Security Concerns at Different Phases of Networks through Blockchain Technology

Thesis submitted in fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE AND ENGINNERING

BY

ANJU DEVI

Department of Computer Science and Engineering
Jaypee University of Information Technology
WAKNAGHAT, DISTRICT SOLAN-173234, H.P., INDIA

30 December, 2023

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislative vide Act No. 14 of 2002)
Waknaghat, P.O. Dumehar Bani, Kandaghat, Distt. Solan – 173234 (H.P.) INDIA
Website: www.juit.ac.in
Phone No. (91) 07192-257999 (30 Lines)
Fax: (91) 01792 245362

Declaration

I hereby declare that the work reported in the Ph.D. thesis entitled “Security Concerns at Different Phases of Networks through Blockchain Technology” submitted at Jaypee University of Information Technology, Waknaghat, India is an authentic record of my work carried out under the supervision of Dr. Amit Kumar, Dr. Geetanjali and Dr. Hemraj Saini. I have not submitted this work elsewhere for any other degree or diploma. I am fully responsible for the contents of my Ph.D. Theses.

Signature:

____

Date:

____

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislative vide Act No. 14 of 2002)
Waknaghat, P.O. Dumehar Bani, Kandaghat, Distt. Solan – 173234 (H.P.) INDIA
Website: www.juit.ac.in
Phone No. (91) 07192-257999 (30 Lines)
Fax: (91) 01792 245362

Certificate

This is to certify that the work reported in the Ph.D. thesis entitled " Security Concerns at Different Phases of Networks through Blockchain Technology” submitted by Anju Devi at Jaypee University of Information Technology, is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

Signature of Supervisor-1:	Signature of External Supervisor- 1:	Signature of External Supervisor- 2:
Dr. Amit Kumar	Dr. Geetanjali	Dr. Hemraj Saini

Dedicated to My Beloved Master & Family. . .

Abstract

A blockchain is a peer-to-peer, distributed, and decentralized network that generates a distributed ledger that provides immutability, transparency, and traceability. Each node has a copy of the distributed ledger in which data is formed as a block, and each block is connected to the preceding block in the chain. A distributed ledger is where data is recorded, and maintained, and endlessly growing transactions are recorded in an ordered manner across multiple computers. Many researchers have applied many approaches but still, there is a scope for improvement to achieve better security, privacy, transparency, efficiency, reliability, throughput, and scalability in different phases in an untrusted environment. Blockchain is used for the security purposes of devices, data, and users with different applications such as vehicles, IoT, industrial, healthcare, voting, and digital transactions.

The presence of malicious nodes can degrade the performance of the system, and the validation of the block that corresponds to the selected miners allows it to be maliciously put onto the blockchain. So, to eliminate these issues used the incentive mechanisms that are a combination of DPSO and M-ITA algorithms to verify miners and blocks using blockchain technology in vehicular networks. The vehicles on the road side units share a lot of information through communication that ensures driver safety and service quality. The DPSO algorithm validates the block whereas the MITA algorithm to check the miner's is trustworthiness. The decentralized approach of this work increased the trust and utility of miner's upto 65% and 20% respectively whereas the compromised miners are reduced upto 44%.

Many researchers have proposed encryption schemes to protect data, but they have also led to inadequacies in most of the proposed approaches like data privacy, centralize control, security, corrupt, processing time. Encryption technology requires more time to manage keys and encrypt and decrypt data, which can result in increased vulnerability to eavesdropping and man-in-the-middle attacks.

The CP-ABE blockchain-based encryption technique is proposed to secure the data in untrusted environment by employing IPFS cloud storage to minimize user effort. The decentralized approach of this work reduces the encryption and decryption time by 23% and 37% respectively when compared with the existing approach. Furthermore, a decentralized IPFS cloud server is expected to guarantee integrity, authenticity, and confidentiality.

To enhance the system's throughput, a user authentication mechanism that combines PKI and ECC algorithms is being implemented, improves the user’s authenticity, and reduced the latency using blockchain technology in industrial applications. PKI gives the digital certificate to the authenticated users only for a limited period after that gives permission to access the industrial applications. ECC used to distribute and manage the keys because of centralized authority can be overwhelmed. Every time checks the authentication of users if not authorized then revokes the certificate immediately and stops the interface with IIoTs. The performance of the proposed approach is better when compared to the existing approach that increased the systems throughput and users authenticity upto 73% and 93% respectively, and reduced the latency upto 6.77% in industrial applications.

Acknowledgements

First of all, I thank the giant God who took me out of every difficulty and helped me to finish this thesis work. It is my privilege to take the prospect to thank all the individuals who were with me to accomplish this target. A number of experiences have been encountered in JUIT and I would like to thank those dozens of remarkable individuals. First, and for most, I would like to thank head of the department Prof. (Dr) Vivek Sehgal and Dr. Amit Kumar my supervisor, under whose guidance, I have completed my Ph.D. work. He always treated me like his daughter. I always appreciated favoritism as well as I also never missed the admonishment of a father in his presence. He always makes me comfortable to talk. His presence in every departmental presentation gave moral support to me. Ever since he has supported me not only in research but also offers potential suggestions and motivation throughout the rough road of finishing this thesis. Words cannot express to thank him for spending lots of hours to re-evaluate my reports and thesis. I could not complete this work without his enormous support in many ways.

I am also thankful to Dr. Geetanjali and Dr. Hemraj Saini my external supervisor, for her/his encouragement and support during this Ph.D. journey. I remember, he always used to say that "I taught you to do small things carefully in a systematic way". Indirectly he always encourages me to move ahead. He tried to make me a hardworking person. When the experimental results were not satisfactory then instead of scolding me, he always appreciated my efforts. He made me understand to have patience during experiment results and taught me to do constant hard work to achieve the objectives of the research. His endless efforts and attention toward my work pushed me ahead to finish this research work. No expression of thanks will be sufficient for his enormous patience while reading my thesis. I have learned to do work systematically from him. During the most challenging time when I was starting to write my thesis, he gave me the freedom to move on and provided constant help to complete my thesis work and made this a successful speculation. I owe my sincere thanks to the worthy administration department of JUIT, Prof (Dr) Rajendra Kumar Sharma (Vice-Chancellor), Prof (Dr) Ashok Kumar Gupta (Dean A & R), and Maj Gen Rakesh Bassi (Retd.) (Registrar) provides the laboratory facility as well as other necessary permissions during Ph.D research work. I want to thank the committee members, Dr. Nancy Singla, Dr. Nishant Sharma and Dr. Rakesh Bajaj, whose comments and feedback helped me a lot to improve my research work. I would like to thank all the faculty members of

Computer Science and Engineering for their valuable support and suggestions throughout my work.

Special Acknowledgement: I want to pay heartfelt thanks to my parents, my daughter Ruhani and a special thank to my husband Rajan Sangwan for their continual guidance and help, whenever I needed for their supports, prayers, and all-around support. At last, I would like to thank beloved God for showering blessings and holding me in every difficult situation. I experience your grace and guidance every moment of my life. You are the one who is always with me in every good and bad experience of my life. Ever since I have no words to thank you for whatever you have done for me. Thanks for guiding and being with me always. Thank you, lord. . . Anju Devi

List of Abbreviations

ABI	Application Binary Interface
BARS	Blockchain Anonymous Reputation System
BBARS	Blockchain Based Anonymous Rewarding scheme
BCH	Bitcoin Cash
BTEV	Blockchain integrated Traffic Event Validation
CA	Certificate Authority
CA	Centralized Authority
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
DDPoS	Downgrade Delegated Proof of Stake
DHT	Distributed Hash Table
DMCDS	Distributed Miners Connected Dominated Set
DoS	Denial of Service
DPS	Data Preservation System
DPSO	Discrete Particle Swarm Optimization
DR	Demand Response
EC-ACS	Elliptical Curve Certificateless Aggregate Cryptography Signature scheme
ECC	Elliptic Curve Cryptography
HIBC	Hierarchy Identity Based Cryptography
IBC	Identity based Cryptography
ICN	Information-Centric Networking
IIoT	Industrial Internet of Things
IoTs	Internet of Things
IoV	Internet of Vehicles
IPFS	InterPlanetary File System
LTC	Litecoin
MA-ABS	Multi-authority attribute based signature
M-ITA	Multi-Interactive Two-Stage Auction
PKI	Public key Infrastructure
PoPUF	Proof of Physical Unclonable Functions

PoS	Proof of Stake
PoW	Proof of Work
RA	Registered Authority
RSU	Road Side Units
SDTE	Secure Data Trading Ecosystem
UAN	Unmanned Aerial Vehicles
VANETs	Vehicular Networks

List of Figures

List of Tables

Table of Contents

CHAPTER 1

INTRODUCTION

1.1 Introduction

The Internet helps people with social and economic development and provides information instantly that drastically reduces human efforts. The centralized authority is commonly used to manage the data on the internet, which may lead to numerous issues including data security. The centralized network is a single point of failure, offers limited speed and no fault-tolerant setup, and even the data may lost due to any hardware failure occurs. Nowadays, the Internet of Things (IoT) is popular that developed by Ashton in 1999 [1], which communicates with many devices over the Internet to track, perceive, and monitor information entering the environment without the need of human interaction. The network is highly concerned with security problems including privacy and traceability because all information is maintained and controlled by centralized authorities.

Therefore, Satoshi Nakamoto introduced the bitcoin in a decentralized network in 2008 [2] using the blockchain application. A blockchain is a peer-to-peer, distributed and decentralized network and generates a distributed ledger that provides immutability, transparency, and traceability. Each node is having a copy of the distributed ledger in which data is formed as a block, and each block is connected to the preceding block in the chain. A distributed ledger is a place where data is recorded, maintained, and endlessly growing transactions are recorded in an ordered manner across multiple computers. The new block is always broadcasted into the entire network so that all nodes in the network will be able to update their ledger with current information, as shown in Figure 1.1. The broadcasted block is always validated by the selected miners and stored the block in the blockchain, and then the block is broadcasted in the network.

Blockchain [3] stores and tracks the record of every transaction where assets can be tangible (car, land, house, shop) or intangible (copyright, patents, intellectual property). It is used to eliminate risks like trustworthiness, security, and reduce the waiting time. It maintains the record of every transaction in the network that can be accessed later by any authorized users.

The first block is known as the genesis block because it is not linked with the preceding hash block. Each block contains transactions, a timestamp, a nonce, a difficulty target that is used for cryptographic operations, and a hash of the previous and current block, as shown in Figure 1.2.

The timestamp shows the time when the block is created, and miners use a nonce, which is a random value, for authentication purposes, and a difficulty target for miners is used to mine a certain block. A hash function takes an arbitrary length of the input string, such as numeric values, alphabets, and audio and video files that transforms into a predetermined length of output. The output length of a hash value depends on the hashing algorithm that is used such as SHA-256 and SHA-512 generate 256 and 512 bits as output respectively.

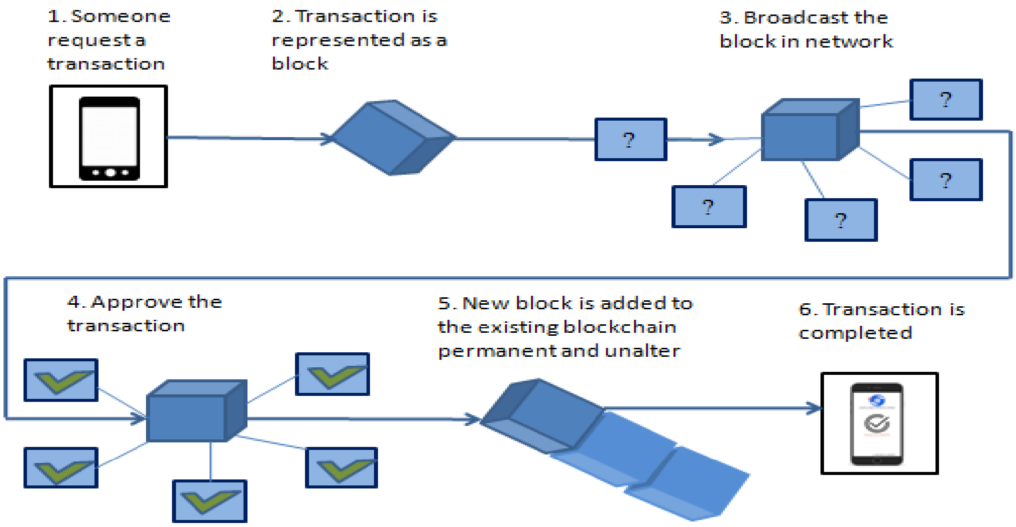

1. Someone request a transaction
2. Transaction is represented as a block
3. Broadcast the block in network
?
?
?
?
?
4. Approve the transaction
5. New block is added to the existing blockchain permanent and unalter
6. Transaction is completed

Figure 1.1: Structure of the Blockchain

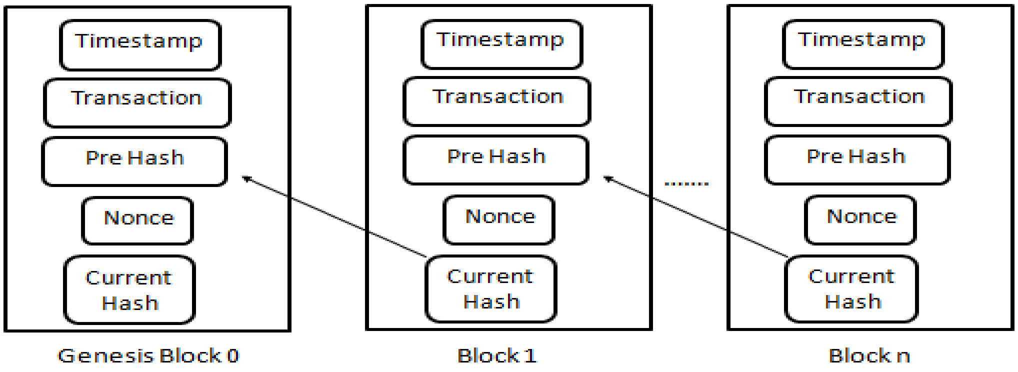


Figure 1.2: How to Blockchain Technology works

Blockchain Benefits:

- It has a decentralized structure, which means that no individual can operate or administer the system.

- Unlike other databases, blockchain stores data in blocks that are connected using a cryptographic hash.
- Transactions are efficient, private, and secure.
- The blockchain ledger has an immutable characteristic.
- Through a distributed ledger, the network reduces the agreement time and quickly stores transactions on the blockchain.

1.2 Different kinds of Blockchain

There are several kinds of blockchain networks such as private, public, hybrid, and consortium blockchain as illustrated in Figure 1.3.

1.2.1 Private Blockchain

A permissioned blockchain is another name for this type of blockchain that can join the networks after receiving permission from an authorized party such as Hyperledger. In addition, it has excellent throughput, trust, speed, and tight security compared to the public blockchain. Hyperledger is introduced by IBM for time-related purposes that are generally used in industries for making smart contracts and non-financial purposes.

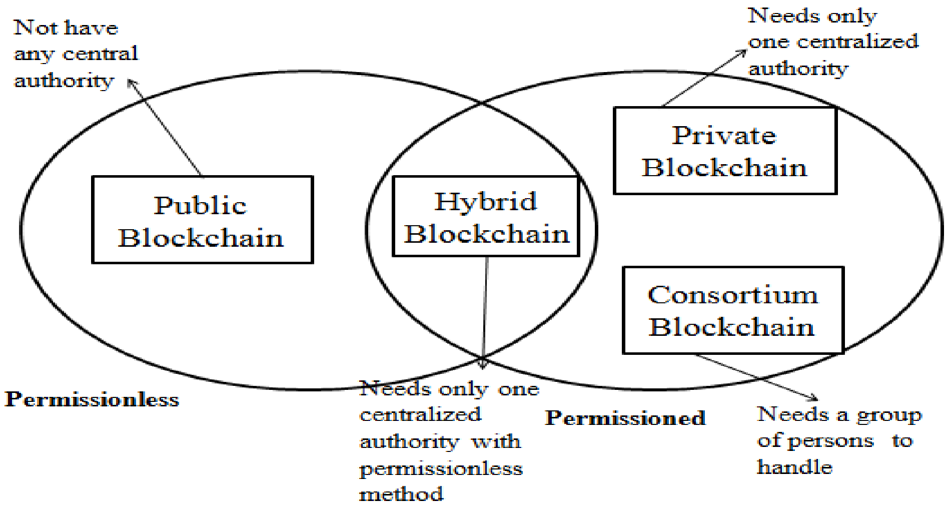


Figure 1.3: Different Types of Blockchain

1.2.2 Public Blockchain

This kind of blockchain is also known as a permissionless blockchain which allows anybody to join the network without taking any permission from third party such as Bitcoin and Litecoin.

Bitcoin is the first and largest cryptocurrency on the blockchain with a marketplace that eliminates the double-spending problems within seconds can send or receive the currency over the world. It is broadly used in the real world, and some countries accept bitcoin as payment. Litecoin is similar to Bitcoin but four times faster than Bitcoin and its name is LTC cryptocurrency, and it has lower transaction fees compared to Bitcoin. It takes only two minutes to go through all the transactions. There is a limited supply in bitcoin of 21 million, while in Litecoin it is 84 million.

1.2.3 Hybrid Blockchain

Combination of private and public blockchain, it needs a single authority to handle permissionless transactions like ripple. Thus, we can use the public blockchain to build a network of distributed ledgers that can be accessed anywhere in the world, while a private blockchain controls the adjustments in the distributed ledger. Ripple takes low transaction costs, less energy consumption, a little bit of time for confirmation, and reliability.

1.2.4 Consortium Blockchain

A private blockchain serves a single person, whereas a consortium blockchain serves a group of people from various organizations. It is perfect for organizations where several participants take the permission. Ethereum is used for making smart contracts for financial and non-financial purposes.

