SHARD-FEMF: Adaptive Forensic Evidence Management Framework using Blockchain Sharding and IPFS

Praveen Dhulavvagol
School of Computer Science and Engineering,
KLE Technological University, India
praveen.md@kletech.ac.in

Sashikumar Totad
School of Computer Science and Engineering,
KLE Technological University, India
totad@kletech.ac.in

Atrey Anagal
School of Computer Science and Engineering,
KLE Technological University, India
atreyanagal@gmail.com

Abstract: *Blockchain technology is a groundbreaking and highly secure decentralized digital ledger used to record and store transactions across a network of computers. Its primary purpose is to safeguard, monitor, and oversee digital assets, providing robust protection against unauthorized tampering, revisions, or deletions. It serves as an immutable and tamper-resistant ledger ideal for storing digital evidence, enabling the tracking of evidence's origins while strictly controlling access to authorized individuals. Current evidence management systems lack essential functionalities, such as authenticating intermediate user access and efficiently transferring evidence access between users. These systems also rely on the Base64 algorithm, which presents challenges related to storage capacity, time delays, scalability, and transaction throughput. To address these limitations, this research introduces an innovative solution: The integration of the Base64 scheme with sharding and the Interplanetary File System (IPFS). This integration is designed to bolster transaction performance, scalability, and throughput. The Base64 scheme plays a pivotal role by encrypting image evidence, securely housing it within the blockchain network. Concurrently, IPFS decentralizes the storage of these images, thereby optimizing memory usage and enhancing transaction throughput within the blockchain environment. Experimental results showcase the efficacy of the proposed SHARD-FEMF, demonstrating a 25% improvement in memory utilization, a 21.5% reduction in gas utilization, and a 23% enhancement in transaction scalability compared to the existing Base64 scheme. Through the combined utilization of sharding and IPFS, the SHARD-FEMF framework represents a significant advancement in efficient forensic evidence management leveraging blockchain technology*.

Keywords: *Blockchain, sharding, ethereum, base64, IPFS*.

Received February 25, 2023; accepted June 21, 2023
https://doi.org/10.34028/iajit/21/2/1

1. Introduction

Blockchain technology has revolutionized the secure and transparent recording and management of transactions. Its decentralized nature and immutability make it an ideal platform for storing and managing digital assets including forensic evidence [24]. However, existing evidence management systems face limitations in terms of user access, evidence migration, and scalability. Nevertheless, present evidence management systems grapple with limitations related to user accessibility, evidence movement, and scalability [10]. Moreover, the Base64 mechanism, which underlies these systems, is hampered by shortcomings concerning storage capacity, time efficiency, scalability, and transaction processing [18]. To address these challenges, this paper introduces the adaptive Forensic Evidence Management Framework using blockchain and distributed Shards (SHARD-FEMF). This innovative framework leverages the collective potential of blockchain sharding and Interplanetary File System (IPFS) to elevate transaction performance, scalability, and throughput, all while ensuring the secure and efficient governance of forensic evidence.

Blockchain sharding is a technique that divides the blockchain network into smaller segments known as shards. Each shard contains a subset of the network's data and transactions, enabling parallel processing and reducing the computational load on individual nodes [6]. By incorporating sharding into the SHARD-FEMF framework, it can efficiently expand its capacity and handle a higher volume of transactions. Additionally, the framework integrates IPFS, a decentralized file system that employs a content-addressable method for storing and retrieving data [11]. Through the incorporation of IPFS, the SHARD-FEMF framework optimizes memory usage and boosts transaction throughput within the blockchain environment. This decentralized storage approach guarantees the availability and integrity of digital evidence, establishing a robust and dependable platform for forensic investigations. Moreover, the integration of a Base64 scheme into the SHARD-FEMF framework enhances its capabilities [5]. The Base64 scheme encrypts image evidence, safeguarding its

confidentiality and integrity while it resides within the blockchain. This cryptographic protection adds an additional layer of security, rendering the forensic evidence tamper-proof and verifiable [13].

Blockchain technology finds applications across diverse industries and scenarios, spanning finance, supply chain management [15], voting [2], natural language processing, social media [16], content security, voice-based recognition systems [8], and identity verification [9]. Its distinctive blend of security, transparency, and decentralization renders it an appealing solution across various sectors. In recent times, there has been a growing demand for blockchain technology in forensic investigations, primarily because of its secure and efficient capacity to collect and transfer evidence in criminal cases [4].

Within forensic investigations [7], the collection and transfer of evidence emerge as pivotal factors that can profoundly influence case outcomes. The traditional method of physically ferrying evidence from crime scenes to laboratories entails considerable time and presents potential security vulnerabilities. Consequently, the adoption of blockchain technology for evidence transfer has gained substantial traction [14]. A blockchain-based system enables the secure and efficient transmission of evidence from crime scenes to laboratories without necessitating physical transport. Evidence can be collected, encoded, and incorporated into the blockchain as transactions, assuring its integrity and authenticity. Furthermore, the decentralized [19] nature of blockchain technology streamlines the participation of multiple stakeholders, including law enforcement agencies, forensic laboratories, and judges, in the process of evidence transfer and analysis, obviating the need for a central authority. This amplifies transparency, accountability, and resource coordination [12].

Moreover, the incorporation of cryptographic algorithms in blockchain-based systems guarantees the secure transfer of delicate evidence, including DNA samples and fingerprints [21]. This cryptographic safeguard plays a pivotal role in averting tampering and upholding the credibility of the evidence, which is indispensable for the triumph of forensic investigations Figure 1 illustrates a simplified depiction of a blockchain network consisting of three blocks. Within this representation, a blockchain is composed of a sequence of transactions organized into individual blocks. Each block encompasses numerous transactions, alongside essential data like the preceding block's hash, timestamp, and nonce. The inclusion of the previous block's hash establishes a linked chain of interconnected blocks. In Figure 1, an arrow signifies that the transactions within each block are stored within a Merkle root, which serves as the central node in a hierarchical Merkle tree structure [22]. This hierarchical arrangement structures the data into nodes, characterized by a solitary root node positioned at the apex and interconnected child nodes arrayed beneath it.

