Hindawi
Security and Communication Networks
Volume 2023, Article ID 9870186, 1 page
https://doi.org/10.1155/2023/9870186

Retraction

Retracted: Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] G. Subathra, A. Antonidoss, and B. K. Singh, "Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme," *Security and Communication Networks*, vol. 2022, Article ID 3167958, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 3167958, 13 pages
https://doi.org/10.1155/2022/3167958

Research Article

Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme

G. Subathra,[1] **A. Antonidoss**,[1] **and Bhupesh Kumar Singh**[2]

[1]*Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai 603103, Tamil Nadu, India*
[2]*Arba Minch Institute of Technology, Arba Minch University, Arba Minch, Ethiopia*

Correspondence should be addressed to G. Subathra; subigt10@gmail.com and Bhupesh Kumar Singh; dr.bhupeshkumarsingh@amu.edu.et

Received 1 March 2022; Revised 8 June 2022; Accepted 23 June 2022; Published 8 July 2022

Academic Editor: Ruhul Amin

By the development and advancement of blockchain technique, Internet of Things (IoT) proliferation driven devices and the application of blockchain-enabled IoT alter the view and operating infrastructure of the smart networks. The blockchain is responsible for supporting decentralized systems and offers secured means of authentication, management, and access to IoT system thereby deploying smart contracts offered by Ethereum. The increasing demand and the blockchain expansion generate huge volume of sensitive data. The growing demand and expansion of blockchain-IoT systems is generating large volume of sensitive data. Furthermore, distributed denial-of-service (DDoS) attacks are regarded as the most promising threats for smart contracts in the blockchain-based systems. Therefore, there is a need to detect and classify the attack type and the data should be stored in server more securely with the use of blockchain and data aggregation method. For this purpose, this presented technique aims at introducing decentralized consensus blockchain and Interplanetary file system (IPFS) based data aggregation for effective classification and data storage. The attack is detected using meta-hyperparameter random forest (MHP-RF) classifier. Once the attack is detected, the transaction information is stored in server securely by means of smart contract-based blockchain system. The transaction handling stage classifies the transaction type as normal or abnormal one which then followed by execution of business logic by smart contract thereby appending the transaction of blockchain in the network cloud. The consensus blockchain technique is employed with the use of PoW-enabled scheme integrated with Elgamal-based data aggregation. Therefore, the system security is improved and the intrusion is prevented greatly. The performance analysis of the system is analyzed in terms of accuracy, precision, recall, F-score, Encryption time, decryption time, execution time, and space complexity. The attained outcomes are compared with traditional approaches to prove the effectiveness of proposed strategy. The proposed system is said to be effective in time consumption, classifier performance, and in overcoming space complexity issues.

1. Introduction

With the advanced emergent of information divergence, mechanism of cloud storage is becoming a popular and necessary one in day-to-day life. The cloud storage aids in enabling the individuals or enterprises for attaining cloud data anywhere and at any time, from which this kind of feature brings out excellent convenience for living [1]. As with the quantity of Internet of Things (IoT) devices increases, it is more vital than ever to provide a safe framework for storing as well as using IoT data either in or out of Smart nodes. Blockchain and smart contracts enable the creation of secure data storage and access configurations [2, 3]. Nevertheless, there exists some challenges and disputes in the system of existing cloud storage. In particular, there is a need of shared data for encryption and to guarantee the privacy of data in the upcoming era of big data which increases the difficulty to maintain data security thus reducing data sharing greatly [4]. The Internet of things (IoT) is a new and interesting technology that connects a massive growth of connected devices to the Internet and allowing them to capture and exchange data to assist people in monitoring

and responding to changes in order to boost efficiency [5, 6]. Furthermore, several cloud storage schemes are functioned by means of a centralized concern that has strong capability of supervising and storing the data. The corporation could be perceived as a third party which inherits single point of failure flaws ineluctably [7]. Last but not the least one, the upgrade of devices with rise of wages for employees has impact on centralized cloud storage cost. Hence, for ensuring better data availability and privacy, a flexible access control should be achieved over the data encrypted and thus altering the storage of data from centralized systems to decentralized system that not only has lower cost but too could relive the desired concern from single point failure on comparing centralized system.

Providentially, bit-coin advent has obsessed the growth of blockchain technique, the technology of blockchain is decentralized ledger thought at which the transaction and data are not in third party control, and the information that were stored in the blockchain cannot be interfered [8]. Smart healthcare based on IoT innovation has been suggested to enhance performance and quality, overcome geographical boundaries to perform monitoring system, assess illness risk, and build disease prediction. Monitoring equipment of health data to achieve intelligent healthcare has lately received a lot of interest with the emergence of the Internet of Things (IoT) [9, 10]. Consequently, blockchain has sturdy data reliability and constancy. Recently, there was a unique increase in identity theft, security breaches, and data loss. It was reported that about 3,813 data breaches which leads to 4.1 billion records expose at first 6 months of 2019 [11]. Intentional breach or illegal access becomes a major threat which is presented because of the inappropriate maintenance and execution of the access control scheme.

IPFS and the Hyperledger fabric was typically regarded as the distributed storage application, which employs blockchain as a core infrastructure that attracts huge attention recently. The blockchain is considered as a decentralized storage database which is a novel computer technology application like consensus mechanism, cryptography, smart contract, point-to-point transmission, and other machineries.

Modern mobile smart health devices are defined by their miniaturization and ultralow power consumption, which results in limited computing and storage capacity. As a consequence, smart health devices need additional compute and storage technology [12, 13]. Several researchers of cloud storage field focus on ensuring data security, system of individual data control depending on blockchain was presented in [14]. This system could guarantee enhanced rate of data privacy. To address the challenging issues of data security maintenance and data sharing that impede big data advancement, a blockchain-based access management framework for enhancing big data platform privacy plays a significant role [15]. In the meanwhile, health chain splits transaction for publishing info from transactions for good data access, and encrypts the data as stored within IPFS, decreasing connection and computation costs while ensuring privacy [16, 17]. Nevertheless, these systems do not offer the power for data owner for controlling the flexibility and efficiency of data.

For solving these issues, storage system provides an end-to-end manner of encryption. This scheme stores the hashing value of data on the blockchain on offering validating data integrity means. The blockchain technology and the peer-to-peer network storage were too utilized in the platform of cloud [18], this stage unravels an uploaded information as several parts of data, thus encodes each portion of information. The data encrypted are sent by means of smart contracts for each node that offers storage service, user may pay for storage service to be the storage node which needs to submit stored data proof for preventing storage node from stored data removal. Nevertheless, in these systems, the process of data encryption is not fully controlled by the data owner.