1.3 Applications of Blockchain

Blockchain has a wide range of applications such as healthcare, cryptocurrency, insurance, IoTs, Evoting, smart contracts, data storage, and supply chain, as shown in Figure 1.4.

1. Smart contract

With the advent of Blockchain technology, human lives have completely changed, and less effort is required. A Smart Contract [4] is a blockchain application in which we set conditions in the code and maintain trust between the parties because everything is transparent. Wherever, traditional contracts based on paper have a high possibility of errors, less security, and do not establish complete trust between parties.

2 Management of records

Almost every individual's data are recorded in paper formed by the government, including their marital status, birth certificates, and death certificates, among others. To make any changes in the data, one must physically go to the government office, which is frustrating, time-consuming, costly, and avoidable. By using blockchain technology, all this type of data keeps secure that can never be altered.

3 Industries

The industry is also a blockchain application where data can be shared, even unused data at a marketplace level. Many of the companies used the Blockchain technology to secure their data and trustworthiness that increased the assessment of industries and enterprises [5], [6].

4 Cryptocurrency

Blockchain uses the first bitcoin technology that eliminates the fund's problem, which helps to transfer digital currency [7] from one person to another within a few seconds that is time-consuming, fully secure, and decentralized all over the world without extra charges.

5 E-voting

Voting is a blockchain application [8] in which we can cast our votes directly through the blockchain if the identity of a person is built on the blockchain. Only qualified voters may vote, and no one is able to vote twice due to its characteristics such as tamper-proof, transparency, and traceability. Hence, decreases the risks of fraud voter with lower cost of the operating process.

6 Healthcare/ Medical

Patient's data will be safe with secret signatures when blockchain technology is adopted in the medical industry [9]. And only the certified individual can access the data, which is in encrypted form that stored on the blockchain.

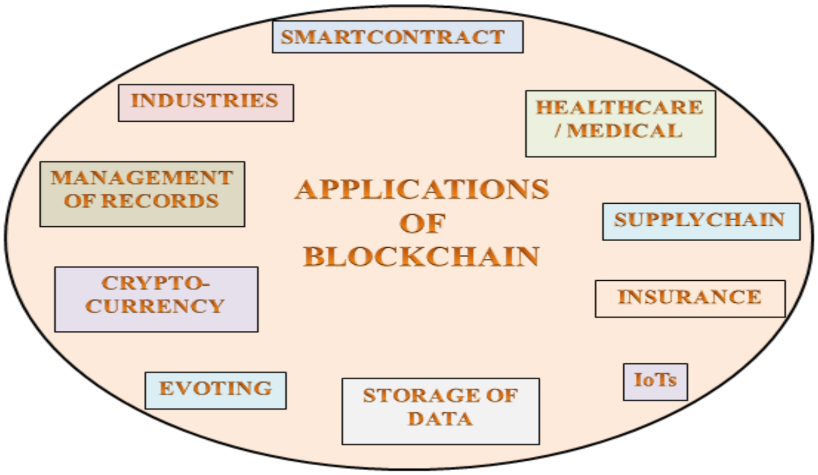


Figure 1.4: Applications of Blockchain

7. IoTs

After the arrival of the Internet of Things [10–11], the life of a human has changed completely. As soon as it comes to the network, it starts working automatically. Smart devices communicate wirelessly with each other that send and receive data across environments.

8 Supply Chain

The supplier side uses the blockchain network to verify the product's originality that is received from the customer side. So, it creates a good, trustworthy bond between the customer and the supplier so there is no chance of fraud. Several approaches have already been used, such as IBM, blockverify, and provenance in the supply chain for product authentication.

9 Insurance

Insurance [12] firms also used blockchain technology, which is policyholder for transaction purposes such as registering insurance policies and other insurance activities between the companies.

10 Data Storage

The blockchain technology used for data storage, it provides data with security, privacy and integrity due to its features. All data records are kept in a decentralized way, which decreases the possibility of data tampering, and hacking.

1.4 Motivation

The blockchain is a distributed peer-to-peer network that is considered for future applications because it provides security, trustworthiness, traceability [13], and immutable [14]. In real life, a huge amount of data is shared all over the globe which generates a lot of issues in the management of the whole network. Several studies [15–16] have attempted to reduce system complexity, increase scalability, and ensure immutability and there are great chances of breaching security and leakage of user privacy.

Several hindrances arise from devices such as denial of service attacks, compromised miners, system throughput, trustworthiness, and so forth. Therefore, the security of the data should be up to mark by using secure encryption/decryption algorithms during transmission. These techniques make it almost impossible for intruders to decrypt the secret message without a secret key. Moreover, less intensive computational complex encryption/decryption algorithms make the whole system efficient and faster, and reduce the risk of eavesdropping. Therefore, authors have used blockchain to provide privacy, integrity, and trustworthiness with different computationally complex techniques [17–18].

In other research, it is mentioned that a malicious node may upload malicious data to the blockchain network, due to which the performance [19] of the system decreases, and some researchers proposed user authentication mechanisms [20–22] for the protection of data by making a more complex system. An unauthenticated user can expose data and disturb the network's performance significantly. There are a numerous of issues with different levels are mentioned as below:

- Identification of malicious nodes is hard to distinguish.
- Lack of system throughput, authentication, scalability and accuracy of users
- Centralized authority is used to manage and control the sensitive information.
- Higher cost and time is involved in data encryption and decryption in decentralized environment.
- Centralized cloud storage is used.
- There need a blockchain-enable approach to prevent collisions between miners, DoS, eavesdropping attacks, Sybil attack, DDoS attack, and block verification.

Consequently, enhancing the security of one parameter can have significant implications on other parameters, including throughput, accuracy, delay time, and trust. Therefore, the system must be secured in order to meet all other performance requirements. Mainly, security is provided at the user, device, and data levels to preserve the privacy and security of the data across the transmission. So, the motivation of this thesis is to solve above issues with the help of the following approaches:

1. First, the security in device phase on vehicle applications by using blockchain based incentive mechanism, where the device comes and contact with roadside units (RSU), and then it starts communication with other vehicles. The privacy of the device needs to be protected because if miners are compromised or malicious then it may leads to many incidences at road.
2. Second, the security in data phase is achieved by using the encryption and InterPlanetary File System (IPFS) cloud server for outsourced data, which secures the transmitted and stored data in blockchain technology.
3. Finally, secure the user phase in the industrial applications that is used for the authentication of users during the data transfer in blockchain technology.

The above given methods improved the security in three phases of network with different applications which helps to reduce the delay time, improve the system throughput, reduce DoS (Denial of Service) attacks, improve the miner's utility, increases the detection rate, trust and quality of the devices. The results have been improved through more than one parameter at each phase that is investigation through experiments. Our work is accurate and proven through the problems analyzed compared with existing approaches.

1.5 Research Objectives

The main goal of the thesis is to provide security at all three phases of networks as an incentive mechanism, a data encryption algorithm with IPFS storage, and a user authentication methods are proposed.

1.5.1 An incentive mechanism to verify miners and blocks in Vehicle Networks

A secure incentive mechanism is required to detect and eliminate malicious or untrustworthy vehicles regardless of whether they connect to a roadside unit. Using Multiattribute Two-stage

Auction (MITA) approach, miners are selected based on the parameters like trust degree, data quality, and privacy to validate the blocks. The miners are rewarded/punished on the basis of their behavior in the networks. The malicious nodes are identified and eliminated to improve trust and quality and lowering DoS attacks. A discrete swarm particle optimization (DPSO) mechanism is proposed to eliminate various issues and improve the system's performance in an untrusted environment. The existing approaches are analyzed and validate the effectiveness of the proposed method.

1.5.2 Secure Outsourced Data by using Access Control Scheme and IPFS

A large amount of information is exchanged, so it needs to secure the data and the storage space. Many researchers have proposed encryption/decryption schemes to protect user data in the centralized and decentralized environment but involve a higher processing cost that results in attacks like eavesdropping and man-in-middle attacks. Executing the transaction in a decentralized environment requires a huge amount of Gas used in ethers is also observed. To address these problems, propose a blockchain-based access control mechanism to reduce processing time and transaction costs. In addition, a decentralized IPFS cloud server is expected to provide integrity, authenticity, and confidentiality. The experimental results of the proposed approach are better when compared with the existing approach.

1.5.3 Secure Users Authentication in Industrial Applications Using Blockchain Technology

To secure industrial applications many methodologies like identity, deep reinforcement, attribute-based, and certificateless signatures are proposed in the blockchain. These approaches reported less throughput, high latency, and issues in user authentication. Therefore, a user authentication approach is proposed to ensure authenticity through the public key infrastructure (PKI) and elliptic curve cryptography (ECC) and store the contract on the IPFS server. The PKI gives the digital certificate to the authenticated users for a limited period to access the industrial applications. The PKI can revoke the digital certificate from the users when their behavior is inappropriate. The ECC is used to distribute and manage the public/private keys to all the users of the blockchain network. The proposed approach provides better results and reduces the authentication time, enhancing the accuracy and throughput than the existing approach.

1.6 Outline of Thesis

The thesis is organized in the six chapters.

CHAPTER 1 presents the introduction of the blockchain along with motivation and research objectives. In addition, introduces the background knowledge of blockchain and its importance in security purposes, benefits and types. Further, presents blockchain techniques, applications, and structure. And securities issues that arise in each level of blockchain are described.

CHAPTER 2 describes the literature review on the blockchain technology with device, data, and user phases in the network.

CHAPTER 3 presents incentive mechanisms to validate miners and blocks in device phase with the DPSO and MITA approaches.

CHAPTER 4 studies the access control mechanism with IPFS server in data phase to build a system computationally efficient.

CHAPTER 5 covers the proposed user authentication PKI and ECC approach with proper simulation and shows that how digital certificates and keys are distributed among blockchain users.

CHAPTER 6 describes the concluding remarks of the thesis, and potential future work.

CHAPTER 2
LITERATURE REVIEW

This chapter presents a widespread study of published research articles related to the area of research with a focus on their concepts and outcomes. The literature survey is always valuable to identify the research gaps and their requirements.

2.1 Reviews on Blockchain Technology

This section contains the literature review on the security aspects of using blockchain technology and its summary is given in Table 2.1

To authenticate the users, Fotiou et al. [23] presented a blockchain-based decentralized information-centric networking (ICN) approach to provide the user's security. The owner of the data can share his/her consent via transactions with their subscribers in the blockchain network. Initially, the owner configures the public and private keys of the subscribers using the Hierarchy identity based cryptography (HIBC) technique. The transactions are stored on the blockchain along with the supporting details ensure the integrity of data. However, due to limited resources, the efficiency of the network is the major concern in the blockchain.

Shafagh et al. [24] proposed a blockchain-based data-centric approach in IIoT applications to eliminate the issues related to centralized systems in data and device phases. As per the approach, the access control scheme is trustworthy and manages the data for the IoT devices. The issues like latency, efficiency, scalability, and privacy are observed that need to be addressed.

Dickson et al. [25] presented a Blockverify and Everledger-enabled blockchain method that provides data security in supply chain applications. Blockverify has been physically delivered to the organization, while Everledger is available digitally and physically in its supply chain. Nowadays, IBM and Provenance approaches are commonly used in supply chain applications. Guo et al. [26] developed a Multi-authority attribute-based signature (MA-ABS) technique based on blockchain to preserve patient confidentiality in the healthcare system. It ensures the anonymity and immutability of medical and patient records, but the approach is very computationally intensive.

Gu et al. [27] proposed a blockchain-enabled malware detection approach on Android devices to overcome issues of centralized systems, such as failure, detection of malicious nodes, and reduced response time. To enhance data anonymity and privacy, Khalilov et al. [28] proposed a blockchain-enabled digital currency system on the bitcoin platform. The transactions of the digital system on the blockchain network might be used to track users' activity. Kravitz et al. [29] developed a blockchain-enabled identification approach that uses a private or permissioned blockchain network, which increases the security of both the user and the device phases. The identities of the users and devices are protected from malicious users/devices through the privacy-preserving

Shresthal et al. [30] proposed a blockchain-enabled approach for vehicular networks. It improved the delivery time to protect the data and devices and reduce the chances of attack, but the mining attacks are unable to be resolved. Zheng et al. [31] presented a blockchain-based method for vehicle applications to authenticate devices and users level in which smart devices can communicate with each other. The vehicles are efficiently able to protect transactions from malicious nodes. The certificate authority (CA), roadside units (RSU), and cloud is used to secure the privacy of users and devices. The CA validated the registered vehicles and stored the data on the cloud server to decrease its load. The user identity may be revealed from the network if the CA is fraudulent.

Table 2.1: Literature Reviews on Blockchain technology

Sr. No	**Author's name**	**Applications**	**Platform**	**Type of Security Services**	**Traditional approach limitations**	**Benefits of Proposed approach**
1.	Fotiou et al. [2016]	Information-centric networking [23]	Namecoin [Bitcoin]	On users phase	Efficiency is the main concern because of limited resources	To authenticate users
2.	Shafagh et al.	IoT devices[24]	Bitcoin	On data and	Single authority,	Trust, scalability and latency in

	[2017]			device phases	and efficiency	IoT devices
3.	Dickson et al. [2018]	Supply chain [25]	Permissioned Blockchain	On data phase	Higher communication cost, hardly to identify malicious devices	Easily find out the malicious devices, lower transaction cost and time
4.	Guo et al. [2018]	Healthcare [26]	Consortium blockchain	On data phase	Breach patient's privacy	To make sure the security of records and immutability
5.	Gu et al. [2018]	IoT in mobile [27] devices	Consortium blockchain	On device phase	Higher communication cost, malicious devices present	To discover the malicious nodes, reduced cost and time
6.	Khalilov et al. [2018]	Digital cash system [28]	Bitcoin	On data phase	Data privacy and traceability a big challenge	Secure user transaction, anonymity, and privacy
7.	Kravitz et al. [2017]	IoT applications [29]	Permissioned Blockchain	On user and device phases	Centralize authority, scalability and latency issues	To enhance the security of devices/users
8.	Shresthal et al. [2019]	VANET Networks [30]	Bitcoin PoW (Regional	On device and data	Devices Latency and Security	Reduced the delivery time, low probability of

			Blockchain)	phases	problems.	attack
9.	Dong Zheng et al. [2019]	VANETs [31]	Bitcoin (Public Blockchain)	On device and user phases	User's privacy can be compromised	Enhanced the privacy of the devices and users
10.	Shihan Bao et al. [2019]	Intelligent transportation system [32]	Proof of Work (Public blockchain)	On device phase	Key managed by single authority, to eliminate the privacy of whole system	Ensure system security, privacy, location, identification, and quick transactions
11.	Hong et al. [2019]	IoT applications [33]	IoT device platform using blockchain	On device phase	Security issues presents in IoT devices	Guarantees the security, integrity and non-repudiation
12.	Kalla et al. [2020]	Covid-19 [34]	Consortium platform	On data and users phases	Effects privacy	To improve the scalability, security, privacy, throughput, scalability
13.	Hussien et al. [2021]	Healthcare Industrial [35]	Private blockchain	On data phase	single authority, privacy, transparency issues	Improved patient’s data security and confidentiality
14.	Anju et al. [2021]	Internet of Vehicle applications	Ethereum platform	On device phase	Centralize control, trust and quality,	Reduces the malicious nodes during the

		[36]			issue between devices	communication data, improves the utility of system and trust between devices
15.	Tan et al. [2022]	Governance public sector [37]	Blockchain permissioned/permissionless platform	On data and device phases	Data security, privacy and system throughput problems	Improve the systems throughput

Bao et al. [32] proposed a blockchain-enabled pseudonym method to protect the identity and location of the system. The system executes transactions very quickly, but the keys are managed by a central authority which makes the approach challenging. Hong et al. [33] proposed a lightweight authentication approach based on blockchain in IoT applications. Each sensor communicates with others through a peer network which makes the whole system slow and vulnerable.

Kalla et al. [34] presented a blockchain-enabled approach to protect the data and privacy of the user during the COVID-19 pandemic. It has solved many problems as scalability, immutability, privacy, and centralization. Hussien et al. [35] presented a blockchain-based healthcare method for safeguarding the data and privacy of the user, but scalability is a major concern. Anju et al. [36] proposed a blockchain-based reward system that increases the utility of the system of vehicles and improves the trust, quality, and detection rate for malicious nodes. The multi-interactive two-stage auction mechanism is used for the selection of trusted miners. In addition, the DSPO mechanism is used to enhance the utility of miners for the detection of trusted nodes. Only the trusted miners confirm the blocks as valid or invalid. Rana et al. [159] proposed a dynamic state estimation algorithm that is used for sensing and transmitting information in IoTs network but due to increases the latency then also increases the possibility of security issues. Rathee et al. [160] proposed a blockchain based scheme that protected the vehicles in an untrusted environment and reduced the malicious devices.

Raniyal et al. [161] proposed a user authentication approach that improved the user’s anonymous but key overhead and centralized authority still present so needs to do works. Kunwar et al. [162] proposed a compact triple band antenna scheme for good radiation quality. Kumar et al. [163] proposed a data transmission protocol in IoTs that provided the authenticity and confidentiality of data, security can be breached because of a centralized dependency. Patel et al. [164] proposed a routing protocol in IoT applications that improved the capacity and reduce the delay time but used the decentralized technology delay time can be further reduced. Biswash et al. [165] proposed a multi home agent and pointer based approach that reduced the delay time in wireless networks but can be further improves the system performance. Meena et al. [166] proposed machine learning and deep neural approaches in IoTs that improved the performance of the system but this approach can be further enhances with blockchain technology. Tan et al. [37] presented a blockchain-based method in government sectors to improve data privacy and security. Some constraints are needed to be eliminated, such as timing, societal relevance, and enhanced security in public sector. Blockchain is performed on different levels, such as devices, data, and users with several applications. However, the improvement in one parameter may affect some other parameters. Moreover, there are many other security issues at different levels that are mentioned in Tables 2.2, 2.3, and 2.4.