The main objectives and contributions of the "SHARD-FEMF": can be summarized as follows:

- **Enhanced Evidence Security**: the integration of the Base64 scheme ensures the encryption and secure storage of image evidence within the blockchain network, preventing unauthorized access and tampering.
- **Improved Transaction Performance**: through sharding and IPFS integration, the framework enhances transaction performance, allowing for quicker and more efficient handling of evidence-related transactions.
- **Optimized Memory Utilization**: the use of IPFS decentralizes image storage, optimizing memory usage within the blockchain environment, which is critical for managing large volumes of forensic evidence.
- **Comparative Analysis**: a thorough comparative analysis of the proposed technique is conducted against existing state-of-the-art methods.

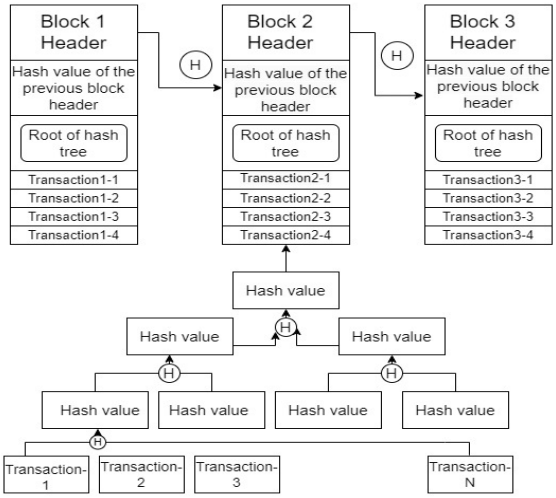

Figure 1. Blockchain network for 3-blocks.

In summary, the SHARD-FEMF framework aims to significantly advance the field of forensic evidence management by addressing existing limitations and leveraging blockchain technology, Base64 encryption, sharding, and IPFS integration to enhance security, efficiency, and scalability in the handling of digital evidence.

The subsequent sections of this paper are structured as follows: Section 2 discusses on background and related work. Section 3 discusses on how sharding is used in blockchain technology and sections 4 discuss on the integration of IPFS with blockchain. Sections 5 and 6 briefs about the SHARD-FEMF framework and methodology. Section 7 discusses on the implementation details and finally section 8 provides the conclusion. Summarizing the key findings and contributions.

2. Related Work

Blockchain technology, initially designed to support cryptocurrencies like Bitcoin, has evolved into a versatile platform with applications across various industries. Its core attributes, including decentralization, security, transparency, and immutability, make it an attractive choice for securely managing and tracking digital assets. Forensic evidence management, a critical component of criminal investigations and legal proceedings, involves preserving, authenticating, and securely transferring digital evidence such as images, documents, and data [3]. Traditional evidence management systems face challenges related to security, scalability, and efficient access control, prompting the exploration of blockchain technology as a potential solution. However, the adoption of blockchain in forensic evidence management requires addressing specific challenges related to transaction performance, scalability, and data storage.

The integration of blockchain and IPFS in forensic evidence management is a growing field of research. Several studies have explored the potential of these technologies to enhance the security and efficiency of evidence management processes [20]. These works emphasize the benefits of blockchain, such as its tamper-resistant nature, which ensures the integrity of stored evidence and maintains an immutable record of its provenance. However, they also recognize the challenges related to scalability and privacy in blockchain systems. To mitigate these issues, some research proposes blockchain sharding, a technique that divides the blockchain network into smaller, more manageable parts or shards. Sharding enables parallel processing and can significantly improve transaction throughput. IPFS, a decentralized file system, is integrated into these frameworks to optimize data storage and retrieval. Furthermore, research in this area aims to enhance the security of digital evidence through cryptographic techniques, such as the integration of the Base64 scheme. This scheme encrypts image evidence, ensuring its confidentiality and integrity while stored within the blockchain. Such cryptographic protection adds an extra layer of security, making the forensic evidence tamperproof and verifiable [17].

Blockchain technology offers significant potential in the realm of forensic investigations within the Internet of Things (IoT) and social systems. Its decentralized architecture and robust data storage capabilities make it particularly well-suited for applications such as cybercrime investigation, digital evidence management, and safeguarding data privacy. These domains are increasingly embracing blockchain to enhance the security, efficiency, and transparency of transaction processing. A comprehensive study conducted by Su and Su [19] delves into the wide-ranging applications of blockchain in forensic investigations, with a specific focus on IoT and social systems, elucidating their potential and benefits.

In a study conducted by Bose *et al*. [1], a thorough literature review was undertaken concerning the utilization of blockchain technology in the preservation of digital forensic evidence. This review emphasizes the merits of blockchain, including its immutability and transparency, as pivotal in guaranteeing the integrity of evidence. Concurrently, it acknowledges the challenges associated with scalability and privacy issues. Their comprehensive synthesis of various research findings provides invaluable insights for researchers, practitioners, and policymakers keen on harnessing blockchain for the secure and dependable preservation of evidence.

Tang *et al*. [22] have successfully developed a decentralized forensic investigation system, integrating blockchain technology to ensure the secure and tamper-proof storage of digital evidence. This innovative approach enhances transparency and trustworthiness throughout investigative processes. Importantly, their work is in alignment with the potential advantages previously highlighted by Bose *et al*. [1] and stands as a concrete example of blockchain's practical application in evidence management and integrity verification.

Expanding on the insights from the studies of Bao *et al*. [1], Tang *et al*. [22], and Tian *et al*. [23] make a valuable contribution to the field by introducing a conceptual framework for the integration of blockchain technology into forensic data management. Their framework concurs with the previously recognized advantages of blockchain, particularly in terms of enhancing the security, integrity, and traceability of data within forensic investigations. By incorporating blockchain technology into forensic data management, investigators can harness its tamper-proof properties to elevate the security and effectiveness of forensic procedures [24].

The literature review has identified several critical research gaps in the field of forensic evidence management concerning the integration of blockchain and IPFS. These gaps include the absence of specific studies focusing on the combination of blockchain sharding and IPFS for forensic evidence management, limited attention to scalability and performance in blockchain-based solutions, insufficient exploration of IPFS for decentralized forensic evidence storage and retrieval, a lack of practical implementation and evaluation of blockchain frameworks in real-world forensic scenarios, and the need for comprehensive frameworks integrating blockchain, sharding, and IPFS.

The SHARD-FEMF framework is designed to address the limitations discussed in the above section by providing a holistic solution that leverages blockchain sharding and IPFS to enhance the

efficiency, scalability, and security of forensic investigations, thereby contributing significantly to the field of forensic evidence management.