Blockchain, on the other hand, was expressly created for digital money transactions. As a result, sustaining with the attribution data development speed in respect of block formation speed and storage efficiency is quite tough. To address the issue, we developed an agricultural commodities provenance platform that integrates IoT, IPFS, and blockchain. First, we offered that a data storage solution is based on IPFS and blockchain for the massive amounts of data generated all throughout product relocation process. IPFS-based storage and query approaches are also presented. The smart contracts deployed in IoT environment are prone to several attacks. DDoS attacks are having intention to suspend and interrupt the networks or the online sources by means of blocking streams of data traffic in a way that the desired source are unusable. So as to prevent attacks on smart contracts, the timely recognition of attacks using IDS as blockchain-IoT system is a research issue and a fundamental need.

Also, the command-and-control server (bot-master) makes IoT sensor a botnet over the Internet and thus aims at interrupting smart contracts that works with DDoS attacks. As a consequence, this kind of malicious activities may cause serious utilization of resource on fog nodes. Therefore, the smart contracts will be congested by large number of legitimate user requests. Hence, to overcome these existing issues, this work focuses on implementing an integration technique of IDS with the smart contracts in the system of blockchain IoT for thereby mitigating the issues of DDoS attack.

The system is designed to connect all required devices. In other words, IPFS is a peer-to-peer file system that may provide high-throughput block storage in a content-addressed fashion. Based on the open source IPFS protocol and blockchain technologies, we develop a data storage paradigm. The modules of the system are principally concerned with data encapsulation, data analysis, and data management. The data encapsulation module primarily collects and encapsulates video, picture, and sensor data that has been supplied. The data management system module includes the IPFS, database, and blockchain.

In case of huge volume of sensitive data generated in the blockchain-based IoT system, it is essential to implement a strong and effective security mechanism for the aggregation

of data. The novelty of this work aims at presenting decentralized consensus blockchain and interplanetary file system (IPFS)-based data aggregation for effective classification and data storage. The attack is detected using meta-hyperparameter random forest (MHP-RF) classifier. The information regarding the transaction is stored in the server securely with the use of blockchain-based smart contract scheme. On using this, the privacy and security of the system is enhanced in an effective manner.

The enduring portion of manuscript is structured as shown. Section 2 is the detailed depiction of various existing techniques study employed thus far. The proposed methodology is described in Section 3 in a detailed manner. Section 4 is the performance analysis of suggested technique. Section 5 concludes overall workflow of system.

2. Related Works

A detailed study analysis on various existing techniques related to decentralized storage system in blockchain and IPFS are carried out in this portion.

The author in the work [19] presented a novel technique of identity-based proxy re-encryption (IBPRE) that are data owner manipulative and is signified as (DOM-IBRE). This was accomplished on integrating blockchain, IPFS technique, and IBPRE techniques. This suggested scheme was competent of evading the certificate management complexity thereby enhancing the storage of big data security and amends the efficacy of sharing in big data. The security assessment of this system was made by means of chosen plain text attack (CPA) in the standardized model thereby simulating the pairing-based cryptography (PBC) libraries on comparing them with PRE approaches which reveals that the suggested model offers better performance the efficiency of big data sharing. In addition, this approach offers enhanced outcome by reducing the exponential and bilinear pairing's computation time.

An efficient consensus technique was implemented in [20] for enhancing the consensus process efficiency in blockchain. The sensing data that were generated from IoT devices that were desired to logistics process will be encrypted and were aggregated as blockchain for ensuring the security of data. However, records of stored logistics were audited securely through leveraging the blockchain network at which both logistics demands and IoT data could not be deleted or tampered for evading the disputes.

A scheme of health chain that is the large-scale privacy-preserved health data was presented in [21] depending on the blockchain technologies at which the health data were encrypted for conducting the access control that were fine-grained. More specifically, the users could add or revoke the authorized doctors through user transaction leveraging for the management of key effectively.

A secured system for the access and storage of Electronic Medical Records (EMR) was presented in [22] on considering the integrity, confidentiality, and availability of those records. The presented work aims at offering a centralized system for storage intended for the healthcare institutions over the globe on considering the features that were secured on the system of decentralized interplanetary file system (IPFS). The system storage takes the utilization of blockchain ecosystem for sensitive storage of data. This technique too implements the role-dependent access control (RBAC) so as to access the storage.

A homomorphic integrated with blockchain-dependent FL model was presented in [23] for addressing the problems. This in turn offers the gradient protection of privacy through employing homomorphic and employs smart contrast-dependent scheme for reputation and the strategy of on- or off-chain storage correspondingly for solving the trust FL and issues of blockchain storage. By the end, this in turn estimates the presented technique on providing the analysis of qualitative privacy and thereby conducting the preliminary investigations on the performance of model.

A technique for consortium blockchain was executed in [24] for the secured trading of data with the transparency of information. Also, the hash list of the data traded was maintained through the roadside units convoyed through filters of bloom intended for dissolute look-up, so as to evade the duplication of data. The integrity and reliability of data trading were ensured through the utilization of digital signature scheme depending on elliptic curve bilinear pairing. For the availability of long-term traded data, the external distributed storage that is the interplanetary file system (IPFS) could offer high capacity and reliable storage of resources.

Rahman et al. [25] present a lightweight framework with hybrid FL that includes blockchain smart contracts for controlling the training plan edge, federated node participation authentication, and trust management, as well as the edge nodes' reputation with the dataset uploaded or the models. The scheme too aids entire dataset encryption, inference process, and the model training. The entire node of federated edge too performs the additive encryption, whereas the blockchain employs the multiplicative encryption for aggregating the model parameters that were updated.

In [26], a technique was investigated that integrates the blockchain technology with IoT and offered detailed analysis of blockchain-enabled IoT technology and the IIoT systems. The existing research was categorized as data management and storage system, cloud computing (data auditing and finance), big data, and the industrial sectors (like energy, supply chain, and healthcare sector). The insightful discussion depends on various categories which too was presented in this work.

A blockchain-based technique was presented in [27] which depends on patient-driven interoperability and thus discusses in what way this could be leveraged by blockchain. The facilitation of blockchain aids in patient identity, data liquidity, data immutability, clinical volume of data, and incentives.

A new architecture of decentralized blockchain system was suggested in [28] termed BEdge Health which integrates offloading of data and sharing data in the hospital networks that were distributed. Initially, the scheme of data offloading was presented at which the mobile devices could offload

health data to the nearby server of MEC on behalf of effective computation along with privacy awareness. However, a data sharing scheme was too presented that enables exchanges of data over healthcare users through IPFS and leveraging blockchain.

A blockchain dependent scheme for decentralized storage and authentication was projected in [29] for the BC solid at which the user's data was independent of the varied web application and thus switches the service of data storage can be independent of multiple web applications more easily without any trusted third party relying. At the same time, this scheme in turn guarantees the ownership of data with privacy of user through the blockchain miner leveraging for performing authentication using certificateless cryptography. Also included is a hypothetical instantiation for demonstrating how the transactions in BC solids were processed.

