International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I5P128

Volume 73 Issue 5, 339-358, May 2025

Original Article

Privacy-Preserving E-Fir Systems Using Blockchain and Enhanced Silk Moth Optimization

E. Juliet Priscilla[1*], S. Nallusamy[1], D. Sobya[2], P. Divya[1]

[1]*Department of Adult and Continuing Education and Extension, Jadavpur University, Kolkata, India.*
[2]*Department of Computer Science & Engineering, Institute of Engineering and Management, University of Engineering and Management, Kolkata, India.*

[*]*Corresponding Author : julipriscy@gmail.com*

Received: 28 February 2025 Revised: 21 March 2025 Accepted: 22 April 2025 Published: 31 May 2025

Abstract- *Currently, various forms of crime are happening worldwide. The document prepared to file any perceptible crimes committed is called the Electronic First Information Report (e-FIR). These records make it possible to be systematically registered, but there is a potential threat of unauthorized access through hacking. For this reason, this database has serious problems with data integrity and transparency. The submitted concept presents a clarification as an essential component of a smart city environment. However, there are many risks to the information collected, especially those with centralized management. Thus, a novel blockchain-based platform has been introduced for the safe and privacy maintenance of criminal data. This network is divided into multiple channels to protect the anonymity of the data. The new Spiral Silk Moth Optimization Algorithm (SSMOA) is utilized to generate an effective key for the blockchain encryption module in cloud systems. It makes use of smart contract-controlled private blockchains to guarantee secured data storage. The combined compression and synchronized optimization raise the rapid security of privacy details. The suggested smart contract-based paradigm eliminates the necessity for a third trusted party by enabling users to negotiate suspicions using transparent and immutable data. By comparing the execution time of key retrieval and block execution timings, the submitted work has proved to be the best concept through simulation strategy.*

Keywords *- Smart city, FIR, Criminals, Compression, Blockchain, Encryption key, Optimization, Security.*

1. Introduction

The e-FIR system plays a pivotal role in law enforcement, requiring victims or their representatives to report serious crimes to local police stations formally. Centralized systems used to keep criminal records and assault data have several flaws, including the possibility of just one source of failure. Maintaining such data within local databases under police stations creates new problems. Two main concerns are data tampering and false registration. Data tampering occurs when a higher authority inside the institution manipulates key data without supervision. To remedy this, data should be digitally signed and dispersed across multiple institutions to maintain transparency. To ensure the unbreakable integrity and security of offense data, adopting a decentralized system becomes critical. Blockchain technology's enormous popularity can be ascribed to its intrinsic decentralization, which revolutionized previous approaches by abolishing centralized control and including numerous entities in the authentication of record validity. However, the centralized nature of e-FIR databases poses significant risks, including vulnerability to compromise and the potential for false registrations [1-3]. These vulnerabilities undermine transparency and data integrity within the e-FIR system. The growth of the Internet of Things (IoT) tends to transform various sectors, comprising the development of smart cities and advancements in supply chain management and healthcare. Smart cities leverage interconnected resources to offer intelligent services, aiming to address urban challenges and enhance citizen well-being. However, the widespread adoption of IoT devices raises privacy concerns owing to the extensive gathering of personal data. Thus, the information can be vulnerable to unauthorized access or misuse [4-6]. Over the last ten years, large-scale data breaches have made billions of user accounts vulnerable. Malicious apps have also been known to reveal personal data directly without the user's permission on multiple occasions [7]. To safeguard user privacy and regulatory initiatives, such as the General Information Protection Regulation's "right to be forgotten" directive, it is needed to halt this trend. These problems pose challenges for researchers carrying out studies that would otherwise profit from easy, passive, long-term data collection techniques to find new biomarkers and create digital treatments. An open and reliable process is needed when sharing data with unreliable third parties, with the guarantee of two factors mentioned below.

- Posterior privacy, which prevents personal information from being shared for purposes other than the study for which the subject has given consent,
- The data must be used exclusively for the intended purpose of this study.

It seems that one viable option for offering a safe, decentralized setting for information sharing is blockchain technology [8]. Additionally, each of these services is creating its own blockchain framework, which creates challenges for international information exchange between different blockchain systems. The following list contains the most widely used applications of blockchain technology. A blockchain-based smart contract application platform for distributed computing and software sharing was introduced in [9, 10]. A decentralized Public Key Infrastructure (PKI) put up on blockchain expertise was presented in [11]. The writers created a brand-new Certcoin framework by utilizing the benefits of the Namecoin and Bitcoin systems, which ensured security. Using the BlockChain (BC)-based file storage program MetaDisk, a peer-to-peer cloud-storing decentralized network has been demonstrated [12-14]. Decentralized IoT are described as software stacks that make use of the Bitcoin BC. The emerging blockchain CC technology offers some benefits as follows. It offers a distributed node consensus algorithm, which is an automatic script code, namely a smart contract for data management. Another one is a chain block encryption for data validation and stuffing progress.

Numerous techniques, including clustering, prediction, compression, and Energy-Efficient (EE) routing systems, are offered in the previous writings to lower transmission costs and energy consumption. IoT applications use centralized device-to-user communication to transfer data between users. As a result, more sophisticated security measures are needed. The traditional cryptography schemes don't work as well in IoT applications. Because these applications are centralized networks, problems with data authentication and integrity are particularly serious. Various cryptography schemes were presented in the literature. Network concerns, including energy consumption, memory capacity, and transmission expenses, must be taken into account when implementing security measures [15-17].

A skilled user can modify the smart data linked to a particular system. Intelligent integrity might be applied to e-FIR data kept in a central database of the station in entirely connected, smart city or digital compatibility scenarios. Privacy protection suggests that e-FIR data has effective integrity, which makes it suitable for integrating into a smart megacity environment. The task of managing accessibility to the BC utilizing smart contracts will fall to a gateway. Thus, in the submitted approach, an intellectual framework is utilized to use a collective BC ledger and fraud-resistant, tamper-proof smart contracts to ensure e-FIR data integrity. False e-FIR registering progress is additionally addressed by bringing together the admin and user credentials and storing these on the BC to facilitate audits. The proposed work provides a structure and concept of a BC that relies on secure and Privacy-Preserving Technologies (PPT) in IoT mechanisms. It also ensures security and privacy while increasing public sector trust that any device can adopt. The major key points are provided as follows.

- To promote transparency by dividing up the authority over the e-FIR, data is kept in a centralized information system in a police station among different organizations at a specific location and time.
- To permit the recording of the information obtained by the criminal data system and to compress it effectively using an Enhanced Principal Component Analysis (EPCA) approach.
- Compress and reduce data size, thereby lowering costs and transmission time.
- The key generation system can be done through the SSMOA scheme.
- The network devices read the data, and any detected data is appended with the security key dynamically created using SSMOA.
- To safeguard the criminal data gathered by e-FIR systems and include a study on the application of technologies to assure privacy in cloud systems.

The remaining parts are regulated as given. The theoretical foundation for this work is presented in Section 2, along with a discussion of FIR analyzing systems and their relevant methodologies. The analysis of the application of blockchain technology to protect privacy environments is done in Section 3. The architecture that is suggested to address the privacy issue in the selected scenario is described in Section 4. The results of simulations carried out to assess the security test operational efficiency of the new architecture on the deployed smart contract are deliberated in Section 5. Section 6 wraps up by outlining the conclusions and talking about the future steps.

2. Literature Survey

In a smart city with the Internet of Everything (IoE)-connected smart places such as schools, cars, hospitals, infrastructure, etc., sharing massive amounts of data every day, the city should also have a smart and safe method for managing e-FIR criminal data from a police station [17]. As soon as a cognizable offense, like kidnapping, murder, rape, or theft, is devoted, it is a straightforward document that the victim or someone on his/her behalf may have written out and filed with the police. In certain Commonwealth nations, there are a disproportionate number of police officers to citizens, so entering an accusation, as well as reporting an incident in person, takes time. The primary concerns are the integrity of non-registration and the false registration of e-FIR data. These issues remain the result of inefficiency, police corruption, and

the absence of accountability. In the beginning, e-FIR data is locally deposited in a central DB of stations, and these later get shared with police station HeadQuarters (HQ). Because the e-FIR DB is controlled locally inside the police station, it can be simply manipulated [18]. To protect national security, it is critical to understand the complexities of crime classification.

2.1. Cognizable Offenses

These offenses can be recognized across borders. The process will be easier to complete if you have reliable and time-stamped records. Recognizing the specifics of offense classification is critical. Cognizable crimes are serious felonies that police can apprehend without a warrant. Murder, robbery, dowry death, kidnapping, and other crimes are all possible.

2.2. Non-Cognizable Offenses

These offenses are less serious and cannot be prosecuted without a warrant. Forgery, deception, and assault are just a few examples. A lawsuit can be filed for any type of offense, but an FIR can only be filed for crimes that have been deemed legally punishable.

Criminal records are one of the most sensitive sections of public information. Integrating records of crime into a blockchain can expose susceptible categories of public information and can protect document rigidity and dependability. Also, it can often keep data safe from intruders. This study proposes a blockchain-based approach to handling criminal records that aids in data protection and integrity. As a result, using blockchain technology to address this issue can assist in better responding to security challenges [19-22].In essence, blockchain technology is a distributed, decentralized DB. It upholds a chain structure of data blocks among involved nodes, creating an ever-expanding, cryptography-based data record that is unchangeable. Every block logically contains a blockhead and a block body. Every block in the blockchain is represented as a Merkle tree and includes all the transactions that took place within it. The hash value in the blockhead is concatenated with each block. The transaction information will be synchronized to the entire network by the blockchain using the consensus mechanism, and each client will store the most recent transaction information, creating a decentralized storage method. The system's overall performance won't be impacted when a few nodes fail [23]. Blockchain-based technologies allow the creation of decentralized, highly protected PPTs in which no third-party organization controls the transactions. This technology improves information security and privacy by distributing encrypted data throughout the network. Using BC technology, instead of integrating it into the centralized DB as in a traditional centralized scheme, new information is included in a block and made accessible to every one of the nodes in a distributed network. A hash value is created, usually by employing the secure hash algorithm 256 bits (SHA256) for cryptographic progress, and identifies every single block in a BC [24]. The following block (child) is linked to and stores the current header points in the block to its parent's hash. The block content changes at any time, the hash associated with those blocks will be updated, and this modification will spread across the network to render that block invalid. This mechanism explains why this technology is decentralized and dispersed with no middleman or other reliable third party. Private keys are allocated to these participants so they can digitally sign and authenticate the transactions they complete [25].

This technology has become more well-known in the big data era as the best way to safeguard data integrity and guarantee data quality. Every node in the network can copy and verify any data held within the blockchain. This offers a dependable defense against intrusions that compromise data integrity. Many Machine Learning (ML) [37] systems and practices are presented in a brief amount of time to speed up the analysis of massive data measurements and increase IoT productivity. Specific ML techniques, like decision trees, clustering, neural networks, and Bayesian networks, can identify trends coming from a wide range of sources in various kinds of datasets. It makes appropriate decisions based on its analysis, just like humans can. Similarly, more optimization schemes have been introduced to improve data security, encryption levels and so on. The development of a system built on BC for logistics data and the use of optimal key generation for privacy preservation. In this case, the original logistics data is sanitized using an ideal key produced by the Perceptive Craving Game Search (PCGS) optimizing structure [26-28].

