


## A Blockchain-Based Model Proposal to Enhance Digital Forensics Readiness

Mehmet MERAL<sup>\*1</sup> , Hasan Hüseyin SAYAN<sup>2</sup> 

<sup>1</sup> Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı, Ankara, Türkiye

<sup>2</sup> Gazi Üniversitesi, Teknoloji Fakültesi, Elektrik-Elektronik Mühendisliği, Ankara, Türkiye

(Alınış / Received: 20.12.2024, Kabul / Accepted: 26.03.2025, Online Yayınlanma / Published Online: 25.04.2025)

### Keywords

Digital forensics  
Incident response,  
Digital forensics readiness,  
Blockchain technologies

**Abstract:** Effective incident response mechanisms are crucial for maintaining system continuity during security incidents. Equally important is the secure preservation of forensic evidence and chain of custody records for potential legal proceedings. However, traditional methods of incident response and evidence handling can be vulnerable to tampering as they rely on the assumption of a pre-existing level of trust among the involved parties. In this study, we propose a blockchain-based model, DFIRChain, to record all operations within digital forensics and incident response (DFIR) processes on a private permissioned Hyperledger Fabric blockchain, from alert management to case management. By integrating our blockchain-based model into DFIR processes, we aim to ensure the integrity and authenticity of evidence, enhance legal compliance, and contribute to organizations' digital forensic readiness.

## Adli Bilişime Hazır Bulunmayı Artırmak için Blok Zincir Tabanlı Bir Model Önerisi

### Anahtar Kelimeler

Adli bilişim,  
Olay müdahalesi,  
Adli bilişime hazır olma,  
Blok zincir teknolojileri

**Öz:** Etkili olay müdahale mekanizmaları, güvenlik olayları sırasında sistem sürekliliğini korumak için çok önemlidir. Aynı derecede önemli olan, olası yasal işlemler için delillerin ve koruma zinciri kayıtlarının güvenli bir şekilde saklanmasıdır. Bununla birlikte, olay müdahale ve delillerin yönetilmesine ilişkin geleneksel yöntemler, ilgili taraflar arasında önceden var olan bir güven düzeyinin varsayımına dayandığından, tahrifata karşı savunmasız olabilir. Bu çalışmada, alarm yönetiminden vaka yönetimine kadar adli bilişim ve olay müdahale (DFIR) süreçlerindeki tüm işlemleri, özel izinli Hyperledger Fabric blok zincirinde saklamak için blok zinciri tabanlı bir model olan DFIRChain'i öneriyoruz. Blok zincir tabanlı modelimizi DFIR süreçlerine entegre ederek delillerin bütünlüğünü ve orijinalliğini sağlamayı, yasal uyumluluğu geliştirmeyi ve kuruluşların adli bilişim incelemelerine hazır bulunmalarına katkı sağlamayı amaçlıyoruz.

### 1. Introduction

When a security incident occurs in information systems, it is crucial to have an incident response mechanism in place to ensure system continuity. These processes, known as incident response, are managed by specialized teams within organizations. These teams monitor event logs collected from various sources prior to a security incident and initiate incident response processes when they detect a situation that could compromise the system. These

processes aim to maintain the continuity of information systems. However, it is also important at this stage to securely store forensic evidence and chain of custody records, which may be relevant to a future disciplinary investigation, insurance claim, or legal proceedings. This concept, known as forensic readiness, reduces effort and costs when a forensic investigation is required [1].

In the context of information systems, forensic readiness is defined as an organization's ability to

\*Corresponding author: mehmetmeral@gmail.com

preserve, collect, and analyze digital evidence in a manner compliant with legal processes [2]. To achieve this, organizations centrally store all event logs generated by computer systems and employ hashing and timestamping techniques to demonstrate that the records have been preserved without alteration.

Forensic investigation processes in organizations typically begin with a breach detected during security monitoring activities, a subpoena from a court, or an external claim by a third party. In an organization that has adopted the concept of forensic readiness, it is assumed that incident response teams have proactively collected sufficient evidence before any investigation is launched.

The International Organization for Standardization (ISO) developed a standard for forensic readiness in IT systems. ISO/IEC 27043, Information technology — Security techniques — Incident investigation principles and processes, provides guidance on how to implement a forensic readiness program [3]. The standard offers a structured approach to preparing for potential legal proceedings involving digital evidence.

Valjarevic and Venter [4] proposed a harmonized model designed to facilitate forensic readiness processes. Their model presents a systematic framework aimed at safeguarding potential digital evidence and maintaining chain of custody records throughout the entire lifecycle of a cyber incident, from initial detection to the conclusive closure of the investigation. This proactive approach is essential for preserving the admissibility and reliability of evidence in subsequent legal or internal inquiries.

However, the harmonized model developed by the researchers assumes that a level of trust exists among the involved parties, and it does not address scenarios where such trust is absent. In contexts where inter-organizational collaboration or external investigations are necessary, the lack of a defined mechanism for establishing and maintaining trust can significantly impede the effectiveness and impartiality of the forensic process.

This study proposes a blockchain-based remodeling of incident response systems, building upon the harmonized forensic readiness model presented by Valjarevic and Venter. Cyber incident response teams operating within organizational security operation centers (SOCs) are tasked with executing forensic readiness procedures in accordance with legal frameworks. In their daily operations, these teams are responsible for examining and preserving computer records that may serve as evidence in future investigations. However, it is theoretically possible for stored evidence, chain of custody records, and associated cryptographic hashes to be maliciously altered prior to submission in court or to be

compromised by events such as cyberattacks or disasters that could result in data loss or destruction.

Blockchain can allow all stakeholders involved in incident management to track the incident status, actions, and outcomes. Furthermore, it enhances the auditability of incident response and forensic investigation activities, guaranteeing legal compliance and accountability. The model proposed in this study aims to manage incident response and digital forensic processes on the blockchain, thereby contributing to organizations' digital forensic readiness.

The second section of this study presents a literature review of similar studies in this field, while the third section describes the current state. The fourth section introduces the developed model and explains the design of this model.

## 2. Related Studies

Several studies have proposed blockchain-based models for digital forensic processes.

Jaquet Chiffelle et al. [5] developed a time-stamped and blockchain-based model that demonstrates that digital evidence is protected from tampering from the time it is admitted to laboratories until it is presented to the courts. In their subsequent work, the researchers sent the developed model to a public blockchain system and designed a system that can verify the evidence using the QR code found in the PDF file returned by the blockchain system [6].

Lone and Mir [7] proposed a blockchain model called Forensic-chain based on Ethereum to protect the chain of custody in forensic processes in their first study. In their second study, they transferred the developed system to Hyperledger Fabric, a private permissioned blockchain infrastructure, and performed its verification [8].

Li et al. [9] proposed a model called IoT Forensic-Chain (IoTFC) for recording evidence collected by the Internet of Things (IoT) on the blockchain. They proposed to store the chain of custody in an effective and simple way by adding all IoT connection points in the blockchain, thus ensuring transparency in audit processes.

Kim et al. [10] proposed a two-tier blockchain infrastructure for managing and storing evidence in cybercrime investigations: hot and cold blockchain. In the proposed model, cold blockchain is defined as a blockchain system which stores big volume data which does not see any frequent changes such as video recordings. Hot blockchain refers to the second blockchain network used in the model which stores low-volume data such as chain of custody records and investigation steps. Since this data requires frequent

updates, the blockchain network is called as the hot blockchain.