2.1.1 Related Work on Blockchain Technology on Device Phase

In this section, several blockchain-based approaches are mentioned in the device phase with different applications.

Dongxiao et al. [38] presented a blockchain-enabled reputation approach to protect IIoT appliances to overcome the issues like transparency, dependability, and privacy which leads to an issue in the system efficiency. Yang et al. [39] implemented blockchain on the device to overcome attacks and improve overall efficiency. A Downgrade Delegated Proof of Stake (DDPoS) approach proposed in which consensus and trading nodes collaborate. The trading node generates the transactions whereas consensus node verifies the blocks.

Sun et al. [40] developed a blockchain-enabled solution that enhances the system's performance and throughput. Huang et al. [41] introduced a credit-based blockchain solution to Industrial applications that improve system security, and eliminates single points of failure. In addition, some hindrances are present, like data quality and storage. Kerrache et al. [167] proposed an Unmanned Aerial Vehicles (UAN) approach for detection of malicious nodes in vehicular networks where can securely communicate. Wang et al. [42] presented a blockchain-based reputation strategy in industrial applications to improve system safety and effectiveness. The normal nodes after authentication got a reward otherwise got a penalty. The result showed the proposed approach is better, safer, and more efficient. Asif et al. [43] presented a blockchain-based proof of physical unclonable functions (PoPUF) technique for device authentication that records the unique physical fingerprint. It needs to resolve the issue of scalability, data access, and sharing capabilities. Ahmed et al. [44] presented an identity-based blockchain-integrated encryption key mechanism for IoT devices but the level of the security needs to be improved. Table 2.2 presents several research studies of blockchain technology in the device phase with their limitations and benefits.

2.1.2 Related Work on Blockchain Technology on Data Phase

Blockchain can be used in the data phase to improve the security level. Table 2.3 summarized the existing works in the data phase and mentioned their limitations and benefits.

Table 2.2: Literature Survey of Blockchain Technology on Device Phase

Sr. No	**Author's name**	**Application**	**Platform**	**Type of Security Service**	**Traditional approach limitations**	**Benefits of Proposed approach**
1.	Liu et al. [2019]	Industrial IoTs[38]	Ethereum Blockchain	On device phase	Product transparency and single authority issues	Increased system transparency and guarantee built the trust bond between customers
2.	Yang et al. [2019]	Financial [39]	Hyperledger	On device phase	Unable to detect the malicious	Eliminate collusion attack, low

					devices	consumption of resources and high efficiency
3.	Sun et al. [2019]	IoTs [40]	Bitcoin	On device and data phases	Issues in throughput and Denial of Service attack	Enhanced the throughput of the system
4.	Junqin Huang, et al. [2018]	Industrial Internet of Things (IIoT) [41]	Raspberry Pi (PoW)	On device and data phases	Devices may be compromised	Guaranteed the system and data security in IIoT
5.	Wang et al. [2019]	IIoTs [42]	Ethereum platform	On device phase	Eliminate the system security because of malicious nodes may occurred	Enhanced the devices Authenticity
6.	Asif et al. [2020]	Internet of Energy [43]	Raspberry	On data and device phases	Scalability, energy consumption	Enhanced the data security and privacy, reduced latency, and maximize the efficiency
7.	Ahmed et al.	IoT [44]	Proof-of authenticati	On device	Centralized control,	Reduced computational

	[2022]		on	phase	devices security	load, protect devices

Li et al. [45] developed a data preservation system (DPS) approach based on the blockchain technology to ensure the privacy of medical data. However, data security needs to be optimized by minimizing costs and reaction time. Dai et al. [46] proposed a secure data trading ecosystem integrated with blockchain (SDTE) that provides data security. Liang et al. [47] proposed a data transmission technique with the Fabric blockchain platform to ensure data security and reliability in industrial applications. They managed the data in the network through the centralized authority which may create an issue of privacy and data security. Vora et al. [168] proposed a blockchain based approach that secured and stored their patient's data in healthcare system. Makkar et al. [169] proposed a blockchain based federated learning empowered approach in IIoTs that improved the efficiency and security of data.

Xu et al. [48] presented a fine-grained access control approach coupled with blockchain to safeguard IoT data. This work was computationally complex in data encryption and decryption and needed a high waiting time for the users. Arcinas et al. [49] developed a blockchain-integrated technique for securing the student's data on the blockchain through the bitcoin platform. It ensures data security, privacy, and trustworthiness, but it takes additional time, and cost for encryption and decryption. Chen et al. [50] suggested a blockchain-integrated proxy re-encryption solution that provides privacy to the patient's data and also enhances the system's performance.

2.1.3 Related Work on Blockchain Technology on User Phase

Blockchain can be used in user phase to improve the security level. Table 2.4 summarized the existing works in user phase and mentioned their limitations and benefits.

Ha et al. [51] offered a blockchain-integrated solution to financial applications and ensure the security of buyers and sellers. Li et al. [52] suggested a blockchain-integrated ring signature method that secured the user's identity and their personal data. But the security level needs to be improved with efficiency, scalability, and throughput. Nguyen et al. [53] developed a reinforcement learning approach based on blockchain to protect the data of the mobile users. It enhanced the user's privacy, reduced energy consumption and latency.

Table 2.3: Literature Survey of Blockchain Technology on Data Phase

Sr. No	Author's name	Application	Platform	Type of Security Service	Traditional approach limitations	Benefits of Proposed approach
1.	Li et al. [2018]	Medical [45]	Ethereum platform	On Data and users phase	Data can be tampered, unauthenticated users can access the data	Guaranteed the data and users privacy
2.	Dai et al. [2019]	Trading Ecosystem [46]	Ethereum Platform	On Data phase	Unauthenticated users can access, and required more time	Reduced the data modification, reduced the time
3.	Liang et al. [2019]	Industrial Internet of Things [47]	Fabric platform	On Data phase	Low data security, high transaction cost	Enhanced the security and reliability of data
4.	Xu et al. [2020]	Internet of Things [48]	Permissioned Platform	On Data phase	Single authenticated authority, overhead, complexity high	Reduced users overhead, security, prevent illegal users to access data
5.	Arcinas et al.	Educational data	Bitcoin	On Data phase	Leakage students data,	Ensured the privacy, and

	[2021]	[49]			and high cost	trustworthy
6.	Chen et al. [2021]	Medical data [50]	Hyperledger platform	On Data phase	Data tampered, leakage, and storage issues	Improved the safety of data during sharing

Using a blockchain-integrated access approach, Qin et al. [54] developed a method for recording user's behavior on the blockchain network. This work required to improve the data and user security with better flexibility. Lax et al. [55] presented a Blockchain-based technique that allows users to set up the privacy settings on social networks. Ahsan et al. [56] presented a blockchain-enabled technique for improving data, user, and device authentication in IoT applications. There is also needs to strengthen the security of IoT applications.

Table 2.4: Literature Survey of Blockchain Technology on User Phase

Sr. No	Author's name	Application	Platform	Type of Security Service	Traditional approach limitations	Benefits of Proposed approach
1.	Ha et al. [2019]	Marketplace [51]	Proof-of-work	On data and users phases	Centralized control, privacy issues	protect data from hackers
2.	Li et al. [2020]	Transactions [52]	Public blockchain	On users and data phases	Issues with data leakage, and user privacy	Guaranteed data security and user identity confidentiality
3.	Nguyen et al. [2020]	Mobile applications	Mobile edge computing blockchain	On users phase	High energy consumption, and users	Enhanced the users security

		[53]	network		security	
4.	Qin et al. [2020]	Internet of Things applications [54]	Hyperledger fabric blockchain	On user and data phases	Unauthenticated users access the data	Improved the users reliability
5.	Lax et al. [2021]	Social network [55]	Ethereum platform	On users phase	Misbehave parties, user security issues	Enhanced users privacy in social network
6.	Ahsan et al. [2022]	Internet of things [56]	Ethereum platform	Data, user and device phases	Users privacy, devices reliability and limited storage	Improved the data storage, and users/devices privacy and authentication

2.2 Summary of the Chapter

Blockchain is used for the security purposes of devices, data, and users with different applications such as vehicles, IoT, industrial, healthcare, voting, and digital transactions. Many researchers have applied many approaches but still, there is a scope for improvement to achieve better security, privacy, transparency, efficiency, reliability, throughput, and scalability in different phases in an untrusted environment.

CHAPTER 3
INCENTIVE MECHANISMS TO VERIFY MINERS AND BLOCKS IN VEHICULAR NETWORKS

The vehicular networks share large amount of data that may lead to several issues trust, data quality, DoS attack, and data alteration chances. To securely data transfer between vehicles in an untrusted environment used the incentive mechanism.

3.1 Introduction

This chapter presents incentive mechanisms to verify miners and blocks using blockchain technology in vehicular networks. The vehicles on the road share a lot of information through communication that ensures driver safety and service quality [57]. This information regarding the networks needs to be stored by authenticated miners.

Blockchain technology is popular due to its feature traceability, decentralization, trustworthiness, transparency, and immutability. The combination of blockchain technology with the Internet of Vehicles may result in a safe and secure network. The researchers used the byzantine algorithm to eliminate the data-sharing problems [58]. Some authors proposed security mechanisms integrated with blockchain technology in the internet of vehicle applications as reputation and lightweight schemes. Another one used the proof-of-reputation scheme that enhanced the trust between vehicles when sharing data among them [59]. Wang et al. proposed an anonymous rewarding scheme integrated with blockchain technology (BARS) to ensure security between vehicles while sharing information [60].

A blockchain-integrated remote attestation security scheme proposed that ensures data privacy and integrity among vehicles [61]. Chen et al. [62] proposed blockchain-integrated vehicle mechanisms that ensure the efficiency and safety of the shared data. The existing approaches enabled to eliminate the data sharing issues in the internet of vehicles; however, the selection of miners may create issues as they can share invalid information in the network. Therefore, a better stake-based voting system under a delegated proof of stake mechanism (DPoS) is used to select legitimate miners. Still, there are issues in vehicular networks with blockchain technology. Some of the issues are discussed below:

Miner Selection: The selection of a miner with high stakes becomes an extremely significant concern and may be a threat. Malicious miners may behave well in the beginning to make their goodwill reputations, and later these malicious miners act as trusted miners and refuse the trusted ones. Consequently, these malicious miners are present in the blockchain network and can damage the whole system by propagating invalid information [63].

Block Validation: Malicious miners also take part in the block selection phase and collide with other legitimate miners, and successfully produce counterfeit information and the double-spend attack if they are in the majority. Therefore, it is important to propose a blockchain-integrated IoV approach that selects legitimate blocks and miners and ensures system security in the untrusted environment as well.

To overcome the mentioned issues, blockchain integrates with the IoV with incentive mechanisms such as optimization schemes and auction schemes are proposed to ensure secure, reliable, optimized, and trusted blockchain-based vehicle architecture [64, 65]. The incentive mechanism is constituted of miners, requesters, and platforms. For the maximum utility of miners, the platform assigns blocks to suitable miners and incentives to the concerns. On the other hand, the auction approach selects trusted miners to increase the efficiency of the platform. The traditional approaches have issues in the selection of miners and blocks. The block assignment approaches have been used frequently by researchers to optimize system proficiency, whereas the auction approaches have been generally used in the blockchain to facilitate participation through participants as miners.

Another research shows how to pick robust miners for the blockchain-integrated system [66]. They used a block assignment scheme to select the blocks that will involve many miners, thus enhancing the system's performance. The miner-centric and platform-centric are the two phases of an incentive mechanism to select blocks for trusted miners. The miner-centric approach enhances the effectiveness of miners and simultaneously assigns suitable blocks to miners with a time slot to develop the utility of miners [67]. The platform-centric approach enhances the effectiveness of the system and selects the appropriate miner through the auction approach [68]. In the block selection process, only interested miners propose their bids on the system, and trusted miners select the block and give incentives to honest miners and a penalty for dishonest miners. The positions of the miners are changing frequently, and the next block will be given to legitimate miners dynamically [69].

3.1.1 Objective and Contribution

The main objective of the proposed approach is to enhance privacy and security and remove the unfairness issues created by miners in the vehicular network using blockchain technology. The data quality and trust value of IoVs are stored on the blockchain network dynamically.

The platform-centric scheme with a combination of the multiattribute and two-stage auction is used for miner selection to enhance the system's effectiveness. Many authors have already proposed different IoV approaches, but the security issues in IoVs via blockchain technology need to eliminate. The main contribution of this work is given below:

- To ensure vehicle security in data transmission for roadside units, sensors, vehicles, IoTs, and other devices.
- The process of selecting trusted vehicles in the auction approach (M-ITA) by calculating the level of reliability and confidentiality that reduces the chances of data alteration in IoVs.
- The DPSO approach is used to improve the miner's utility in IoVs [70].
- The experimental analysis demonstrates that MITA with DPSO approach performs better and also eliminates several existing issues.

The mechanism for validating blocks is divided into two stages; selection of the miner and the block, as shown in Figure 3.1. During the first phase, the platform-centric approach is used to select the miner based on the submitted biddings. In the second phase, the miner-centric approach is used to validate the blocks and provide the incentive to the corresponding miner.

3.2 Related Work

Many researchers used blockchain technology in a variety of ways to provide tight security in vehicular networks. Several trust and security-based mechanisms have been implemented such as probabilistic, privacy-preserving [71–72], cryptography, security management [73], trustworthy storage [74], resilience, and security [75]. Chen et al. [76] suggested an information offloading strategy in IoVs that minimized latency and eliminate unwanted data from the network. They used the max-min function for task execution and an optimization approach to improve the system's efficiency and performance. In another work, a demand response (DR) approach is proposed to ensure the trustworthiness, privacy, and efficiency of the smart grid system through the clinching auction [77].

To improve satisfaction, Huang et al. [78] presented a sorting genetic algorithm with blockchain technology that reduced the transaction cost of an electric vehicle system. Kang et al. [63] proposed an optimization technique integrated with blockchain by using the reputation and contract theory that helps to enhance trust in the system. Wang et al. [64] developed an optimal strategy and an auction technique for mobile systems that ensure system utility, security, and privacy. Jiao et al. [79] suggested an approach that is both constant and multi-demand integrated with the public blockchain that provides efficiency, optimal social welfare, and trustworthiness. In the constant-demand method, every miner bids to predetermine the resource quality, whereas, during the multi-demand method, miners submit their bids and demands via using the auction scheme. In these approaches, some hindrances present such as throughput, bandwidth, and miner's effectiveness so need to enhance. Thakur et al. [80] proposed a double auction method integrated with blockchain technology that reduced the computation overhead, and energy loss, and enhanced efficiency.

Choubey et al. [81] presented an auction technique integrated with blockchain and a ranking algorithm to increase the security, trustworthiness, and privacy of electric vehicle systems while encouraging the greatest number of system participants. Another [82, 83] proposed a double auction integrated with blockchain technology in a mobile crowdsensing system to improve the system utility, and security, and increase the number of participators that needs to be further enhanced. This approach is implemented on the bitcoin platform [84] that sends the cryptocurrency from one place to another. This platform used a proof-of-work consensus approach that is computationally intensive and restricted the block size to 1 MB and needed 10-12 minutes to propose a new block. Even though the Ethereum platform is used to create the smart contract for both financial and non-financial applications and a block can be created in 12 seconds. It needs some ether in advance to compile the contract, whereas Hyperledger Fabric is a private platform best for time-related applications developed by IBM. Several comparative studies are also done to evaluate various blockchain platforms such as Ethereum, Bitcoin, Litecoin, Peercoin (a derivative of Bitcoin), Hyperledger, MultiChain (combinations of user's permission as well as improved data ledger), Cardano, Waltochain [85, 86]. The analysis of different blockchain platforms can be done in terms of energy consumption, consensus algorithm, usability, efficiency, security, and scalability.

Park and colleagues [92] presented a credit-based incentive structure integrated with blockchain technology that eliminated the node's issues of being unsatisfied, egotistic, impatient, and not being given credit for their efforts. Besides that, an incentive scheme is developed at a low cost so that no guarantee of security, trust, or privacy needs to be further improved in the future. Yang et al. [93] presented a decentralized trust management system for vehicle networks based on blockchain technology to enhance trusted nodes, traffic safety, and other factors as well. Their strategy outperforms the existing one, but it desires to enhance the privacy, security, and trustworthiness in networks of vehicles. Lu et al. [94] suggested a blockchain-integrated anonymous reputation system (BARS) that protects the privacy and increases trust in the vehicular network. However, several hindrances as high time, key, and storage overhead, destroy the whole security in the vehicular system if malicious nodes are in the majority. Baldini et al. [95] presented a blockchain-integrated trust management approach for IoVs that provides the certificate only to the authenticated vehicles through the PKI

Li et al. [96] developed a blockchain-integrated privacy-preserving technique that enhances reliability, security, and anonymity and reduces the time in the detection of malicious identities. Knirsch et al. [97] proposed a blockchain-integrated protocol for a decision tariff that preserved the security, trustworthiness, reliability, transparency, and privacy of electric vehicles. There are some charging (energy) stations that send bid requests for tariffs and store bids on the blockchain to enhance traceability but have transaction costs overhead. Ijaz et al. [98] proposed a blockchain-integrated reward and penalty mechanism that increased trustworthiness and system security and decreased malicious devices.

Many researchers have proposed various methods to protect the IoV network's security, whereas only a few researchers have applied blockchain integrated with the IoV networks. In this work, the IoVs are integrated with blockchain so that vehicles can converse with others in an untrusted situation. Some issues are still present such as unutilized miners, data quality, and low detection rate of malicious devices in IoV networks.