Furthermore, to find the best key generation procedure, an Arithmetic Optimization Algorithm (AOA) is run to maximize the PSNR value. The individuality of this work is determined by its layout of the AOA-based optimal way to generate keys for the best cryptographic technique [29]. Karim [30] made recommendations in a follow-up study on how to protect V2V and V2I transmission in the VANET environment from numerous cyber attacks. The goal is to build an Attribute Identity-Based Signature (AIBS), a hybrid cryptography structure that integrates ABS and IBS models to protect transmission and offer efficient message authentication and integrity. A BC-based solution has been introduced for managing complaints involving both cognizable and non-cognizable offenses. The report from the police will be hashed and posted over this network after being encrypted and deposited within the Inter-Planetary File System (IPFS). The complaint, alongside its timestamp, has been saved on the blockchain network, so the petitioner is going to have solid proof against the police if they choose not to file a formal complaint or deny receiving one under duress. Maintaining every file in an unchangeable DB makes it impossible for someone to tamper with the FIR or NCR and remain undetected [31].

In the context of managing criminal FIR data within smart city environments, the combination of BC technology presents promising solutions. The challenges posed by centralized e-FIR databases, including data integrity issues and susceptibility to hacking and false registrations, underscore the need for robust privacy protection mechanisms [16]. In summarizing all these studies, the following points are described shortly,

- Centralized e-FIR Database Challenges: The centralized nature of e-FIR databases introduces vulnerabilities such as false registrations, non-registration, and data integrity concerns. Local deposition of e-FIR data in central databases of police stations allows for easy manipulation, leading to inefficiency, corruption, and lack of accountability [9].
- Crime Classification and Blockchain Integration: Cognizable offenses, such as murder and kidnapping, require reliable and time-stamped records for efficient processing. Blockchain integration offers a decentralized and immutable database that ensures document rigidity and data integrity. Thus, it helps to enhance security and compliance with legal requirements [17-18].
- Blockchain Technology Overview: BC technology, characterized by its distributed and decentralized nature, offers secure PPT without reliance on third-party organizations. Utilizing cryptographic techniques and consensus mechanisms, blockchain ensures tamper-proof records and enhances data integrity, making it an ideal solution for safeguarding sensitive criminal data [19-20].
- Integration with IoT and Data Security: Integrating blockchain with IoT enhances security, intelligence, and big data storage capabilities. By incorporating blockchain encryption frameworks and secure data accumulation schemes, the wireless network's security is bolstered, ensuring the confidentiality and integrity of transmitted data [21-23].
- Optimization Techniques and Future Directions: Optimization techniques, such as the Spiral Silk Moth Optimization Algorithm (SSMOA), contribute to the effectiveness of blockchain-based systems. Researchers will soon be revising how to link BC technology with the latest technological advancements to further enhance data security and privacy [24-25].

Existing approaches for safe data aggregation provide attack protection; nevertheless, they have limitations in terms of memory space, energy, and transmission costs. Gateways allow network devices to send data to the network's base station/server. The data delivered by the device is combined with a hash key generated during the SSMOA creation procedure. Then, a compression-based data aggregating model is used to lower data size and subsequent transmission costs. The compressed data, now enhanced with security features, is transmitted using BC encryption and efficient key generation. The suggested routing strategy effectively selects the best routes for securely sending data while using less energy. Big data storage, intelligence, and better security can, therefore, be achieved by integrating BC technology with IoT. In this paper, a BC-built encryption framework is used to provide security for the wireless network.

This article presents a secure data accumulation scheme that adds BC encryption to the routing process along with a compression technique. Although the current techniques for aggregating the secured data provide defense against attacks, they have drawbacks such as energy consumption, memory requirements, and transmission costs. Network devices could use gateways to send data to the Base Station (BS) or server. An effective hash key can be generated and added to the data, i.e., transmitted by the device, using some optimization techniques.

For judicial investigations, a BC-based system for storing, processing, retrieving, and updating case records is suggested [43]. Additionally, BCfixes issues like disk failures, trust, and data loss against hostile attacks, as well as problems with current distributed storage ecosystems. Its ability to decentralize, protect transactions, authorize access, and immutably secure the validity and integrity of digital evidence for its admission to court.

The e-FIR system interface can connect to information kept in registered local DBs, enabling more thorough analyses and the acquisition of fresh data. In addition, automobiles can use blockchain technology to interact in anonymity with location services, protecting file privacy from unauthorized persons.

The submitted plan is different in several ways from the strategies being used now. To be more precise, an intelligent framework built on smart contracts has been used to investigate how the blockchain might be able to preserve the reliability of the e-FIR DB retained in a police station. Finally, by comparing them with the conventional Privacy Protecting scheme, the compression and optimization of the BC-based systems using SSMOA suggested in this paper have proved to be easier to maintain, more secure, and less expensive models.

3. Proposed Model

The submitted framework takes advantage of the benefits of blockchain technology by making a speech, as the e-FIR data in the station could have intelligent integrity provided to it. A centralized DB in an entirely linked smart (digital)city interoperability scenario is provided.

To provide transparency, the idea is to distribute authority over e-FIR data among various entities, with the data being kept in a central police station DB. It is assumed that a citizen's identity kept back in a national DB is secure and safe. Users' System Interfaces (SI) for e-FIR registration are connected to the national DB for user authentication.

A system is created in which criminal files are handled on a public BC using a public/private cryptographic key to safeguard records with PPT. The e-FIR is implemented on the Ethereum public blockchain framework utilizing the Proof-Of-Work (POW) concept because this platform is primarily employed by the general public.

The system is made up of two types of infrastructure: police stations and the EthereumBC. The police stations serve as network nodes, storing the hash of the e-FIR. Before being sent to the BC network, an e-FIR record is time-stamped. Each police station keeps a printed version of the e-FIR. Therefore, when an e-FIR has been included in the system, it cannot be changed or altered, ensuring record transparency.

3.1. Need for Submitted Procedure

If a message from any node is continuously traversing the path, and the final data has not yet been verified at the receiving node, the intermediary node is considered malicious. Generally, an encryption mechanism is described. The biggest disadvantage is that device data is delivered to the receiver without a compression technique, which increases communication costs. Therefore, the new compression model is essential.

BC technology is a developing technology for cloud computing that offers numerous benefits, including an encrypted chain block structure utilized for validating and storing data alongside a distributed node consensus mechanism for data upgrades and smart contracts for effective data management.

This integration of BC technology and optimization enhances security, intelligence, and large-scale data storage capabilities. ABC-based encryption mechanism is used here to provide security in wireless networks. Also, a secured e-FIR system is presented to incorporate a compression technique with BC encryption for safety.

One must choose to employ a private BC in order to do away with the current computational overhead. Even with this kind of BC, smart contracts guarantee the immutability of the system because the conditions recorded in the contracts are unchangeable.

It should be noted that only the government will have access to the BC; users will not. Only the examined user and the governmental organization exchange information. Encryption is one way to potentially comply with the pseudonymization requirements.

When data is encrypted, it becomes unreadable directly and can only be decrypted using an SSMOA-based optimized key or two security keys. BC's fundamental feature is the extensive use of network cryptography, which provides reliability for all network interactions. Optimization is the process of determining the best potential solution(s) to a specific problem. As issue complexity has increased in recent decades, the requirement for innovative optimization strategies has become more apparent than ever. Prior to the introduction of heuristic procedures, mathematical optimizing techniques were the only instruments available for issue optimization. They are primarily predictable and suffer from one main flaw: local optima entrapment. Some of them, such as gradient-based algorithms, also need the derivation of the search space. This makes them extremely inefficient when dealing with real problems. Hash functions are the foundation of BC, providing various properties such as pre-image resistance, collision resistance, etc.

A BC is essentially a data structure made up of a connected list of network nodes, with each one holding a number of blocks, each containing the cryptographic data derived from the block before it. When a block header gets generated, a new block is formed, and a hash is made using key pairs and a digital signature. A hashing mechanism is then utilized to continuously create new blocks based on the previous block's hash. The optimized private and public keys are used to construct a hash, which assures the block's integrity. In the network, each node is assigned a trust measure based on its participation in data transmission and the number of successful transfers with adjacent nodes. Security is ensured through BC encryption technology, employing multiple encryption keys for various data types. The data is divided into blocks, creating a BC, which is then transmitted to the base station. This method enhances both security and overall network performance.

3.2. System Architecture

The different terms involved in the submitted work are provided briefly. They are utilized in various ways for improving FIR data registration, compression and blockchain encryption, as provided in upcoming Figure 1. In the registration block, The Superintendent of Police (SP) at HeadQuarters (HQ) establishes a unique account address for each police station, known as the police station hash, which is subsequently registered/ stored via a smart contract on the BC ledger. Some of the details are integrated into the hash for auditing purposes of an individual station, such as the city, address of the station, admin or in charge, and all investigators with their names. The HQ officials would update the station's credentials and generate a fresh transaction on the BC. A notification of the latest appointment will be conveyed to all participating station addresses. Likewise, a similar action would be followed for police station administrators.

Users interact with the SI in the user block by providing an Identification Number (ID) for validation. This ID only permits the filing of an e-FIR for cognizable offenses connected to the SI. The user will not be able to edit an e-FIR that has recently been presented and remains pending because any changes would modify the original hash value.