The LEChain model, developed by Meng Li et al. [11], proposes storing the chain of custody records in a tamper-proof manner on the blockchain, while also anonymizing the identities of witnesses and jurors in the American justice system to protect their privacy, leveraging the security element provided by blockchain technology.

Alqahtany and Syed [12] proposed a comprehensive framework called ForensicTransMonitor. The study finds that blockchain has been successfully applied in digital forensic science in areas such as cloud environments, the Internet of Things, and storing chain of custody. However, it highlights the lack of a framework that encompasses the entire process from the beginning of a forensic investigation to its completion. For this purpose, the authors developed a private permissioned Hyperledger Fabric blockchain infrastructure.

Özdemir [13] studied the applicability of sharing cyber threat intelligence in blockchain using the permissioned blockchain. The researcher developed a new threat sharing model in Hyperledger Fabric.

Prior to the advent of blockchain technology, a study called "Secure Audit Logs to Support Computer Forensics" by Scheiner and Kelsey [14] in 1999 proposed a method employing mathematical computations to safeguard log records within computer systems against tampering, effectively rendering them impervious to reading, modification, or deletion by malicious actors. This proposed methodology enabled organizations to transparently maintain computer records prior to any cyber incident, thereby ensuring forensic readiness when required. Drawing upon this research and leveraging the Merkle tree data structure, a security information and event management (SIEM) product named LogSentinel has been developed by a commercial entity [15]. LogSentinel utilizes blockchain technology to store these records, ensuring the immutability of computer logs.

Moreno et al. [16] proposed a model that records system events and cyber incidents in two separate blockchain systems running on Hyperledger Fabric to improve incident response processes in big data ecosystems. The study is limited to incident response processes in ecosystems that process large amounts of data from sensors, such as industrial control systems.

Distinct from the aforementioned studies, this research proposes a novel model that manages operations within digital forensics and cyber incident response processes, recording evidence and chain of custody records on a blockchain before a forensic

investigation is initiated, thereby enhancing forensics readiness. When a forensic examination is required, digital forensic stakeholders, such as expert witnesses, law enforcement agencies, and judicial bodies, can seamlessly participate in the system via the blockchain.

### 3. Current Situation

#### 3.1. Incident response frameworks

Computer Emergency Response Teams (CERTs) are the teams tasked with detecting, investigating, and preventing cyberattacks. The first CERT was established in 1988 at the Software Engineering Institute of Carnegie Mellon University. CERTs can operate at the national level to monitor and detect cyberattacks against a country, or they can be established at the corporate level to monitor the organization's attack surface. These structures operating at the corporate level are also known as Computer Security Incident Response Teams (CSIRTs).

Rapid response and evidence collection are crucial in the event of a cyberattack or data breach to identify the attackers and determine if they have access to other systems. In large-scale organizations, especially those operating in finance, healthcare, and manufacturing, the establishment of a Security Operations Center (SOC) to manage cyber incident response is becoming increasingly common. CSIRT teams operate within SOCs and typically manage their processes manually or using software called Security Incident Response Platforms (SIRP).

Cyber incident response processes are defined as a systematic response to cybersecurity incidents [16]. Various frameworks have been developed for incident response processes by the National Institute of Standards and Technology (NIST), Carnegie Mellon University, and the International Telecommunication Union (ITU) [17-19].

The terms "event", "incident", and "case" are frequently used in cybersecurity incident response processes. Their definitions in the NIST framework are given below:

**Event:** An observation in a computer system that cannot be immediately determined to be harmful or harmless. Examples include a user logging in from a different location or entering an incorrect password five times in a row [17].

**Incident:** A violation or attempted violation of information security policies, such as a user clicking on a link in a phishing email [17].

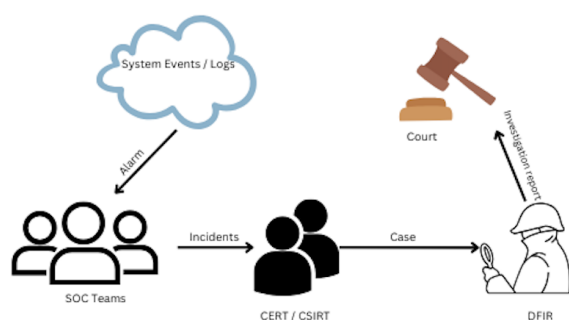
**Case:** A forensic investigation initiated on computer systems following a cyber incident, a claim, or a subpoena from a judicial investigation.

Events are the basic building blocks of cybersecurity incident response. They represent any observable change or activity in a computer system. Events can be generated by various sources, including user actions, system logs, network traffic, and security tools. While some events may indicate malicious activity, others may be benign or even part of normal system operation.

Incidents are a subset of events that pose a threat to information security, such as unauthorized access, data breaches, and malware infections. Identifying and responding to cyber incidents is crucial for protecting an organization's sensitive information and maintaining its overall security posture.

Cases represent the formal investigation and handling of cyber incidents. Once a cyber incident is identified, a case is typically opened to manage the incident response process. This process involves activities such as preservation, acquisition, analysis, and reporting.

In SOC, analysts monitor system event logs and report any suspected cyber incidents to CSIRT teams, which handle incident response. The cyber incident response process may be completed without any forensic examination or, if necessary, may be referred to forensic teams or institutions for forensic examination. These teams initiate the case review process called digital forensics and incident response (DFIR). The forensic process also involves data preservation, acquisition, analysis, and reporting. The expert report prepared at the end of the process is submitted to the courts if necessary. In all these processes, it is a legal requirement to securely store evidence and access records related to evidence. In organizations that operate with the concept of being prepared for forensic examinations, system logs and access records to evidence are stored in a way that is admissible in court. This concept is shown in Figure 1.



**Figure 1.** Incident Response and Digital Forensics Processes

However, in many organizations, forensic investigation processes are typically initiated following an external notification or a court-issued

subpoena. Forensic readiness is often overlooked in the daily operations of SOC and CERT activities. Traditional DFIR processes, which rely on physical records or centralized databases, are susceptible to manipulation and unauthorized access. The lack of integration between SOC, CERT, and DFIR processes, coupled with the absence of regular inter-team communication, hinders visibility during incident response, compromises the integrity of chain of custody records, and prevents the verification of these records' authenticity by third parties.

### 3.2. Digital forensic frameworks

Digital forensic processes are carried out within the specific methodological approaches to ensure the admissibility of digital evidence in courts. Various researchers and institutions have developed different digital forensic models to optimize this process and make it more systematic. While some of these models focus on traditional digital forensic procedures, emphasizing evidence collection and analysis phases, others incorporate additional aspects such as legal compliance and process management.

The first model in the digital forensics was introduced by the Digital Forensic Research Workshop (DFRWS). DFRWS was established in 2001 in the United States to advance digital forensic research. The model outlines a structured forensic investigation process consisting of identification, preservation, collection, examination, analysis, presentation, and decision-making [20]. Key principles of the model include data integrity, traceability, and secure evidence handling. The model also emphasizes the challenges of tampering detection and the reliability of digital evidence.