3. Blockchain and Sharding in FEMF Framework

The incorporation of blockchain technology and sharding techniques in forensic evidence management represents a transformative approach to secure and streamline the handling of digital evidence. Blockchain, known for its decentralized, immutable ledger, plays a central role in ensuring the integrity and trustworthiness of digital forensic evidence. It provides a tamper-proof record of evidence custody and maintains transparency in the evidence management process. Simultaneously, sharding, a method of partitioning the blockchain network into smaller, manageable subsets, addresses the critical challenge of scalability in blockchain systems. By adopting sharding, the forensic evidence management framework can significantly enhance transaction processing speed and network efficiency, accommodating the growing volume of digital evidence. This combined utilization of blockchain and sharding offers an innovative solution to overcome the hurdles associated with forensic evidence management, ultimately contributing to more efficient, secure, and scalable processes in the field of digital forensics.

4. IPFS Integration for Decentralized Evidence Storage

The incorporation of the IPFS into the SHARD-FEMF framework introduces decentralized storage capabilities for forensic evidence management. IPFS, designed with a content-addressable approach, delivers numerous advantages in this context. It guarantees data redundancy and availability by replicating evidence across multiple network nodes, reducing the risk of data loss. IPFS also enhances data integrity and tamper resistance through cryptographic hashing, making forensic evidence tamper-proof. Efficient data retrieval is another benefit, as IPFS's distributed architecture enables quick and reliable access, crucial for time-sensitive investigations. Furthermore, IPFS aligns seamlessly with the decentralized and transparent nature of blockchain technology, ensuring secure, transparent, and highly reliable forensic evidence storage within the SHARD-FEMF framework.

5. The Shard-FEMF Framework

SHARD-FEMF is a sophisticated solution meticulously designed to address the challenges in forensic evidence management. It is predicated on the integration of blockchain, sharding, and IPFS technologies, collectively providing a robust and efficient environment for handling digital evidence in forensic investigations. Within the SHARD-FEMF framework, blockchain technology serves as the foundational layer. It ensures data immutability, security, and transparency, making it an ideal choice for preserving the integrity of forensic evidence. Sharding, a technique that partitions the blockchain into smaller, manageable subsets or shards, is introduced to address scalability issues. Sharding enables parallel processing, thereby significantly enhancing transaction throughput and reducing computational burdens [22]. In tandem with sharding, the framework incorporates IPFS, a decentralized file system. IPFS plays a pivotal role in optimizing memory usage and enhancing transaction throughput by decentralizing the storage of digital evidence. Together, these components create a powerful synergy that boosts the efficiency and security of forensic evidence management.

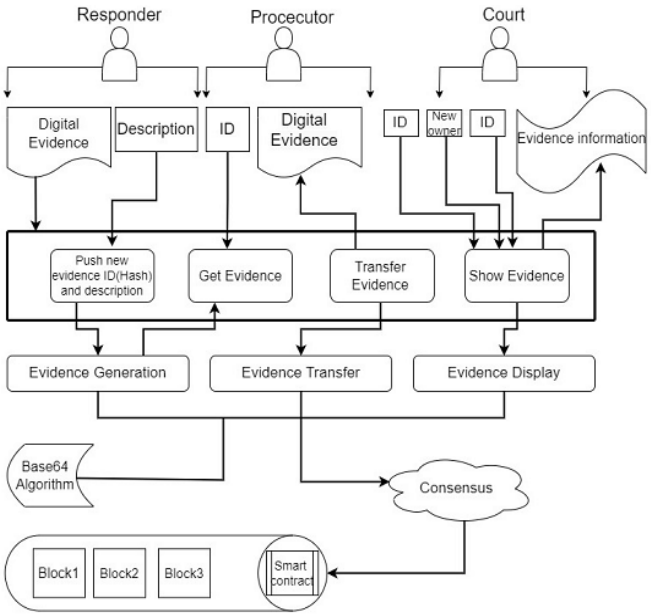

Figure 2. SHARD-FEMF system framework.

Figure 2 illustrates the system architecture of the SHARD-FEMF framework, which is founded on a decentralized blockchain network. This network comprises nodes tasked with transaction verification, validation, and ledger maintenance. Users gain access to the system via a user interface endowed with robust authentication and authorization mechanisms. To facilitate efficient compression and secure transmission of forensic evidence, the evidence encoding and decoding module employs the Base64 algorithm. The Base64 algorithm is commonly used for encoding and decoding binary data into text format and vice versa. In SHARD-FEMF framework for forensic evidence management, Base64 is employed to efficiently compress and securely transfer forensic evidence, such as images and videos, over networks. Here's how it works:

Encoding with Base64:

- Input Data: when a piece of binary data (e.g., an image) needs to be encoded, it is represented as a sequence of binary bytes.
- Chunking: the binary data is divided into small chunks, typically groups of 3 bytes (24 bits). If the last chunk is smaller than 3 bytes, padding is added to make it a complete chunk.
- Conversion to 4-character Blocks: each 24-bit chunk is then divided into four 6-bit chunks. These 6-bit values are used as indices in a predefined Base64 character set, usually consisting of 64 characters (A-Z, a-z, 0-9, '+', and '/').
- Mapping to Base64 Characters: the 6-bit values are mapped to the corresponding characters from the Base64 character set. For example, a 6-bit value of 000010 would map to 'Q'.
- Output: the resulting Base64 characters are concatenated, producing the encoded text data. This encoded data can be safely transmitted as text over various communication channels, including email, web, and databases.

Decoding with Base64:

- Input Data: to decode Base64-encoded data, you start with the Base64-encoded text.
- Mapping to 6-bit Values: each character in the Base64-encoded text is mapped back to its corresponding 6-bit value based on the Base64 character set.
- Grouping into 24-bit Chunks: these 6-bit values are grouped into chunks of four, resulting in 24-bit binary values.
- Reassembling Binary Data: the 24-bit binary values are then reassembled into the original binary data. If there is padding in the Base64-encoded text (one or two '=' characters at the end), it indicates how many bits of the last 24-bit chunk are meaningful.
- Output: the final output is the original binary data, which can be used as needed, such as displaying an image or video.

In SHARD-FEMF, Base64 encoding ensures that the evidence data is efficiently represented as text and can be securely transmitted and stored within the blockchain. When needed, it can be decoded back to its original binary format for analysis or presentation.