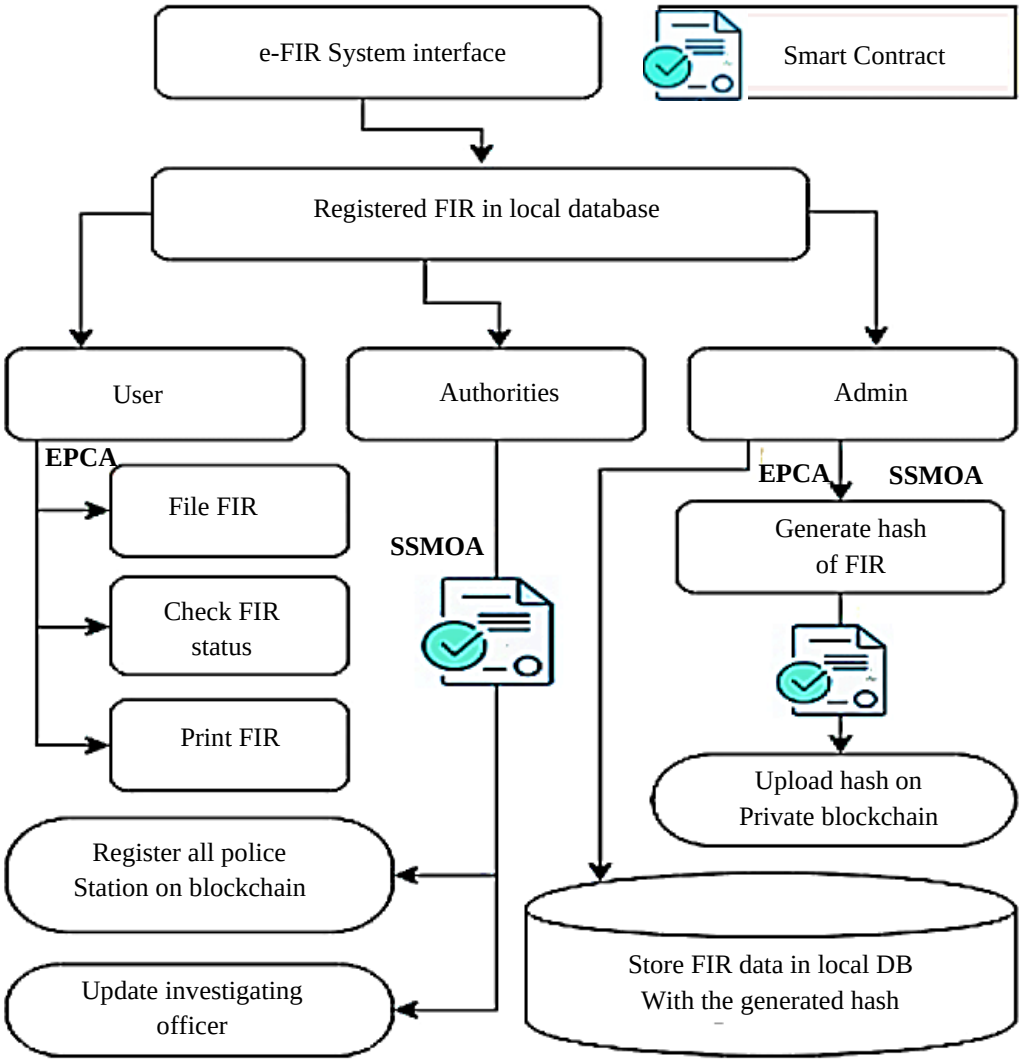

Fig. 1 Complete work modules

Thus, it would designate modifications to the initial e-FIR data and identify fraudulent activity. The user must include the additional information when submitting an e-FIR, such as the date, time, and location of the offense, the reporting, and a thorough account of the offense, entire personal information about the complainant and the accused, and any more details about the proof of the stolen property. In the admin block, all blockchain transactions must be approved by the administrator. Whenever a user delivers an e-FIR, the station administrator appoints one of the investigators to check out the case and validate the information provided by the user.

The administrator produces a hash of the e-FIR and uploads data to the shared private blockchain if the data is verified as correct using a smart contract. Furthermore, before getting uploaded to the police station's central DB, the user-supplied e-FIR data are signed digitally based on the precise hash computed for those e-FIR data. The hash will act as their unique identifier. The admin will reject the transaction and drop the case along with the transaction if fraudulent e-FIR details are discovered. If a police admin or user station intentionally files an erroneous e-FIR in contrast to someone else, the accused user is entitled to request an audit from the SP of the incorrect e-FIR. This hash data is shared with the SP along with all other case data, such as the name and address of the city and police station, the police administrator, the investigating officer, and the information from the claimed e-FIR that was submitted against the accused individual.

They have been incapable of getting rid of their actual identities as recorded in the BC in order to eradicate evidence indicating they had no role. This is due to the fact that the credentials of every party involved in filing e-FIRs remain preserved on the BC as hashes. BC also records the timestamp of each block transaction to help in recognizing the participation of an individual in fraud.

3.3. Blockchain Model and Smart Contracts

Additionally, BC fixes weaknesses like trust, data loss, and disk failures against hostile attacks, as well as problems with current distributed storage ecosystems. The legality and integrity of digital evidence are guaranteed for its admissibility in a court of law by the BC's ability to safeguard transactions, authorize access, decentralize, and ensure immutability. A public BC is a preferable method for judicial inquiries because it guarantees the highest level of decentralization, trust, anonymity, and security. The dishonest miners need a significant amount of processing and the ability to control over 50% of the network; public chains on the scale are large, which allows for a collusion-free network. In the context of PoW, it is meant that to ensure network validation, and miners must solve the difficulty problem and alter blocks once in a small period before a new valid block is added to the chain. Therefore, in contrast to private and consortium chains managed by collusion between the groups of registered nodes, public BC permits fairness in block ordering. Maximum security, anonymity, openness, and corruption will be brought about by a public chain-free network that allows for the optimization of framework throughput.

This technology appears to be a viable solution to the aforementioned issue in this context. These ideas are integrated by smart contracts, which are blockchain-based automated execution scripts that enable dispersed, highly automated workflows [32]. Scripts kept on the blockchain are called smart contracts. A smart contract has no presumptions and can function as a reliable third party. Programming codes can be used to store contracts, which will be executed automatically by blockchain when certain requirements are met. They can operate autonomously and instinctively in a predetermined way. Symmetric encryption algorithms are utilized to secure the documents presented in the ledger [33]. When considering cost, speed, and accuracy, smart contracts perform better than traditional contracts. They have the option to record user privacy preferences by determining whether or not to monitor them. If monitoring of a user becomes necessary, for instance, the government obtains a court order permitting the monitoring. Then, the privacy preferences are modified in the contract to allow FIR data monitoring. Managing a transaction to a smart contract initiates the contract. Based on information from the triggering transaction, it is then carried out autonomously and automatically on every node in the network in a predetermined way. The authors note that smart contracts allow for the management of data-driven exchanges between network entities, creating unbreakable interaction rules.

3.4. Access Controlling Modules

The requirements are stated at the opening of this section when designing the previously mentioned architecture, considering the information provided. The scenario in Figure 2 serves as the foundation for accessing and controlling the proposed modules. In Figure 2, the IPFS protocol connects to the BC through port 5001 [20]. This protocol receives an e-FIR file first. The IPFS next applies SHA-256 to convert the file into a binary value to generate the hash value. When the file is added to the IPFS network, a unique address is created. The hash value of the file's address and the digest of its contents are then concatenated. The blockchain stores this concatenated hash value to guarantee the e-FIR file's transparency and integrity. The user's private keys are used to encrypt the submitted documents. Here, the user names the e-FIR victim along with other authorized users, including the police and the victim's family. The victim's signature can be used to follow the document across the whole network. The user's private and public keys can be used to decrypt the documents and to access them correspondingly. Figure3 illustrates how to use the IPFS protocol to post an e-FIR to the BC.

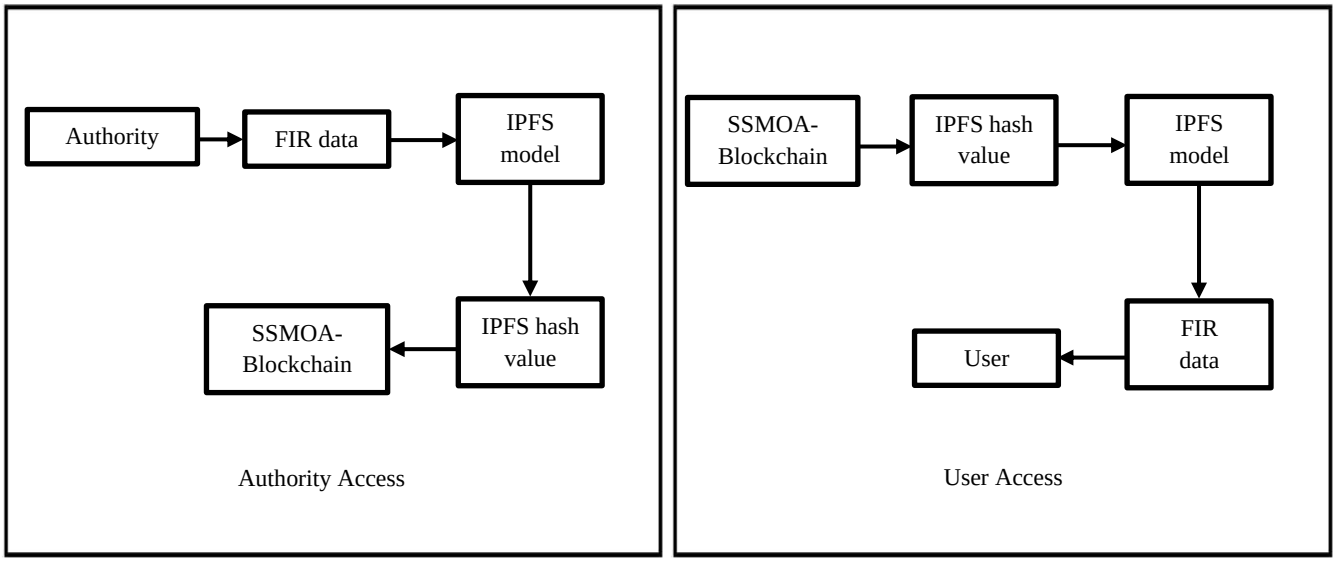

Fig. 2 Access Controlling Modules

The user sets up the privacy preferences when monitoring and requires access to their files for their cases (as per Figure 2). A smart contract that is resistant to fraud and tampering is used in a smart system to ensure e-FIR data integrity via a distributed BC ledger. To tackle false e-FIR registration, admin and user credentials are collected and stored on the blockchain for auditing purposes. The private blockchain houses a smart contract that has this data registered. At this stage, the user's private and public keys are also generated. Whenever there is a key-generating process, the SSMOA-based optimized key can be generated for a well-secured system. When the authorities need the data, they can register or update the criminal FIR directly from the secured blockchain by using a system that bypasses the gateway.

Furthermore, once a smart contract is registered, its privacy preferences can only be altered by authorized addresses. The gateway retrieves the public key that corresponds to each DB by making a connection to the DB that stocks the keys. The gateway relates to the blockchain and uses the smart contract to verify the exact hash key privacy settings after recovering the public key using SSMOA. The gateway of authority saves these registered FIR cases in a storage service, provided their privacy preference permits them to be taken through step-by-step progress. However, nothing is saved or registered if the users prohibit the DB or any wrong key. The progress involved in the new scheme is provided clearly in the upcoming section.

3.4.1. Enhanced PCA Concept

The captured data is compressed effectively using an enhanced type of PCA. It creates a range of frequency differences and the least amount of storage for characters that appear frequently. The fundamental idea underlying PCA is to diminish the dimensionality of complicated police Investigation Data (ID), which encompasses numerous interrelated variables while preserving the variance presented in the initial FIR data. To do this, the initial variables are changed into a new set of variables called principal components [25].

These components are independent and structured in such a way that the original components maintain the mainstream of the variability found in all the initial variables. The procedure for transferring information to the gateway consists of two phases. The criminal data accumulated in the gateway is denoted as P_{gd}. Subsequently, an encrypted message P'_{gd} is produced by executing an XOR operation between the original FIR data $P_{gd}$and a safeguard key SK_{gd}. The SSMOA-based optimized key module is employed to acquire the safeguard key and merge it with the encrypted data. P'_{gd}. The resultant encrypted FIR data is then compressed (referred to as CP'_{gd}) and dispatched to the gateway from all connected devices like blockchain, FIR data and key storage devices. The pseudo-code for enhanced PCA compression is described in a simple manner as follows.