The U.S. Department of Justice (DOJ) Cybercrime Laboratory developed a structured approach for digital evidence examination called Digital Forensic Analysis Methodology. It consists of six key phases: forensic request and preparation, data collection and duplication, identification and preliminary analysis, in-depth forensic analysis, discovery of new data sources, and forensic reporting [21]. The methodology emphasizes evidence integrity, proper chain of custody, and systematic analysis techniques such as timeline reconstruction, network traffic analysis, and malware examination.

The INTERPOL developed the "Digital Forensics Laboratory Global Guidelines" in 2019. The guidelines establish international standards for digital forensic processes. It ensures consistency, reliability, and legal compliance in handling digital evidence across forensic laboratories worldwide [22].

## 4. The Proposed Model

We propose a smart contract-based model operating on a blockchain infrastructure to enhance the trust, interoperability and accountability in the digital forensics and incident response process. In this model, an immutable record is generated for every intervention impacting the chain of custody within incident response and digital forensic processes.

A blockchain is a data structure comprised of interconnected units called blocks [23]. All transactions related to this data structure are stored in distributed ledgers. Each block contains a hash value, timestamped transaction data, and the hash value of the preceding block. Any modification to a previous block will alter its hash value, thereby disrupting the chain. This mechanism ensures transparency, security, auditability, and verification.

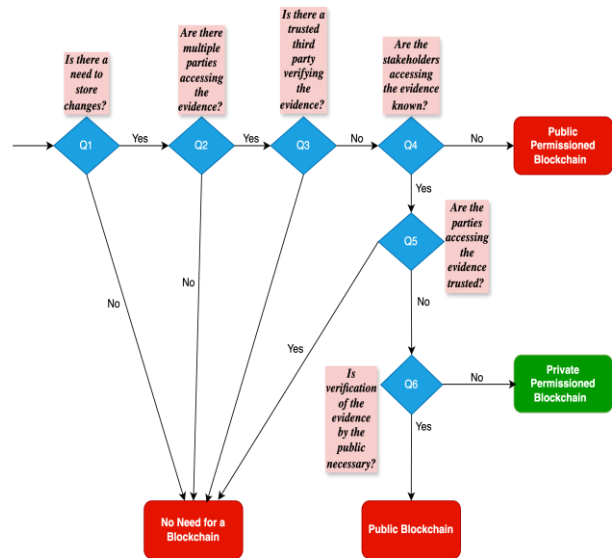
In digital forensic investigations, a digital fingerprint of all examined evidence is generated using hash functions. Verifying that the evidence remains in its original state as seized prior to its presentation in court is crucial. Logging any actions performed on the evidence, both pre-investigation and post-investigation, with timestamps on the blockchain ensures the evidence's integrity, authenticity, and auditability.

Consequently, blockchain technology offers several advantages for incident response management, including enhanced visibility, accountability, security, and trust. Furthermore, by leveraging smart contracts to trigger and execute predefined actions and workflows, communication and collaboration among SOC, CERT, and DFIR teams can be facilitated more rapidly and accurately. Through encryption and distributed storage, blockchain safeguards incident response data against unauthorized access, tampering, or loss.

#### 4.1. Determining Blockchain Requirements

Blockchain architectures are categorized into two types based on their access control mechanisms: permissionless and permissioned blockchains. Permissionless blockchains, also known as public blockchains, allow any individual to participate in the network. Due to their complete decentralization, permissionless blockchains have been successfully implemented in the financial domain. In contrast, participation in permissioned blockchains requires authorization from a predefined central authority. Permissioned blockchains are suitable for organizational structures where entities are acquainted but do not fully trust one another. Permissioned blockchains have found their usage in enterprise systems such as logistics and manufacturing. Permissioned blockchains can be further classified as either public or private. Private permissioned blockchains are also referred to as consortium blockchains [23].

In our implementation, the decision tree developed by Wüst and Gervais [24] was adapted and utilized to determine the feasibility of blockchain usage and to select the appropriate type of blockchain (Figure 2).



**Figure 2.** Blockchain Decision Tree Adapted from Wüst and Gervais [24]

The following questions were addressed within the decision tree:

Question 1: Is there a need to store changes?

Question 2: Are there multiple parties accessing the evidence?

Question 3: Is there a trusted third party verifying the evidence?

Question 4: Are the stakeholders accessing the evidence known?

Question 5: Are the parties accessing the evidence trusted?

Question 6: Is verification of the evidence by the public necessary?

Wüst and Gervais state that blockchain usage is suitable in scenarios where multiple participants do not mutually trust each other, and there is no trusted third party available to verify the evidence. In digital forensics, storing any changes to the evidence handling is essential; access to evidence is periodically required by different institutions; and there is no “independent” third party to verify the evidence. Based on the results of the first three tests, we can conclude that “blockchain usage is suitable for digital forensics.” The remaining tests will determine which type of blockchain should be used. In forensic processes, the stakeholders accessing the evidence are known but there is a lack of trust among them. Since verification of the evidence by the entire public is not necessary, it is understood that a private permissioned blockchain infrastructure is the most suitable solution for our system design.

## 4.2. Selecting the most suitable blockchain system

Based on the requirements discussed in the previous section, public blockchain platforms such as Bitcoin, Ethereum and Solana were considered unsuitable for our study due to its permissionless nature. These platforms lack the controlled access required for our applications.

We evaluated the suitability of open-source permissioned blockchain platforms: Hyperledger Fabric, R3 Corda and Quorum for our digital forensics and incident response model. Each platform offers unique characteristics in terms of consensus mechanisms, transaction throughput, scalability, and security features.

Hyperledger Fabric, developed by the Linux Foundation, provides a robust infrastructure for the development of consortium blockchains. It enables multiple institutions to establish consortiums and construct a blockchain network. One of the most significant features of Hyperledger Fabric is its ability to separate endorsement from administration, which enhances the overall performance of the blockchain network [25]. Additionally, its channel mechanism ensures privacy by allowing the creation of separate channels for different consortiums. Due to its modular architecture and support for various consensus mechanisms, Hyperledger Fabric is well-suited for diverse industries, including supply chain management, healthcare, and finance.

R3 Corda is a distributed ledger technology (DLT) specifically designed for the financial industry. Unlike traditional blockchain systems, R3 Corda does not employ generic consensus mechanisms, namely proof-of-work or proof-of-stake [26]. Instead, it utilizes a notary service to achieve consensus. R3 Corda's architecture prioritizes privacy and confidentiality as each participant maintains a different ledger.

Quorum is an enterprise-focused blockchain platform built on the Ethereum protocol, specifically designed for the financial sector. It extends Ethereum's capabilities by adding transaction and contract privacy and a voting-based consensus mechanism [27]. These modifications enable Quorum to offer high-performance transaction processing along with privacy-centric enhancements. However, its reliance

on the Ethereum ecosystem raises concerns regarding governance and potential cost implications.

Another open-source distributed ledger technology, IOTA is considered an option for our model due its use in digital forensic research although it is permissionless blockchain. IOTA differs from traditional blockchains because it uses a unique data structure that allows transactions to happen anytime and in parallel [28].

In a research study by Gürfidan and Tatlı [29], the performance and security characteristics of Hyperledger Fabric and IOTA were comparatively examined in the field of digital forensics. The research findings found that the IOTA Tangle platform showed a better performance compared to Hyperledger Fabric in terms of transaction throughput. However, the researchers emphasized that Hyperledger Fabric, due to its permissioned network structure, is a more suitable solution for fulfilling security needs at the enterprise level. Being permissionless and lacking access control and governance mechanisms make IOTA less suitable for our model.