A fully decentralized approach for solving blockchain-based issues was suggested in [30] which were implemented with the use of Ethereum smart contract approach and the proxy re-encryption technique that were expensive computationally by means of multiple oracles for giving encrypted shared data storage access on the decentralized and public storage platforms like IPFS. The smart contracts aids in validating the outcomes depending on the encrypted outcome majority that were determined by oracles. Thus, for this reason, reputation mechanism was integrated with suggested smart contracts for rating the oracles depending on the nonmalicious and malicious behaviors. The work [31] aims at enhancing traditional system for managing. It has two levels of privacy and security with the use of blockchain and deep learning models. Ref. [32] presented a privacy-preserving-dependent security approach for Internet of vehicles (P2SF-IoV). This integrates the deep learning and blockchain model to overcome privacy-related issues Framework for Internet of Vehicles (P2SF-IoV). P2SF-IoV integrates blockchain and deep learning technique to overcome aforementioned challenges, and works on two modules. An integrated framework for improving security and privacy in cyber twin-dependent automated IoT is used in [33]. A framework of automated system DLTIF was introduced for cyber threat intelligence modeling and identification of threat kinds [34]. In [35], a Deep-Learning (DL)-enabled and blockchain-based scheme was designed for securing the data processing framework for the CAV framework. An anomaly-based intrusion detection system was proposed through decentralizing the existing cloud-dependent architecture for security to the local fog nodes [36].

3. Proposed Work

A brief explanation on the suggested methodology is illustrated in this section. Figure 1 shown below portrays the entire workflow of suggested technique.

The suggested detection scheme consists of three stages like traffic processing stage, intrusion detection stage, and the transaction handling stage. The hosting of these stages is held at the fog nodes. In the traffic processing stage, data preprocessing and selection of features are carried out. In the intrusion detection stage, the detection and classification of attack is done, and in the transaction handling stage, the blockchain-enabled data aggregation scheme along with smart contract is applied to check and recognize whether the transaction is normal or abnormal.

3.1. Data Preprocessing and Feature Selection. The sensed data from the IoT sensors should move over a series of preprocessing functions for offering better and normalized data to the classifier network. In this preprocessing stage, the removal of socket information is carried. The network data contains destination and source IP address with port numbers in the network which is essential for deleting the desired information for ensuring unbiased recognition. After that, the data is being normalized. The process of data preprocessing is done with the use of normalization technique since the traffic network comprises of varied range of repeated and redundant features. Thus, there is a need to eradicate this redundant information. This aids in eradicating the excess time consumed for training and testing in the detection system. Also, the detection efficiency of the system is enhanced widely. The traffic related to blockchain network has varied magnitude values. For this purpose, standard scalar normalization approach is employed for scaling the feature values.

In the database, the statistical data consist of several variations which make the classifier process a difficult one. Thus, during learning, these difficulties should be taken into account and eradicated. Hence, the values of each variable should be normalized for ensuring the minimum values of each attribute which is null and the highest one. This makes classifier a more similar value thus preserving the variation among the attributable values. By this, the unwanted traffic network is removed. This technique in turn transforms the feature observation such that the distribution of incoming traffic might have the mean values of 0 and the standard deviation to be 1. This is helpful in the proposed system as it excludes bias without the statistical properties manipulation from the incoming traffic. The function of transformation is being expressed by means of the following equation:

$$s_b = \frac{\mathrm{val}_m - \mu_b}{\sigma_b}. \tag{1}$$

Here, s_b refers to the features standard score employed in the detection scheme and $b \in \{b1, b2, b3, \ldots, bn\}$. The corresponding feature value in the IoT traffic is being signified by means of val_m. The standard deviation and mean of feature are signified with the use of σ_b and μ_b correspondingly and is being expressed using the following equation:

$$\mu_b = \left(\sum_{m=1}^{L} \mathrm{val}_m / L \right),$$
$$\sigma_b = \sqrt{1/L \sum_{m=1}^{L} (\mathrm{val}_m - \mu_b).^2} \tag{2}$$

By this, the unwanted traffic network is removed. Thus, after normalization approach, feature selection is made.

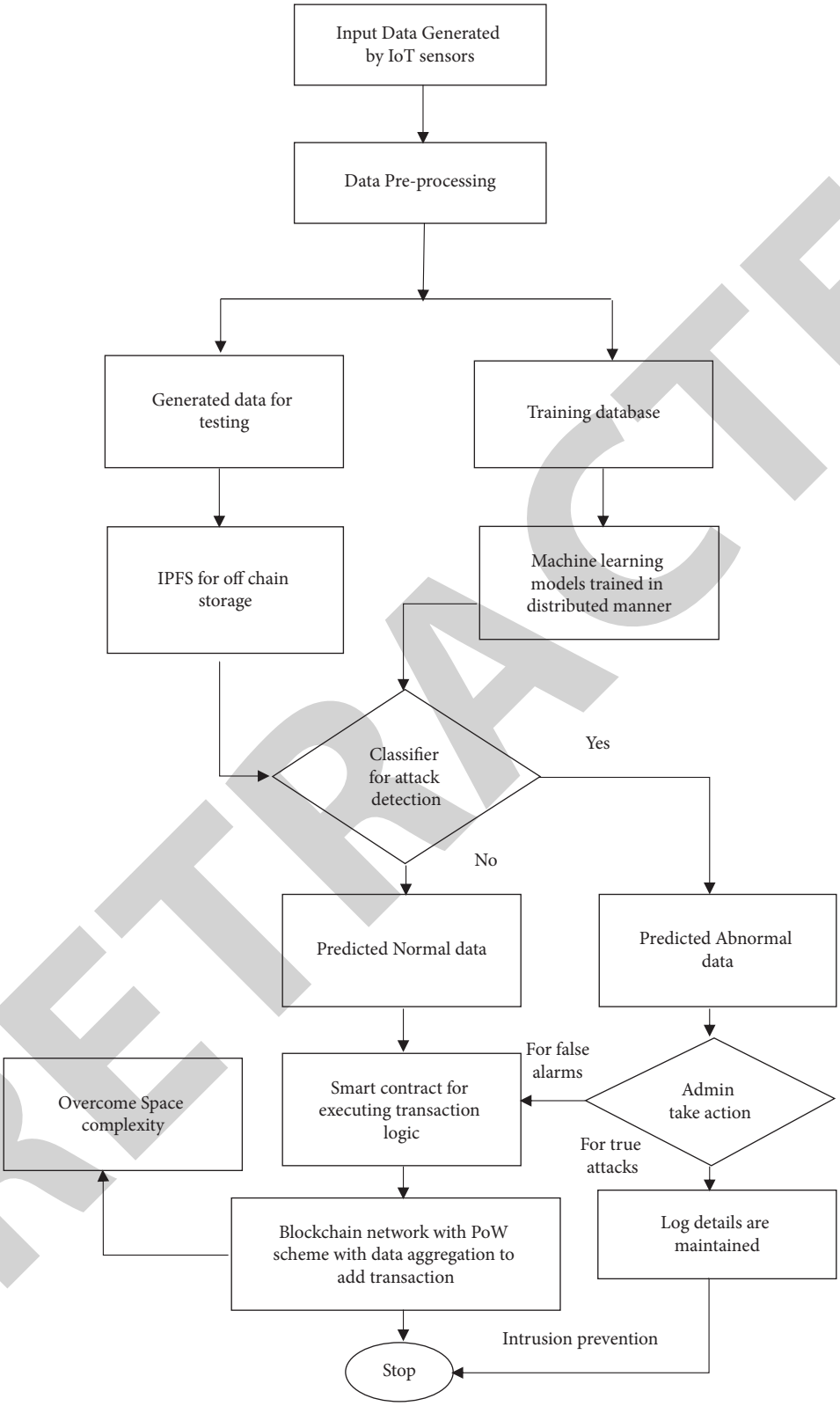

Figure 1: Flow of the proposed system.