Pseudocode 1: Enhanced PCA compression

$P_{gd}(0) \leftarrow P_{gd}(id-1)$;
for $t \leftarrow 1$ *to* t_{max} *do*
$P_c(t) \leftarrow ortho_{norm}\left(S_{gdi}^k P_{gd}(t-1)\right)$;
end
$P_{gdi} \leftarrow P_{gd}(t)$;

In this method, a minor scalar value denoted as αis utilized to ensure that Pgdiis non-negative definite and Īdis an identity matrix. To achieve this objective, it is recommended to perform a singular orthogonal iteration for each incoming subsequence Pgdi, using the previous subspace Pgd(id−1) as the initial input. In other words, when receiving the gateway data block Pgdi, the symmetric data auto-correlation matrix Sgdi can be replaced by Equation (1).

This results in the following approach for estimating the subspace of interest: $P_c(t) \leftarrow ortho_{norm}\left(S_{gdi}^k P_{gd}(t-1)\right)$. Depending on how S_{gdi}^k is chosen, several approaches can be acquired to trace the subspace.

$$S_{gdi} = P_{gdi}.P_{gdi}^T + \alpha \bar{I}_d \quad (1)$$

The autocorrelation matrix block estimator is the easiest and the most successful approach.

3.4.2. Cryptographic Approach

Cryptography is a widely used technique in numerous data transmission strategies to implement security. The new scheme uses homomorphic cryptography, which allows it to operate on the original text's cipher text without requiring the decryption key details. The use of a 'key' facilitates the assurance of security issues like authenticity and non-denial.

It is an essential component responsible for generating the codes employed for encoding and decoding the confidential data and the session code. This will be shared among gateway blocks while synchronizing or transmitting data through an insecure network. This key is generated using the SSMOA module.

3.4.3. Blockchain with Hash Techniques

Regularly adding a security key to the data block is imperative. For this, one can use a hash function produced by SHA-256. Since this hash is also known as irreversible progress, it is possible to calculate the hash key from the source data. However, it is not possible to compute the key from the user's perspective in reverse [32]. Figure 3 depicts the complete structure of the BC.

The hash key is calculated using the same formula as the earlier block, while a fresh block is included in the BC. In the fresh block, the data and the key are stored. The modification between the hash key and the data is visible to any attacker trying to obtain the information [33]. This type of technology

can be utilized to indicate expensive issues linked to insecure and inefficient data storage. The swift expansion of Bitcoin has resulted in a rise in the usage of BC techniques. Recently, BC technology has been employed in some IoT applications to enhance big data management and security [31-35]. These projects demonstrate beneficial effects on data security.

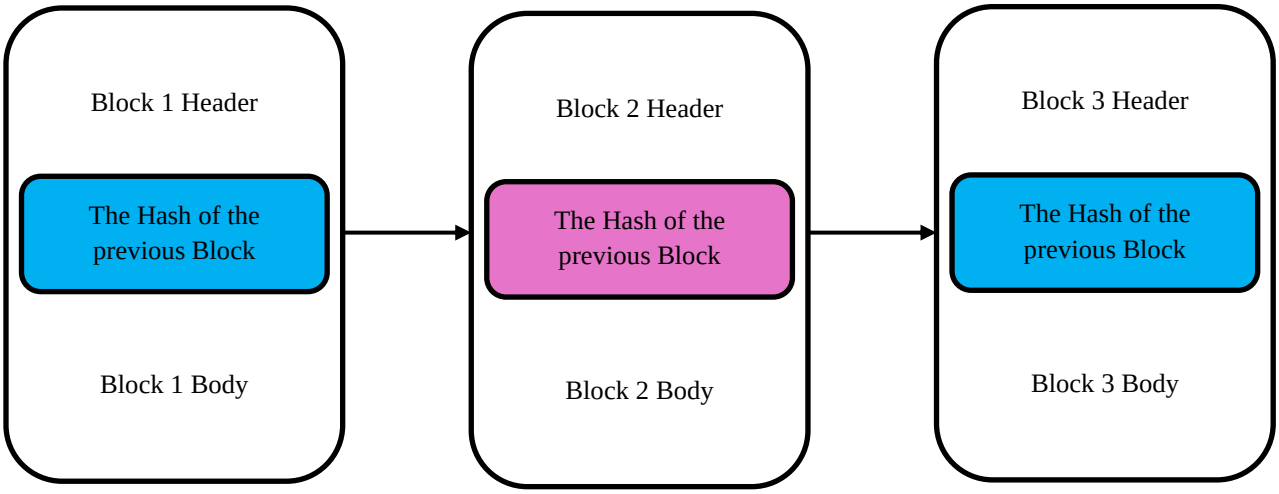

Fig. 3 Blockchain arrangement

3.4.4. SSMOA Model

In this model, the encryption key is appended to the data gathered from the IoV devices for security purposes. This section explains the security key generation process. The process of designing the dynamic key with a spiral silk constructor unit yields the silk moth web [36-40]. Radial, spiral, and spherical lines (triple lines) are used to create the non-uniform moth web. The user enters the displacement distance among the lines, and the spaces between the lines are fixed but unequal on the web, as shown in Figure 4(a). It has three behaviors in spiral web formations. They are surge, zigzag, and loop (with spherical shape). In any of the web formations, either the upper and lower halves of the surge and zigzag lines or the spherical form can be retrieved from the looping lines. As per the flow diagram Figure 4(b), the best value using SSMOA progress can be calculated. The parameter initialization, Spherical-Linked Transfer Functions (STFs), initial distance evaluation, and finally, optimum distance are assessed as the step-by-step process involved in SSMOA.

Fig. 4(a) Spiral Web Forming Silk Moth

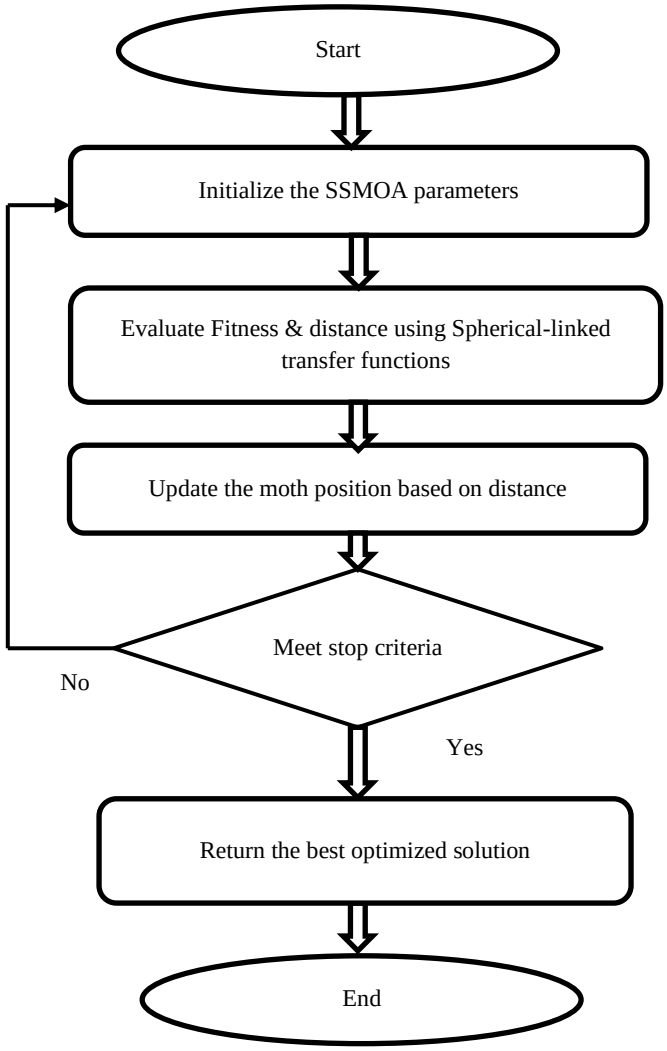

Fig. 4(b) Flowchart of SSMOA

The Spiral Silk Web Constructor (SSWC) unit parameters must be understood in order to retrieve the key. The SWC unit functions in a manner akin to that of a moth weaving an orb web. With these dual lines that are not uniformly spaced, a moth web construction is created. Spiral line construction begins with the Initial Distance (dini) being set from their reference point. The moth then advances up to the distance dini from the reference point. When creating spiral lines, the user sets the incremental distance among the radial lines, which is represented by the symbol Δdi. The spiral line is depicted counterclockwise. As a result, the silk moth moves according to the distances among dini and Δdito form the spiral lines of the web. As it transitions from one radial line to another, the distance traveled is measured.

$$d_1 = d_{ini} + \Delta d \tag{2}$$

$$d_{next} = d_1 + \Delta d \tag{3}$$

The silk moth releases the sticky silk thread to adhere to the walls as the first stage of development. Subsequently, it looks for a different spot to join the thread and begins creating "Y"-shaped baselines. After that, a triangular supporting structure forms. Next, the dual lines inside the frame are created. Nevertheless, the creation of a "Y" shape was not carried out during the web development. The user will supply the angular displacement of the X-axis on its positive side and the radial line length during the dynamic web construction process. Starting at the reference frame point are the radial lines. The angular displacement (a_{di}) from the locus axis and the increment in a_{di} for the following radial line are indicated by Δa_{di} and provided according to the user's selection. The values provided for the variables a_d and Δa_{di} determine how many radial lines should be utilized on the web.

Similarly, those distance values in spherical form [41, 42] also guide the development of the security key. STFs are the foundation of virtual aural reality, and an enormous SRTF configuration with exceptional spatial resolution of medical data is necessary for a conceptually transparent depiction. Therefore, reconstructing STFs coming from a more compact data set usually requires interpolation; spherical harmonics present an interesting approach principally for this kind of data processing. It highlights the important energy in low orders, which is noteworthy ever since the spherical distortions need to be truncated to a particular order in reality.

Virtual audiovisual reality is based on Head-Related Transfer Functions (HRTFs), and perceptually transparent symbols necessitate a substantial collection of Head-Related Transfer Functions (HRTFs) with high spatial resolution. Consequently, HRTFs are often reconstructed through interpolation from a smaller dataset, with spherical harmonics proving to be a particularly effective method for this purpose. By doing the following, the quantity of HRTFs needed and the computational expense of reconstructing them will be immediately decreased. The modern study investigated various pre-processing methods and found that time-aligning the HRTFs with subsample accuracy before processing the spherical harmonics created the finest results. The Spherical Harmonics Transform (SHT) can be used to break down a square integral operation on the sphere $f(\rho)$ into a set of coefficients and weights, $Cs_{nm,}$

$$CS_{nm} = h \int_0^{2\pi} \int_0^{\pi} f(\rho) \mathcal{S}_n^m(\rho)^* sin\partial d\partial \, d\varphi \tag{4}$$

where $\rho = (\varphi, \partial)$ provides the elevation ∂ = [-90◦;90◦] (90◦ @ 'z' positive), azimuth φ=[0◦;360◦) (calculated counter clockwise across the xy-plane, early@ positive 'x'), and the complex conjugate, (.)* SH($\mathcal{S}_n^m$) of *n* as order and *m* as degree are demarcated,

$$\mathcal{S}_n^m(\rho) = \sqrt{\frac{2n+1(n-m)!}{4\pi(n+m)!}} \mathfrak{k}_n^m \sin\partial \, e^{jm\varphi} \tag{5}$$

In addition to the related Legendre functions $\mathfrak{k}_n^m$ and the imaginary, $j=\sqrt{(-1)}$ part. In reality, the SHT must be discretized to a limited number of ɋ sample points,

$$\vartheta_{\text{ɋ}} = \vartheta_{\text{ɋ}=1} \dots \vartheta_{\text{ɋ}=\text{ɋ}}.$$

$$Cs_{nm} \approx \sum_{\text{ɋ}}^{\text{ɋ}} \alpha_{\text{ɋ}} f(\vartheta_{\text{ɋ}}) \mathcal{S}_n^m(\vartheta_{\text{ɋ}})^* \tag{6}$$

Equation (6) is achieved by using the quadrature weights $\vartheta_{\text{ɋ}}$, which stands for every area$f(\vartheta_{\text{ɋ}})$. The biggest *SH* order $\acute{N}$ is directly restricted by this spatial sampling of FIR data. The Inverse Fourier Transform (IFT) is used to create the impulse responses from the complex spectra for a given length of data samples and sampling rate. This transformation is also performed to diminish the error function. This type of filter is used to detect unwanted/repeated data. It is applied to minimize the variations among non-criminal and other FIR-related data parts. It will analyze both the similarities and variations in the input data. It is employed to reduce feature duplication and increase FIR data feature relevance.