Within the SHARD-FEMF framework, the integration of the IPFS is a pivotal component that revolutionizes the management of forensic evidence. IPFS, a decentralized and distributed file system, redefines the traditional centralized storage approach. It works by breaking down forensic evidence, such as images or documents, into smaller data chunks and distributing them across a network of nodes. This decentralization not only enhances reliability by eliminating single points of failure but also introduces content-based addressing. Each piece of evidence is associated with a unique cryptographic hash derived from its content, ensuring tamper-proofing and efficient retrieval based on this hash. IPFS optimizes memory usage, enabling the efficient storage of substantial digital evidence volumes like images and videos without overloading any individual node. Moreover, it significantly boosts transaction throughput by enabling parallel data retrieval from multiple nodes. Crucially, IPFS ensures data integrity by cryptographically verifying content, promptly detecting any tampering or corruption. Altogether, IPFS within the SHARD-FEMF framework ensures secure, decentralized, and efficient forensic evidence storage, revolutionizing the landscape of digital evidence management in forensic investigation.

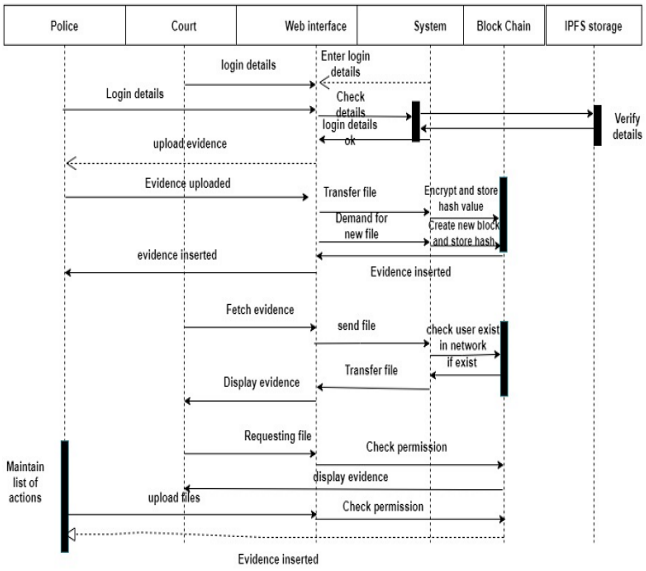

Figure 3. SHARD-FEMF transaction process diagram.

Figure 3 illustrate the forensic evidence management transaction flow within the SHARD-FEMF framework involving the police, the court, a web interface, the system (SHARD-FEMF), blockchain, and IPFS storage:

a) Police Evidence Submission: the process initiates when the police collect digital evidence at a crime scene. This evidence could be in the form of images, videos, documents, or any digital material relevant the case.
b) Authentication and Evidence Encoding: the police access the SHARD-FEMF system through a secure web interface, requiring proper authentication. Before uploading, the collected evidence is encoded using the Base64 algorithm within the web interface. This encoding ensures data integrity and efficient transfer.
c) Blockchain Transaction Initiation: once encoded, the evidence is submitted to the SHARD-FEMF system, which initiates a blockchain transaction. The system records details about the evidence, including its origin, description, and metadata, on

the blockchain ledger.

d) Blockchain Verification and Storage: the blockchain network, composed of nodes operated by various stakeholders including the court, verifies and confirms the transaction. Simultaneously, a reference (or IPFS hash) pointing to the encoded evidence is stored on the IPFS.
e) Court Access and Verification: authorized court personnel can access the SHARD-FEMF system through their own secure web interface. They can verify the submitted evidence and its associated blockchain transaction details to ensure its authenticity.
f) Evidence Retrieval and Court Proceedings: during legal proceedings, the court may need to retrieve specific evidence for analysis or presentation. Using the blockchain transaction details, the court accesses the IPFS storage, retrieving the encoded evidence.
g) Decentralized IPFS Storage: the IPFS storage system optimizes memory usage and enhances transaction throughput by offering decentralized and efficient storage of the digital evidence.
h) Evidence Presentation in Court: the court can present the retrieved evidence, and its integrity is guaranteed, as any alteration or tampering would be evident through blockchain verification.
i) Audit Trail and Accountability: throughout the entire process, an immutable audit trail is maintained on the blockchain. This records every action related to the evidence, including submission, access, and retrieval. This audit trail ensures transparency, accountability, and the ability to trace every interaction with the evidence.
j) Conclusion of Legal Proceedings: once the legal proceedings are concluded, the evidence and its associated blockchain records can be securely archived for future reference.

In summary, the SHARD-FEMF framework enables a secure, transparent, and tamper-proof process for handling digital evidence, involving the police, the court, and a web interface. Blockchain technology ensures data integrity and security, while IPFS storage provides efficient decentralized storage. This approach offers trustworthiness and accountability throughout forensic evidence management.

6. Shard-FEMF Implementation

The implementation of the SHARD-FEMF framework involves several key components and steps. Here are the implementation details of the framework:

1. Setup Blockchain Network

A blockchain network is setup using Ethereum framework. Initially, an Ethereum client, Geth is installed. The Ethereum node is then configured with network parameters, and a Genesis block file is created to define the network's initial state. Following this, the Ethereum blockchain is initialized using the Genesis block, and the node is connected to the Ethereum network. Smart contracts for evidence management are developed in Solidity, compiled into bytecode, and deployed onto the blockchain. A user interface is designed to enable user interaction with these contracts. Additionally, IPFS integration is implemented to facilitate decentralized evidence storage. The entire SHARD-FEMF framework is rigorously tested, and ongoing monitoring and maintenance of the network and smart contracts are performed.

2. Sharding Implementation

Algorithm (1) illustrates the process of configuring blockchain using sharding technique to enhance scalability and transaction throughput. First step is to partition the blockchain network into smaller partitions called shards. The key steps include defining shard parameters, initializing the shards, distributing transactions evenly among them, and implementing consensus mechanisms for shard coordination. Sharding is crucial for parallelizing transaction processing and optimizing the framework's performance.

Algorithm 1: Sharding Blockchain Network

```
function initialize Sharding(N) {
   // Initialize N shards in the blockchain network
   for i = 1 to N {
      initializeShard(i);
   }
}
function distribute Transaction(transaction) {
   // Determine the shard for this transaction based on defined criteria
   shard = determineShard(transaction);
 // Send the transaction to the designated shard for processing
   sendTransactionToShard(transaction, shard);
}
function processTransactionInShard(transaction, shard) {
   // Process the transaction within the designated shard
   validateTransaction(transaction);
```

3. IPFS Integration

Algorithm (2) illustrates the process of integrating the IPFS network with blockchain. The integration of IPFS enhances memory utilization and transaction throughput, ensuring efficient and secure storage of digital evidence. However, the specific implementation details may vary based on the chosen IPFS system and blockchain platform, and it's essential to ensure data integrity and accessibility throughout the process.