3.2. Feature Selection. Once the preprocessing stage is completed, features are mapped and are being selected. For this purpose, density-based spatial clustering is employed. This technique is mostly introduced for mapping and selecting features and is a nonparametric algorithm. In this, the given data points are linked together closely. It assembles the data that were separated from the sparse points of data for getting clusters or dense groups. This does not need a

number of clusters as parameters instead they are capable of identifying the clusters depending on the data. The value of homogeneity is then recognized for the resultant clusters that are employed for the process of identification. High rank mapping refers to enhanced performance is obtained based on the features though the lower ratings expose that these features will offer no such significant part in evaluation. The homogeneity range is determined for each feature if they are organized from higher to lower by descending order. As of the homogeneous data, unique high-ranking features are mapped which could be chosen for more process.

3.3. IPFS for Off-Chain Storage. PFS is a technique for storing and transferring content. Like in the blockchain world, each user operates their own node (server). To begin, IPFS is decentralized since content is loaded from thousands of peers rather than a single centralized server. Every bit of data is cryptographically hashed, yielding a secure, one-of-a-kind content identity with which nodes may communicate and exchange files. The sensed and preprocessed data from IoT sensor is send to the IPFS cluster node that are closer which offers edge intelligent node service. This edge intelligent-based technique offers IPFS-dependent off-chain storage which are connected to the fog nodes that are local in a distributed manner.

IPFS is regarded as the peer-to-peer distributed file system which employs DHT for tracking the information. Moreover, this is a new technique for sharing distributed file. This IPFS consists of web application which makes the users a simple one for the users for working in it. The IPFS employs hash tables for storing package of packet. The nodes of IPFS could offer data blocks of data. The unique hash signifies the saving data result without any consideration of IPFS data size. This IPFS could store hash for retrieving data. Once the data is prepared for adding in IPFS network, data is then split as small chunks. The chunk is being recognized but their own hash. After that, the chinks are distributed for several nodes in the network that have their hash closer to peer ID. When the user requests for chunk, request traverses are retrieved for the nodes at which hash exists in this with the use of DHT. The entire chunks are combined simply for showing major intend after visiting the entire existed chunks. Moreover, distributed portion of DHT represents that whole table is being spread over varied locations.

This off-chain storage is responsible for management of resources, load balancing, network scalability, and the redundant data removal from the network traffic. By this manner, this offers a decentralized and distributed way for data processing. The IPFS-dependent cluster offers data copying between multiple peer nodes and thus enables off-chain storage model in a collaborative manner. This decreases the actual data hurdles stored in blockchain network thus improving the blockchain network scalability. In IPFS cluster, each peer is being identified through secret key or peer ID which could share information between them through mutual synchronization. The records are kept regarding the generated actual data by the network of IoT nodes. The two valuable resources that are employed from using IPFS are bandwidth and the energy consumption. The bandwidth is responsible for determining the stored data cost in IPFS at which only one byte of data devours one point of bandwidth. The energy consumption is responsible for determining the cost for running the access and shared resources that is computed depending on the time of CPU needed for running those access.

3.4. Attack Detection Using Meta-Hyperparameter Random Forest (RF) Classifier. For the purpose of classification, meta-hyperparameter random forest approach is employed at which the training trees were constructed and after that the mode of class output was attained. This type of supervised classification depends on decision taking tree models that divides the class which has high number of votes in each tree, and the classes are separated into feature subsets. This supervised learning technique will be stronger on comparing others. Initially, this is employed for ensuring high precision for both regression and identification actions. Next, in case more trees occur the trees overcrowding in design is not allowed and is having the capacity for handling larger and huge array of data. In due course, by the dependability of a huge information proportion, meta-hyperparameter Random Forest classifier is capable of handling the missing values. The classification algorithms once applied separately will produce accurate outcomes. The implementation of this approach may lead to IDS performance improvement. For differentiating the attack types, the classification process is employed and by this it is easy to compute the values of trust. The presented classifier technique is capable of generating randomly selected collection of learning the decision-making zones of dataset. For estimating the trusted value of classifier, the distance is estimated as follows:

$$\mathrm{TCV}(j,i) = \sqrt{\left(v_{n_{\mathrm{fea}}}(j,1) - v_{n_{\mathrm{fea}}}(i-1)\right)} + \left(v_{n_{\mathrm{fea}}}(j,1)\right) - \left(v_{n_{\mathrm{fea}}}(i,1)^2\right). \tag{3}$$

Since the prototypes are considered through the behavior of standard data, the characteristics that are irregular are thus computed using the following equation:

$$A_{n\_\mathrm{fea}} = \left[A_{n_{\mathrm{fea}}}\mathrm{TCV}\right]. \tag{4}$$

This in turn allows the presented classifier for assessing usual characteristics and to discriminate the qualities that are irregular. The data's confidence value is estimated as shown as follows:

$$V_{\mathrm{tv}} = \left(v_{n_{\mathrm{fea}}}\mathrm{TCV}\right), \tag{5}$$

Here, V_{tv} signifies the data trusted value. Based on the trusted value, then the authentic data is being recognized and for the attack classification the following expression is carried out:

$$\mathrm{Attack} = \sqrt{\sqrt{\left(F_{n_{\mathrm{fea}}}(j,1) - A_{n_{\mathrm{fea}}}(i-1)\right)} + \left(F_{n_{\mathrm{fea}}}(j,1) - \left(F_{n_{\mathrm{fea}}}(i,1)\right)^2\right.}. \tag{6}$$

Thus, the normal and abnormality of data is estimated and the attack is classified and is computed as a form of attack data and is signified as shown as follows:

$$v_A = \left(v_{n_{\text{fea}}} \text{type}\right). \tag{7}$$

Here, V_A denotes the type of attack in the data; based on the attack-type values, the type of attack is determined. Thus, the attack is detected and classified, and the blockchain logic with smart contract is applied for secured transaction purpose.