Therefore, in this chapter of the thesis DPSO and MITA algorithms are proposed for the validation of miners and blocks that increases the system's performance and eliminates the malicious nodes.

The proposed approach is evaluated and the results show that the trust values, data quality, block utility, miner effectiveness, and detection of malicious nodes are improved and reduced DoS attacks. The miners are selected (based on the attributes of the community and historic practices) through a multiattribute two-stage approach. Furthermore, it has applied the incentive mechanisms (DPSO and MITA) to resolve the miners' and block's efficiency.

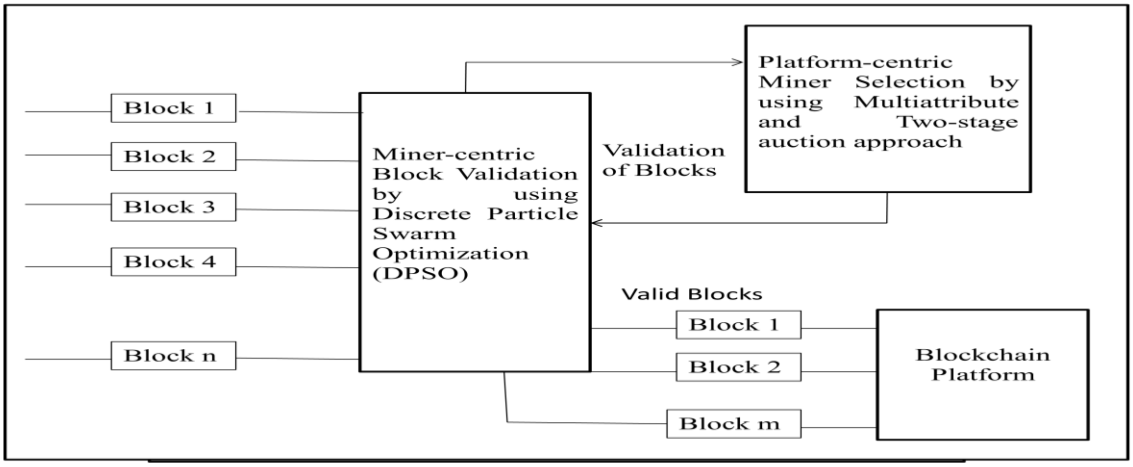

Block 1
Block 2
Block 3
Block 4
Block n
Miner-centric Block Validation by using Discrete Particle Swarm Optimization (DPSO)
Validation of Blocks
Platform-centric Miner Selection by using Multiattribute and Two-stage auction approach
Valid Blocks
Block 1
Block 2
Block m
Blockchain Platform

Figure 3.1: Selection Procedures of Miners and Blocks

3.3 Proposed DPSO and MITA in Vehicular Networks

In this section, the proposed incentive mechanism is explored that includes the miner-centric and platform-centric to enhance the system performance. An appropriate block is assigned to a legitimate miner through a multiattribute two-stage auction for block validation. Several vehicles or devices are connected and communicate through wireless in Figure 3.2. Each vehicle serves as a data supplier and requester and stores the data in nearby roadside units. In addition, it ensured the communication of vehicles to vehicles and other devices without delay. The miners are selected through the value generated by the MITA algorithm based on trust and the quality of devices. The generated value must be greater or equal to 0.50 for selected miners.

Then the comprehensive score of the selected miners is calculated and the top 6% of miners will be rewarded and miners select blocks to validate through the DPSO method, as illustrated in

Figure 3.3. The entire process helps to eliminate issues like trustworthiness, security, and unfairness up to some extent.

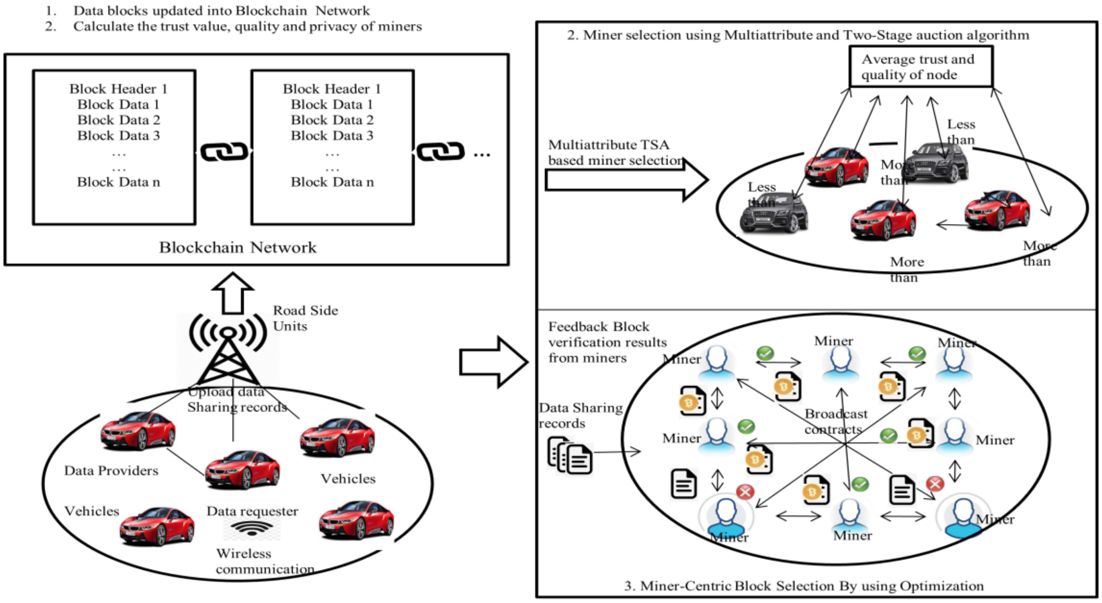

1. Data blocks updated into Blockchain Network
2. Calculate the trust value, quality and privacy of miners
Block Header 1
Block Data 1
Block Data 2
Block Data 3
…
…
Block Data n
Block Header 1
Block Data 1
Block Data 2
Block Data 3
…
…
Block Data n
…
Blockchain Network
Road Side Units
Upload data Sharing records
Data Providers
Vehicles
Vehicles
Data requester
Wireless communication
2. Miner selection using Multiattribute and Two-Stage auction algorithm
Average trust and quality of node
Multiattribute TSA based miner selection
Less than
Less than
More than
More than
More than
Feedback Block verification results from miners
Data Sharing records
Miner
Miner
Miner
Miner
Miner
Broadcast contracts
Miner
Miner
Miner
3. Miner-Centric Block Selection By using Optimization

Figure 3.2: Blockchain Integrated with Internet of Vehicles

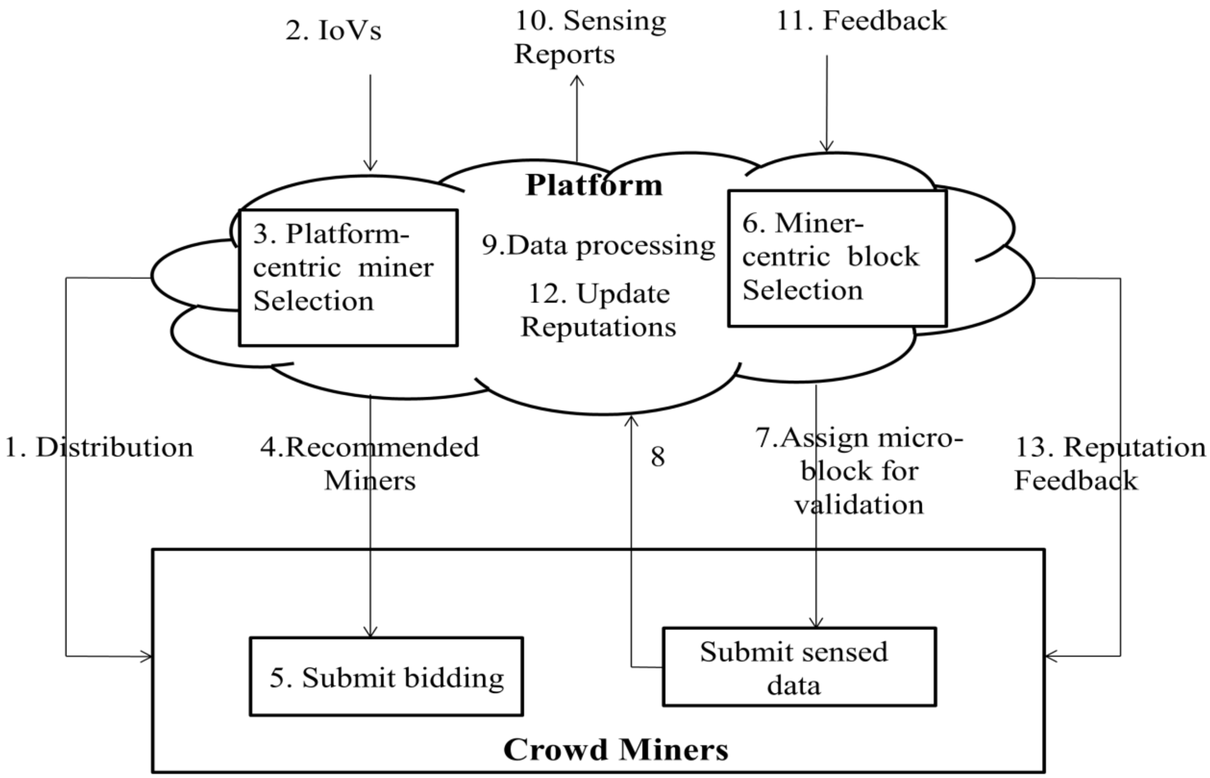


Figure 3.3: Process of Blockchain Internet of Vehicles

The flow chart of the proposed BIoVs is illustrated in Figure 3.4 through the incentive mechanism. If the average trust value of a node is greater or equal to 0.5 then its comprehensive score is computed for the trusted nodes else the node is treated as a malicious node. The utility of the trusted node is calculated and top 6% nodes selected and incentivized miners. The data of trusted miners is stored in the blockchain network while malicious nodes are unable to join the network. And, every time the position of miners are dynamically updated, so the chance of data transmission possibility goes to low. The algorithm for selection of miners and blocks is described in Algorithm 3.1 and 3.2 in sections 3.3.1 and 3.3.2 respectively. The notations used in algorithms with descriptions are given in Table 3.1.

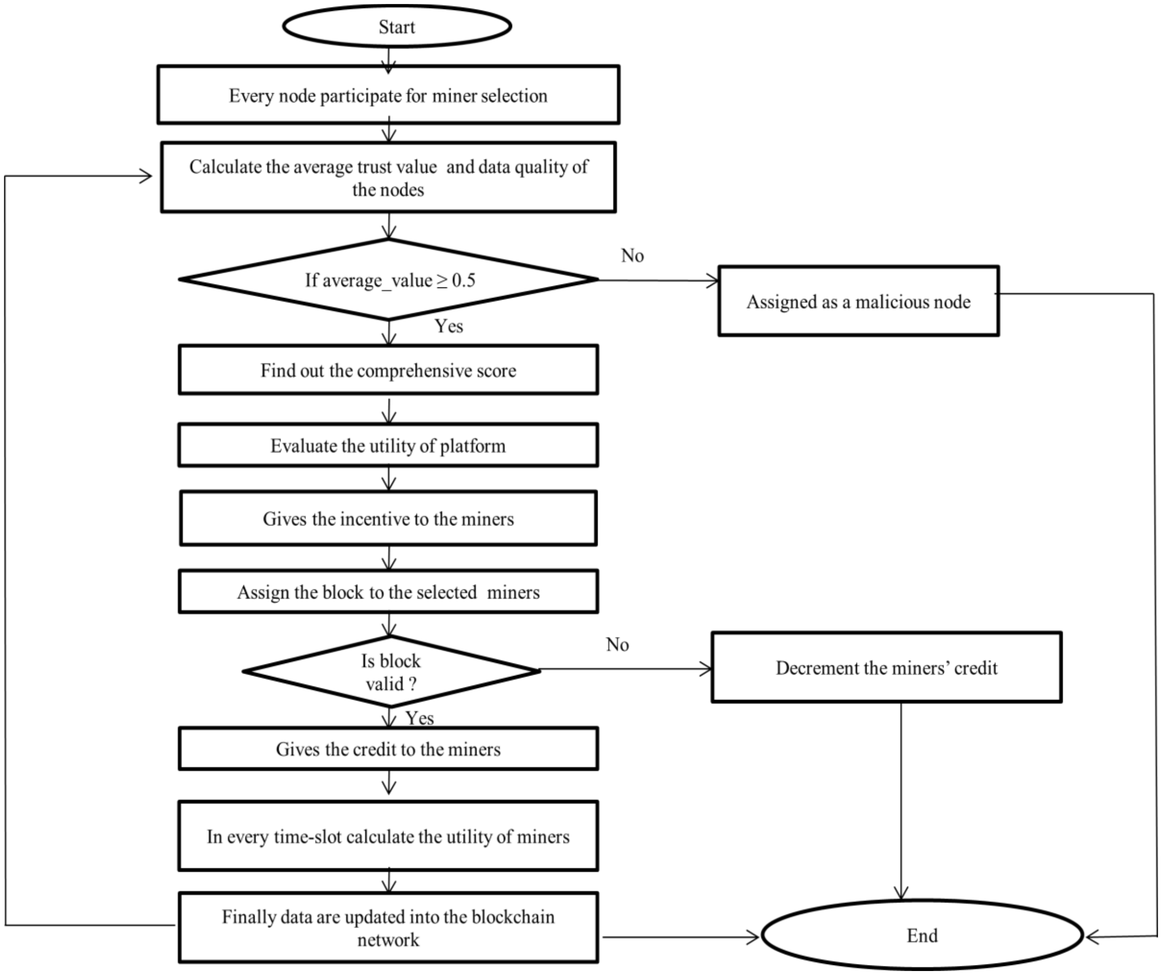

Start
Every node participate for miner selection
Calculate the average trust value and data quality of the nodes
If average_value ≥ 0.5
No
Yes
Assigned as a malicious node
Find out the comprehensive score
Evaluate the utility of platform
Gives the incentive to the miners
Assign the block to the selected miners
Is block valid ?
No
Yes
Decrement the miners' credit
Gives the credit to the miners
In every time-slot calculate the utility of miners
Finally data are updated into the blockchain network
End

Figure 3.4: Flow chart of the Proposed Approach

Let t$_i$ denote the number of i^{th} miners, where blk$_j$ denotes the j^{th} block and miner t$_i$ is favored to confirm the block blk$_j$.

Wherever Valid *(*blk$_j$*)* represents the specific blk$_j$ is a legitimate. As illustrated in equation 1, A$_{ij}$ offers the payment to t$_i$ through the system, and R$_{ij}$ is the payment offers to t$_i$ for validating the blk$_j$. Let us consider e$_j$ specify the costs of t$_i$ in each time period, consequently $R_{ij} = z_i * G_{ij}$ wherever 0 < z_i < 1 after that, calculates A$_{ij}$ via the given equation:

$$A_{ij} = (G_{ij} / s_j) * e_j \tag{1}$$

Where G$_{ij}$ represents the confirmation time of IoV via t$_i$ in favor of performing blk$_j$, where s$_j$ is the entire validating time of Vehicle blk$_j$, and e$_j$ denotes the incentives after validation of blk$_j$. In the proposed system, here suppose that (e$_j$/s$_j$) >=1. The utility of miners is calculated through the given equation:

$$L_{ij} = \begin{bmatrix} A_{ij} - R_{ij} \ \ if & \\ & Block\ is\ legitimate \\ & Otherwise \\ 0, Block\ is\ not\ legitimate & \end{bmatrix} \tag{2}$$

Table 3.1: Considered Notations with their Descriptions

Notations	Descriptions
t$_i$	i^{th} number of miner
blk$_j$	j^{th} number of block
Valid(blk$_j$)	A validset of blk$_j$
L$_{ij}$	The utility of t$_i$ through validation of blk$_j$
A$_{ij}$	Offer payment to t$_i$ through the platform
R$_{ij}$	The cost of miner for validating the blk$_j$
G$_{ij}$	The sensing time of vehicles t$_i$ that spend validation of blk$_j$
s$_j$	Total sensing time of vehicles to blk$_j$ requested
e$_j$	Incentives for block validation
m$_{ij}$	A contribution that t$_i$ brings through validating the blk$_j$ for the system
M$_j$(T)	Total profits of platform corresponding to blk$_j$
A$_j$(T)	Total incentives of miners for validation of the blocks blk$_j$

To determine the IoV system's efficiency/utility by using the consequent calculation with consideration to blk$_j$:

$$\overline{L_j} = M_j(T) - A_j(T) \qquad (3)$$

In cases where $M_j(T) = \sum t_i \in Valid(blk_j) * m_{ij}$ realizes the total income of the platform corresponding to blk$_j$, while m$_{ij}$ indicates the contribution that t$_i$ confirms blk$_j$. $A_j(T) = \sum t_i \in Valid(blk_j) * A_{ij}$ is the total amount paid to subsequent miners for performing blk$_j$. In Algorithm 3.1, blocks are determined with time for the miners, and simultaneously, miners in Algorithm 3.2 submit their bids on the system corresponding to interested miners.