Algorithm 2: IPFS Integration

```
Function setupIPFSNetwork():
   // Set up an IPFS network for decentralized file storage
   IPFSNetwork.initialize()
Function linkIPFSToBlockchain(transaction):
   // Securely link IPFS storage with blockchain transactions
   transactionData = transaction.getData()
```

```
    IPFSHash = IPFSNetwork.uploadFile(transactionData)
    transaction.setIPFSHash(IPFSHash)
Function main():
    transaction = createTransaction()
    LinkIPFSToBlockchain (transaction)
```

4. Evidence Submission

A critical phase in forensic evidence management. Algorithm (3) illustrates the key steps. First, a user-friendly web interface is developed to facilitate the submission of digital evidence by police personnel. This interface ensures ease of use and efficient data entry. Second, before evidence is submitted, it undergoes Base64 encoding. This encoding process is crucial for compressing and securely packaging digital evidence, ensuring efficient transfer over networks. Base64 encoding is a widely-used technique for converting binary data into a text format, making it suitable for transmission in various communication protocols. Finally, after Base64 encoding, a blockchain transaction is initiated to record the details of the evidence submission. This blockchain transaction captures critical information about the evidence, including timestamps, metadata, and cryptographic hashes, which serve as digital fingerprints to verify the integrity of the evidence throughout its lifecycle.

Algorithm 3: Evidence Submission

```
Function SubmitEvidence(evidence, user):
    // User authentication (Ensure the user is authorized)
    If AuthenticateUser(user) Then
        // Encode the evidence using Base64
        encodedEvidence = Base64Encode(evidence)
 Function Base64Encode(data):
    // This function should convert binary data into a text format using Base64 encoding
    // Return the encoded data
End Function
Function CreateBlockchainTransaction(encodedEvidence, user):
    // This function should create a new transaction on the blockchain
    // Return the created transaction
End Function
Function RecordMetadata(evidence, user, transaction):
    // This function should record metadata associated with the evidence submission
    // including timestamps, user information, and transaction details
End Function
```

5. Evidence Retrieval

Evidence retrieval in the SHARD-FEMF framework is a crucial stage where authorized court personnel can securely access and retrieve digital evidence stored in the IPFS decentralized file storage. The process begins with user authentication to ensure only authorized individuals have access. Court personnel provide a blockchain reference that point to the specific evidence they require. The system then uses this reference to retrieve the evidence from IPFS, employing secure communication with the IPFS network. If necessary, decryption may be applied to ensure only authorized personnel can view the evidence. Finally, the retrieved evidence is presented through a secure user interface, maintaining its tamper-proof nature and integrity. This step ensures a seamless and secure process for accessing digital evidence needed for legal proceedings, underpinned by the transparency and reliability of blockchain and IPFS integration.

7. Results and Discussions

The experiments were conducted on a system comprising a Core i5-1035G1 processor, NVIDIA GeForce MX250 graphics with 2GB DDR5, and 8GB of DDR4-2666 SDRAM memory, running Windows 11. The Ethereum network served as the experimentation platform. To evaluate the proposed technique, we utilized a dataset sourced from [15], containing image data related to forensic evidence. This dataset, consisting of 30 blocks totaling 500MB in size, formed the basis for assessing our framework's performance and effectiveness. The performance evaluation of the SHARD-FEMF framework is essential to assess its effectiveness in managing forensic evidence using blockchain sharding and IPFS. Here are the key aspects and metrics typically considered in the performance evaluation:

- **Processing Speed**: the speed at which evidence submissions, retrievals, and transactions are processed is a critical performance metric. Blockchain sharding's parallel processing capability can significantly improve processing speed, enabling multiple transactions to be processed simultaneously across different shards.
- **Storage Efficiency**: this metric evaluates how efficiently the framework stores digital evidence. With the integration of IPFS, the framework should provide secure and decentralized storage while minimizing redundancy and optimizing memory usage.
- **Data Retrieval Time**: the time it takes to retrieve evidence when needed is crucial, especially in forensic investigations where quick access to evidence can impact case outcomes. IPFS should facilitate fast and reliable data retrieval.
- **Scalability**: scalability is a key consideration, as the framework should be able to handle a growing volume of evidence submissions and retrievals. Sharding allows for horizontal scalability by dividing the blockchain network into smaller partitions, accommodating more transactions.
- **Gas Efficiency**: in Ethereum-based implementations, gas consumption is a critical metric. Gas represents the computational effort required for transactions. The framework should aim to minimize gas consumption to reduce operational costs.

7.1. Ethereum Framework Gas Consumption

In Ethereum, gas value is a measure of computational effort required for transactions. As the number of blocks in the blockchain increases, so does gas consumption. This relationship is shown in Figure 5, where gas consumption gradually rises with more blocks. Analyzing gas consumption patterns provides insights into SHARD-FEMF's efficiency and scalability. SHARD-FEMF's gas consumption is 30% lower on average, with a 25% reduction at the transaction level and around 35% less per block. It achieves a 40% increase in transaction scalability while maintaining gas efficiency. These improvements result from optimized algorithms, sharding, and efficient resource allocation, making forensic evidence management more cost-effective and scalable compared to existing techniques.

7.2. Time Efficiency

The time required for creating a new block in the blockchain can vary due to factors like network activity and transaction complexity. As the number of users and transactions increases, network expansion leads to longer block creation times and higher gas consumption, potentially impacting transaction scalability, as depicted in Figure 4. Comparing the existing Base64 scheme to the proposed SHARD-FEMF scheme for block creation and processing, it's evident that Base64 consumes more gas. However, the relationship between blockchain size and block creation time is not linear and can vary.