3.5. Smart Contract for Transaction Logic Execution. The creation of smart contract is made possible in blockchain by predefining the desired needs of transaction to be met. There were several inputs for starting the transaction in their own for exchanging crypto-currencies. With the utilization of smart contracts in the blockchain technology, each and every agreement is being validated, enforced, and signed in an automatic manner thus eradicating the needs of mediator by saving money and time. For instance, the voting system in election is also implemented based on the blockchain technology. The open service that are decentralized therefore replaces resilient parties, trusted parties, and the brittle address location with the peer-to-peer algorithmic markets that replaces ineffective monolithic services. The transaction ledger decentralized is employed in the Bitcoin, Ethereum system, and other blockchain networks. Those ledgers were employed for smart contract transaction that worth the dollar billion over peer-to-peer global networks. At this transaction, it is necessary for managing central system with other parties. The stored information at this ledger kinds could be accessed offline and are permanent.

A smart contract is the computer codes lines set which is stored in blockchain and is performed automatically once the party in network needs to execute smart contract. In this approach, smart contract is employed for the log agreements in immutable and serialized manner. The relevant events are managed and controlled thereby functioning as per the terms of other smart contracts.

The process starts with the beginning of user request to blockchain. After that, the members of network reverted back that the blockchain in turn stores the information of transaction and data in the shared distributed database once it was accepted and validated. The history of immutable transaction prevents the malicious users from performing destructive actions in the network system. This is obvious that the blockchain aids in enhancing entire system's ability thereby preventing most of the security threats through chaining, hashing, and ledger definition distribution. The issues of secured transaction or the events are improved already through employing public blockchain as the decentralized system due to the immutable data history. None can change them as everyone has the copy of this in their memory.

3.6. Blockchain Network and Data Aggregation Using PoW and Elgamal Approach. ElGamal cryptosystem is a cryptography approach that uses public and private key concepts to secure communication between two systems. It is an asymmetry algorithm that uses public and private keys to encrypt and decode data. This strategy is regarded to be very efficient when it comes to data transfer via a private or public networking, in addition to software security. The data is stored in server securely with the use of blockchain methodology and the data aggregation scheme. For data aggregation, Proof-of-Work (PoW) is employed. Essentially, PoW is the incentive-dependent consensus approach technique that needs entire participants to compere rewards over the cryptographic block recognition racing game. To compete the block generation of PoW, each miner should resolve computing intensive hashing problems. In detail, the valid solution for PoW needs querying cryptographic function exhaustively for the partial generated preimage from the candidate block. At last, the hash code of candidate block should satisfy predefined issues in the parameter h that is the one that are having fixed bit length as zeros. The major intention of consensus approach is to bring the entire nodes of agreement, i.e., to trust each other in the environment at which nodes do not trust one another. The entire transaction in new block is being validated and a new block is added afterwards to the blockchain mechanism.

The suggested blockchain-enabled Data Security approach sustains the file within the server at a high-level feature of security. The data handling logics from the server end with the norms of proper cryptosecurity use the logic of query parameterization for surfing the server. The level of accuracy for maintain the data in the server is improved highly. Algorithm 1 shows the handling of secured information and blockchain logic for transaction using Elgamal approach.

The data manipulation and prevention are significant for processing data thereby offering integrity and consistency. Several techniques were employed so far for the ensuring integrity of data such as data signature and encryption. However, the in-built feature of the blockchain methodology ensures data integrity. The blockchain's immutable nature aids in recognizing data tampering. A decentralized and distributed storage of data is built in blockchain for managing data on network in user's local device, thus for assuring that the chain is not get collapsed. If hacking attempt for block is carried then this could recognize them easily through digital ledger thereby locating variation among previous tests and thus rejects the mismatching one which is a malicious one. Since it is a decentralized system, everyone in the block must verify data which is to be stored, shared, and this could not be altered or else deleted. This makes the system a highly secured one and a robust one on comparing centralized system.

4. Performance Analysis

The performance assessment of suggested technique is analyzed and the attained outcomes are projected in this section.

The performance evaluation of attack detection classifier is analyzed in terms of accuracy, precision, recall, and *F*-score in (%). Table 1 provided shows the estimated values.

Table 1 is the illustration of comparative analysis of accuracy, precision, recall, and F-score values of the suggested classifier model. The outcomes attained infer that the

Input: Text Information (Data) or Document from user end (Plain text).
Output: Encrypted Cipher Blocks on Server End.
Step 1: gather plain text or the data from user end
Step 2: the string variables are generated termed Enc_Key and smart credential generated are assigned as
StringEnc_Key = Cred
Step 3: a byte variable is created for storing encrypted bytes, for instance: byte[100]_Bytes = Encoding_Unicode_GetBytes(Enc_Text)
Step 4: a new object is created for performing encryption depending on the procedure of advanced encryption by Rijndael process.
Rijndael_Encryptorenc = Rijndael_ Encryptor.Create
{
$\text{RFC}_{2898_{\text{DeriveBytes}}\text{DerivedBytes}}$ = new$\text{RFC}_{2898_{\text{DeriveBytes}}}$
(Enc_Key, newbyte[100] (0x49, 0x50, 0x51, . . . , 0xn)
}
Step 5: the key storage space is generated by means of derived bytes earlier I n the previous step
Step 6: the temporary encrypted data storage space is generated using derived bytes from third step and the generated key storage space by step 5
Encryptor_Key = Derived_Bytes.GetBytes(32)
Encryptor_Data = Derived_.GetBytes(16) + Encryptor_Key
Step 7: for storing cipher values, memory stream is created one by one for generating encrypted data storage space by step 6.
Step 8: the encrypted data is stored in the storage space in the format of bytes.
Step 9: Return encrypted text
Memory_Streamms = newMemory_Stream
Crypto_Stream{ms, Enc_Create_Encryptor, 𝕊
Crypto_Stream_Mode[Write]}
clear_Bytes; \\Clear the temporary cache
return EncryptedText;
Step 10: the query is inserted for generating the data in server end
Command_ObjectCmd = new Command_Object;
Cmd(″Insert Into Data_Table(File_ID, $\text{File}_{\text{data}}$, $\text{File}_{\text{Length}}$, Date_Time)Values(@FID, @FileName, @FileLength, @DT)″, Connection_String);
Cmd.Parameters.Add(Server_Parameter(″@FID″,))1;;
Cmd.Parameters.Add(Server_Parameter(″@FileData″, EncryptedText)); //refer Step–9
Cmd.Parameters.Add(Server_Parameter (″@FileLength″, EncryptedText.Length));
$\text{Cmd.Parameters.Add}(\text{Server}_{\text{Parameter}}(″@DT″, \text{Server.DateTime.Now}))$;
Step 11: the information is stored in server successfully

Algorithm 1: Handling secured information and blockchain logic for transaction using Elgamal approach

Table 1: Comparative analysis of accuracy, precision, recall, and *F*-score.

Machine learning techniques	Accuracy (%)	Precision (%)	Recall (%)	*F*-score (%)
Proposed model (meta-hyperparameter random forest)	99.57	98.82	97	98.39
DT-decision tree	93	98	94	97
RT-random tree	90	98	92	93
DTb-decision table	92	94	91	94
NB-Naive Bayes	91	98	90	94
BN-Bayesian network	90	98	98	95

suggested technique offers enhanced rate of performance metrics in terms of accuracy, precision, recall, and F-score values on comparing existing models for classification. Thus, the effective detection and classification of attack and their type are attained by means of the proposed scheme.