3.3.1 Block Validation Process

This method is used to select appropriate blocks for the miners with the help of the miner-centric scheme using the DPSO algorithm to enhance the efficiency of miners as given in Algorithm 3.1. Table 3.2 describes the notations with their descriptions and the effectiveness of the miner is determined by the following equation:

$$L_i = \Sigma_{j=1}^{t} L_{ij} \qquad (4)$$

Table 3.2: Block Validation Notations and their Descriptions

Notations	**Descriptions**
L$_i$	The effectiveness\utility of t$_i$ during every time period
R$_i$	Overall cost of t$_i$.
e_i^t	Incentives of t$_i$.
Z_i^k	Set of blocks that assigned to t$_i$ during *k*th iteration.
Z_{ij}^k	blk$_j$ assigned to t$_i$ during *k*th iteration.
miners$_i^k$	Dynamically miners updated of t$_i$ during *k*th iteration.
m_{ij}^k	A payment IoV to facilitate t$_i$ brings to blk$_j$ during *k*th iteration.
miners$_{ij}^k$	Updating the position of miners for blk$_j$ during *k*th iteration

P $^{k-1}_{pgrti}$	The highest personal value of Z during the (k-1)th iteration.
P $^{k-1}_{ggrt}$	The Global greatest value of Z $^{k-1}_{i}$ during (*k-1)*th iteration.
x	Alter local & global parameters correspondingly.
hash$_1$, hash$_2$	The values of hash
rand$_1$, rand$_2$	The values of random
$\overline{\min ers}{}^{k-1}_{i}, \overline{P}{}^{k-1}_{pgrti}, \overline{P}{}^{k-1}_{ggrt}, \overline{Z}{}^{k-1}_{i}$	The consequent operators after updating dimensionally.

To pick a block for a miner, Max {L$_i$} represents an objective function calculated through the given condition $R_i \le e_i^t$, where R*i* indicates the entire cost of t$_i$, and $S_i = \Sigma_{j=1}^{t} r_{ij} \,.\, e_i^t$ to facilitate the incentive of t$_i$ to the miners who helps to validate the blocks. The DPSO algorithm is used to solve the block sensing concerns. The entire time is divided into multiple time slot Z $^{k}_{ij}$ represents for the *k*th iteration and is calculated using the following equation, whereas blk$_j$ is chosen during t$_i$. By using the DPSO Z $^{k}_{ij}$ and Z $^{k}_{i}$ calculated during the *k*th iteration, which updates the particle position. After that, the objective function calculation is:

$$Z_{ij}^{k} = \begin{bmatrix} 1, \, if \; blk_j \to t_i \\ 0, \, otherwise \end{bmatrix} \tag{5}$$

Therefore, the constraints circumstances addicted to the form of equations:

$$\text{Max} \sum_{j=1}^{t} L_{ij} Z_{ij}^{k} \tag{6}$$

If blocks are valid then miner's positions are changed in every time slots then takes the maximum utility of miners. In equation7, Overall cost of the miners for assigned block to miners should be less than the incentive to the miners.

$$\sum_{j=1}^{t} R_{ij} Z_{ij}^{k} \le e_i^t \tag{7}$$

To calculate the fitness gathering of particles via below subsequent formula during the proposed algorithm:

$$Fit(Z_i^k) = \sum_{j=1}^{t} m_{ij}^{k} Z_{ij}^{k} \tag{8}$$

Wherever Z_i^k represents the particle's quality, such as $Z_i^k = (Z_{i1}^k, Z_{i2}^k, ...Z_{im}^k)$. m_{ij}^k represents the function of miner's t$_i$ intended for IoV validation blocks *blk$_j$* during the *kth* iteration. After that, optimizing the *Fit* (Z_i^k) can optimally allocate the *blk$_j$* intended for t$_i$ via the DPSO algorithm. The position of miners is dynamically updated every time wherever *miners$_i$* represents a numerous miners t$_i$, and miners$_i^k$ = *(miners$_{i1}^k$ miners$_{i2}^k$ miners$_{im}^k$)*, where *miners$_{ij}^k$* represent the updated position of miners during the *kth* iteration intended for *blk$_j$*. To calculate the updated position of *miners$_{ij}^k$*, through a certain equation:

$$miners_{ij}^{k} = [0,\ if\ Z_{ij}^{k} = Z_{ij}^{k-1}$$

$$Z_{ij}^{k},\ Unchanged] \qquad (9)$$

Wherever *miners$_{ij}^k$* = 0 represents the miner's position not changed for *blk$_j$*, while *miners$_{ij}^k$ = Z$_{ij}^k$* represent the location of miners affected during the *kth* iteration. Where P_{pgrti}^{k-1} and P_{ggrt}^{k-1} denotes the personal and global greatest value of Z_i^{k-1} correspondingly, and *x* assigns the weight for local and global search, where x should be 1 > x >0.

$$\min ers_i^k = x.\min ers_i^{k-1} + hash_1.rand_1.(P_{pgrti}^{k-1} - Z_i^{k-1}) + hash_2.rand_2.(P_{ggrt}^{k-1} - Z_i^{k-1}) \quad (10)$$

$$Z_i^k = Z_i^{k-1} + \min ers_i^k \qquad (11)$$

Two parameters are taken, hash$_1$ and hash$_2$ for hash values wherever each block associated to previous block with the help of hash value that are changed during the *kth* iteration to precisely the confidence levels. To satisfy the given restrictions takes three constant parameters such as hash$_1$, hash$_2$, and x. Furthermore, it takes two random values, rand$_1$ and rand$_2$, where rand$_1$, rand$_2$ ∊ [0, 1] because positions change incessantly when a block is affix and dynamics of the blockchain IoV devices. As shown in the given equations, the personal, global, and miner values are updated instead of the initial value set dimensionality:

$$\min ers_i^k = x.\overline{\min ers}_i^{\,k-1} + hash1.rand1.(\overline{P_{pgrti}^{k-1}} - \overline{Z_i^{k-1}}) + hash2.rand2.(\overline{P_{ggrt}^{k-1}} - \overline{Z_i^{k-1}}) \qquad (12)$$

$$Z_i^k = \overline{Z_i^{k-1}} + \min ers_i^k \qquad (13)$$

P_{pgrti}^{k-1} and P_{ggrt}^{k-1} denotes the personal and global greatest value corresponding to Z_i^{k-1}. In this dissertation, $\overline{\min ers}_i^{k-1}, \overline{P_{pgrti}^{k-1}}, \overline{Z_i^{k-1}}, \overline{P_{ggrt}^{k-1}}$ consequent operators are updated whereas 0 sets the initial value.

3.3.2 Miner Validation Process

By using the auction and a two-stage approach, the miners are selected on the basis of trusted value, data quality of miners. To encourage the miners to participate in vehicular network then calculates the threshold values using the auction algorithm [83]. The Multiattribute and ITA auction algorithms enhanced the utility of the system, as illustrated in Algorithm 3.2. The notations that are used for miner's selection describe in Table 3.3.

Table 3.3: Miners Selection Notations and their Descriptions

Notations	Descriptions
Q_{it}	Data quality of t_i.
D_{it}	Trust degree of t_i.
$A_{i(t+1)}$	The privacy sensitivity of t_i.
Q_i^j	The accurate quality of t_i for sensing jth vehicle.
I_j	The instant interruption in the jth sensing vehicle.
D_i^j	The perfect trust of t_i for sensing jth vehicle.
$r_{i(t+1)}$	An comprehensive score of t_i for (t+1)th vehicle.
x_1, x_2	Weight assign for Q_{it} and D_{it} correspondingly.
$R_{(t+1)}$	Threshold multi-attribute score for (t+1)th sensing vehicle of t_i
A_{t+1}	Multi-attribute thresholds of privacy sensitivity score for (t+1)th the sensing vehicle of t_i.
M_{t+1}	Multi-attribute thresholds bidding score of platform for (t+1)th

The innovative sensing vehicle of t_i that desires to obtain a piece in the consequent attributes can be computed: (Q_{it}, D_{it}, $A_{i\,(t+1)}$). Q_{it} and D_{it} correspond to the average quality and trust of vehicle t_i. And, to evaluate the values of Q_{it} & D_{it} from the t_i chronological data whereas $A_{i(t+1)}$ denotes the privacy of miners t_i and Q_{it} calculates the value through the subsequent equation:

$$Q_{it} = \begin{bmatrix} \dfrac{\sum_{j=1}^{t} Q_i^j I_j}{\sum_{j=1}^{t} I_j} \ \ if\ t \neq 0 \\ 0,\ otherwise \end{bmatrix} \tag{14}$$

Wherever Q_i^j represents the accurate data quality of t_i in favor of sensing j^{th} of IoV whereas I_j senses the j^{th} of IoV to take the time through the Ebbinghaus Forgetting Curve. Where curve represents chronological data eventually on ending decomposes equal to 0. Moreover, the constraint I_j is calculated by a consequent equation that is supported according to the Ebbinghaus Forgetting Curve:

$$I_j = \begin{bmatrix} 1,\ \ if\ \ j = t \\ e^{-\frac{1}{j}},\ \ else\, 1 \leq j < t \end{bmatrix} \tag{15}$$

Where, D_i^j correspond to the accurate trust degree intended for sensing IoV consequent to t_i. The standard trust D_{it} that is related to quality calculates through consequent formula:

$$D_{it} = \begin{bmatrix} \dfrac{\sum_{j=1}^{t} D_i^j I_j}{\sum_{j=1}^{t} I_j} \ \ if\ t \neq 0 \\ 0,\ otherwise \end{bmatrix} \tag{16}$$

To calculate the Q_{it} and D_{it} values using the system, as shown in the following equations. After the miners have submitted their bids, announce the privacy $A_{i(t+1)}$ to them. For the duration of bidding, the interested miners consist of $A_{i(t+1)}$ and $s_{i(t+1).}$ The comprehensive score $r_{i(t+1)}$ is calculated through the consequent equation:

$$r_{i(t+1)} = [x_1.Q_{it} + x_2.D_{it}] \tag{17}$$

Whereas x_1 and x_2 are the weights corresponding to Q_{it} and D_{it}, and the sum of the weights equal to 1. The multiattribute auction algorithm combined with the ITA [80] to enhance the systems utility.

Algorithm 3.1: Block Validation Process (DPSO algorithm)

Enter Input data: e_i^t , hash$_1$, hash$_2$, t, x

Print Output data: Valid (blk$_{j)}$

Steps:

```
Block Validation process through DPSO algorithm using Miner-Centric scheme
For every block assigns the $Z_{ij}$ do
    Initialize miners of IoV $\overline{\min ers}_{i}$ with their positions $\overline{Z}_i$
    Evaluate $Z_{ij}$ along with set $\overline{P_{pgrti}} = \overline{Z}_i$
End of For
$\overline{P_{ggrt}}$ = Max { $\overline{P_{pgrti}}$ }
Do while
    For j= 1 toward t subsequently do
        Bring up to date IoV miners with their positions $Z_{ij}$ and it need to satisfy
            $\sum_{j=1}^{t} R_{ij} Y_{ij}^{k} \le e_i^t$
        If F ($Z_i$)>F ( $\overline{P_{grti}}$ )
            $\overline{P_{pgrti}}$ =$Z_i$
        End of if
        else If F ( $\overline{P_{pgrti}}$ ) > F ( $\overline{P_{ggrt}}$ )
            F ( $\overline{P_{ggrt}}$ ) = F ( $\overline{P_{grti}}$ )
        End of if
    End of For
End of do-while loop
Print an appropriate (blk$_j$)
End of the blk$_j$ validation
```

The whole method of the Multiattribute-Two-stage Auction (M-ITA) algorithm concerns the sensing vehicle of t_i, as demonstrated in Algorithm 3.2 below. $E_{(t+1)}$ indicates the bidding threshold value for detecting $(t+1)^{th}$ vehicle of t_i. $R_{(t+1)}$ and $A_{(t+1)}$ represent the newest sensing vehicle's multiattribute and confidentiality threshold value, respectively. From lines 1 through 15, the auction algorithm is divided into two parts. At this point, the issue of unfairness that afflicted the first arriving participant has been resolved. Every time the value of $R_{(t+1)}$ is dynamically updated and calculated using the equation.

$$R_{(t+1)} = \left[\frac{\sum_{i=1}^{N} r_{i(t+1)}}{N} \right] \qquad (18)$$

N indicates the overall miner that is frequently changed in every time slot that is described in details in Algorithm 3.2.

The values of M(T) and A(T) not less than one so at starting point, that is initialized with 1. The locations of the miners are regularly updated, and the threshold bidding value is calculated using ($M_{t+1}(T)/A_{t+1}(T)$). And, the multi-attribute threshold value R_{t+1} is also updated dynamically. The simplified ($M_{t+1}(T)/A_{t+1}(T)$) and R_{t+1} values are evaluated through the given 19 and 20 equations, respectively.

$$\frac{M_{t+1}(T)}{A_{t+1}(T)_{(j+1)}} = \frac{1}{2}\left[\frac{M_{t+1}(T)}{A_{t+1}(T)_{(j)}} + \frac{m(j+1)(t+1)}{A(j+1)(t+1)} \right] \qquad (19)$$

Wherever $(M_{t+1}(T)/A_{t+1}(T))_{(j+1)}$ and $(M_{t+1}(T)/ A_{t+1}(T))_{(j)}$ indicates the bidding threshold values of $(j + 1)^{th}$ as well as j^{th} miners.

$$R_{t+1}^{(j+1)} = \frac{1}{2}\left[R_{t+1}^{(j)} + r_{j(t+1)} \right] \qquad (20)$$

Algorithm 3.2: Miner Validation Process (MITA algorithm)

Enter the Input information:

N=1000, A(T)=1, M(T)=1,

Print Outputs information:

Trusted Miners

Steps:

```
1. While N>=0 do
2. Calculate the Average $Q_{it}$ of the miners
3. Calculate the Average $D_{it}$ of the miners
4. If Average value of ($Q_{it}$ and $D_{it}$ >= 0.5) then
6.   Vehicle is trusted
7.       Calculate the comprehensive score through given equation:
        $r_{i(t+1)} = [x_1.Q_{it} + x_2.D_{it}]$
8. **Else**
        Vehicle is Malicious
9. End of **if**
10. Calculate the values of $R_{(t+1)}$
11. **if** $r_{i(t+1)} \geq R_{(t+1)}$, and $A_{i(t+1)} \leq A_{(t+1)}$
12. Calculates the threshold values of M(T) and A(T) of (t+1)th
13. All time changing value $\frac{M_{t+1}(T)}{A_{t+1}(T)}$ and $R_{t+1}$
14. Otherwise
15. Values of $\frac{M_{t+1}(T)}{A_{t+1}(T)}$ not change
16. End of **if**
17. Store all records in WF.
18. End of **while loop**
```

Whereas $R_{t+1}^{(j)}$ and $R_{t+1}^{(j+1)}$ indicates the multiattribute threshold values of the *j* and *(j* + 1*)*th miners in the same way. The welfare (WF) of the vehicles, which is evaluated by using the following equation:

$$WF = \sum_{i=1}^{t} \sum_{j=1}^{n} L_{ij} + \sum_{j=1}^{n} \overline{L_j} \qquad (21)$$

Moreover, to maximize welfare through the objective functions that is evaluated through the consequent 22 and 23 equations in that order.

$$\sum_{i=1}^{t} \sum_{j=1}^{n} (A_{ij} - R_{ij}) + \sum_{j=1}^{n} \sum_{i=1}^{t} (m_{ij} - A_{ij}) \qquad (22)$$

$$Min - WF = \sum_{i=1}^{t} \sum_{j=1}^{n} (R_{ij} - A_{ij}) + \sum_{j=1}^{n} \sum_{i=1}^{t} (m_{ij} - A_{ij}) \qquad (23)$$

In 23 equations, the value of A_{ij} is always updated while R_{ij} and M_{ij} values are not updated through the system. The value of A_{ij} changes because it acquires the maximum welfare during optimization and auction process.

3.4 Parameter Setting

The authors analyzed the effectiveness of the proposed approach by considering 5 to 1000 IoVs as a part of the network. In this work, several parameters as described in Table 3.4 are used to simulate the scenario. The parameters values of this work as given in Table 3.2 are almost identical with the existing work [63].

Table 3.4: Settings the Simulation Parameters

Parameters Setting	**Values**
Numerous vehicles	5 to1000
Greatest time delay of sensing (j^{th}) vehicles	Three days
Miner price in time slot	1
Blocks budgets	5
Implementation point in time	30 sec
Random numbers: $rand_1$, $rand_2$	[0,1]
Bidding entrance assessment for t^{th} vehicle sensing of t_i	0.7
Multiattribute confidentiality entrance assessment for t^{th} vehicle sensing of t_i	0.5
Weight for data quality	40
Weight for trust degree	60

3.5 Experimental Outcomes

The effectiveness of the proposed, and reputation and contract theory [63] is compared in this section. The existing approach [63] employs subjective logic models; however, the proposed method employs incentive mechanisms such as a fusion of DPSO and M-ITA. The performance of this work is evaluated by measuring the DoS attacks, the detection rate of malicious IoVs, the data quality of IoVs, trusted IoVs, miners' utility, data alteration, and compromised miners.

Through the simulation parameters, to evaluate the trust of the vehicles that is increased upto 65% as shown in Figure 3.5. To ensure that only trusted vehicles can communicate safely within the network. As illustrated in Figure 3.6, to evaluate the performance of the data quality of trusted IoVs with the help of the proposed and existing approaches that enhanced the efficiency of the entire network. As shown in Figure 3.7, the rate of malicious IoV detection is consistent with the current technique. In the existing scheme, the miners were selected according to reputation so that the miners behaved well enough to take a positive opinion. So, the malicious miners later collude randomly with well-behaved vehicles. Hence, a negative opinion may be generated against misbehaving vehicles, while colluding vehicles generate a positive opinion that acts as a trusted miner's. And, Every time miner’s positions are changed so malicious chances is less.