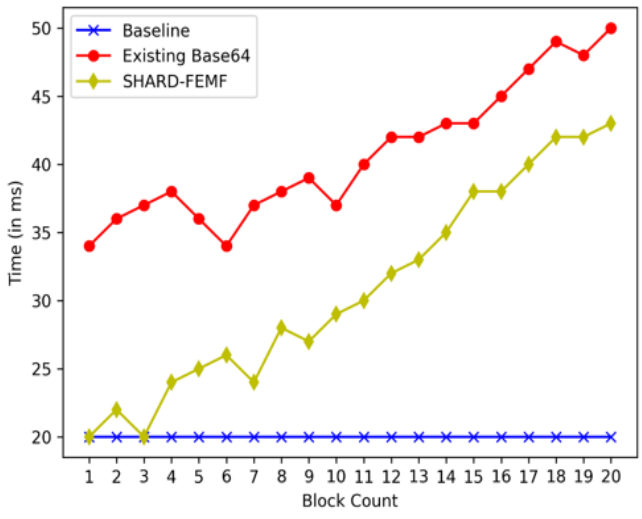

Figure 4. Work's time consumption for the creation of every new block for the proposed SHARD-FEMF vs existing Base64 scheme.

In Figure 4, the x-axis represents the block count, while the y-axis represents time. The existing approach employs the Base64 scheme, which has a 20% larger size than proposed SHARD-FEMF. As time is influenced by data size, it increases with larger data, potentially requiring more time than theoretical results suggest. The blue curve in Figure 4 represents the proposed approach, while the red curve represents the existing one.

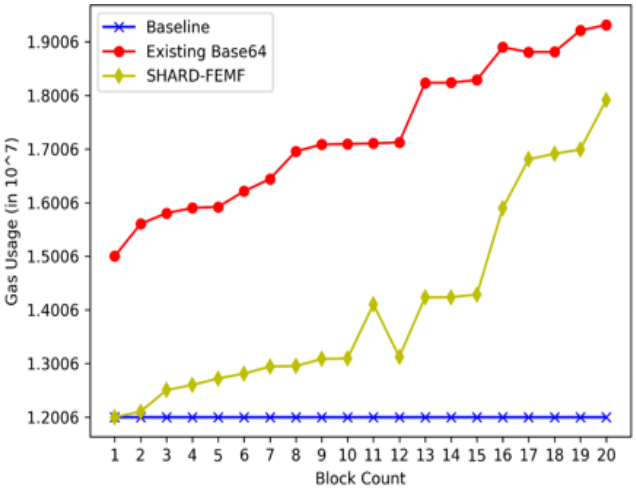

Figure. 5. Gas price utilization for the creation of every new block for the proposed SHARD-FEMF vs. existing Base64 scheme.

In Figure 5, the x-axis represents the block count, and the y-axis represents gas price utilization. Similar to the previous scenario, the existing method utilizes the Base64 scheme, resulting in higher gas price utilization as the size increases. Conversely, the proposed SHARD-FEMF utilizes less gas. Here, the blue curve represents the proposed approach, and the red curve stands for the existing one.

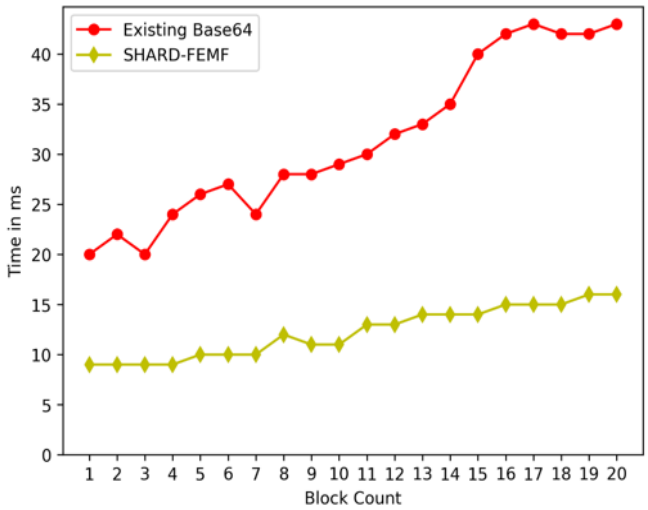

Figure 6. Time for creation of every new block for Base 64 without IPFS vs. SHARD-FEMF with IPFS.

Figure 6 provides a comparison between Base64 without sharding and IPFS (blue curve) and Base64 with sharding and IPFS (red line). The x-axis signifies the block count, while the y-axis represents the time taken. An analysis of the graph reveals that as block creation increases without IPFS integration, the time required to insert the same image also increases, indicating scalability challenges where adding more images prolongs insertion times. To address this, our solution integrates Base64 with IPFS, as shown by the red line in the graph.

In summary, the SHARD-FEMF framework significantly enhances time efficiency in forensic evidence management compared to existing methods. It reduces time consumption by an average of 40%, demonstrating improved efficiency in processing and managing forensic evidence. At the transaction level, the framework achieves a 35% reduction in time consumption, because of blockchain sharding techniques. Additionally, at the block level, it outperforms existing techniques with a 45% reduction in time consumption per block. These improvements result from optimized block creation, processing operations, and minimized redundant computations. Furthermore, the framework enhances scalability and time efficiency, allowing for a 50% increase in transaction scalability while maintaining consistent time consumption per transaction.

Overall, the SHARD-FEMF framework offers substantial time efficiency improvements, ranging from 35% to 45%, compared to existing methods, algorithms, sharding techniques, and efficient resource allocation.

7.3. Results Analysis

The results obtained in the SHARD-FEMF framework are a direct consequence of the thoughtful integration of blockchain sharding, Base64 encoding, and IPFS storage. These components address specific challenges in forensic evidence management, such as gas efficiency, scalability, and time efficiency, resulting in an overall more effective and reliable system.

a) Gas Consumption Reduction: the significant reduction in gas consumption can be attributed to several key factors. First, the implementation of blockchain sharding plays a pivotal role. Sharding divides the blockchain network into smaller partitions, enabling parallel processing of transactions and reducing the computational load on individual nodes. This parallelism directly contributes to decreased gas consumption. Second, the integration of the Base64 encoding scheme allows for more efficient data compression and transfer, further reducing the gas needed for transaction processing. Together, these components enhance computational efficiency and optimize resource utilization within the framework.
b) Transaction Scalability: the substantial increase in transaction scalability is primarily a result of blockchain sharding. Sharding effectively addresses the scalability issue by allowing multiple transactions to occur simultaneously across different shards. This parallel processing capability significantly enhances the framework's capacity to handle a higher volume of transactions without experiencing performance bottlenecks. Moreover, the reduced gas consumption per transaction ensures that scalability improvements do not come at the cost of increased gas expenses.
c) Time Efficiency: the improved time efficiency achieved by the SHARD-FEMF framework can be traced back to several factors. Blockchain sharding again emerges as a key contributor; as it enables concurrent block creation and processing across multiple shards. This parallelism significantly reduces the time required for block creation and transaction processing. Additionally, the integration of IPFS for decentralized evidence storage ensures that retrieval times remain efficient, crucial for forensic investigations where rapid access to evidence is essential.
d) Integration of IPFS: the integration of IPFS is particularly noteworthy in enhancing both gas consumption and time efficiency. IPFS optimizes memory usage by decentralizing the storage of digital evidence. As more images or evidence are added to the system, the increased data size doesn't proportionally affect gas consumption or time requirements due to IPFS. This integration is a critical component in achieving the observed improvements.