The majority of algorithms in this family are carried out in a supervised manner since the relevance of a feature is typically determined by its correlation with class labels. Furthermore, the majority of information-theoretical ideas are confined to discrete variables.

As a result, this family of feature selection algorithms is limited to discrete data. Specific data discretization schemes are necessary beforehand to continuously optimize criminal data feature values. Thus, the final distance of the SSMOA is renewed in SSM line calculations from Equations (2) & (3) as provided below.

$$d_1 = d_{ini} + \Delta d + Cs_{nm} \tag{7}$$

$$d_{next} = d_1 + \Delta d + Cs_{nm} \tag{8}$$

The key should be known in order to retrieve the transmitted data upon receiving it at the aggregator. The security keys are extracted from the created SSM orb web at the points where the spiral, spherical, and radial lines intersect. The numerical values of the intersection points are padded to create the keys' frame. The data is associated with the security key created by the SSWC unit and then passed on by the device. The analytical formula of a fundamental resonant change in web strings can be utilized to highlight the limitations of overlooking changes in geometry in enriched PCA eigenvalue examination. This compression progress is used to lower the transmitting cost and size of the data because adding a security key makes it larger. The creation of random numbers is not addressed by the suggested security plan. As a result, the criminals find it difficult to get the key.

3.4.5. Decryption Process

Finally, decryption requires the inverse progress of the blockchain-encrypted modules, an inverse linear transformation, and the sub-keys in inverted order, which distinguishes it from optimized encryption. The overall procedures followed in the modules are described in steps.

- The FIR data is compressed and encoded using the optimized procedure (SSMOA). The symmetric key is utilized to encode the initial data. At that time, the encoded data in this stage and the preceding stages will be transmitted.
- Before the blockchain encryption, a hash value for the initial investigated data would be created. This value would be utilized to enhance the efficacy of data integrity and security confirmation. This value will be encoded utilizing the personal key.
- The recipient decodes the acknowledged FIR data utilizing reverse progress and the personal key.
- The outgoing data will be decoded using their SSMOA personal key and the authentication and confirmation progress will be executed utilizing the hash task.

As a result, the suggested technique stops malicious nodes from causing data loss and integrity problems. Additionally, it ensures data confidentiality from the authority to the gateway device and, finally, to the update or storage server or blockchain. The use of compression contributes to the reduction of data size, which lowers energy and transmission costs. The original data is obtained by applying the decompression process after the data has been decrypted in the received block. By employing the hash function and security key from the encryption method, the recipient confirms if the data came from authorized users. As a result, the information obtained from malevolent users is ignored.

Furthermore, because the security keys do not match, the data is not accessible to unauthorized users or receivers, making it impossible for them to retrieve the transmitted information. The government user needs to get a court order approving the monitoring before they can begin the process. The gateway needs to receive a court order. The smart contract privacy preferences are modified, enabling the criminal to be watched for a predetermined amount of time, and the order is encrypted utilizing the public key of this authority. After the end of the monitoring period, the encrypted court order is sent to the user, informing them that they have been watched under the order. The contract confidentiality preferences revert to their initial configurations after the monitoring period.

Thus, generating and optimizing cryptographic keys include determining the most beneficial and secure approach to produce, maintain, and employ cryptographic models in a variety of applications. This may involve refining the creation of keys for speed and security, as well as protocols for key exchange, encryption, and decryption.

4. Implementation of Proposed Design

4.1. User Interactions

- User Authentication: Users interact with the system through a secure interface that requires authentication. This authentication process ensures that only authorized users can access and interact with the system.
- Submission of e-FIR: Users submit e-FIRs through the interface, providing details such as the nature of the offense, date, time, location, and personal information of the complainant and accused [30].

4.2. Data Encryption

- Encryption Process: Upon submission, e-FIR data is encrypted using cryptographic techniques to ensure confidentiality and integrity.
- Symmetric Encryption: Symmetric encryption algorithms are employed to secure the data. Each e-FIR is encrypted with a unique encryption key generated for that specific report using the SSMOA process.
- Hashing: Hash functions are applied to create hash values for the encrypted data, enhancing security and integrity.

4.3. Blockchain Integration

- Blockchain Platform: The system utilizes an Ethereum BC platform for decentralized storage and verification of e-FIR data.
- Smart Contracts: Smart contracts are deployed on the blockchain to manage interactions and transactions between different entities in the system.
- Decentralized Storage: Each police station serves as a network node, storing the hash of e-FIR data. This decentralized storage ensures data immutability and transparency [28].

4.4. Key Generation

- Optimized Privy Sharing: The system employs the SSMOA for optimized key generation. This algorithm generates encryption keys with enhanced privacy and security properties. Also, the Levy model is used to

establish a new position in order to lessen the possibility of neighbours overlapping [44].To diversify the search zone, a normal distribution is taken into consideration in place of a random distribution, which was previously used in the search optimization algorithm with Lévy flights.

- Unique Keys: A unique encryption key is generated for each e-FIR, ensuring that each report is securely encrypted and accessible only to authorized parties. Lévy flights can enhance population diversity, helping to prevent premature convergence and enabling the algorithm to escape local optima more effectively.
- Rather than calculating the distance between i and another solution, the radius is calculated using the best solution. These two approaches are helpful in obtaining an improved balance between the exploration and exploitation capabilities of SSMOA, making it faster and more robust compared to MOA.

4.5. Compression Techniques

- Enhanced PCA Compression: It is utilized for data compression, reducing the size of e-FIR data while preserving its essential features.
- Efficient Storage: Compressed e-FIR data is stored efficiently, reducing storage requirements and transmission costs.

4.6. Smart Contract Execution

- Automated Workflow: Smart contracts execute automated workflows based on predefined conditions and rules.
- Transaction Approval: Transactions, such as e-FIR submissions and updates, require approval from designated authorities. Smart contracts facilitate the approval process, ensuring accountability and transparency.

4.7. Scalability, Latency and Bandwidth

Case details are saved in IPFS as off-chain and may be retrieved using an indexed hash key and the private credentials of authorized stakeholders. IPFS is also used to remove redundant data if the officer updates the data. The suggested FIR registration process for the Case Applicant (CA) is digitally time-stamped by the Police Officer (PO), and meta-information is recorded in BC. As a result, on-chain processes are more scalable and updating nodes is done effectively.

The network requirements, including the bandwidth and end-latency requirements, as well as the degree of decentralization, may be achieved directly through the influence of the consensus protocol selection.

4.8. Applications

In a smart grid, smart contracts and BC applications are utilized to improve the grid's flexibility and make energy applications more secure when performing transactions. Numerous research studies can be applied in the electricity sector, Information Forensics and so on.

The blockchain-based meter delivers a unique timestamp block for each transaction, which is then updated on the blockchain. Its unique timestamp block is utilized for examination in a distributed ledger.

Blockchain applications in the smart grid can be classified relating to the different components of the smart grid, as given: Power generation: Blockchain technology will provide dispatching agencies with real-time information on power grid operations. This allows them to create dispatch strategies that maximize profitability. BC technology allows for decentralized power transmission and distribution, addressing issues in traditional centralized systems.

4.9. Merits and Demerits

On the other hand, immutability may be an issue; once data is stored in the BC, it cannot be updated. This is why crypto-currency theft cannot be reversed. However, blockchain is fault-tolerant. If, for any reason, a node or a collection of nodes goes down, the entire network will not be harmed because the nodes that remain will continue to perform as usual, given there are adequate, accurate working components to sustain the service. Blockchain technology, which is based on consensus, enables digital transactions between parties who do not trust one another. The technology uses public and private keys, and if these keys are not kept secure, there is a risk of losing funds.

4.10. Computational Complexity

The e-FIR system typically generates a significant volume of data, which can strain storage capacity in a BlockChain (BC) system. Previous efforts have attempted to mitigate this storage challenge to some degree. To tackle this issue, a BC-based secure e-FIR system is proposed for both officers and general users, utilizing the IPFS protocol to manage storage effectively. This approach distinguishes itself from existing e-FIR systems by its method of addressing storage needs. An e-FIR record is implemented using this protocol, where uploaded data files are encrypted with user private keys. These files can be accessed using public keys and decrypted with private keys. The IPFS protocol facilitates the storage of large amounts of data, including various types of images. Transactions are stored in IPFS, while the corresponding IPFS hash is recorded in a block of the blockchain. Also, particular addresses will be granted the authority to do specific functions that other addresses cannot, such as confirming that e-FIR transactions are initiated from the admin node address while all police stations are registered from the SP node address. A registered user can only access case records using the IPFS private key and its hash object, protecting both the integrity of legal data and user privacy. Holders can change the data to reflect new investigative findings by using suitable authorized keys and access control

measures. This technical overview demonstrates how the proposed solution addresses the challenges of privacy protection and data integrity in criminal FIR DBs. By combining advanced encryption techniques, BC technology, optimized key generation, compression methods, and smart contract execution, the system provides a robust and secure framework for managing e-FIR data.

5. Simulation Effects and Analysis

5.1. Experimental Setup

The primary distinction is that the Ethereum blockchain is primarily concerned with executing programming codes on the network to enable more sophisticated features. A certain amount of gas is used by the smart contract that was created to control each user's privacy preferences and is then stored in the blockchain [33]. Gas refers to the fee, or pricing value, required to conduct a transaction or execute a contract on the Ethereum blockchain platform. The Ethereum blockchain will be directly connected to the MongoDB, Express, React, and Node.js (MERN) stack, which is utilized properly. Users will be able to enter data using the ReactJS interface with this configuration, and MongoDB will store the data.

An Application Programming Interface (API) will be developed using Node.js to facilitate communication between the ExpressJs framework, which will manage incoming requests from the front end, and the MongoDB back end. The Ethereum blockchain is accessed by Web3 providers such as MetaMask. The system's smart contract can still be created with the Remix IDE and implemented in a Web3 Remote Procedure Call (RPC) similar to the environmental settings in the work [18]. Through the Web3 provider, new data contributed to MongoDB can be transferred straight to the blockchain, where it will be saved as an Ethereum network transaction. This produces a visible and unchangeable record of the data. This Python acquires data from MATLAB (the DB) on the specified port number and forwards it to Ganache (same blockchain).