Figure 2 is the representation of comparative analysis made in terms of accuracy, precision, recall, and *F*-score values for the proposed and existing models. The results attained conclude that the recommended method offers improved rate of performance metrics like accuracy, precision, recall, and *F*-score values on comparing traditional classification models. Accordingly, the effective classification and detection of attack and their type are attained using projected system.

Table 2 shows the comparative analysis of encryption time for both blockchain-enabled models and without blockchain model. The proposed PoW with Elgamal blockchain approach is compared with the existing cryptographic techniques and the attained outcomes reveal that the use of blockchain will decrease the encryption time. Thus, the proposed technique has reduced rate of encryption time on comparing existing techniques.

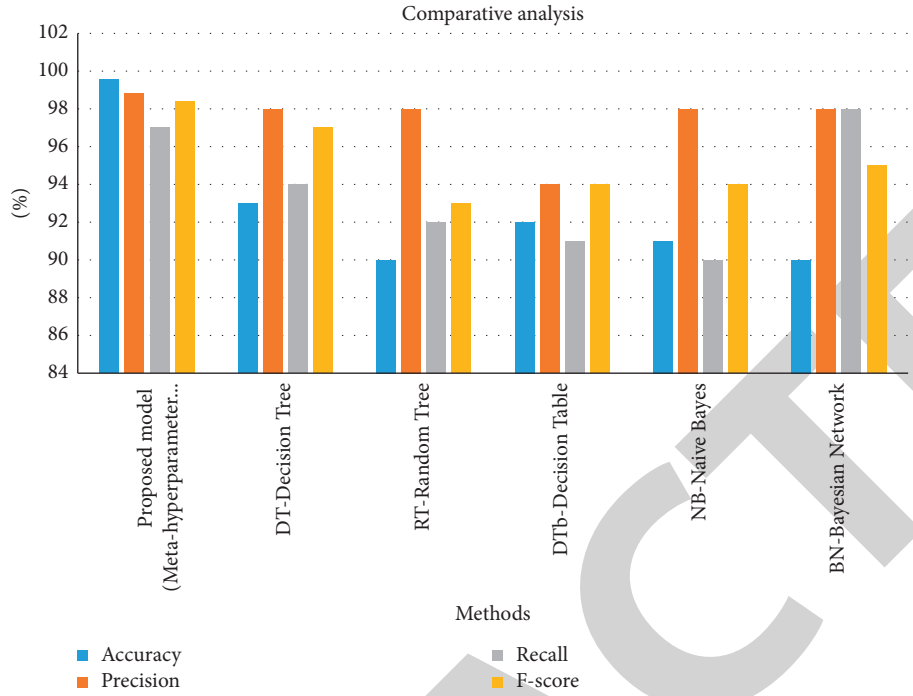

Figure 2: Comparative analysis of classifier performance to detect attack.

Table 2: Encryption time.

File size (KB)	Without blockchain (s)			With blockchain (s)
	Blow fish	RSA	AES	Proposed PoW with Elgamal-based blockchain
20	78	76	70	65
40	78	84	77	71
60	82	85	80	74
80	84	80	78	72
100	90	88	84	79

Figure 3 shows the graphical representation of encryption time comparison for both blockchain-enabled models and without blockchain model. The projected PoW with Elgamal blockchain approach is compared with the existing cryptographic techniques and the attained outcomes reveal that the use of blockchain will decrease the encryption time. Consequently, the proposed technique has reduced rate of encryption time on comparing existing techniques.

Table 3 illustrates the comparative evaluation of decryption time for both blockchain-enabled models and without blockchain model. The proposed PoW with Elgamal blockchain approach is compared with the existing decryption techniques and the outcomes attained expose that the use of blockchain will decrease the decryption time. Hence, the suggested method has decreased rate of decryption time on comparing prevailing methods.

Figure 4 signifies the graphical depiction of decryption time comparison for both blockchain-enabled models and without blockchain model. The projected PoW with Elgamal blockchain approach is compared with the existing decryption methods and the outcomes attained expose that the usage of blockchain will decrease the decryption time.

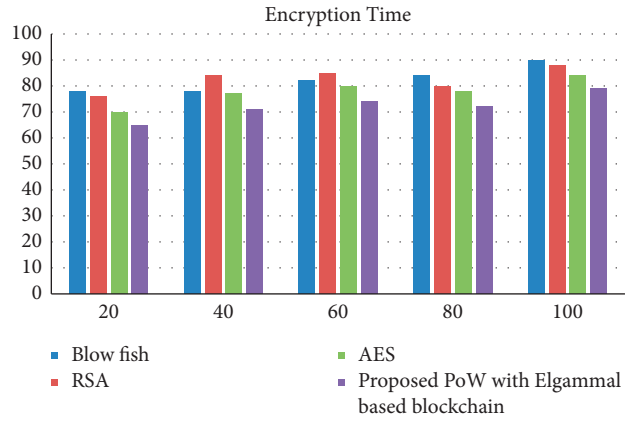

Figure 3: Comparative assessment of encryption time.

Accordingly, the proposed technique has reduced rate of decryption time than traditional methods.

Table 4 shows the comparative estimation of execution time for both blockchain-enabled models and without blockchain model. The presented PoW with Elgamal

Table 3: Decryption time comparison.

File size (KB)	Without blockchain (s)			With blockchain (s)
	Blowfish	RSA	AES	Proposed PoW with Elgamal-based blockchain
20	0.99	1.05	1.5	0.89
40	0.88	0.79	1.1	0.77
60	1.54	1.77	0.8	0.73
80	1.57	0.99	0.8	0.76
100	0.96	1.02	1.1	0.83

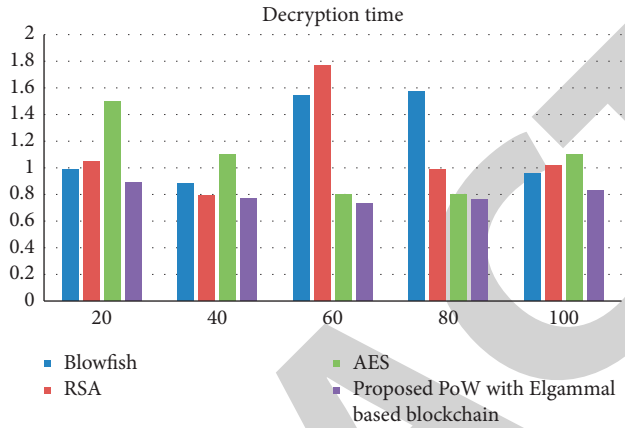

Figure 4: Comparison of decryption time.

Table 4: Comparative estimation of execution time.