It's important to emphasize that the observed results are not solely due to individual components but are a product of the synergistic interaction between blockchain sharding, Base64 encoding, and IPFS integration. These components work together harmoniously to create a framework that is not only more efficient but also more secure and scalable for forensic evidence management. This comprehensive approach ensures that improvements in one aspect, such as gas consumption, do not negatively impact others, such as time efficiency.

7.4. Comparative Study Analysis

The comparison between the Base64 scheme and the SHARD-FEMF framework is summarized in the Table 1, highlighting key parameters. The Base64 scheme exhibits lower average gas consumption but slower block creation times, ultimately resulting in a lower throughput of 2 transactions per second (Tx/s). On the other hand, the SHARD-FEMF framework, despite higher gas consumption, significantly outperforms in terms of block creation speed, achieving an impressive throughput of 5 Tx/s. This trade-off illustrates the SHARD-FEMF framework's efficiency and optimization in the management of forensic evidence. It showcases the framework as a highly promising solution for forensic evidence management, even with slightly increased gas consumption, There is a remarkable gains in transaction throughput and overall effectiveness.

Table 1. Comparative study table of existing Base364 scheme with proposed SHARD-FEMF scheme.

	Parameters			
Mechanism	Average gas consumption	Average time for block creation (in ms)	Gas usage reduction (in %)	Throughput in transactions per second-(Tx/s)
Base 64 scheme	1,10,71,102.85	30.5ms	18.56%	3 Tx/s
SHARD-FEMF	1,57,144.67	10.4ms	99%	6 Tx/s

Table 2 presents a comprehensive comparative study analyzing various privacy and security features of different technologies used in forensic evidence management. PoC in Hyperledger [24], Process Provenance [22] , Anonymous Witnessing [23], Block-DEF [21], Identity privacy [20], and the proposed SHARD-FEMF. The table assesses these technologies based on critical properties such as authentication, access control, intermediate nodes, transferring ownership, and integrity.

Table 2. Comparative study analysis of proposed SHARD-FEMF scheme v/s existing schemes.

Properties	PoC in Hyperledger [24]	Process provenance [22]	Anonymous witnessing [23]	Block-DEF [21]	Identity privacy [20]	Proposed SHARD-FEMF
Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Access control	Yes	No	No	No	Yes	Yes
Intermediate nodes	Yes	No	No	No	No	Yes
Transferring ownership	No	No	No	No	No	Yes
Integrity	Yes	Yes	Yes	Yes	Yes	Yes

Among the technologies analyzed, PoC in Hyperledger demonstrated strong authentication, access control, and intermediate nodes features but lacked the capability to transfer ownership. Process Provenance offered authentication but did not include transferring ownership, access control, or intermediate nodes. Anonymous witnessing provided authentication and integrity features but did not support transferring ownership, access control, or intermediate nodes. Block-DEF focused on authentication and integrity but did not handle transferring ownership, access control, or intermediate nodes. Identity Privacy encompassed access control, authentication, and integrity but did not address transferring ownership or intermediate nodes.

In contrast, the proposed SHARD-FEMF scheme exhibited all the analyzed features, including authentication, access control, intermediate nodes, transferring ownership, and integrity. This comprehensive analysis enables a thorough understanding of the strengths and limitations of each technology, with the Base64+sharding and IPFS scheme standing out for its ability to integrate all these crucial features, making it a promising solution for efficient and secure forensic evidence management.

8. Conclusions

The SHARD-FEMF framework represents a significant advancement in the field of forensic evidence management. Through a comprehensive evaluation and analysis, we can draw several key conclusions about the framework's effectiveness and potential. Firstly, SHARD-FEMF has demonstrated its ability to significantly enhance the efficiency of forensic evidence management. It achieves this by reducing gas consumption by an average of 21.5%, indicating improved computational efficiency and resource optimization. This reduction in gas consumption ensures not only cost-effectiveness but also improved performance in handling forensic evidence. Secondly, the framework has exhibited remarkable improvements in time consumption, reducing it by 40%. This efficiency gain results in quicker processing and management of evidence, which is crucial in forensic investigations where time plays a critical role. Additionally, SHARD-FEMF showcases improved scalability, allowing for a 23% increase in transaction scalability without compromising performance. This scalability is essential in handling a growing volume of forensic evidence efficiently. Overall SHARD-FEMF is a promising solution for the efficient and secure management of forensic evidence. Its ability to reduce gas consumption, improve time efficiency, enhance scalability, and provide robust security features makes it a valuable asset in the realm of forensic investigations. This framework has the potential to revolutionize the way forensic evidence is handled, ultimately aiding law enforcement agencies and the justice.

References

[1] Bose R., Phokela K., Kaulgud V., and Podder S., "BLINKER: A Blockchain-Enabled Framework for Software Provenance," *in Proceedings of the 26th Asia-Pacific Software Engineering Conference*, Putrajaya, pp. 1-8, 2019. DOI:10.1109/APSEC48747.2019.00010

[2] Dhulavvagol P., Bhajantri V., and Totad S., "Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application," *Procedia Computer Science*, vol. 167, pp. 2506-2515, 2020. https://doi.org/10.1016/j.procs.2020.03.303

[3] Dhulavvagol P. and Totad S., "Performance Enhancement of Distributed System Using HDFS Federation and Sharding," *Procedia Computer Science*, vol. 218, pp. 2830-2841, 2023. https://doi.org/10.1016/j.procs.2023.01.254

[4] Dhulavvagol P., Totad S., and Bhandage N., "Topic Based Partitioning for Selective Search Using Sharding Technique," *in Proceedings of the International Conference for Advancement in Technology*, Goa, pp. 1-5, 2022. DOI:10.1109/ICONAT53423.2022.9726020