Among the platforms evaluated, Hyperledger Fabric emerged as the most suitable infrastructure for our research. Hyperledger Fabric offers flexibility in consensus selection, supporting algorithms such as RAFT and Kafka, allowing performance optimization based on specific application requirements. Additionally, it ensures data privacy through permissioned access, private data collections, and channels, restricting transaction visibility to authorized participants. One of the key advantages of Hyperledger Fabric is its support for general-purpose programming languages in smart contract development. This capability was also a crucial factor in the researchers' decision to select Hyperledger Fabric for this model. Table 1 provides a summary of the blockchain selection criteria.

Hyperledger Fabric's modular architecture, pluggable consensus mechanisms, and robust access control capabilities make it particularly well-suited for forensic applications. As a foundational framework for consortium blockchains, Hyperledger Fabric guarantees the immutability of forensic evidence, even in environments where trust among institutions and individuals is limited.

**Table 1.** Blockchain Framework Comparison

Criteria	Hyperledger Fabric	Corda	Quorum	IOTA
Consensus Mechanism	RAFT, Kafka (Pluggable)	Notary-based Consensus	Istanbul BFT, Raft	Tangle (DAG-based)
Access Control	Permissioned	Permissioned	Permissioned	Public
Privacy	Private Data Collections, Channels	Private Transactions	Private Transactions	Masked Authenticated Messaging (MAM)

Smart Contract Language	General-purpose languages	Kotlin, Java	Solidity	Rust, Go
Scalability	Moderate to High	Moderate	High	High
Performance	Optimized for enterprise use	Designed for business transactions	Enterprise-grade, optimized for finance	Enterprise-grade
Suitability for Digital Forensic Applications	High (supports data integrity and controlled access)	Moderate (better suited for financial applications)	Moderate (limited adoption in forensic scenarios)	Low (Permissionless)

### 4.3. Model design

The process begins with the escalation of critical alarms gathered from end-user computers into cyber incidents worthy of being investigated by SOC analysts in the proposed model. During this process, a block is added to the blockchain. All operations throughout digital forensics and incident response (DFIR) are recorded on the blockchain. The model is therefore named DFIRChain.

The block contains information about the incident under investigation, including:

- Hash (SHA-256 or MD5) of the evidence
- Timestamp indicating the time of incident detection
- Investigation records
- Analysis results

By recording all DFIR operations on the blockchain, the DFIRChain model establishes an immutable and tamper-proof audit trail. This comprehensive approach facilitates forensic analysis, promotes collaboration among SOC teams, and fosters accountability throughout the incident response process.

The DFIRChain process consists of three main steps:

#### 1. Alert Management:

- Logs are captured from end-user computers by intrusion prevention systems (IPS) or endpoint detection and response (EDR) systems and brought to the attention of analysts.
- Log entries are analyzed for security risks and vulnerabilities.
- Alerts are recorded off-chain in the model due to performance issues.

#### 2. Incident Management:

- Alerts collected from computer systems are automatically retrieved via APIs through systems called SIEM.
- Analysts convert suspicious alarms into incidents and investigate the incidents.
- Analysts record their observations, notes, and investigation results related to the incident on the blockchain.

#### 3. Case Management:

- Incidents that require detailed investigation are converted into cases by analysts if they are considered to require comprehensive forensic analysis.
- More detailed evidence is collected from the suspicious computers involved in the case, and the hash values of the evidence are added to the blockchain.

### 4.4. Components of the proposed model

The model consists of three core elements of all blockchain systems: assets, participants, and transactions:

**Assets:** Anything of value that is transacted or shared in blockchain systems can be an asset. As discussed in Section 2, the various researchers have proposed to record forensic evidence collected in forensic investigations on the blockchain as an asset. In our proposed DFIRChain model, incidents that SOC analysts are working on and cases that the forensic investigators handle are considered as assets within the system and are stored in Hyperledger Fabric's asset ledger.

**Participants:** In blockchain systems, the actual actors responsible for storing transaction data are considered participants. In the DFIRChain model, participants include SOC analysts, incident response teams, and forensic specialists whose responsibility is to collect information about digital evidence and record it on the blockchain. Participants may have different permissions based on their roles. The blockchain system allows the addition of participants such as lawyers from the legal departments, senior management, and personnel from human resources when necessary. These users can perform activities such as adding or monitoring documents related to forensic processes. Thanks to Hyperledger Fabric's consortium model, courts or law enforcement agencies can also participate in the system when required. Authorization for these individuals is provided by the consortium administrator (admin peer) of the institution operating the blockchain. This authorization is revoked by the administrator once the process is completed. This process contributes to the institution's transparency and accountability regarding forensic processes.



Transactions: Any activity related to access to records is equivalent to a transaction in blockchain systems. In DFIRChain, all information about data collection, investigations, and communication with stakeholders is recorded on the blockchain from the moment the cyber incident is detected. During the incident management phase, all observations of the analyst related to the incident, the systems they access, their notes, and the hashes of the evidence related to the incident form a block on the blockchain. This recording process continues with the escalation of the incident to a case. In case analysis, the hashes of evidence collected from computers, documents, and reports are also recorded on the blockchain. This ensures the immutability of these records (Figure 3).

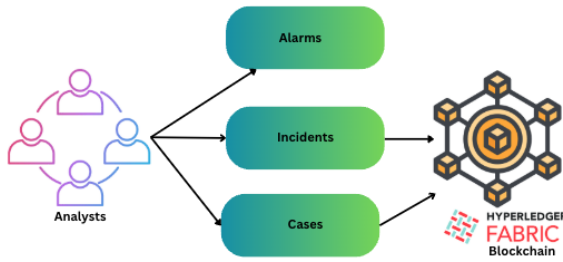


Figure 3. Internal Design

#### 4.5. Model architecture

Departments or organizations join the blockchain as "organizations" and register their identities on the blockchain with digital certificates they receive from the public key infrastructure (PKI) system. Smart contracts (chain code in Hyperledger) manage the recording of evidence. The analyst or forensic expert who wants to record evidence-related transactions accesses the platform running in Docker through a web interface and creates a block on the blockchain for the transaction. A client application is being developed to simulate different actors. For this purpose, users communicate with a web application via HTTP. Requests from users for joining the blockchain, sending transactions, and running smart contracts are transmitted to Hyperledger Fabric via APIs.

DFIRChain is proposed as a model operating at the enterprise level. However, since it utilizes digital certificates for authorization, third-party organizations such as law enforcement agencies, courts, forensic laboratories, and law firms can also participate in the blockchain for verification purposes thanks to PKI infrastructure (Figure 4). Hyperledger Fabric provides a channel system where communication between parties can be managed independently. This ensures privacy and confidentiality between institutions and individuals.