File size (KB)	Without blockchain (s)			With blockchain (s)
	Blowfish	RSA	AES	Proposed PoW with Elgamal-based blockchain
20	5.55	4.57	4.7	3.08
40	3.66	4.05	4	3.16
60	3.04	2.99	3.3	2.11
80	3.78	3.99	3.3	2.98
100	4.22	3.05	3.8	2.84

blockchain approach is compared with the existing cryptographic techniques and the outcomes attained reveal that the use of blockchain will decrease the execution time. Henceforth, the suggested method has decreased rate of execution time on comparing state-of-the-art methods.

Figure 5 symbolizes the graphical depiction of execution time comparison for both blockchain-enabled models and without blockchain model. The projected PoW with Elgamal blockchain approach is compared with the existing decryption methods and the outcomes attained expose that the usage of blockchain will decrease the execution time. Accordingly, the proposed technique has reduced rate of execution time than existing techniques.

The space complexity of the proposed system is estimated to show the advantage of them on overcoming space complexity issues. The estimated result of space complexity for proposed technique is compared with the existing techniques to show the effectiveness of the proposed

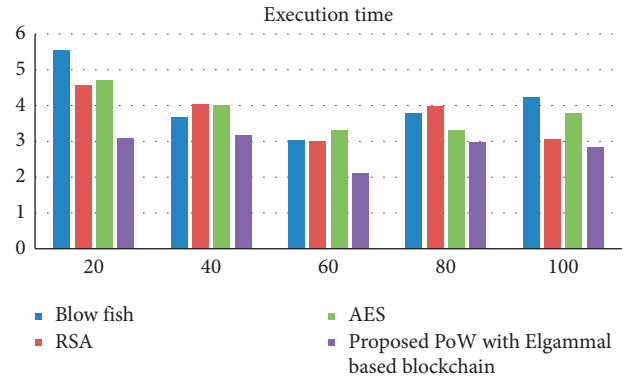

Figure 5: Comparison of execution time.

strategy. The attained outcomes are projected in Table 5 and it infers that the proposed system has consumed less storage space on comparing other existing techniques. Hence, the proposed model is said to be effectual than others.

Table 5: Comparative analysis of space complexity.

Algorithms	Plaintext before encryption (kb)	Ciphertext Kb	Plain text after encryption (kb)
AES	130	517	130
DES	130	188	130
TDES	130	360	130
Blowfish	130	544	130
RC5	130	517	130
Serpent	130	480	130
LW cryptography	130	130	130
Proposed PoW-based Elgamal encryption	128	128	128

5. Discussion

The outcomes attained from Table 1 infers that the suggested technique offers enhanced rate of performance metrics in terms of accuracy, precision, recall, and F-score values on comparing existing models for classification. Thus, the effective detection and classification of attack and their type are attained by means of the proposed scheme. The results attained from Figure 2 conclude that the recommended method offers improved rate of performance metrics like accuracy, precision, recall, and F-score values on comparing traditional classification models. Accordingly, the effective classification and detection of attack and their type are attained using projected system.

The proposed PoW with Elgamal blockchain approach is compared with the existing cryptographic techniques and the attained outcomes from Table 2 reveal that the use of blockchain will decrease the encryption time. Thus, the proposed technique has reduced rate of encryption time on comparing existing techniques. The projected PoW with Elgamal blockchain approach is compared with the existing cryptographic techniques and the attained outcomes from Figure 3 reveal that the use of blockchain will decrease the encryption time. Consequently, the proposed technique has reduced rate of encryption time on comparing existing techniques. In Table 3, the proposed PoW with Elgamal blockchain approach is compared with the existing decryption techniques and the outcomes attained expose that the use of blockchain will decrease the decryption time. Hence, the suggested method has decreased rate of decryption time on comparing prevailing methods.

In Figure 4, the projected PoW with Elgamal blockchain approach is compared with the existing decryption methods and the outcomes attained expose that the usage of blockchain will decrease the decryption time. Accordingly, the proposed technique has reduced rate of decryption time than traditional methods.

In Table 4, the presented PoW with Elgamal blockchain approach is compared with the existing cryptographic techniques and the outcomes attained reveal that the use of blockchain will decrease the execution time. Henceforth, the suggested method has decreased rate of execution time on comparing state-of-the-art methods. Figure 5 offers comparison of projected PoW with Elgamal blockchain approach scheme with the existing decryption methods and the outcomes attained expose that the usage of blockchain will decrease the execution time. Accordingly, the proposed technique has reduced rate of execution time than existing techniques. Table 5 infers that the proposed system has consumed less storage space on comparing other existing techniques. Hence, the proposed model is said to be effectual than others.

6. Conclusion

A decentralized blockchain scheme with attack detection is presented in this approach. The suggested detection scheme consists of three stages like traffic processing stage, intrusion detection stage, and the transaction handling stage. This technique focuses on presenting decentralized consensus blockchain and IPFS-enabled data aggregation for effective classification and data storage. The attack was detected with the use of MHP-RF classifier. Once the attack is detected, the transaction information was to be stored in server firmly through smart contract using blockchain system. The stage of transaction handling classifies the transaction type as normal or abnormal one. The blockchain technique uses PoW-enabled scheme integrated with Elgamal-based data aggregation. Consequently, the system security was enhanced and the intrusion was significantly prevented. The performance analysis of the system was assessed in terms of accuracy, precision, recall, F-score, encryption time, decryption time, execution time, and space complexity. The outcomes attained were related with traditional approaches to prove the efficiency of projected stratagem. The outcomes reveal that the suggested technique was effective in terms of time consumption, classifier performance, and in overcoming space complexity issues. In future, this work is extended by presenting consenses blockchain mechanism with the use of blockchain network with Ethereum blockchain-based proof of authority for data aggregation to add transaction. Additionally, to improve security for security, a homomorphic crypto-scheme is used.s

Data Availability

The data used to support the findings of the study can be obtained from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] Y. E. Oktian, E. N. Witanto, and S.-G. J. I. Lee, "A conceptual architecture in decentralizing computing, storage, and networking aspect of IoT infrastructure," *MDPI*, vol. 2, no. 2, pp. 205–221, 2021.

[2] M. Yang, P. Kumar, J. Bhola, and M. Shabaz, "Development of image recognition software based on artificial intelligence algorithm for the efficient sorting of apple fruit," *International Journal of System Assurance Engineering and Management*, vol. 13, pp. 322–330, 2022.

[3] U. Iqbal and A. Hussain Mir, "Secure and Practical Access Control Mechanism for WSN with Node Privacy," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, 2020.

[4] V. Le, "Improving Security and Performance of Distributed IPFS-Based Web Applications with Blockchain," in *Proceedings of the International Conference on Advances in Cyber Security*, ACes, Penang, Malaysia, August 2021.

[5] R. K. Garg, J. Bhola, and S. K. Soni, "Healthcare monitoring of mountaineers by low power wireless sensor networks," *Informatics in Medicine Unlocked*, vol. 27, Article ID 100775, 2021.