Ganache has the benefit of providing ten distinct accounts, each with 100 ethers, which are exclusively available for development. The scalability of the system depends on the development and deployment of a personal BC that enables us to generate several distinct addresses for every node. Block mining on this BC has the advantage of being extremely fast if an authority is assigned to manage it. This is because the authority is only responsible for using processing power to manage block mining. Ethereum mines on the PoW paradigm; however, by specifying functions in a smart contract and assigning specific addresses to certain activities, Proof-of-Authority (PoA) benefits can be acquired. In a P2P interfacing module, Matlab is contributed to the Python IDE, and this Python is eventually linked to Ganache, an Ethereum blockchain tool. Here, 8 GB of RAM, 128 SSD/640 HDD, Ubuntu 18.04, and an Intel Core I5 2.3 GHz processor are used for powering the gateway.

5.2. Performance Analyses

In the submitted model, some addresses have been identified as authorities (power)to carry out specific tasks, while other addresses cannot, like the registration of all police stations from the SP node address and authorization of e-FIR transactions from the admin node address. As seen in Figure 5, the more e-FIRs that are registered in the police station DB, the greater the number of transactions that take place using smart contracts on the BC ledger. From Figure 5, it is observed that the first test sought to determine how long it takes to connect the gateway to the DB and obtain a user's public key.

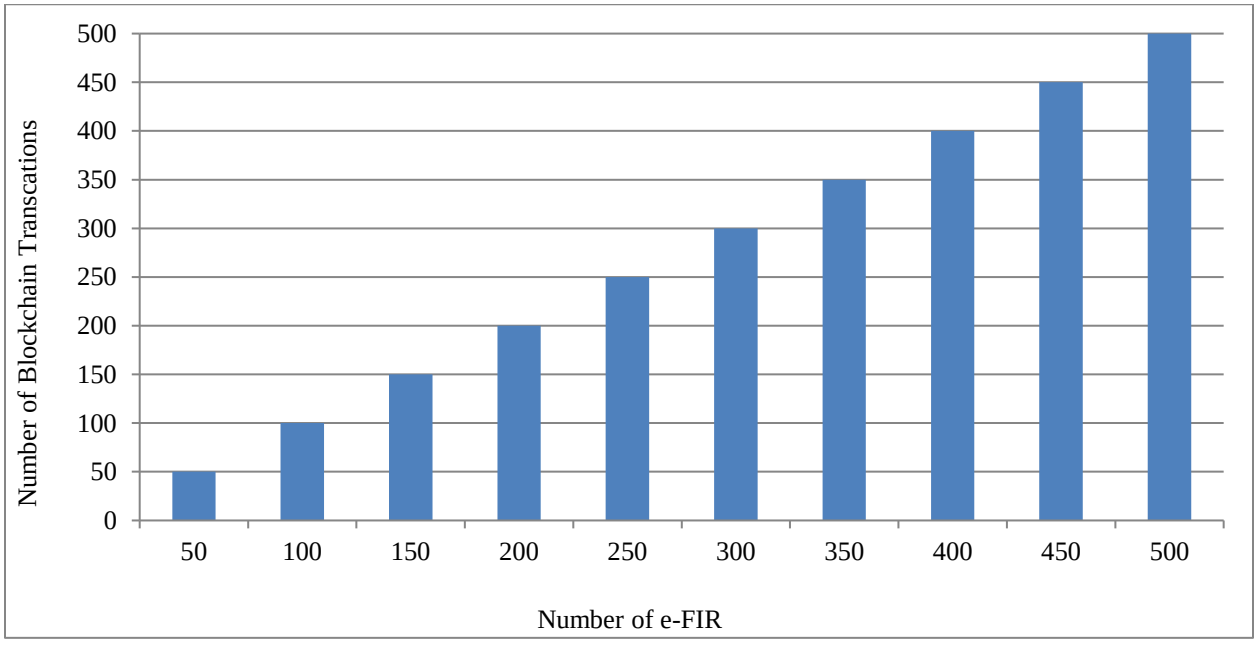

Fig. 5 Number of e-FIRs vs. Blockchain transactions of proposed SSMOA-EPCA

5.2.1. Execution Time Taken

By means of three different local FIR (DB) sizes, such as 100, 1K, and 10K FIRdata, the time required to retrieve 1, 10, 100, and 1000 keys for the sample considerations is calculated. The execution time of key recovery queries varies, and DB sizes are considered, which are listed in Tables 1-3.

Table 1. Comparison of execution time for 10 KB data size

Database Size	Execution Time (s)					
	Blockchain [43]	SHA-128	SHA-256	SHA-512	SSMOA	SSMOA-EPCA
1	1.85	1.73	1.48	1.75	1.39	1.34
10	1.96	1.84	1.66	1.52	1.49	1.45
100	2.43	1.93	1.92	1.63	1.63	1.58
1000	4.65	4.53	4.54	4.31	4.32	4.26

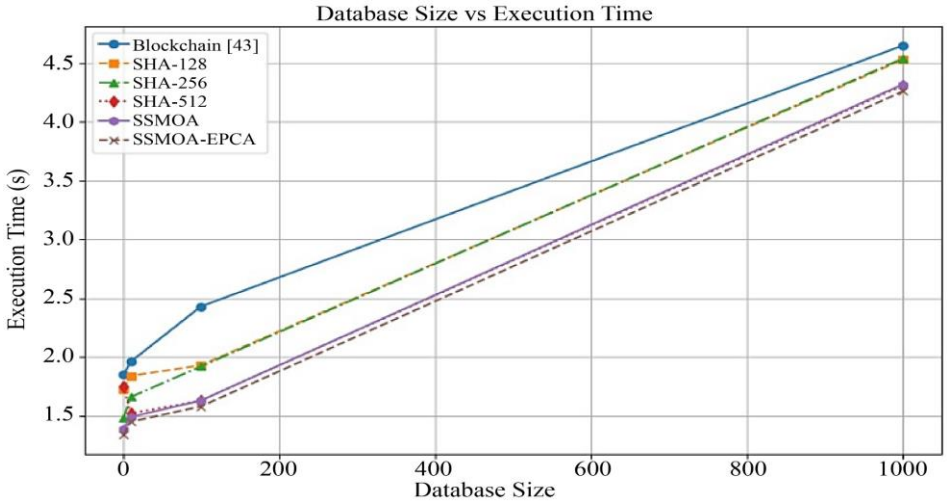

Fig. 6 Execution time for 10 KB data size

Table 2. Execution time for 100 KB data size

DB Size/ Methods	General blockchain	SHA-128	SHA-256	SHA-512	SSMOA	SSMOA-EPCA
1	2.13	1.92	1.84	1.76	1.64	1.48
10	2.46	2.35	2.27	2.19	2.08	1.81
100	7.64	7.52	7.47	7.33	7.18	6.91
1000	10.63	10.54	10.46	10.37	10.26	10.08

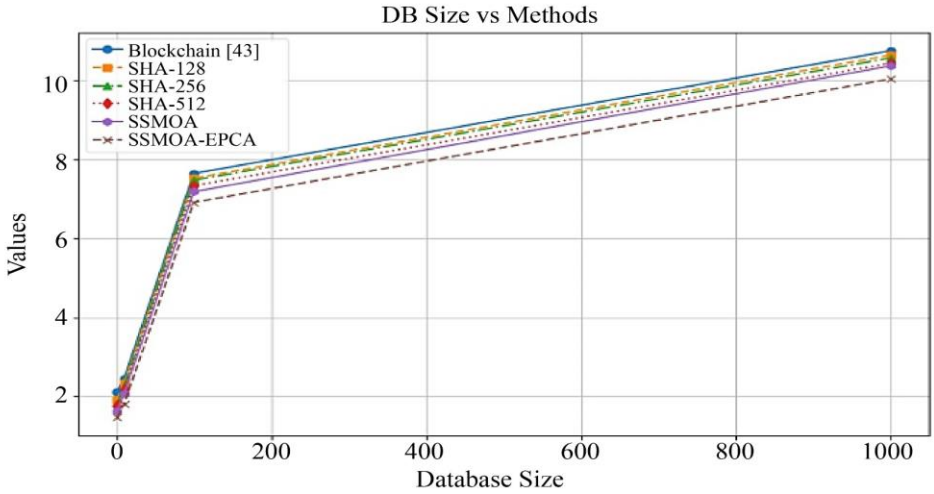

Fig.7 Comparison of execution time for 100 KB data size

Table 3. Comparison of execution time for 1000 KB data size

DB Size/ Methods	General Block chain	SHA-128	SHA-256	SHA-512	SSMOA	SSMOA-EPCA
1	2.14	2.03	1.92	1.86	1.68	1.36
10	2.25	2.14	2.07	1.98	1.84	1.64
100	9.64	9.52	9.45	9.38	9.26	8.92
1000	12.65	12.54	12.45	12.35	12.18	11.88

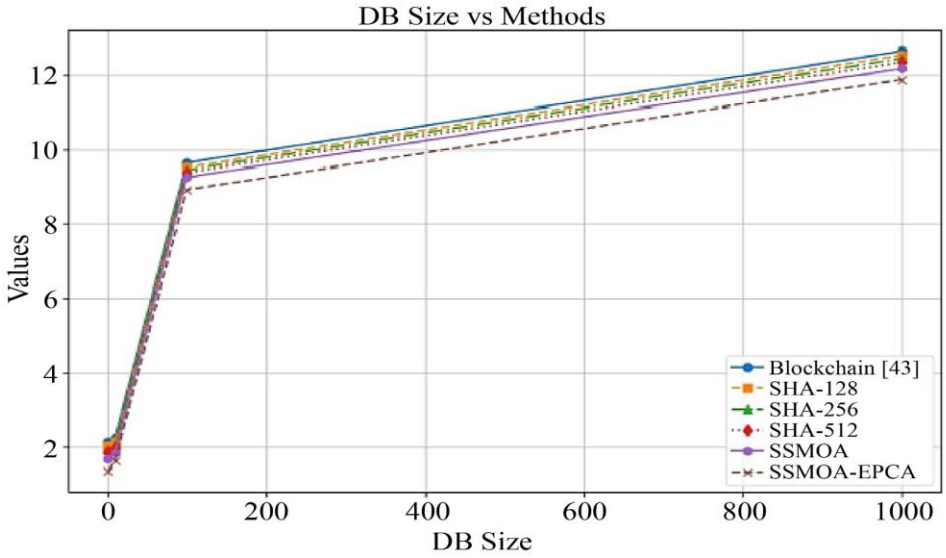

Fig. 8 Comparison of execution time for 1000 KB data size

Table 4. Comparison of blockchain contract registry execution time

Contracts	Execution Time (s)					
	General Blockchain	SHA-128	SHA-256	SHA-512	SSMOA	SSMOA-EPCA
1	0.83	0.72	0.64	0.52	0.49	0.41
10	6.5	5.9	5.2	4.2	3.84	3.29
50	25.8	24.7	23.64	22.48	21.8	19.86
100	41.55	40.62	39.52	38.35	37.46	36.74