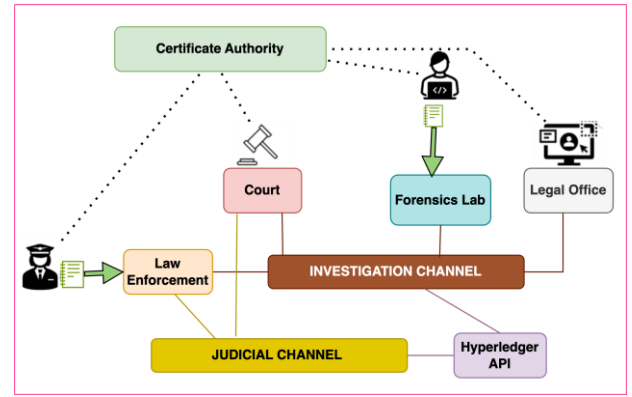


Figure 4. DFIRChain model with inter-agency integration

#### 4.6. Blockchain structure

Records related to cyber incidents, ownership information, and the hash of evidence are stored in the blockchain. A smart contract has been developed to process each transaction on the blockchain. Some sample transaction records in the developed model are shown below.

```

const incidents = [
  {
    ID: '1484780787',
    FirstResponder: 'System Admin - 1',
    Owner: 'IT',
    Title: 'Payload delivery',
    Date: '2024-05-18',
    Severity: 'Critical',
    TLP: 'TLP:RED',
    Description: 'Phishing email clicked and attachment executed',
    Evidence: '56c42374-fdb8-4544-a218-41ffc0a8ab16',
  },
  {
    ID: '1543864516',
    FirstResponder: 'L3 SOC Analyst',
    Owner: 'SOC',
    Title: 'Network activity',
    Date: '2024-05-18',
    Severity: 'Critical',
    TLP: 'TLP:RED',
    Description: 'Reversed C2 traffic from China',
    Evidence: '5af9ac04-9744-4687-ab41-4ee5c0a8ab16',
  },
  {
    ID: '1484780787',
    FirstResponder: 'L1 Analyst',
    Owner: 'MSSP Company',
    Title: 'Payload delivery',
    Date: '2024-03-11',
    Severity: 'Critical',
    TLP: 'TLP:RED',
    Description: 'Attacks that exploit IE vulnerability (CVE-2023-0674)',
    Evidence: '56c42374-fdb8-4544-a218-41ffc0a8ab16',
  },
  {
    ID: '13458641216',
    FirstResponder: 'Forensic Analyst-1',
    Owner: 'DFIR Lab',
    Title: 'Ransomware Attack',
    Date: '2024-02-16',
    Severity: 'Critical',
    TLP: 'TLP:RED',
    Description: 'Malware infected end user machine and encrypted the files',
    Evidence: '5af96bd7-f064-40d3-b99f-50b0950d210f6',
  },
]
  
```

Figure 5. Sample blockchain records

#### 4.7. Application

A prototype was developed to evaluate the proposed blockchain-based digital forensic and incident response model. The prototype was built using Node.js and Express.js. MongoDB was chosen as the database. The blockchain component is integrated using Hyperledger Fabric, where case records are securely stored as immutable transactions. Users can access the system through a web-based interface, create new cases and track forensic cases.

The workflow of the prototype is as follows: When a digital forensic expert creates a new case, she/he



provides the case title, priority level, confidentiality level, detailed information, and collected evidence into the system. This data is first stored in MongoDB for quick access. Simultaneously, the case-related data is sent as a transaction to the Hyperledger Fabric blockchain. Each block recorded on the blockchain contains the case's metadata and SHA-256 hash of the collected evidence. This ensures that the chain of custody is recorded properly, and integrity of the evidence remain intact throughout the investigation process.

In addition, an interface has been developed where users can view all forensic cases stored in the system and their historical records by making queries to the blockchain. Users can also query the blockchain to view all forensic cases stored on the network. Through this interface, the performance of data retrieval processes from the blockchain was measured and latency times were analyzed.

The application allows investigators to register themselves on the system, submit case details, and track incidents and cases in real-time. Each case update is recorded both in the traditional database and the blockchain to maintain consistency. The system architecture ensures that forensic evidence remains immutable and auditable, meeting the requirements of digital forensic investigations. Screenshots of the application's operation are provided in Appendix A.

#### 4.8. Simulated case studies and application to real-world examples

We developed two case studies that simulate forensic investigation scenarios. These simulations assess the model's ability to ensure the integrity of digital evidence and chain of custody. In this section, we also discussed how real-world examples of legal cases and cyber attacks could have been managed if our model had been implemented.

##### Case Study 1: Unauthorized Data Access

A financial institution detects unusual activity in its internal network. An employee accessed and exported sensitive client data without authorization. The security team needs to trace the activity and collect digital evidence.

SOC analysts detect the unauthorized access event through SIEM logs. A case is created in DFIRChain and all logs related to the unauthorized access are recorded on the blockchain. The extracted logs, including access timestamps and IP addresses are hashed and stored on the blockchain.

The evidence is submitted to forensic investigators, and all chain of custody actions are logged on the blockchain. Blockchain-based timestamps confirm the exact time of unauthorized access and data exfiltration. The immutable records prevent any

internal attempts to alter or delete the logs. This helps the organization provide accountability when law enforcement is involved.

##### Case Study 2: Digital Evidence Tampering

A law enforcement agency is investigating a cybercrime. The suspect's laptop is seized, and forensic analysts extract crucial documents as evidence. However, before the case reaches trial, the suspect's claims that the digital evidence was altered during the investigation process, questioning its validity in court.

Upon seizing the laptop, forensic analysts generate hash values (SHA-256) for each extracted document and record them on the Hyperledger Fabric blockchain. All interactions with the evidence, including transfers between forensic analysts and court officials, are logged on the blockchain, creating a verifiable audit trail.

Blockchain records confirm that the hash values of the evidence remain unchanged from the initial extraction, proving that no tampering has occurred. The forensic experts present the blockchain-stored timestamps and hashes in court, demonstrating the authenticity and integrity of the evidence. The judge accepts the evidence, as the DFIRChain model ensures its integrity.

To highlight the importance of proper log storing in incident response and digital forensics, we examine two previous legal cases from and a cyber-attack.

##### Real-World Case Application 1: Weiller v. New York Life Insurance Co.

In the case of Weiller v. New York Life Ins. Co., the court ruled that the evidence presented was invalid because the digital documents were not properly preserved [30]. New York Life Insurance failed to preserve electronic files and logs. The company argued that maintaining such digital information in a safe and secure environment would be costly. However, the court ruled that financial difficulty was not a valid excuse and federal preservation requirements were not satisfied [30]. DFIRChain offers a method for evidence preservation by using distributed storage and blockchain for record-keeping. If implemented, DFIRChain could have helped for storing evidence in a tamper-proof system.

##### Real-World Case Application 2: Kucala Enterprises Ltd. v. Auto Wax Co

The risk of manipulation of digital evidence raises the possibility that evidence may be altered in the process of copying. In Kucala Enterprises Ltd. v. Auto Wax Co., Inc. case, the Kucala Enterprises destroyed digital evidence during the trial process using software called Evidence Eliminator [30]. The court considered this action as willful destruction of evidence and dismissed the case [30]. Should DFIRChain had been

implemented, any unauthorized deletion or manipulation of the software or log would have been recorded as a blockchain transaction in a tamper-proof mechanism.