[6] B. Prasanalakshmi, K. Murugan, K. Srinivasan, S. Shridevi, S. Shamsudheen, and Yu-C. Hu, "Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography," *The Journal of Supercomputing*, vol. 78, no. 1, pp. 361–378, 2022.

[7] T. K. Lohani, M. T. Ayana, A. K. Mohammed, M. Shabaz, G. Dhiman, and V. Jagota, "A comprehensive approach of hydrological issues related to ground water using GIS in the Hindu holy city of Gaya, India," *World Journal of Engineering*, p. 6, 2021.

[8] H. Gao, Z. Ma, S. Luo, Y. Xu, Z. J. W. C. Wu, and M. Computing, "BSSPD: a blockchain-based security sharing scheme for personal data with fine-Grained Access Control," *Privacy Protection and Incentive for AI-Driven IoT*, vol. 2021, Article ID 6658920, 1 page, 2021.

[9] U. Iqbal and A. H. Mir, "Efficient and dynamic access control mechanism for secure data acquisition in IoT environment," *International Journal of Computing and Digital Systems*, vol. 10, no. 1, pp. 9–28, 2021.

[10] V. Jagota, M. Luthra, J. Bhola, A. Sharma, and M. Shabaz, "A secure energy-aware game theory (SEGaT) mechanism for coordination in WSANs," *International Journal of Swarm Intelligence Research*, vol. 13, no. 2, pp. 1–16, 2022.

[11] K. Shuaib, J. Abdella, F. Sallabi, M. A. J. J. o. K. S. U.-C. Serhani, and I. Sciences, "Secure Decentralized Electronic Health Records Sharing System Based on Blockchains," *Journal of King Saud University-Computer and Information Sciences*, 2021, In press.

[12] M. Shabaz and A. Kumar, "SA sorting: a novel sorting technique for large-scale data," *Journal of Computer Networks and Communications*, vol. 2019, Article ID 3027578, 7 pages, 2019.

[13] A. Mehbodniya, J. L. Webber, R. Neware, F. Arslan, R. V. Pamba, and M. Shabaz, "Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data," *Expert Systems*, 2022.

[14] A. Kumari, S. J. M. T. Tanwar, and Applications, "A secure data analytics scheme for multimedia communication in a decentralized smart grid," *Multimedia Tools and Applications*, pp. 1–26, 2021.

[15] Q. Wei, B. Li, W. Chang, Z. Jia, Z. Shen, and Z. J. A. P. A. Shao, "A Survey of Blockchain Data Management Systems," 2021, https://arxiv.org/abs/2111.13683.

[16] E. Guo, V. Jagota, M. E. Makhatha, and P. Kumar, "Study on fault identification of mechanical dynamic nonlinear transmission system," *Nonlinear Engineering*, vol. 10, no. 1, pp. 518–525, 2021.

[17] S. Saralch, V. Jagota, D. Pathak, and V. Singh, "Response surface methodology-based analysis of the impact of nanoclay addition on the wear resistance of polypropylene," *The European Physical Journal - Applied Physics*, vol. 86, Article ID 10401, 2019.

[18] Y. Ba, "A Blockchain-Based CP-ABE Scheme with Partially Hidden Access Structures," *Security and Privacy for Edge-Assisted Internet of Things*, vol. 2021, Article ID 4132597, 16 pages, 2021.

[19] J. He, D. Zheng, R. Guo, Y. Chen, K. Li, and X. J. I. J. o. N. S. Tao, "Efficient identity-based proxy Re-encryption scheme in blockchain-assisted decentralized storage system," *International Journal of Network Security*, vol. 23, no. 5, pp. 776–790, 2021.

[20] H. Li, D. Han, and M. J. M. I. S. Tang, *Logisticschain: A Blockchain-Based Secure Storage Scheme for Logistics Data*, vol. 2021, Article ID 8840399, 15 pages, 2021.

[21] J. Xu, K. Xue, S. Li et al., "Healthchain: a blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[22] S. Routray and R. Ganiga, "Secure storage of electronic medical records (EMR) on interplanetary file system (IPFS) using cloud storage and blockchain ecosystem," in *Proceedings of the 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1–9, IEEE, Erode, India, September 2021.

[23] M. Qi, "A blockchain-enabled federated learning model for privacy preservation: system design," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 473–489, Springer, New York, NY, USA, November 2021.

[24] A. Sadiq, N. Javaid, O. Samuel, A. Khalid, N. Haider, and M. Imran, "Efficient data trading and storage in Internet of vehicles using consortium blockchain," in *Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 2143–2148, IEEE, Limassol, Cyprus, June 2020.

[25] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. J. I. A. Muhammad, "Secure and provenance enhanced Internet of health things framework: a blockchain managed federated learning approach," *IEEE Access*, vol. 8, Article ID 205071, 2020.

[26] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, R. J. S. Amin, and C. Networks, "Blockchain-based internet of things and industrial iot: A comprehensive survey," *Blockchain for Systems Management and Cybersecurity*, vol. 2021, Article ID 7142048, 21 pages, 2021.

[27] A. U. Khan, "Enhanced decentralized management of patient-driven interoperability based on blockchain," in *Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 815–827, Springer, New York, NY, USA, June 2019.

[28] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. J. I. I. o. T. J. Seneviratne, "BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain," 2021, https://arxiv.org/pdf/2109.14295.pdf.

[29] T. Cai, W. Chen, and Y. Yu, "Bcsolid: a blockchain-based decentralized data storage and authentication scheme for

solid," in *Proceedings of the International Conference on Blockchain and Trustworthy Systems*, pp. 676–689, Springer, New York, NY, USA, May 2019.

[30] A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, and R. J. I. A. Jayaraman, "Blockchain-based multi-party authorization for accessing IPFS encrypted data," *IEEE Access*, vol. 8, Article ID 196813, 2020.

[31] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. J. I. T. o. I. T. S. Hassan, "A Privacy-Preserving-Based Secure Framework Using Blockchain-Enabled Deep-Learning in Cooperative Intelligent Transport System," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[32] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, and N. J. I. T. o. I. T. S. Kumar, "P2SF-IoV: A Privacy-Preservation-Based Secured Framework for Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[33] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. J. I. I. o. T. J. Hassan, "BDTwin: An Integrated Framework for Enhancing Security and Privacy in Cybertwin-Driven Automotive Industrial Internet of Things," *IEEE Internet of Things Journal*, 2021.

[34] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. J. I. T. o. I. T. S. Hassan, "DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[35] P. Kumar, R. Kumar, G. P. Gupta, R. J. I. T. o. G. C. Tripathi, and Networking, "BDEdge: Blockchain and Deep-Learning for Secure Edge-Envisioned Green CAVs," *IEEE Transactions on Green Communications and Networking*, 2022.

[36] P. Kumar, G. P. Gupta, R. J. A. C. Tripathi, and C. Sciences, "Design of anomaly-based intrusion detection system using fog computing for IoT network," *Automatic Control and Computer Sciences*, vol. 55, no. 2, pp. 137–147, 2021.