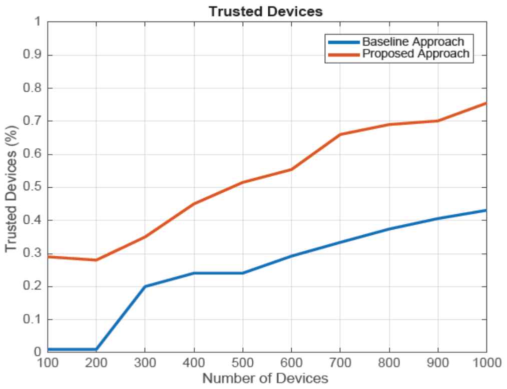


Figure 3.5: Comparison of Trusted Devices with the Baseline and Proposed Approach

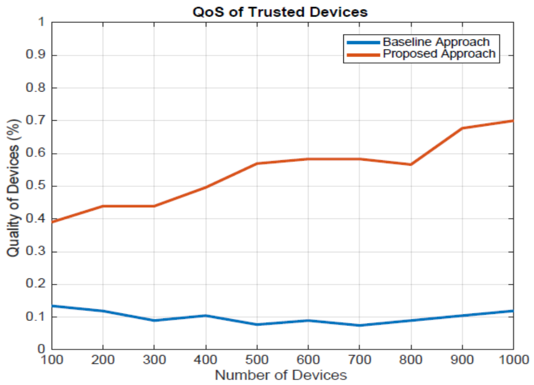


Figure 3.6: Comparison of Quality Devices with the Baseline and Proposed Approach

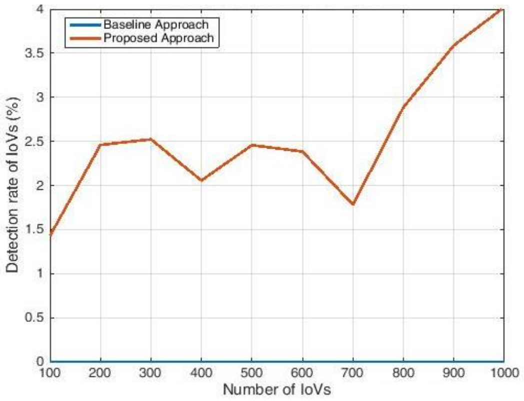


Figure 3.7: The Detection Rate of Malicious Vehicles with Baseline and Proposed Approach

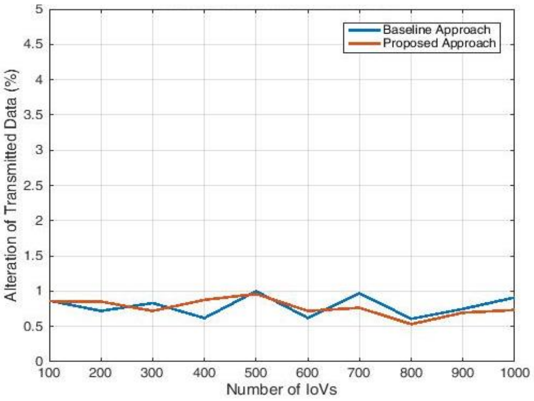


Figure 3.8: Alteration Data with Baseline and Proposed Approach

The proposed approach compared with the baseline approach with fewer amounts of data is altered along with the number of IoVs, as illustrated in Figure 3.8. When comparing the performance of the proposed strategy to the existing one, the number of compromised miners is extremely tiny that is reduced upto 44%, as shown in Figure 3.9. The DoS attack is illustrated in Figure 3.10, the authenticity of the vehicle should be high, and otherwise, the chances of unauthenticated miners can be increased and the proposed approach reduced the DoS attacks are as compared to existing approach. The miner's utility is illustrated in Figure 3.11 that is calculated with the help of an incentive mechanism that is improved upto 20%

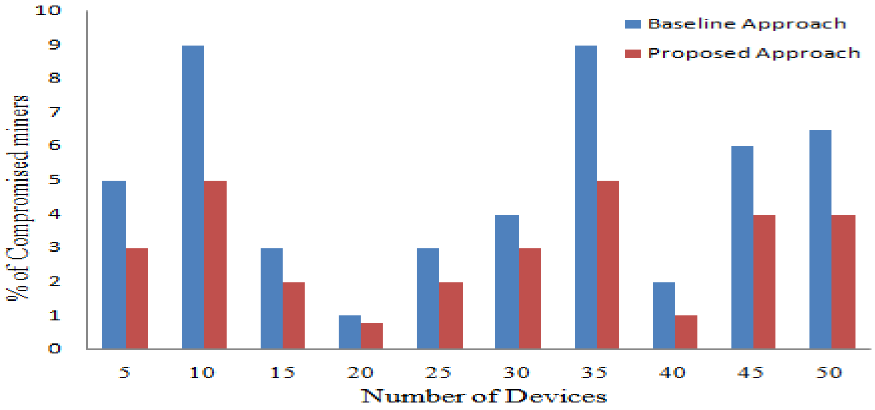


Figure 3.9: Comparison of Compromised Miners with the Proposed and Reputation Approach

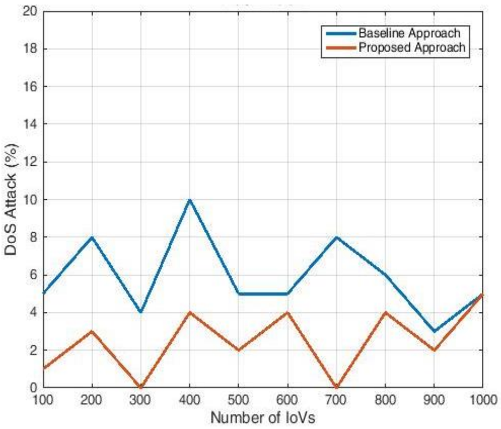


Figure 3.10: DoS Attack with Baseline and Proposed Approach

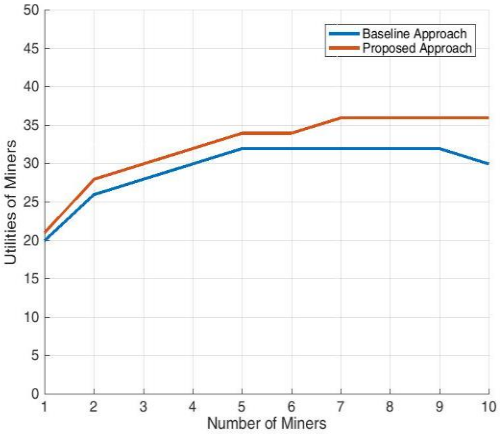


Figure 3.11: Comparison of the Miners Utility with Baseline and Proposed Approach

The first research objective is achieved in this chapter by using DPSO and MITA algorithms. The DPSO algorithm improves the efficiency of the miners whereas M-ITA method improves efficiency of the system. There are a number of real-time applications where blockchain can be used as industrial healthcare, and IoTs to record every activity.

3.6 Summary of the Chapter

This chapter presents incentive mechanisms that are a combination of DPSO and M-ITA algorithms to verify miners and blocks using blockchain technology in vehicular networks. The vehicles on the road share a lot of information through communication that ensures driver safety and service quality. The DPSO algorithm validates the block whereas the MITA algorithm to check the miner's is trustworthiness.

The decentralized approach of this work increased the trust and utility of miner's upto 65% and 20% respectively whereas the compromised miners are reduced upto 44%. The hackers became very smart, that can be implemented various attack strategies and have become successful in performing these attacks as Sybil attacks and DDoS attacks, which are not eliminated through this method.

CHAPTER 4
SECURE ATTRIBUTE-BASED APPROACH TO OPTIMIZE THE TIME OF ENCRYPTION AND DECRYPTION ALGORITHMS

Several companies outsource their data to a cloud server that may lead to several issues like privacy, sharing, and storage space for data creators. The data is usually secured through encryption standards on the cloud but it takes huge amount of time and resources.

4.1 Introduction

Some approaches like attribute-based encryption schemes [99-100] and bilinear pairing [101] allow users to store their data on the centralized cloud server and use ciphertext-policy attribute-based encryption (CP-ABE) approach for the security of data and require low computability. In the centralized system, a single authority is managing and provides trust and if it gets compromised, then all the data may be leaked.

Blockchain technology has the capability to resolve the issues related to the centralized system and provide security to the data. The data is kept in the form of blocks with a timestamp using blockchain technology [102].

Users form a smart contract between them to specify the payment guidelines and tasks. Although, within seconds, transactions are transferred through the wallet digitally [103] without credit and debit cards, papers, bank accounts, and a third party. In order to ensure confidentiality and then verify the legitimacy of the responses, it is a significant security problem using blockchain technology. The author has already proposed a fair-payment protocol [100] and Zyskind et al. [104] have proposed a blockchain-integrated symmetric encryption approach in which the whole network is managed through a decentralized environment with the bitcoin platform. The blocks are created by consuming a lot of energy and time due to the proof-of-work consensus technique, making it difficult to handle a large amount of data instantly.

Data security can be preserved and handled through a non-reshuffle technique [105] that improves scalability and reduces latency. A deep reinforcement learning approach with blockchain integration has been presented by Liu et al. [106] to protect shared and stored data for industrial applications. There are several weaknesses like data security, privacy, flexibility, and scalability is not guaranteed.

IPFS [107] is a decentralized blockchain-based server that is used to provide integrity, authenticity, and confidentiality in the network. Moreover, in this work, an attribute-based approach is also utilized to reduce the time required for encryption and decryption algorithms. The proposed approach is illustrated in Figures 4.2 and 4.3 and its detailed description is also provided in Section 4.5.

4.1.1 Objective and Contribution

A large amount of data including sensitive information is shared and stored in the network regularly. Maintaining privacy and security in the network along with efficiency is very challenging. The chapter aims to improve data security and reduce the encryption and decryption time to make the whole system efficient.

Many researchers have proposed data encryption schemes to keep data secure but this leads to several issues like data privacy, centralized data storage, and higher processing time that are prone to copious perilous attacks like eavesdropping and man-in-middle attack. In addition, due to centralized authority data security and privacy can be compromised.

A decentralized IPFS cloud server is expected to provide integrity, authenticity, and confidentiality. The proposed approach of this study is legitimately aimed at reducing the time, as demonstrated by the experimental results in Section 4.6. The contribution of this chapter is as follows:

- The attribute-based encryption scheme is proposed with blockchain to reduce the encryption and decryption time.
- IPFS is utilized to protect the stored data in an untrusted environment.
- After conducting a thorough analysis and comparison, it has been determined that the proposed approach outperforms the existing approach across various performance parameters.

4.2 Related work

Many authors have proposed different approaches such as searchable encryption schemes [110], symmetric encryption schemes [111], and auditing schemes [112], attribute-based encryption schemes [99-100] to keep data secure. The existing schemes provide data security, but key overhead and unreliable third parties are the main safety concerns. A blockchain-integrated BCPay system is proposed to secure outsourced data and a blockchain-integrated checking-proof protocol to verify the key's fairness [113, 114]. Blockchain-integrated decentralized auditing (Dredas) approach for industrial applications has been presented by Fan et al. [115] which reduced the computational cost. Jiang et al. [116] projected a blockchain-integrated verification search method that secures outsourced data through encryption. For the storage of data on a cloud server, Wang et al. [117] presented a fair payment protocol that integrates with blockchain technology decreased storage costs, and guaranteed fair payment. They used a centralized data framework for storage; the crucial data may get damaged if the centralized party is hacked.

Sun et al. [118] presented a blockchain-integrated ciphertext-policy attribute-based encryption method with insurance applications and data stored on the IPFS that guarantee data security. Li et al. [119] have proposed blockchain-integrated ciphertext-based attribute encryption (CP-ABE) along with a fine-grained access technique for vehicle networks (VANETs) that enhances the efficiency and security of the network. Using blockchain technology, Lin et al. [120] presented a Conditional Anonymous Payment (DCAP) approach that ensures system privacy in financial applications. This scheme outperforms Zerocash, as evidenced by the performance results. Lin et al. [121] suggested a blockchain-enabled group signing and broadcast encryption system that improved the security of cryptocurrency and food supply and chain (PPChain) applications that improves efficiency. Another proposal [122-124] is a blockchain-based secure and transparent method for protecting data and user privacy, authentication, and security during exchanging healthcare data that eliminates the centralized dependency, and scalability.

Kumar et al. [125] offered a blockchain-integrated database strategy for supply chain applications that eliminates difficulties of data security, and centralized administration. Hao et al. [126] presented a blockchain-integrated collaborative system for discreetly outsourcing information storage in an insecure environment. In a centralized cloud, all the data is stored and verified before being transferred to the blockchain. A third party putting data on the cloud is semi-trusted, and if the third party becomes malicious, there is a greater chance of data loss. A blockchain-integrated data verification technique has been suggested by Hao et al. [127] that help to verify the inner and outer groups in untrusted environments with third-party auditing. The decentralized model is implemented through blockchain but needs to overcome issues such as centralized data storage, verification time, and concurrent data management.

A blockchain-integrated provenance outsourced data that provides the integrity, immutability, and security of data [128]. The handling of large amounts of data needs extra storage space so need to improve data capacity, effectiveness, and protection. Benil et al. [129] presented a blockchain-integrated Elliptical Curve Certificateless Aggregate Cryptography Signature technique (EC-ACS) for auditing and authenticating healthcare data. By using a cryptographic algorithm, the patient's medical data is encrypted and give permission for data exchange and put it into the cloud but issues like involvement of a third-party, accessing time, and security are the main concerns.

Many researchers already have proposed blockchain-integrated outsourced computation schemes to improve safety, confidentiality, and efficiency, but they further desire to save the outsourced data. These concerns are resolved by blockchain technology as it has immutability, tamperproof, decentralized, and secure features.

The technique presented in this chapter is a blockchain-integrated outsourced data in an untrusted environment and guarantees the quality of service. The proposed approach is integrated with blockchain technology and data put on the IPFS server that eliminates data loss and privacy concerns in an untrustworthy environment. Thus, it guarantees storage, security, and privacy in an efficient manner

4.3 Preliminaries of Proposed Approach

In this section, the proposed approach is explained in detail. The notations and its description are given in Table 4.1.

4.3.1 Bilinear map

Let us consider, the GP and GG pair belonging to prime order q. GP's generator is p. H = {0, 1} ⟶ GP is the hash function wherever every attribute points to the arbitrary element GP. G= GP * GP ⟶ GG satisfies the two properties:

1. $E(p^c, q^d) = E(c, d)^{pq}$ for all p, q ∈ GP and c, d ∈ Z
2. $E(gg_1, gg_2) \neq 1$ for all gg_1, gg_2 ∈ GP

4.3.2 Access Structure and tree

Let us consider, that AP is a set of attributes of the method while AU is a set of attributes for users (AU should be a nonempty subset of AP). As shown in Figure 4.1, where access tree is represented via AT that contains the leaf as well as non-leaf nodes. Therefore, we generate an access structure AS⊆ [119]. AS is monotone if ∀ BS, CS: BS ∈ AS, BS ⊆ CS and can obtain CS ∈ AS. Let us consider, that the access tree AT represents the intended access structure AS whereas n is a node of AT. Thus, AT is the root node of n where AT_n represents its subtree. AS set the root node of AT then, if n=AS whereas AT_n can be seen like that ATs. The non-leaf node of AT_n is characterized by its child node numbern, but the node n threshold gate SP_n is described by SP_n [1, $number_n$]. As soon as $SP_n = 1$, SP_n=$number_n$ then chooses the threshold gate SP_n is an OR gate, while AND is an AND gate. It is confirmed via user attribute set AU and threshold SP_n for leaf node AT_n. If the user attribute AU satisfies the AT_n then computes the AT_n(AU)=1 and frequent AT_n(AU) recursively.

If n is a non-leaf node, then n_0 represents all child nodes. Additionally, if ATn_0(AU)> k_n after that, display the AT_n(AU) =1. If n is a leaf node attribute (n) ∈ AU, The attribute (n) is the attribute associated with the leaf node n, and the result is AT_n(AU)=1. The following functions are defined in this work to attempt accessing a tree: parent (n) reflects the parent node of n under AT, attribute (n) reflects the attributes of n, number (n) reflects the number of child nodes of n, and index (n) reflects the index of a child node of n.

4.3.3 Blockchain with its Ethereum Technology

Satoshi Nakamoto developed the Bitcoin application using blockchain technology in 2008 [12]. Blockchain is prominent for its characteristics as transparency, security, privacy, immutability, decentralization, and traceability. A circulated ledger is a way where data is recorded, maintained, and endlessly growing transactions in an ordered way across multiple computers of the blockchain network. When the miners validate the blocks and add them to the blockchain with transactions, previous and current hash values, timestamp, nonce, and a difficulty target.

4.3.3.1 Accounts of Ethereum

External accounts and contract accounts are the two kinds of accounts used on the Ethereum blockchain. The external account is managed by the users (private key), who can openly transmit and share transactions. The smart contract is the in-charge of the contract account that receives the transactions from the external account as well as its code.

Table 4.1: Notations and their Descriptions

Notations	Descriptions
do	data owner
du	data user
pb	public key
msr	master key
sc	secret key
sc`	encrypted secret key
AP	attribute set of the system
AU	attribute set of users
AS	access structure
SP	security parameters
ks	symmetric key
ct	Ciphertext
AT	access tree or policy
E_{ks}(EF)	encrypted file

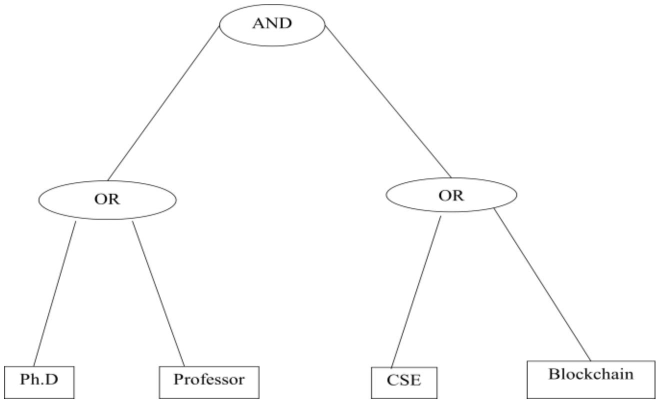


Figure 4.1: Access Tree

4.3.3.2 Transactions in Ethereum

The Ethereum blockchain records all intelligent immutable contract transactions [119], [108], gas price, gas limit, ether value, sender address, hash value, and contract address. The smart contract appears and communicates with the blockchain via online ether wallet using the application binary interface (ABI) and Byte code.