#### Application of a Real-World Cyber Attack to DFIRChain: Equifax

In 2017, Equifax, one of the largest credit reporting agencies in the United States, suffered a data breach. The breach exposed the personal data of 147 million customers [31]. Attackers gained unauthorized access to sensitive data, including names, social security numbers, birth dates, addresses and credit card information by using a previously reported vulnerability. The Equifax incident response team underestimated the vulnerability and didn't take the action to fix the vulnerable software. The victims sued Equifax by opening legal cases to the Equifax. The court ruled Equifax to pay compensation to all victims

as they failed to patch in a timely manner. Equifax refused the claim, but they could not provide sufficient evidence for digital forensics. DFIRChain could have provided transparent tracking of incident response actions to help investigators for checking the actions and logs during the incident.

#### 4.9. Performance analysis

Performance and latency are the most important concerns when using blockchain systems. This section presents the performance tests conducted for the proposed model. To assess the transaction performance of different data sizes on our Hyperledger Fabric network, four test scenarios were run using Hyperledger Caliper. These tests involved processing small (512 KB), medium (1 MB), large (5 MB), and fluctuating (512 KB – 5 MB) data sizes while measuring the key performance metrics.

**Table 2.** Test Scenarios

Scenarios	Description	Block Size	Transactions	Channels
Test 1 - Small Case Add	A case of 512 KB will be added to the blockchain.	512 KB	500	2 Org, 4 Peer
Test 2 - Medium Case Add	A case containing 1 MB of data will be added to the blockchain.	1 MB	500	2 Org, 4 Peer
Test 3 - Large Case Add	A case of 5 MB will be added to the blockchain test system resilience.	5 MB	500	3 Org, 6 Peer
Test 4 - Fluctuating Size	Cases of varying sizes will be sent to the blockchain.	512 KB - 5 MB	5000	3 Org, 6 Peer

**Table 3.** Hyperledger Caliper Test Results

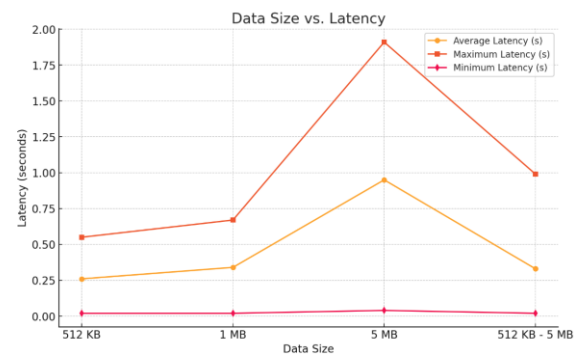
Name	Success	Fail	Send Rate (TPS)	Max Latency	Min Latency	Avg Latency	Throughput (TPS)
small-data (512 KB)	500	0	20,00	0,55	0,02	0,26	20,00
medium-data (1 MB)	500	0	15,00	0,67	0,02	0,34	15,00
large-data (5 MB)	500	0	5,00	1,91	0,04	0,95	5,00
fluctuating-data (512 KB - 5 MB)	500	0	15,30	0,99	0,02	0,33	15,30

The test scenarios shown in Table 2 were developed. These scenarios were defined within Hyperledger Caliper and run on the smart contract deployed in the DFIRChain network. The performance results obtained from the Hyperledger Caliper are shown in Table 3.

In all test scenarios, 500 transactions were successfully run without errors. This shows reliability of our proposed model. The highest transaction rate was observed in the small data scenario (512 KB), reaching 20 TPS. However, as the data size increased, transaction speed decreased, with 5 MB transactions dropping to 5 TPS. In the fluctuating data size scenario, an average TPS of 15.3 was recorded. These results indicate that transaction speed declines as network load increases.

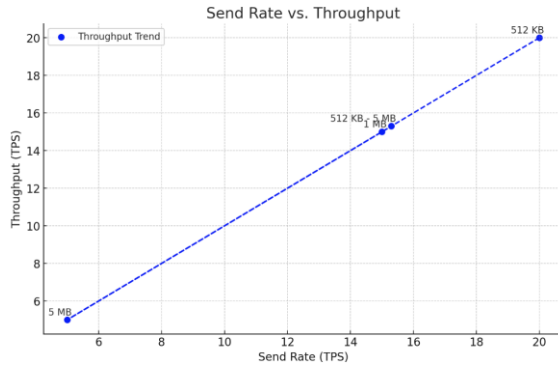
The highest latency was recorded in the large data scenario (5 MB) at 1.91 seconds. In contrast, small data transactions experienced a maximum latency of

0.55 seconds, while fluctuating data sizes resulted in a maximum latency of 0.99 seconds. The average latency for large data transactions was 0.95 seconds, whereas small data transactions exhibited an average latency of 0.26 seconds. Across all test scenarios, the minimum observed latency was 0.02 seconds, particularly for smaller data sizes (Figure 6).



**Figure 6.** Performance Analysis (Data Size vs. Latency)

As the data size increases, the throughput decreases. This is expected because larger transactions take longer to process. However, the fluctuating dataset (512 KB - 5 MB) achieved a TPS close to the medium dataset, meaning that the network adapts well to mixed workloads. Throughput values closely followed transaction speed trends. The measured throughput rates were 20 TPS for small data, 15 TPS for medium data, 5 TPS for large data, and 15.3 TPS for fluctuating-sized data (Figure 7). These results indicate that the system performs efficiently with small and medium-sized transactions but experiences performance degradation in large-scale data processing.



**Figure 7.** Performance Analysis (Send Rate vs Throughput)

Overall, the test results demonstrate that proposed model delivers high performance when handling small to medium-sized transactions but experiences increased latency and reduced transaction speed in large data operations.

#### 4.10. Load tests for a real-world simulation

In blockchain systems, it is important to assess how well system handles increasing numbers of concurrent requests. To evaluate such load tests, we used another test tool, Locust. By using Locust, we measured the real-world performance of the web-based simulation environment. In this section, we provide the result of these load tests.

To assess the scalability of the system under increasingly heavy traffic, three load tests were run. Each test ran for 3 minutes, with varying numbers of concurrent users (Table 4).

**Table 4.** Load Test Scenarios

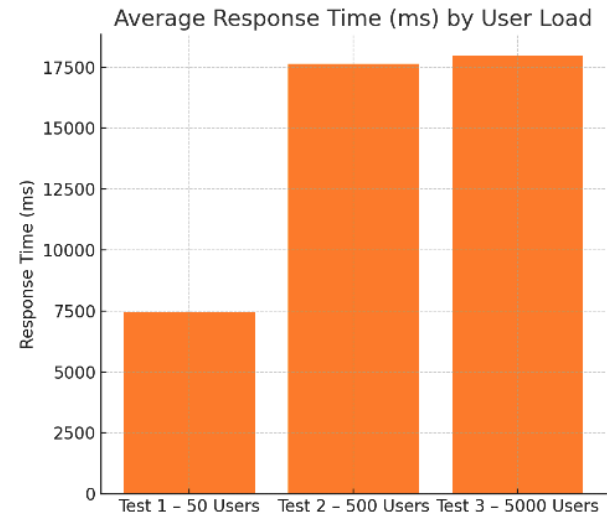
Test	Description	Users	Duration
Test 1	Low-load scenario	50	3 min
Test 2	Medium- scenario	500	3 min
Test 3	High-load scenario	5000	3 min

Each test scenarios sent a HTTP POST requests to the API endpoint. The API endpoint submitted a transaction to the blockchain.

