encryption for edge-assisted Internet of Things. *Internet of Things*. 26, 101220. doi: 10.1016/j.iot.2024.101220.

Easwaramoorthy, S., Ganesh, A., Anitha, R. & Prasanna, V., 2016. Digital forensic evidence collection of cloud storage data for investigation. In *Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT). Chennai, India*. IEEE. doi: 10.1109/ICRTIT.2016.7569516.

Hsu, W. W. & Ong, S. (2007) WORM storage is not enough (Technical Forum). *IBM Systems Journal*. 46(2), 363-369. doi:10.1147/sj.462.0363.

Mincewicz, W. (2020) Blockchain technology and national security-the ability to implement a blockchain in the area of national security. *De Securitate et Defensione. O Bezpieczeństwie i Obronności.* 6 (2) 114-129. doi:10.34739/dsd.2020.02.08.

Narayanamurthy, S., Muthyala, K. & Makkar, G. (2014) WORMStore: A Specialized Object Store for Write-Once Read-Many Workloads. In: *2014 IEEE 22nd International Symposium on Modelling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), 9-14 September 2014, Paris, France. IEEE*. pp. 91–99. https://doi.org/10.1109/MASCOTS.2014.1.

Rana, Sumit Kumar, Rana, Arun Kumar, Rana, Sanjeev Kumar, Sharma, V., Lilhore, U.K., Khalaf, O.I. & Galletta, A. (2023) Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain. *IEEE Access*. 11, 83289–83300. doi:10.1109/ACCESS.2023.3302771.

Roy, U. & Ghosh, N. (2024) BloAC: A blockchain-based secure access control management for the Internet of Things. *Journal of Information Security and Applications.* 87, 103897. doi:10.1016/j.jisa.2024.103897.

Singh, A., Ikuesan, R. A. & Venter, H. (2022) Secure Storage Model for Digital Forensic Readiness. *IEEE Access*. 10, 19469-19480. doi:10.1109/ACCESS.2022.3151403.

Smid, M. & Branstad, D. (2001) The Advanced Encryption Standard (AES). *Journal of Research of the National Institute of Standards and Technology (NIST)*. 106(3).

Sukhwani, H., Wang, N., Trivedi, K.S. & Rindos, A. (2018) Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), 1-3 November 2018, Cambridge, MA, USA. IEEE.* pp.1-8. doi:10.1109/NCA.2018.8548070.

Tong, W. & Qiu, F. (2023) Research on Security Sandbox System Based on Computer Big Data Hyperledger Fabric Blockchain Platform. In *2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), 24-26 February 2023, Changchun, China. IEEE*. pp. 1675-1680. doi:10.1109/EEBDA56825.2023.10090679.

Țicovan, I.V. & Sebestyen, G. (2022) Judicial Surveillance of Cyber-Physical Systems. In *2022 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 19-21 May 2022, Cluj-Napoca, Romania. IEEE*. pp.1-6. doi:10.1109/AQTR55203.2022.9801980.

Țicovan, I.V. & Sebestyen, G. (2024) Forensic Investigation of Data Storage Systems. In *2024 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 16-18 May 2024, Cluj-Napoca, Romania. IEEE*. pp.1-7. doi:10.1109/AQTR61889.2024.10554109.

Ioan Vasile ȚICOVAN is a Ph.D. candidate at the Technical University of Cluj-Napoca (IOSUD-UTCN), within the UTCN Doctoral School. His doctoral research focuses on "Techniques for Investigating and Analyzing IT Systems for the Purpose of Obtaining Judicial Evidence," with an emphasis on cybersecurity and digital forensic analysis. He has contributed to prestigious international conferences, publishing papers such as *"Judicial Surveillance of Cyber-Physical Systems"* (AQTR 2022) and *"Forensic Investigation of Data Storage Systems"* (AQTR 2024). His research interests encompass cybercrime, electronic evidence analysis, data integrity, and IT security.

Ioan Vasile ȚICOVAN este doctorand la Universitatea Tehnică din Cluj-Napoca (IOSUD-UTCN), în cadrul Școlii Doctorale UTCN. Tema cercetării sale doctorale este „Tehnici de investigare și analiză a sistemelor informatice în scopul obținerii probelor judiciare", cu un accent pe securitatea cibernetică și analiza criminalistică digitală. A participat la conferințe internaționale de prestigiu, și a publicat articole, printre care: „Supravegherea judiciară a sistemelor cibernetico-fizice" (AQTR 2022) și „Investigația criminalistică a sistemelor de stocare a datelor" (AQTR 2024). Domeniile sale de interes științific includ criminalitatea informatică, analiza probelor electronice, integritatea datelor și securitatea IT.

Gheorghe SEBESTYEN is a professor at the Technical University of Cluj-Napoca, Computers Department. He received his PhD degree in Computers science in 2003 at the same university. His research interests are in applied informatics, embedded control systems, security of cyber-physical systems and malware detection techniques. He has an experience of more than 35 years in the field of computers, and published approximately 150 articles in journals and conference proceedings. He coordinated numerous research and development projects funded from national and international sources that were meant to apply ITC technologies in various domains, such as industrial control, telemedicine, digital libraries and security. He is a reviewer for some journals, like Sensors, Electronics, Advances in Electronics and Computer Engineering and conferences (e.g. ICCP, AQTR, etc.).

Gheorghe SEBESTYEN este profesor la Universitatea Tehnică din Cluj-Napoca, în cadrul Departamentului de Calculatoare. A obținut titlul de doctor în domeniul Calculatoare în anul 2003, la aceeași instituție. Interesele sale de cercetare vizează informatica aplicată, sistemele de control, securitatea sistemelor cibernetico-fizice și tehnicile de detectare a programelor malițioase. Are o experiență de peste 35 de ani în domeniul calculatoarelor și a publicat peste 150 de articole în reviste de specialitate și în volumele conferințelor științifice. A coordonat numeroase proiecte de cercetare-dezvoltare finanțate din surse naționale și internaționale, având ca scop aplicarea tehnologiilor TIC în diverse domenii, precum controlul industrial, telemedicina, bibliotecile digitale și securitatea informatică. Este recenzor pentru mai multe reviste științifice, precum Sensors, Electronics, Advances in Electronics and Computer Engineering, precum și pentru conferințe internaționale de prestigiu cum ar fi ICCP, AQTR etc.