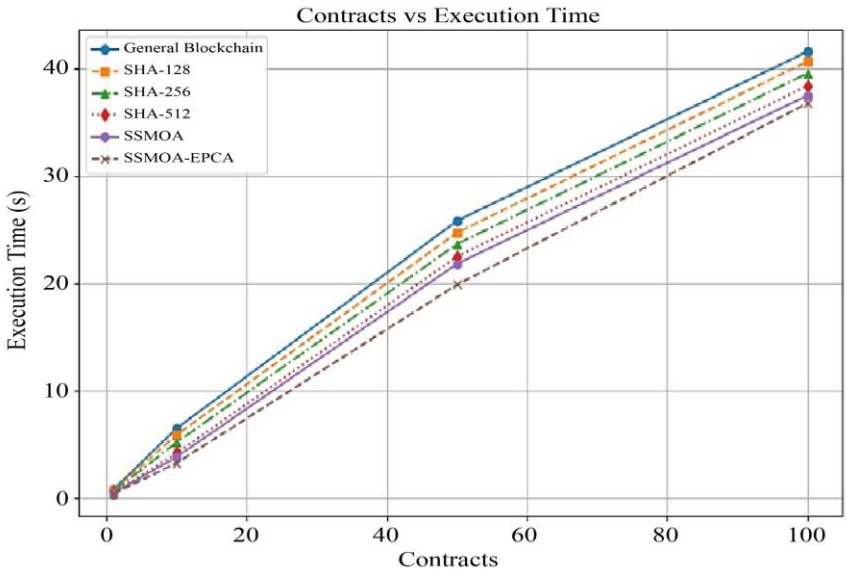

Fig. 9 Time of execution for a blockchain contract registry

The previous NyaYa system [43] is considered a general blockchain model and compared with the SSMOA-based criminal FIR data-secured system. To validate smart contracts, the Mythril open source program [13] is used. This tool tests for transactional security issues such as origin, re-entrancy, order dependence, and time-stamp dependencies that could be abused. The new SSMOA-EPCA FIR system is further separated as compressed data and without compressed data. These are also compared and listed in the above table. These are plotted in separate graphs for 100, 1K and 10K, as depicted in Figures 6 to 8.

The duration required for contracts to be registered on SSMOA-based blockchain via the gateway, taking into account that every registered FIR data is associated with a specific contract. An Intel Core processor was used to host the SSMOA blockchain for this experiment. Next, it is connected to the blockchain using the web3.js library for registering and validating the contracts. The execution times are then measured for the registration of 1, 10, 50, and 100 contracts. The results are shown in Table 4 and also plotted in Figure 9. These findings show that any number of contracts that are uploaded concurrently has a linear effect on the time required to register a transaction on the blockchain. Next, the connecting gateway time to the SSMOA blockchain is assessed by using the address of every contract that was generated to conduct a search within the blockchain. The time taken to retrieve the contract address from the DB by the gateway was overlooked. The findings displayed in Table 5 demonstrate that the time required to obtain a contract preserved on the SSMOA blockchain is not significantly affected by its rise in the number of blocks (also in Figure 10).

Table 5. Time required for blockchain blocks for various models

Blocks	Execution Time (s)					
	Blockchain [43]	**SHA-128**	**SHA-256**	**SHA-512**	**SSMOA**	**SSMOA-EPCA**
1	0.72	0.65	0.57	0.45	0.42	0.32
10	0.84	0.72	0.63	0.47	0.46	0.34
50	0.86	0.78	0.67	0.49	0.47	0.35
100	0.93	0.81	0.73	0.52	0.49	0.38

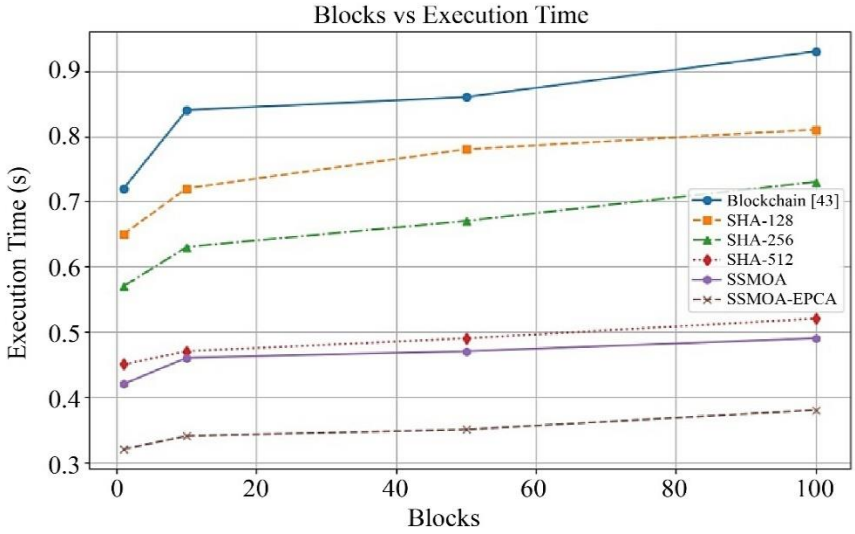

Fig. 10 Execution Time comparison for different blockchain models with different number of blocks

5.2.2. Network Bandwidth, Latency and Throughput

The network bandwidth of the suggested strategy is compared to traditional [43] designs in Figure 11. The bandwidth of Ethereum is between 200 and 300 Kbps. The utilization of bandwidth has improved since more transactions have been embedded in blocks as a result of off-chain record storage. Among other parameters, latency and throughput are the main factors on which an efficient network depends. The response time for each transaction, or the time it takes to verify that a transaction has been added to the BC, is referred to as latency. The block frequency is another name for this lag. The comparison of the schemes' signature latency is shown in Figure 12. The signature operation is optimized, verified, and stored in hashed form using the suggested method. This results in a quicker verification process for creating signatures. The standard BC providing latency is 980 ms at a block key size of 100 bytes, while SSMOA's is 850 ms. The signature latency is 560 ms, in contrast. The average signing latency for the SSMOA scheme is 695 ms, whereas the conventional blockchain scheme has an average of 798 ms. As can be seen, the scheme performs better than the aforementioned schemes, with an average latency of 430 ms. As a result, the plan

suggests a roughly 35% reduction in signature latency compared to traditional methods. Throughput, which is affected by the delay among transactions and each block size, is the number of transactions handled per second. Transactions Per Second (TPS) is the unit of measurement for this pace. Similar to the latency comparisons, the throughput is also depicted in Figure 13.

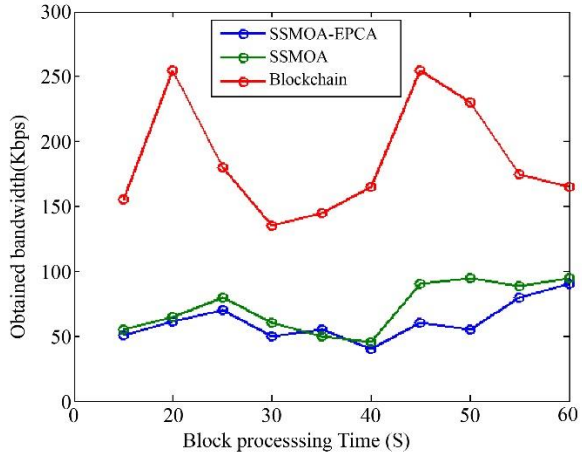

Fig. 11 Processing time vs. attained bandwidth

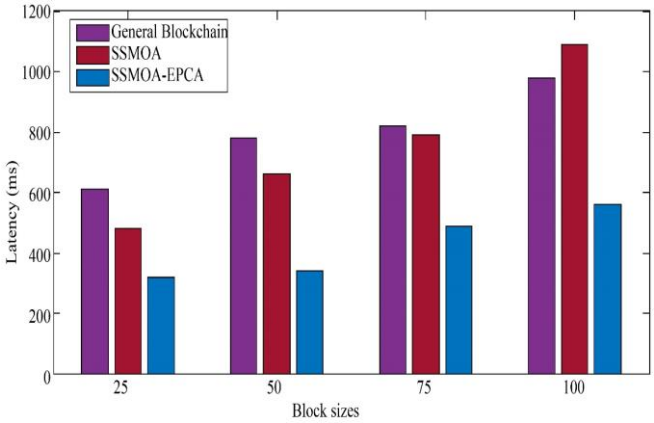

Fig. 12 Latency comparisons for various blocks

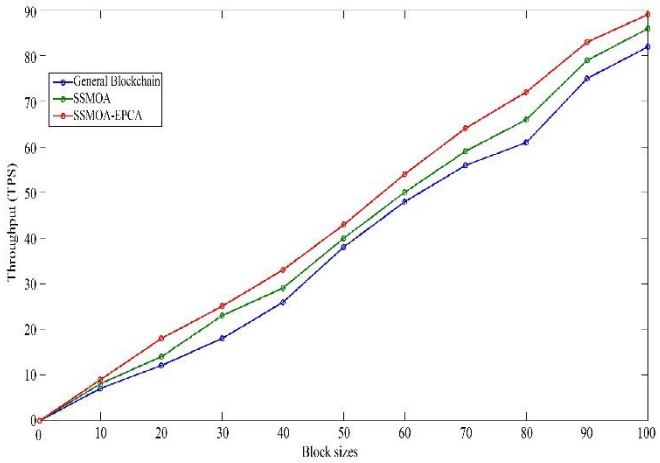

Fig. 13 Throughput analyses for various blocks

5.2.3. Consensus Models

As an essential part of a smart city environment, the study addresses the issues of e-FIR integrity and false registration incorporated with police stations using a distributed blockchain approach. The e-FIR scheme is instigated on the Ethereum blockchain and uses PoW as a consensus procedure to authorize transactions and yield new hash values. It delivers fast verification speed and 50% crash fault tolerance with better scalability. Table 6 expresses an evaluation of several consensus strategies.

Table 6. Several consensus systems

Characteristics	PoW	PoS
Crash fault tolerance	50%	50%
Byzantine fault tolerance	50%	50%
Scalability	>100s	<100s
Throughput (TPS)	<100	<1000
Verification speed	Strong	Strong

5.2.4. Smart Contracts with Hashing Algorithms

In the submitted model, a smart contract for the Ethereum blockchain is created using a Solidity programming language in the Remix IDE, which receives data as a hash and stores it on the BC. The functions in the smart contract include updating the investigating officer, uploading a hash on the BC, and registering all police stations. Several hashing algorithms are used during the execution of the recommended BC-based framework to test the impact of these hashing algorithms on the performance of the submitted framework. Specifically, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 are employed. SHA-512 (512 bits) is thought to be the most sophisticated and secure hashing algorithm, as provided in Table 7. Since SHA-1 (single bit) is not as secure as SHA-512, there is less hashing security. In BC, SHA-256 (256 bits) can ensure data integrity by providing a robust hashing security level while utilizing a moderate gas value.