**Table 5.** Load Test Results

Test	Total Requests	Failures	Avg Response Time
Test 1	682	11	7.454 ms
Test 2	622	28	17.638 ms
Test 3	578	19	17.956 ms

As shown in the result (Table 5), there was a significant increase in average response time from 50 users to 500 users. Average response time increased significantly from Test 1 to Test 2, from 7,5 seconds to 17,6 seconds. This was followed by a stable response time between 500 and 5000 users which shows us the saturation level was reach at 500 users. Failure rates is acceptable but highlights performance bottlenecks under real blockchain conditions.



**Figure 8.** Locus Load Tests

#### 4.11. Comparison of the proposed model with existing models

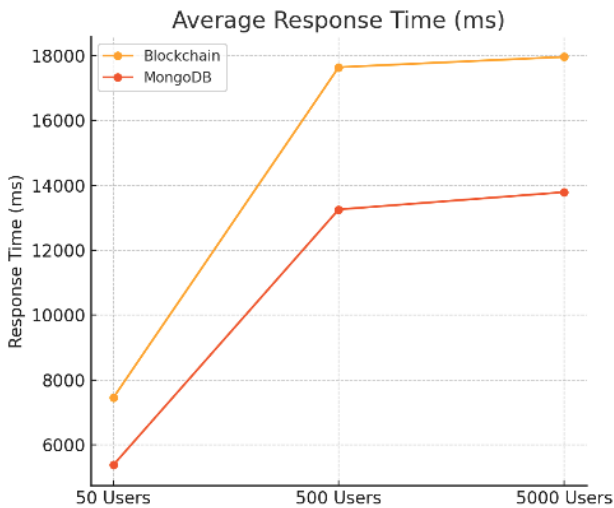
In this section, the proposed digital forensics and incident response model, DFIRChain, will be compared with existing digital forensics models discussed in the previous section, DFRWS, DOJ, and INTERPOL.

DFIRChain provides significant advantages in evidence integrity and traceability by leveraging decentralized and tamper-proof recording mechanisms. Unlike traditional forensic models, which rely on manual documentation and centralized storage, DFIRChain ensures immutable evidence tracking and real-time verification. Our model enhances chain of custody transparency and automates forensic validation. This helps in improving efficiency in legal proceedings. Table 6 highlights the key features in which DFIRChain provides better approaches than traditional frameworks.

**Table 6.** Comparison with Existing Digital Forensics Models

Feature	DFIRChain	DFRWS Model	DOJ Model	INTERPOL Model
Chain of Custody	Immutable tracking with blockchain-based record	Chain of custody is manually documented	Chain of custody is manually documented	Chain of custody is manually recorded
Data Integrity	Hashing, digital signatures, and blockchain	Hashing functions	Hashing functions	Hashing functions
Traceability	Complete traceability as all transactions is permanently recorded on the blockchain	Limited traceability due to human-dependent processes	Limited traceability due to human-dependent processes	Limited traceability due to human-dependent processes
Tamper Prevention	Immutable record structure makes evidence tampering impossible	Limited tamper prevention mechanisms	Traditional forensic methods attempt to prevent tampering	Security procedures aim to prevent tampering
Decentralized Structure	Uses a decentralized structure, eliminating reliance on a central authority	Relies on centralized systems	Relies on centralized systems	Relies on centralized systems

The traditional frameworks of digital forensics use conventional relational database for storing chain of custody and hash of the evidence. These databases are centralized and open to disruption or cyber-attacks. They are not also tamper-proof as opposed to blockchain's immutability. However, these databases offer better performance than blockchain. We compared the performance of DFIRChain with traditional digital forensic models. To evaluate this comparison, we used our web-based simulation platform to store the collected evidence details in a MongoDB database, representing the traditional digital forensic models. We used average response time as metric to compare how MongoDB and DFIRChain was performed under the same test scenarios we discussed in the previous section (Figure 9).

**Figure 9.** Performance comparison of blockchain and MongoDB.

As expected, MongoDB achieves higher throughput and a more efficient response time than DFIRChain. The result demonstrates that tradeoff between performance and immutability should be considered in choosing an application of digital forensics.

The proposed model was also compared to other blockchain based digital forensic models discussed in

Section 2, Forensic-Chain [8], LEChain [11] and ForensicTransMonitor [12]. Each of these models utilizes blockchain technology to enhance forensic investigation processes. However, all these studies focus on post-incident forensic analysis. DFIRChain, on the other hand, integrates incident response and extends to forensic case management. DFIRChain meets industry requirements, whereas the other models primarily focus on enhancing evidence management across various domains.

**Table 7.** Comparison with Blockchain-Based Digital Forensics Models

Feature	DFIRChain	Forensic-chain	LEChain	Forensic TransMonitor
Incident Response	✓	×	×	×
Digital Forensic	✓	✓	✓	✓
Chain of Custody	✓	✓	✓	✓
Case Management	✓	×	×	×

## 5. Conclusion

The decentralized nature of the blockchain ensures that incident response-related transaction records are protected from tampering. Data is stored on a decentralized network, making it difficult to attack a single point and increasing data security. The immutability of blockchain technology increases the accountability of organizations using the proposed model. The model allows legal and technical units of the organizations to participate in the blockchain, enabling them to verify data. If necessary, the law enforcement agencies, courts, forensic laboratories, and law firms can form a consortium and join the blockchain through a channel and make the necessary verifications. The model makes it easier to comply with legal requirements related to data protection such as GDPR (General Data Protection Regulation) of

the EU. Secure and transparent data storage can help to meet these regulatory requirements.

Real-world implementation studies of the model will be carried out in future work. It is planned to expand the application's scope by adding new functionalities that enable forensic experts to register in the system, track assigned cases and incidents in real time, and assign cases to other users or institutions. With this enhancement, every update to a case investigated will be recorded in both the traditional database and the blockchain, ensuring data consistency and interoperability. In ongoing research, the more functional tests with near real time data will be conducted for performance and latency to measure the success of the system and explore development opportunities.