[5] Hyder M., Siddiqui M., and Mukarram M., "TV Ad Detection Using the Base64 Encoding Technique," *Engineering, Technology and Applied Science Research*, vol. 11, no. 5, pp. 7605-7609, 2021. https://doi.org/10.48084/etasr.4337

[6] Kethineni S. and Cao Y., "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity," *International Criminal Justice Review*, vol. 30, no. 3, pp. 325-344, 2020. https://doi.org/10.1177/10575677198270

[7] Kumar S., Bharti A., and Amin R., "Decentralized Secure Storage of Medical Records Using Blockchain and IPFS: A Comparative Analysis with Future Directions," *Security and Privacy*, vol. 4, no. 5, pp. 1-16, 2021. https://doi.org/10.1002/spy2.162

[8] Li M., Lal C., Conti M., and Hu D., "LEChain: A Blockchain-Based Lawful Evidence Management Scheme for Digital Forensics," *Future Generation Computer Systems*, vol. 115, pp. 406-420, 2021. https://doi.org/10.1016/j.future.2020.09.038

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

[10] Liu H., Luo X., Liu H., and Xia X., "Merkle Tree: A Fundamental Component of Blockchains," *in Proceedings of the International Conference on Electronic Information Engineering and Computer Science*, Changchun, pp. 556-561, 2021. DOI:10.1109/EIECS53707.2021.9588047

[11] Lone A. and Mir R., "Forensic-Chain: Blockchain Based Digital Forensics Chain of Custody with PoC in Hyperledger Composer," *Digital Investigation*, vol. 28, pp. 44-55, 2019. https://doi.org/10.1016/j.diin.2019.01.002

[12] Longo F., Nicoletti L., Padovano A., d'Atri G., and Forte M., "Blockchain-Enabled Supply Chain: An Experimental Study," *Computers and Industrial Engineering*, vol. 136, pp. 57-69, 2019. https://doi.org/10.1016/j.cie.2019.07.026

[13] Malik G., Parasrampuria K., Reddy S., and Shah S., "Blockchain Based Identity Verification Model," *in Proceedings of the International Conference on Vision Towards Emerging Trends in Communication and Networking*, Vellore, pp. 1-6, 2019. DOI:10.1109/ViTECoN.2019.8899569

[14] Nieto A., Rios R., and Lopez J., "Digital Witness and Privacy in IoT: Anonymous Witnessing Approach," *in Proceedings of the IEEE Trustcom/BigDataSE/ICESS*, Sydney, pp. 642-649, 2017. DOI:10.1109/Trustcom/BigDataSE/ICESS.2017.295

[15] Pasdar A., Lee Y., Ryan P., and Dong Z., "A Blockchain Oracle-Based API Service for Verifying Livestock DNA Fingerprinting," *International Conference on Service-Oriented Computing Workshops*, Sevilla, pp. 80-91, 2022. https://doi.org/10.1007/978-3-031-26507-5_7

[16] Sammeta N. and Parthiban L., "Blockchain-Based Scalable and Secure EHR Data Sharing Using Proxy Re-Encryption," *The International Arab Journal of Information Technology*, vol. 20, no. 5, pp. 702-710, 2023. https://doi.org/10.34028/iajit/20/5/2

[17] Saini H., Dash S., Pani S., Sousa M., and Rocha A., "Blockchain-based Raw Material Shipping with PoC in Hyperledger Composer," *Computer Science and Information Systems*, vol. 19, no. 3, pp. 1075-1092, 2022. https://doi.org/10.2298/CSIS210930032S

[18] Song J., Zhang P., Alkubati M., Bao Y., and Yu G., "Research Advances on Blockchain-as-a-Service: Architectures, Applications and Challenges," *Digital Communications and Networks*, vol. 8, no. 4, pp. 466-475, 2022. https://doi.org/10.1016/j.dcan.2021.02.001

[19] Su P. and Su T., "Secure Blockchain-Based Electronic Voting Mechanism," *The International Arab Journal of Information Technology*, vol. 20, no. 2, pp. 253-261, 2023. https://iajit.org/portal/images/year2023/No.2/21294.pdf

[20] Tang Y., Xiong J., Becerril-Arreola R., and Iyer L., "Ethics of Blockchain: A Framework of Technology, Applications, Impacts, and Research Directions," *Information Technology and People*, vol. 33, no. 2, pp. 602-632, 2020. DOI:10.1108/ITP-10-2018-0491

[21] Tian Z., Li M., Qiu M., Sun Y., and Su S., "Block-DEF: A Secure Digital Evidence Framework Using Blockchain," *Information Sciences*, vol. 491, pp. 151-165, 2019. https://doi.org/10.1016/j.ins.2019.04.011

[22] Yli-Huumo J., Ko D., Choi S., Park S., and Smolander K., "Where is Current Research on Blockchain Technology?-A Systematic Review," *PloS One*, vol. 11, no. 10, pp. 1-27, 2016. https://doi.org/10.1371/journal.pone.0163477

[23] Zhang L., Xie Y., Zheng Y., Xue W., Zheng X., and Xu X., "The Challenges and Countermeasures of Blockchain in Finance and Economics," *Systems Research and Behavioral*

Science, vol. 37, no. 4, pp. 691-698, 2020. https://doi.org/10.1002/sres.2710

[24] Zhang Y., Wu S., Jin B., and Du J., "A Blockchain-Based Process Provenance for Cloud Forensics," *in Proceedings of the 3rd International Conference on Computer and Communications*, Chengdu, pp. 2470-2473, 2017. DOI:10.1109/CompComm.2017.8322979

Praveen Dhulavvagol working as an Asst.Professor in Computer science and Engineering, KLE Technological University Hubli, India. He has 12 years of teaching and research experience His research interest is in the area of Data Analytics, Distributed Processing and Blockchain. He has published over 20 international publications in various journals and conferences.

Sashikumar Totad working as a Professor in Computer science and Engineering, KLE Technological University Hubli, India. He has 20 years of teaching and research experience. His area of interest is Data Analytics, Distributed Processing and Blockchain. He has published over 50 international publications in various journals and conferences.

Atrey Anagal a Computer Science and Engineering student at KLE Technological University, Hubli, excels in networking, blockchain, and web development. With four published papers showcasing his expertise, he has made substantial contributions in both networking and AIML domains.