Table 7. Several consensus algorithms

Hash functions	Average gas used ($x10^3$)
SHA-1	40.5
SHA-224	43.5
SHA-256	47
SHA-384	58
SHA-512	65

5.2.5. Security Model

In this module, technology has been promoted, storage media costs have been reduced, and appropriate security measures are offered. Data affecting legal matters transitioned from physical to digital media and is managed in a coordinated manner. The suggested model has the potential to create everlasting records, unchangeable reports, maintenance contract transactions, and many other things in the framework of smart contracts. With the right consensus method, crucial data may be digitally stored and shared between Blockchain nodes, allowing for the creation of useful reports, operational

excellence, and a trustworthy environment. It rigorously keeps all network nodes in sync and updates the shared ledger continuously. To maintain the security, confidentiality and anonymity of criminal records, they are kept on a public blockchain that uses public/private key cryptography. Thus, from these simulating behaviors, the submitted design can be used in real-world systems based on the outcomes of the aforementioned simulations.

6. Conclusion

The SSMOA-based EPCA architecture makes use of smart contracts, a private blockchain, and an efficient cryptographic scheme to provide anonymization. To complete this work, the most recent approaches to protect privacy on platforms are reviewed. The submitted method is used to ensure privacy in FIR investigation applications and is also described for other IoT scenarios. Thus, the submitted work appears to be the first to offer an optimized blockchain-based solution for privacy in data systems. Additionally, the encryption module uses the SSMOA concept to create keys and collect data securely based on enhanced PCA-based compression. Crucial information is protected by strong security keys. By including this optimized security key with discovered and gateway data, unauthorized users or hackers are prohibited from accessing the files. Consequently, the attackers cannot get the initially collected FIR data without the key. In the future, the outcomes verified that the suggested architecture could be put into practice. Implementing a system that stores all the city's FIRs on a single blockchain would be unfeasible due to scalability and performance concerns. Also, the detection of various attacks will be intended to occur in these systems. The ability of the system to meet the time requirements for registering multiple cases taken by the multiple police stations of one or more cities is another factor that determines the scalability of this implemented system.

Further work will also focus on improving self-executing smart contracts with business scenarios, end-user identity management, and access control policy developments on smart contracts; scalability and availability improvements for real-time transaction handling, and lightweight consensus design solutions for high QoS and low network latency for the advancement of BC-based smart transportation. Further implementations can also increase the observability of benefits and the degree of trialability of the proposed communication model.

Conflicts of Interest

This study primarily focuses on simulations to validate the proposed system. Real-world implementation would require further development and rigorous security testing to ensure robustness in practical scenarios. Storing FIR data from multiple cities on a single blockchain with large networks has scalability challenges. Future research should explore efficient data sharing or partitioning techniques to address this issue effectively.

References

[1] Abdul Rehman Javed et al., "Future Smart Cities: Requirements, Emerging Technologies, Applications, Challenges, and Future Aspects," *Cities*, vol. 129, no. 1, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Tanweer Alam, "Cloud-Based IoT Applications and Their Roles in Smart Cities," *Smart Cities*, vol. 4, no. 3, pp. 1196-1219, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Shashvi Mishra, and Amit Kumar Tyagi, "The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications," *Artificial Intelligence-Based Internet of Things Systems*, vol. 1, no. 1, pp. 105-135, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Maisha Afrida Tasnim et al., "Crab: Blockchain Based Criminal Record Management System," *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, vol. 11342, pp. 294-303, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[5] Kirti Marmat, and Anand More, "E-Fir Using E-Governance," *International Journal for Innovative Research in Science & Technology*, vol. 3, no. 2, pp. 4-9, 2016. [Google Scholar] [Publisher Link]

[6] Saurabh Singh et al., "Convergence of Blockchain and Artificial Intelligence in IoT Network for the Sustainable Smart City," *Sustainable Cities and Society*, vol. 63, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Shaukat Ali et al., "Privacy and Security Issues in Online Social Networks," *Future Internet*, vol. 10, no. 12, pp. 1-12, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] Myeonghyun Kim et al., "Design of Secure Decentralized Car-Sharing System using Blockchain," *IEEE Access*, vol. 9, no. 1, pp. 54796-54810, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Tanzeela Sultana et al., "Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices," *Applied Sciences*, vol. 10, no. 2, pp. 1-21, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Fadele Ayotunde Alaba et al. "Smart Contracts Security Application and Challenges: A Review," *Cloud Computing and Data Science*, vol. 1 no. 2, pp. 15-41, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Meryem Ammi, Shatha Alarabi, and Elhadj Benkhelifa, "Customized Blockchain-Based Architecture for Secure Smart Home for Lightweight IoT," *Information Processing & Management*, vol. 58, no. 3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] A. Sasikumar et al., "An Efficient, Provably-Secure DAG Based Consensus Mechanism for Industrial Internet of Things," *International Journal on Interactive Design and Manufacturing (IJIDeM)*, vol. 17, no. 5, pp. 2197-2207, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Nikunjkumar Sureshbhai Patel et al., "Blockchain-Envisioned Trusted Random Oracles for IoT-Enabled Probabilistic Smart Contracts," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14797-14809, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Mahima John, and Abhijeet R. Raipurkar, "Improving Data Integrity and Security in Cloud Environments: A Blockchain-based Method," *Grenze International Journal of Engineering & Technology*, vol. 10, no. 2, 2024. [Google Scholar]

[15] D. Praveena Anjelin, and S. Ganesh Kumar, "Blockchain Technology for Data Sharing in Decentralized Storage System," *Intelligent Computing and Applications: Proceedings of ICICA 2019*, Springer Singapore, vol. 1172, pp. 369-382, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] A. Sasikumar et al., "Blockchain-Based Decentralized User Authentication Scheme for Letter of Guarantee in Financial Contract Management," *Malaysian Journal of Computer Science*, vol. 1, no. 2, pp. 62-73, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Karl Wüst, and Arthur Gervais, "Do You Need a Blockchain?," *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland, pp. 45-54, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[18] Thomas Kerber et al., "Ouroboro Scrypsinous: Privacy-Preserving Proof-of-Stake," *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 157-174, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Sara Saberi et al., "Blockchain Technology and Its Relationships to Sustainable Supply Chain Management," *International Journal of Production Research*, vol. 57, no. 7, pp. 2117-2135, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] Haifeng Yu et al., "OHIE: Blockchain Scaling Made Simple," *2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 90-105, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Barbara Bigliardi et al., "The Digitalization of Supply Chain: A Review," *Procedia Computer Science*, vol. 200, pp. 1806-1815, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Yizhong Liu et al., "A Flexible Sharding Blockchain Protocol Based on Cross-Shard Byzantine Fault Tolerance," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2276-2291, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Deepa Pavithran et al., "Towards Building a Blockchain Framework for IoT," *Cluster Computing*, vol. 23 no. 3, pp. 2089-2103, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] P. Velmurugadass et al., "Enhancing Blockchain Security in Cloud Computing with IoT Environment using ECIES and Cryptography Hash Algorithm," *Materials Today: Proceedings*, vol. 37, pp. 2653-2659, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Muhammad Rehan Anwar, Desy Apriani, and Irsa Rizkita Adianita, "Hash Algorithm in Verification of Certificate Data Integrity and Security," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 3, no. 2, pp. 181-188, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Sachi Nandan Mohanty et al., "An Efficient Lightweight Integrated Blockchain (ELIB) Model for IoT Security and Privacy," *Future Generation Computer Systems*, vol. 102, no. 1, pp. 1027-1037, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Basim Aljabhan, and Muath A. Obaidat, "Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO)," *Sustainability*, vol. 15, no. 8, pp. 1-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Zhi Li, Fuhe Liang, and Henan Hu, "Blockchain-Based and Value-Driven Enterprise Data Governance: A Collaborative Framework," *Sustainability*, vol. 15, no. 11, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Hui Pang et al., "Smart Farming: An Approach for Disease Detection Implementing IoT and Image Processing," *International Journal of Agricultural and Environmental Information Systems*, vol. 12, no. 1, pp. 55-67, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] Ahmad Karim, "Development of Secure Internet of Vehicle Things (IoVT) for Smart Transportation System," *Computers and Electrical Engineering*, vol. 102, no. 3, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] Sushil Kumar Singh, Shailendra Rathore, and Jong Hyuk Park, "Block IoT Intelligence: A Blockchain-Enabled Intelligent IoT Architecture with Artificial Intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721-743, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[32] Lelio Campanile et al., "Risk Analysis of a GDPR-Compliant Deletion Technique for Consortium Blockchains Based on Pseudonymization," *International Conference on Computational Science and its Applications*, vol. 12956, pp. 3-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[33] Ghadah Aldabbagh et al., "Blockchain for Securing Smart Grids," *International Journal of Computer Science & Network Security*, vol. 21, no. 4, pp. 255-263, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[34] Lokesh Yadav et al., *Nullifying the Prevalent Threats in IoT Based Applications and Smart Cities Using Blockchain Technology*, Low Power Architectures for IoT Applications, pp. 241-261, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[35] Rujuta Shah, and Sridaran Rajagopal, "M-DPS: A Blockchain-Based Efficient and Cost-Effective Architecture for Medical Applications," *International Journal of Information Technology*, vol. 14, no. 4, pp. 1909-1921, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[36] Aaliya Sarfaraz, Ripon K. Chakrabortty, and Daryl L. Essam, "The Implications of Blockchain-Coordinated Information Sharing within a Supply Chain: A Simulation Study," *Blockchain: Research and Applications*, vol. 4, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] Xiaoning Qian, and Eleni Papadonikolaki, "Shifting Trust in Construction Supply Chains Through Blockchain Technology," *Engineering, Construction and Architectural Management*, vol. 28, no. 2, pp. 584-602, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] Candido Diaz et al., "Silk Structure Rather Than Tensile Mechanics Explains Web Performance in the Moth-Specialized Spider, Cyrtarachne," *Journal of Experimental Zoology Part A: Ecological and Integrative Physiology*, vol. 329, no. 3, pp. 120-129, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[39] Shunsuke Shigaki et al., "Time-Varying Moth-Inspired Algorithm for Chemical Plume Tracing in Turbulent Environment," *IEEE Robotics and Automation Letters*, vol. 3, no. 1, pp. 76-83, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[40] Mahsa Jamshidi Dolatabad et al., "Evaluating Agile Practices in Green Supply Chain Management Using a Fuzzy Multicriteria Approach," *Discrete Dynamics in Nature and Society*, vol. 2022, no. 1, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[41] Fabian Brinkmann, and Stefan Weinzierl. "Comparison of Head-Related Transfer Functions Pre-Processing Techniques for Spherical Harmonics Decomposition," *Audio Engineering Society Conference: 2018 AES International Conference on Audio for Virtual and Augmented Reality, Audio Engineering Society*, vol. 1, no. 1, pp. 102-116, 2018. [Google Scholar] [Publisher Link]

[42] Angel Arranz-Gimon et al., "A Review of Total Harmonic Distortion Factors for the Measurement of Harmonic and Interharmonic Pollution in Modern Power Systems," *Energies*, vol. 14, no. 20, pp. 1-38, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[43] Ashwin Verma et al., "NYAYA: Blockchain-Based Electronic Law Record Management Scheme for Judicial Investigations," *Journal of Information Security and Applications*, vol. 63, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[44] Essam H. Houssein et al., "Lévy Flight Distribution: A New Metaheuristic Algorithm for Solving Engineering Optimization Problems," *Engineering Applications of Artificial Intelligence*, vol. 94, 2020. [CrossRef] [Google Scholar] [Publisher Link]