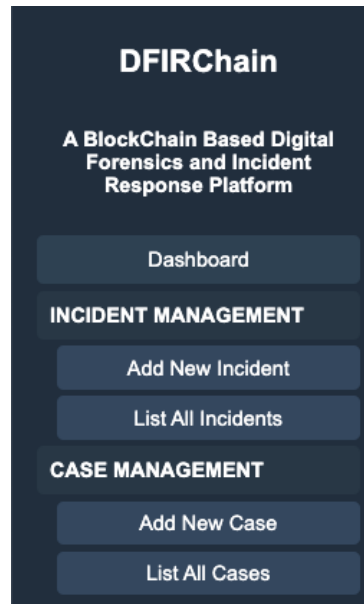
## References

- [1] Sachowski, J. 2019. Implementing Digital Forensic Readiness. 2nd Edition. CRC Press, New York, 503p.
- [2] Communications-Electronics Security Group. Digital Continuity to Support Forensic Readiness; The National Archives, Richmond, UK, 2011.
- [3] International Standards Organization and International Electrotechnical Commission, ISO/IEC 27043 – Information Technology – Security Techniques – Digital Evidence Investigation Principles and Processes. 2012. Geneva, Switzerland.
- [4] Valjarevic, A., Venter, H. 2013. A Harmonized Process Model for Digital Forensic Investigation Readiness. IFIP Advances in Information and Communication Technology, vol 410. Springer. Berlin, Heidelberg.
- [5] Jaquet-Chiffelle, D., Casey, E. 2020. Bourquenoud, J., Tamperproof Timestamped Provenance Ledger Using Blockchain Technology, FSI Digital Investigation. 33.
- [6] Burri, X., Casey, E., Bollé, T., Jaquet-Chiffelle, D. 2020. Chronological independently verifiable electronic chain of custody ledger using blockchain technology, FSI Digit. Investig. 32.
- [7] Lone, A. H., & Mir, R. N. 2018. Forensic-chain: Ethereum blockchain based digital forensics chain of custody. Sci. Pract. Cyber Secur. J, 1, 21–27.
- [8] Lone, A. H., Mir, R. N. 2019. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital investigation. 44–55.
- [9] Li, S., Qin, T., Min, G. 2019. Blockchain-based digital forensics investigation framework in the internet of things and social systems. IEEE Trans. Comput. Soc. Syst. 1433–1441.
- [10] Kim, D., Ihm, S.Y., Son, Y. 2021. Two-Level Blockchain System for Digital Crime Evidence Management.
- [11] Li, M., Lal, C., Conti, M., Hu, D. 2021. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Gener. Comput. Syst. 406–420.
- [12] Alqahtani, S.S., Syed, T.A. 2024. ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. Information. 109.
- [13] Özdemir, A. 2021. Cyber threat intelligence sharing technologies and threat sharing model using blockchain. M.S. - Master of Science. Middle East Technical University.
- [14] Schneier, B., Kelsey, J. 1999. Secure audit logs to support computer forensics. ACM Trans. Inf. Syst. Secur. 2. 159–176.
- [15] LogSentinel. 2018. Merkle trees and I.T. clouds, <https://github.com/LogSentinel/merkle-trees-documentation/releases/download/v0.1/MerkleTrees.pdf> (Access Date: 12.11.2024).
- [16] Moreno J., Serrano M.A., Fernandez E.B., Fernández-Medina E. 2020. Improving Incident Response in Big Data Ecosystems by Using Blockchain Technology. Applied Sciences.
- [17] NIST SP 800-61. 2004. Computer security incident handling guide. <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf> (Access Date: 13.11.2024)
- [18] CMU/SEI-TR-015. 2004. Defining incident management processes for CSIRTs. [https://insights.sei.cmu.edu/documents/1606/2003\\_002\\_001\\_14102.pdf](https://insights.sei.cmu.edu/documents/1606/2003_002_001_14102.pdf) (Access Date: 13.11.2024).
- [19] ITU-T X.1056. 2009. Security incident management guidelines for telecommunications organizations. [https://www.itu.int/dms\\_pub/itu-t/opb/tut/T-TUT-ICTS-2022-PDF-E.pdf](https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-PDF-E.pdf) (Access Date: 14.11.2024).
- [20] Palmer, G. 2001. “A Road Map to Digital Forensics Research”. Report From the First Digital Forensic Research Workshop (DFRWS)
- [21] DOJ. 2008. Digital Forensics Analysis Methodology. <https://www.justice.gov/sites/default/files/usa/legacy/2008/02/04/usab5601.pdf> (Accessed Date: 12.03.2025)
- [22] INTERPOL. 2019. Global Guidelines for Digital Forensics Laboratories. [https://www.interpol.int/content/download/13501/file/INTERPOL\\_DFL\\_GlobalGuidelinesDigitalForensics](https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics) (Accessed Date: 12.03.2025)

- [23] Gupta, M. 2017. Blockchain For Dummies. 3rd IBM Limited Edition. John Wiley & Sons Inc. 51p.
- [24] Wüst, K., Gervais, A. 2018. "Do you need a blockchain?". 2018 Crypto Valley, Conference on Blockchain Technology (CVCBT). 45–54. IEEE.
- [25] Baset, S. A., et al. 2018. Hands-On Blockchain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer. Packt Publishing, Limited.
- [26] R3. 2024. Corda 5.2: Key Concepts. <https://docs.r3.com/en/platform/corda/5.2/key-concepts.html> (Accessed Date: 10.03.2025).
- [27] GoQuorum. 2025. GoQuorum Documentation. <https://goquorum.readthedocs.io/> (Accessed Date: 10.03.2025).
- [28] IOTA. 2025. IOTA Architecture: Consensus. <https://docs.iota.org/about-iota/iota-architecture/consensus> (Accessed Date: 10.03.2025).
- [29] Gürfidan, R., Tatlı, M. 2023. Performance Comparison of Secure Storage Methods for Digital Forensic Evidence. Uluslararası Sürdürülebilir Mühendislik ve Teknoloji Dergisi. 7(2). 131-138.
- [30] Ami-Narh, J. T., & Williams, P. A. H. 2008. Digital forensics and the legal system: A dilemma of our times. Paper presented at the 6th Australian Digital Forensics Conference 10.4225/75/57b268ce40cb6
- [31] Equifax Data Breach. <https://archive.epic.org/privacy/data-breach/equifax/>. (Accessed Date: 25.03.2025)

## Appendices

### Appendix A. User Interfaces of the Simulated Web Application for the Proposed Model





Create a New Case

**Case Details**

Title \*

Assign Analyst \*

Select Analyst
▼

Severity \*

Select Severity
▼

Date \*

dd.mm.yyyy, --:--
📅

TLP \*

Select TLP
▼

Description \*

Evidence \*

Choose File

No file chosen

Create Case

Case Management					
TITLE	ANALYST	SEVERITY	DATE	TLP	DESCRIPTION
Data Breack	analyst2	Low	3/5/2025	WHITE	Pll data leaked online.
System Breach	analyst3	Low	3/15/2025	WHITE	Unauthorized access detected
Phishing Attack	analyst3	High	3/14/2025	AMBER	Phishing email clicked
DDoS	analyst2	Medium	3/7/2025	GREEN	DDoS is ongoing
Malware Infection	analyst4	Critical	3/7/2025	RED	Malware infected PC detected.
Data Leak	analyst1	Low	3/7/2025	WHITE	Data Leak Detected
Phishing Domain	analyst3	Medium	3/7/2025	GREEN	A new impersonating domain registered.
Brute-Force	analyst1	Medium	3/7/2025	WHITE	Brute-force attack is performed.
Unauthorised scan	analyst4	High	3/8/2025	AMBER	Unauthorised scan detected.
Critical Open Port	analyst2	Medium	3/5/2025	WHITE	Critical open port detected:SSH
Open Port	analyst1	Low	3/7/2025	GREEN	Open port detected
Open Port	analyst2	Medium	3/7/2025	WHITE	FTP port detected.
Zero Day Exploit	analyst4	Critical	3/12/2025	RED	Zeroday exploited
Fake Social Media	analyst2	Medium	3/8/2025	AMBER	Fake social media detected
CVE Vulnerability	analyst3	High	3/9/2025	WHITE	CVE Detected
Malware Infection	analyst1	Low	3/8/2025	WHITE	Malware infected PC detected.
Data Leak	analyst1	Medium	3/9/2025	WHITE	Data leak discovered
Sql Injection	analyst2	Critical	3/15/2025	WHITE	Sql injection detected
Data Lost	analyst4	Critical	3/16/2025	RED	Data lost reporrted
DNS Amplification	analyst1	High	3/8/2025	WHITE	DNS Amplification observed.