4.3.4 Smartcontract

Smart contact is a set of programs in blockchain that executes when predetermined conditions are met [119], [108].

4.3.5 IPFS

The InterPlanetary File System (IPFS) is a distributed file system that allows devices to store and connect through a unified file system via a distributed hash table (DHT) without the interference of a third person. It is a decentralized data storage technique that stores a large amount of data in a distributed way to improve data security and provides a prefix code starting with Qm corresponding to uploaded files.

4.4 Proposed CP-ABE Approach

In this work, the CP-ABE approach is proposed to secure data using the Ethereum blockchain, smart contracts, and IPFS. The interaction process of different components is shown in Figure 4.2. The following components are used to create the scenario of this work:

4.4.1 Data owner: Encrypt and upload files to the IPFS, create smart contract, and access policy.
4.4.2 Data user: Accesses the data from the IPFS and decrypts the file.
4.4.3 Smart-contract: Compile and deploy the Smart-contract.
4.4.4 IPFS: IPFS cloud stores the data owner’s encrypted file.
4.4.5 Myetherwallet: Acts as an interaction between smart contract and blockchain.
4.4.6 Ethereum blockchain: All data gets recorded on the blockchain.

The steps of the Figure 4.2 are given in details as given below:

1. A smart contract is created and compiled through data owner in solidity language named CP-ABE.
2. The data owner stores the cipher text, IPFS hash value, and file ID.
3. The data user wants to access the file from the data owner.
4. The data owner encrypts and stores the data so that only authenticated users can access it.

5. The ciphertext key for the valid time is received by the data user so corresponding to that can decrypt the data.

6. The data owner uploads it to the IPFS cloud.

7. The owner then gets a unique IPFS code corresponding to the files.

8. After this, the data owner gives this code to the data user.

9. Data users can access files or data with security from the IPFS cloud.

10. Myetherwallet acts as an interaction between blockchain and smart contracts that helps to deploy as well as interact with the contract.

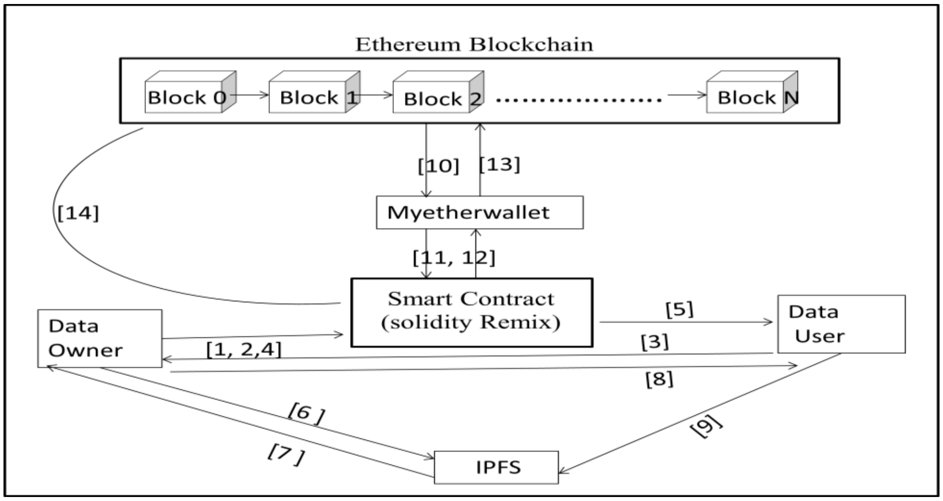


Figure 4.2: The Proposed Approach using Blockchain Technology

11. Deploy a smart contract on the blockchain using byte code.

12. Interact by interacting with the smart contract using ABI code on the blockchain.

13. All transactions that are publicly visible on the blockchain, including the gas consumed, contract address, gas limit, hash value, and many other details.

14. At last, the same number of accounts along with addresses and ethers appears in blockchain and solidity.

Data can be transferred and shared securely through blockchain as shown below algorithms:

1. Setup (AP ⟶ (pb, msr)): AP represents the system's attribute set taken as an input that is executed by the data owner (do). Inside this phase, we get the master msr and public pb keys output. Simultaneously, a smart contract is deployed on the blockchain named CP-ABE. As shown in steps 1 and 2 of Figure 4.2, Records files EF with file ID encrypted as Eks(EF)(everyplace ks represents the symmetric key)and later uploads to the IPFS cloud. Simultaneously, hashed with the file ID and put the smart contract on the blockchain (10, 11, 12, 13 and14). The data owner receives the unique code of the corresponding file after uploading as shown in steps 4, 6, and 7 of Figure 4.2. The proposed approach is CP-ABE based taken from these references [108], [118].

Public key (pb) = $\{\mathrm{GP},\ gg_1, gg_2, gg_1^{\ c}, gg_2^{\ d}, E(gg_1, gg_2)^d, \mathrm{H}\}$ (24)

Master key (msr) = {c, d ∈ Z} (25)

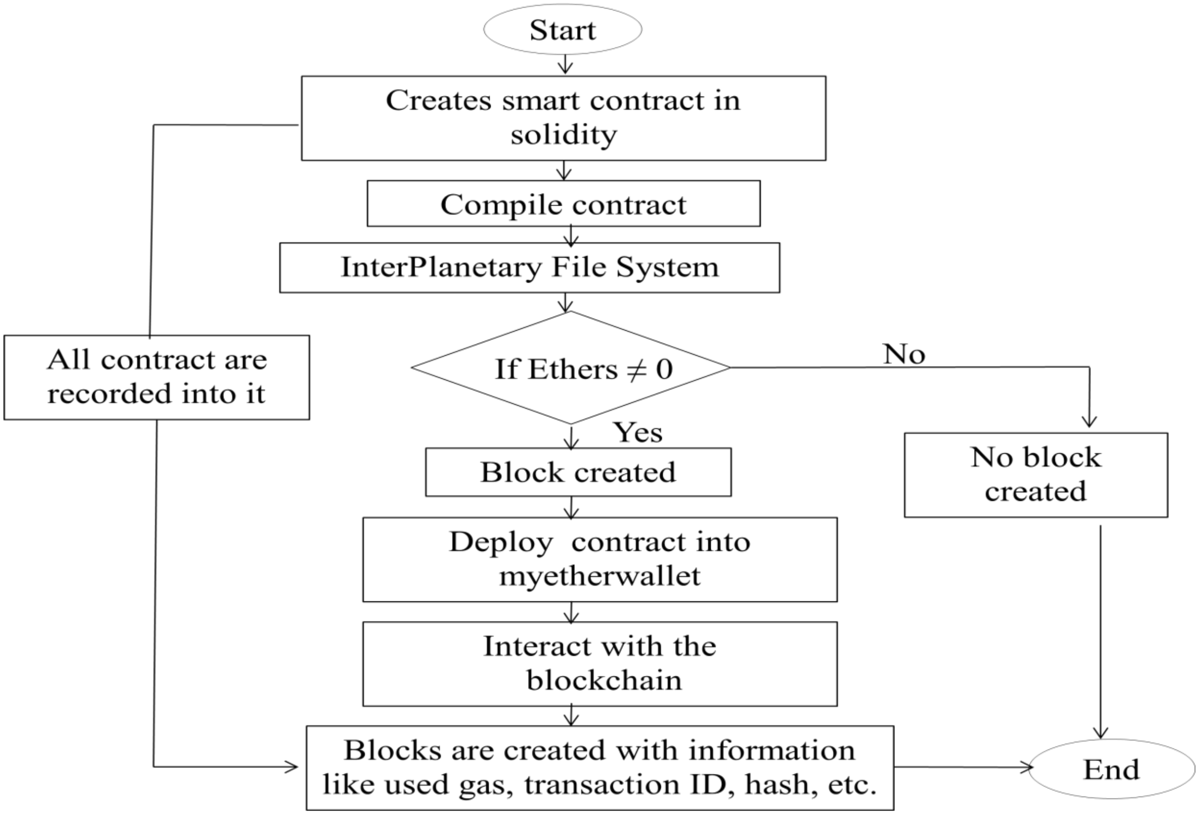

Start
Creates smart contract in solidity
Compile contract
InterPlanetary File System
If Ethers ≠ 0
No
Yes
All contract are recorded into it
Block created
No block created
Deploy contract into myetherwallet
Interact with the blockchain
Blocks are created with information like used gas, transaction ID, hash, etc.
End

Figure 4.3: Flow Chart of the CP-ABE Proposed Approach

2. Encrypt ((pb, ks, AS) ⟶ ct): The public key pb, AS access structure, and ks symmetric key are taken as inputs, whereas ct is output. Encryption time is required to take the plaintext and convert it to ciphertext. As illustrated in step 4 of Figure 4.2, the data owner stores the ciphertext ct inside the smart contract.

The data owner selects the q with d degree. Each node n in AS is preferred from top-down which is starting from the AT root node. The threshold node sets to be (n_n, sp_n) for every node of n. The threshold value of k_n and d_n are:

$$k_w = d_w+1 \tag{26}$$

Through the data owner to choose the random number r ∈ Z, place q_{AT} (0) = r, that are initializing from the origin node AT. The data proprietor arbitrarily chooses the coefficient for achieving the polynomial. To set the value for every node such as q_n (0) = $q_{parent\ (n)}$ (index $_{(n)}$), where parent $_{(n)}$ is the parent node of n with index $_{(n)}$. After that, compute the coefficients of the leaf node arbitrarily as well as calculate the ciphertext ct as specified:

$$ct= \{AS,\ S`=ks.\ E(gg_1, gg_2)^{dr},\ S=(gg_1, gg_2)^{r}$$

$$\forall n \in N: S_n= gg_1^{\ c}.q_n(0), S_n`= H(attribut\ e_{(n)})^{qn(o)}\} \tag{27}$$

3. Key Generation ((msr, AU) ⟶ sc): Within this phase, the data owner (do) assigns the attributes and access policy to the data user (du) for some valid time. The attribute set of users AU and master key msr are in use as contribution, while the secret or private key sc of users is returned as an output. As shown in steps 3, 6, 7, and 8 of Figure 4.2, sc' represents the contract's encrypted secret key. To select the random number r ∈ Z and after that each attribute j∈ AU has generated the private key sc.

$$sc= \{Q= gg^{(d+cr)},\ \forall j \in AU: gg^{r}.H(_{j)}^{\ r_j},\ Q`= gg^{c.r_j}\} \tag{28}$$

4. Decrypt ((pb, sc, ct) ⟶ ks): The data user executes this phase and accesses the data within the valid period. It receives encrypted secret key sc' and ciphertext ct as of the smart contract. And decryption time is the other way around, restoring the plaintext, from the received ciphertext. To decrypt the sc' key by using a decryption algorithm because of secret key sc. The public key pb, secret key sc, and ciphertext ct take as an input parameters. After being satisfied with the access policy AT then decrypts the encrypted key ks otherwise cannot do. As shown in steps 5 and 9 of Figure 4.2, data consumers can receive the encrypted file E_{ks}(EF) from the IPFS cloud and decrypt the encrypted file EF' during the key ks and output the file EF.

1. It is a down-top method that is opposite to the encryption phase where n is leaf node so that j=attribute (n). If j! ∈ AU then Decrypt Node (sc, ct, n) = null. If j ∈ AU then

Decrypt Node (sc, ct, n) = E(Q_j, S_n)/E(Q_j`, $S_n$`) (29)

$$= E(gg,gg)^{qn(0).c.r} . E(H,gg)^{qn(0).c.r} \,/\, E(gg,H)^{q_n(0).c.r}$$

$$= E(gg,gg)^{q_n(0).c.r}$$

2. If n does not represent a leaf node, then decrypt it as specified below. All nodes N that are a child of n, after that it performs the M_N= Decrypt ((sc, ct, N) where $M_n \neq$ null and AU_n a random k_n- the size of children nodes (N). If it is not existing then sets the child node sets like as M_n=null otherwise, calculate the M_n

M_n= $E(gg,gg)^{qn(0).c.r}$ (30)

The decryption phase calls to the decrypting node used for root node AT of AS if the data user sets AU satisfied the AS then calculates:

M_{AT}= Decrypt (sc, ct, AT) = $E(gg,gg)^{c.r,p}$ (31)

ct= S`.M_n/E(Q, S) (32)

Afterward, the data user decrypts the encrypted file E_{ks} (EF) and takes the original file EF.

4.5 Parameter Setting

The authors analyzed the encryption and decryption time of the proposed approach by considering 50 attributes in the network. In this work, several parameters as described in Table 4.1 are used to simulate the scenario. The values of parameters of this proposed approach as given in Table 4.2 are almost identical with the existing work [100].

Table 4.2: Settings the Simulation Parameters

Notations	**Explanations**
Contract Creation (Gas Used)	1211793
IPFS	QmYvbqzZh2YDkbQCfELqJm46HLLo3WHEkQyib1MytMQsit
Ethers	100
Number of Attributes	50
Secure Hash algorithm	256 bits

Random Numbers a, b	3, 4
Encryption time	0.035 ms
Decryption time	0.11 ms

4.6 Experimental Outcomes

At present data security and privacy is the main concern. Many approaches are proposed to eliminate the problems as centralization, authenticity, and complexity to maintain the data security. To proposed the CP-ABE approach to secure the data in the untrusted environment by using IPFS for storing the data for minimize user effort. The performance of proposed approach gives the better result as compared to existing functional encryption solution [100].

As illustrated in both Figure 4.4 and 4.5, the proposed approach performance is compared to the existing approach, where encryption and decryption time are reduced upto 23% and 37% respectively. Therefore, the chances of the eavesdropping and man-in-middle attacks are minimized.

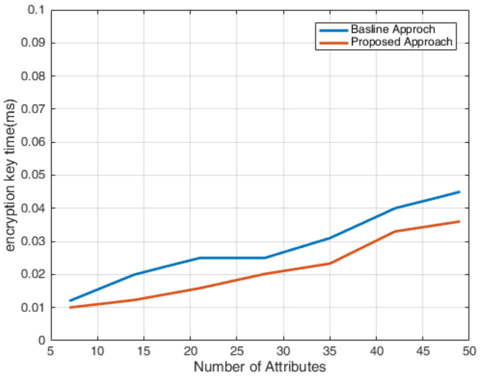


Figure 4.4: Comparison of Encryption time with the Baseline and Proposed Approach

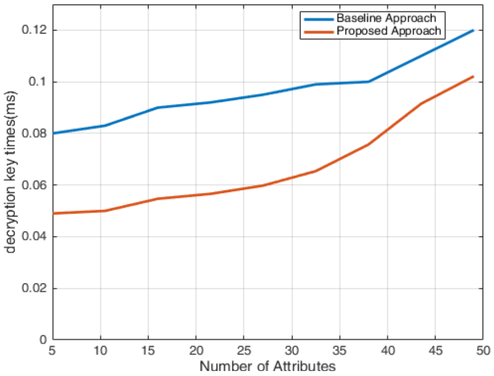
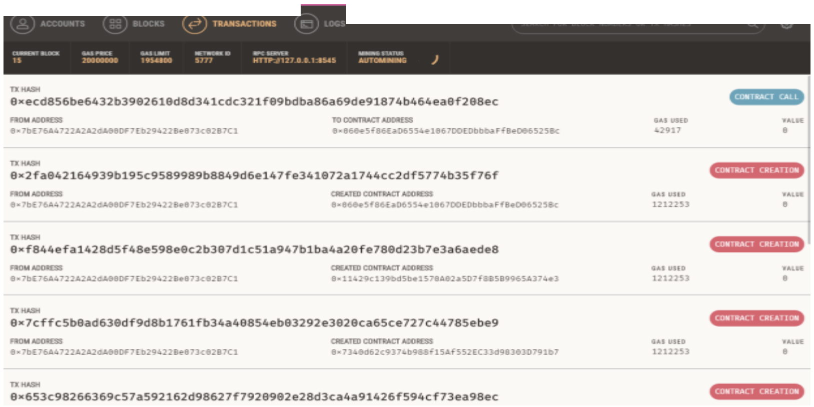


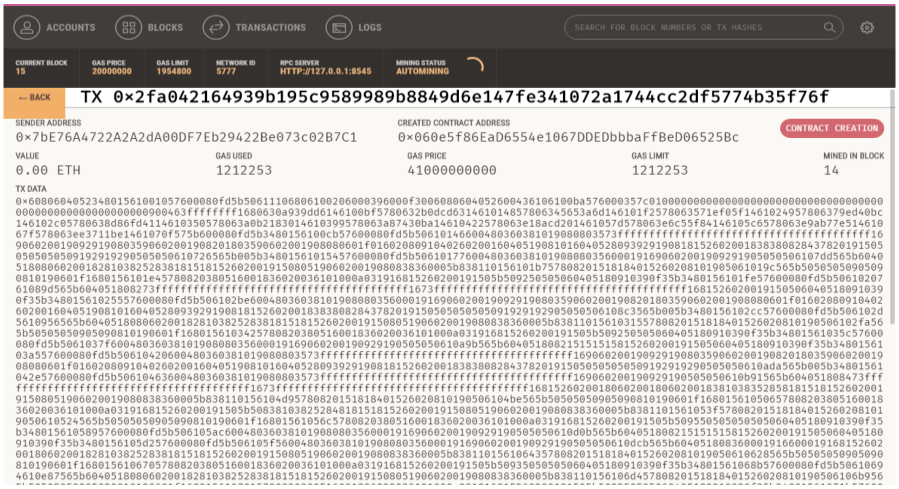
Figure 4.5: Comparison of Decryption time with the Baseline and Proposed Approach



```
CURRENT BLOCK  GAS PRICE  GAS LIMIT  NETWORK ID  RPC SERVER              MINING STATUS
15             20000000   1954800    5777        HTTP://127.0.0.1:8545   AUTOMINING

TX HASH
0×ecd856be6432b3902610d8d341cdc321f09bdba86a69de91874b464ea0f208ec                    CONTRACT CALL
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED  VALUE
0×7bE76A4722A2A2dA00DF7Eb29422Be873c02B7C1   0×860e5f86EaD6554e1067DDEDbbbaFfBeD06525Bc   42917     0

TX HASH
0×2fa042164939b195c9589989b8849d6e147fe341072a1744cc2df5774b35f76f                    CONTRACT CREATION
FROM ADDRESS                                 CREATED CONTRACT ADDRESS                     GAS USED  VALUE
0×7bE76A4722A2A2dA00DF7Eb29422Be873c02B7C1   0×860e5f86EaD6554e1067DDEDbbbaFfBeD06525Bc   1212253   0

TX HASH
0×f844efa1428d5f48e598e0c2b307d1c51a947b1ba4a20fe780d23b7e3a6aede8                    CONTRACT CREATION
FROM ADDRESS                                 CREATED CONTRACT ADDRESS                     GAS USED  VALUE
0×7bE76A4722A2A2dA00DF7Eb29422Be873c02B7C1   0×11429c139bd5be1570A02a5D7f8B5B9965A374e3   1212253   0

TX HASH
0×7cffc5b0ad630df9d8b1761fb34a40854eb03292e3020ca65ce727c44785ebe9                    CONTRACT CREATION
FROM ADDRESS                                 CREATED CONTRACT ADDRESS                     GAS USED  VALUE
0×7bE76A4722A2A2dA00DF7Eb29422Be873c02B7C1   0×7340d62c9374b988f15Af552EC33d98303D791b7   1212253   0

TX HASH
0×653c98266369c57a592162d98627f7920902e28d3ca4a91426f594cf73ea98ec                    CONTRACT CREATION
```

Figure 4.6:Deploy and Interact contracts on Blockchain

Each block has its transaction cost, contract address and hash value, as illustrated in Figure 4.6, with the help of myetherwallet to interact with blockchain. As shown in Figure 4.7, the contract is viewed on the blockchain, which contains the gas limit, gas price, the sender's address, byte code, and almost all the information to store the data. As illustrated in Table 4.3, the gas costs of the parameters which are used in a smart contract are reduced. As illustrated in Figure 4.8, to put the file or data on the IPFS through smart-contract, then gets the unique ipfs code corresponding to the file. Data on IPFS is encrypted, authenticated, confidential, and stored in an encrypted format. To compare proposed and existing approach performance, as illustrated in Figure 4.9, which gives better outcomes in terms of cost and time.



CURRENT BLOCK 15
GAS PRICE 20000000
GAS LIMIT 1954800
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:8545
MINING STATUS AUTOMINING

TX 0×2fa042164939b195c9589989b8849d6e147fe341072a1744cc2df5774b35f76f

SENDER ADDRESS
0×7bE76A4722A2A2dA00DF7Eb29422Be073c02B7C1

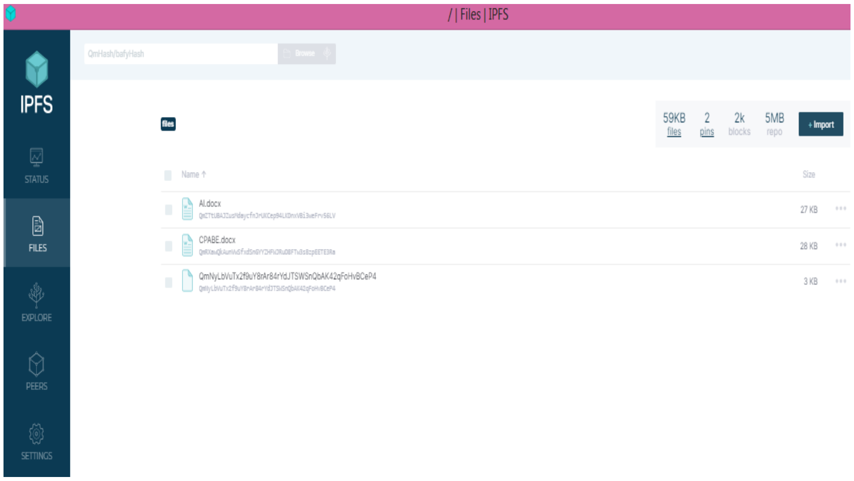
CREATED CONTRACT ADDRESS
0×060e5f86EaD6554e1067DDEDbbbaFfBeD06525Bc

VALUE 0.00 ETH
GAS USED 1212253
GAS PRICE 41000000000
GAS LIMIT 1212253
MINED IN BLOCK 14

TX DATA

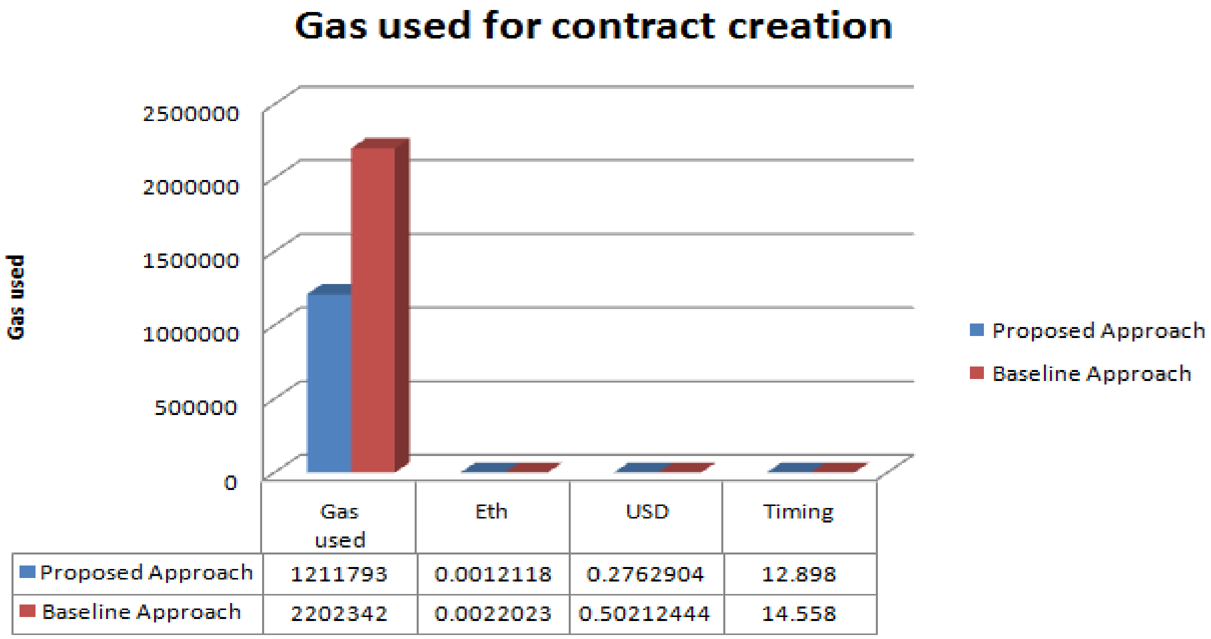
```
0×608060405234801561001057600080fd5b50611106806100206000396000f3006080604052600436106100ba576000357c0100000000000000000000000000000000
00000000000000000000900463ffffffff1680630a939dd6146100bf5780632b0dcd6314610148578063456 53a6d146101f2578063571ef05f1461024957806379ed40bc
146102c05780638d86fd4114610350578063a0b2183014610399578063a87430ba14610422578063e18acd201461057d578063e6c55f84146105c6578063e9ab77e514610
67f578063ee3711be1461070f575b600080fd5b3480156100cb57600080fd5b50610146600480360381019080803573ffffffffffffffffffffffffffffffffffffffff16
906020019092919080359060200190820180359060200190808060 1f0160208091040260200160405190810160405280939291908181526020018383808284378201915 05
05050505091929192905050506107 26565b005b34801561015457600080fd5b50610177600480360381019080803560001916906020019092919050505061 07dd565b6040
518080602001828103825283818151815260200191508051906020019080838360005b838110156101b7578082015181840152602081019050610 19c565b5050505090509
0810190601f1680156101e4578082038051600183602003610100 0a031916815260200191505b5092505050604051809103 90f35b3480156101fe57600080fd5b50610207
61089d565b604051808273ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200191505060405180910 39
0f35b34801561025557600080fd5b506102be6004803603810190808035600019169060200190929190803590602001908201803590602001908080601f01602080910402
60200160405190810160405280939291908181526020018383808284378201915050505050509192919290505050610 8c3565b005b3480156102cc57600080fd5b506102d
5610956565b604051808060200182810382528381815181526020019150805190602001908083836000 5b838110156103155780820151818401526020810190506102fa56
5b50505050905090810190601f168015610342578082038051600183602003610100 0a031916815260200191505b50925050506040518091039 0f35b34801561035c57600
080fd5b5061037f6004803603810190808035600019169060200190929190505050610a9b565b604051808215151515815260200191505060405180910390f35b34801561
03a557600080fd5b50610420600480360381019080803573ffffffffffffffffffffffffffffffffffffffff169060200190929190803590602001908201803590602001 9
08080601f0160208091040260200160405190810160405280939291908181526020018383808284378201915050505050509192919290505050610ada565b005b34801561
042e57600080fd5b50610463600480360381019080803573ffffffffffffffffffffffffffffffffffffffff169060200190929190505050610b91565b604051808473fff
fffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200180602001806020018381038352858181518152602001
9150805190602001908083836000 5b838110156104d957808201518184015260208101905061 04be565b505050509050908101906 01f168015610506578082038051600 18
36020036101000a031916815260200191505b508381038252848181518152602001915080519060200190808383600005b8381101561053f57808201518184015260208101
9050610524565b50505050905090810190601f16801561056c5780820380516001836020036101000a031916815260200191505b509550505050505060405180910390f35
b34801561058957600080fd5b506105ac600480360381019080803560001916906020019092919050505061 0d0b565b604051808215151515815260200191505060405180
910390f35b3480156105d257600080fd5b506105f5600480360381019080803560001916906020019092919050505061 0dcb565b604051808360001916600019168152602 602
00180602001828103825283818151815260200191508051906020019080838360005b83811015610643578082015181840152602081019050610628565b505050509050 90
810190601f16801561067057808203805160018360200361010 00a031916815260200191505b5093505050506040518091039 0f35b34801561068b57600080fd5b5061069
4610e87565b604051808060200182810382528381815181526020019150805190602001908083836000 5b8381101561 06d4578082015181840152602081019050610 6b956
```

Figure 4.7: Contract details on Blockchain



Name ↑	Size
AI.docx QmZTtUBAJZusMdaycfnJrUKCep94LKDnxVBi3weFrv56LV	27 KB
CPABE.docx QmRXawQkAunVwSfxdSnGYYZHFWJRuD8FTw3sBzpEETE3Ra	28 KB
QmNyLbVuTx2f9uY8rAr84rYdJTSWSnQbAK42qFoHvBCeP4 QmNyLbVuTx2f9uY8rAr84rYdJTSWSnQbAK42qFoHvBCeP4	3 KB

Figure 4.8: Files on IPFS in encrypted form



	Gas used	Eth	USD	Timing
🟦 Proposed Approach	1211793	0.0012118	0.2762904	12.898
🟥 Baseline Approach	2202342	0.0022023	0.50212444	14.558

Figure 4.9: Comparison of Gas Used During Contract Creation with the Proposed and Functional Approach

Table 4.3: Gas costs among diverse operations is used in CP-ABE (Gasprice=1gwei, and 1 Eth=228 USD)

Parameter	Contract Creation	set hash	Set cipher	Set secret key	Set Time	Get Time	Get secret key
Gas Used	1211793	84545	46161	44852	44848	43049	27961
Eth	0.0012118	0.0000845	0.0000462	0.0000449	0.0000448	0.000043	0.000028
USD	0.276290	0.019266	0.0105336	0.0102372	0.0102144	0.009804	0.006384

4.7 Summary of the chapter

In the present era, concerns about data security and privacy have escalated significantly. Many approaches are proposed to eliminate issues like centralization, authenticity, efficiency, and complexity to maintain privacy and security. In this work, the CP-ABE blockchain-based encryption technique is proposed to secure the data in the untrusted environment by employing IPFS cloud storage to minimize user effort. The decentralized approach of this work reduces the encryption and decryption time by 23% and 37% respectively when compared with the existing approach. The proposed approach helps to eliminate many attacks which are possible due to the high computational complexity of algorithms.

CHAPTER 5
USER AUTHENTICATION IN INDUSTRIAL APPLICATIONS THROUGH BLOCKCHAIN

Several industries improve the data security that may lead to several issues as user's authenticity and latency. To use the user authentication approach to improve the data security.

5.1 Introduction

Many industries want to enhance the privacy of their transferred data. The Industrial applications [130] continue to grow inside or outside so data moves from one place to another. Kevin [131] designed the industrial application that describes the network in a uniquely identified that can transfer data without a human interface. Many researchers have already used diverse approaches as reputational systems, attribute-based schemes, multi-authority ciphertext policy, and deep learning to secure the data from unauthorized users is a challenge.

Blockchain technology developed in 2008 [12] that is famous for its feature as transparency, security, privacy, immutability, and decentralization. It is a distributed database that preserves the privacy of data, and endlessly growing transactions in an orderly way across multiple computers.

Many researchers proposed approaches with blockchain in industrial applications for better data protection. The data precautions and scalability approach in IIoT applications [132] that is integrated with the blockchain but some issues are present as data security, storage, and authenticity. So, to increase the data security in industrial applications it depends on the user's authentication [133]. The dispute is that when numbers of users increased then turn down the user's authenticity and increases the latency. However, to reduce these existing issues to propose a hybrid authentication approaches to increase the authenticity of users. In crowdsensing applications used the public key infrastructure and elliptic curve cryptosystem approaches for users via Tao et al. [134] anonymous authentication scheme has been developed. Wang et al. [135] developed a blockchain-integrated transfer learning strategy in industrial applications to improve the data security. Most of the data is transferred outside so that the security of users and data remains a concern. InterPlanetary File System (IPFS) [136] is a narrative technology that stores and transfers the data in a dispersed way to store a large amount of data their needs a cloud server. This paper [137] eliminates the issues related to data security to enhance the system performance and secure the data from unauthenticated users in industrial applications.

Therefore, to propose a blockchain-integrated authentication approach that reduces the existing issues. The proposed approach enhanced the user's authentication where data can access with authenticity and reduced the latency and uploaded into the IPFS server.

5.1.1 Objectives and Contributions:

The proposed approach eliminates the issues that are authenticity, system throughput, and latency in industrial application. Here, the contributions of this work are given below:

- The blockchain technology integrated with the user authentication mechanism that solves the single point of failure, user's authenticity, and latency. The proposed mechanisms are combinations of public key infrastructure (PKI) and elliptic curve cryptosystem (ECC) where PKT makes the functions of the IIoT systems as well as the ECC to generate and manage the keys respectively.
- The outcome demonstrates that our plan outperforms the current methodology to enhance the system throughput.
- The IPFS cloud stores the data through contract that is a decentralized technology and stored data is secure, authenticate, confidential and enough storage space.

5.2 Related Work

Nowadays, more awareness has been given to secure the IIoT applications through the authentication mechanisms. Many authors proposed a diverse approaches to enhance the data security, authentication, traceability, scalable, storage space, cost and confidentiality in IIoTs. Liu et al. [38] presented a blockchain-based anonymous reputation framework in IIoT application which increased the transparency, decentralized, reliability and tamperproof. Zhao et al. [138] projected a blockchain enabled key enabling technology in industrial applications that provides the security and traceability of data. Kumar et al. [139] presented a Blockchain-enabled edge computing system that reduces the latency, power consumptions, increased the security and trust in IIoT applications. Furthermore, needs to optimize cost, improves the performance in industrial applications in the future. Huang et al. [140] projected a blockchain-integrated chameleon hash which reduced the existing approach issues such as centralized, computation, authentication, and security in industrial applications but further needs to improve. Sharma et al. [141] proposed a deep learning enabled with blockchain in IIoT applications that helps to remove some issues as centralized security, efficiency so that needs to work in this field in future. Yu et al. [142] proposed a blockchain integrated bilinear Diffie-hellman approach in IIoT that helps to remove some issues such as data security, track the users and revoke the malicious users. Huang et al. [143] proposed a credit-based consensus system to assure openness, safety, single point of failure in industrial applications as storage space, and data confidentiality in industrial applications. A blockchain integrated IIoT applications that are proposed by Wan et al. [144] to create a secure system. Vishwakarma et al. [145] recommended a blockchain-enabled authentication method for IoT applications which incorporates the elliptic curve digital signature with sophisticated encryption standard techniques. To [146, 147] propose learning and optimization technique that improved the reliability and scalability of industrial data. Lorenzo et al. [148] suggested a blockchain-integrated access system in the industrial internet of things (IIoT), that provides the confidentiality, adaptability, and reliability in data, but throughput, latency are the issues. Jia et al. [149] suggested a blockchain-integrated aggregation method that combined with homomorphism encryption and federated learning approach for industrial data protection. Qiu et al. [150] projected a blockchain integrated dueling deep q-learning scheme in IIoTs to enhance the confidence, and throughput. To proposed a blockchain-integrated verification cryptographic method [151, 152] that improves the security of data in IIoTs. Singh et al. [153, 154] proposed a blockchain integrated novel credential protocol and user authentication approach that improves the user’s integrity. Mu et al. [155] developed a blockchain-based user privacy solution in mobile edge computing, which reduced operations complexity and burden while increasing user privacy. Kostal et al. [156] proposed homomorphic encryption approach that secures the identity of voters in voting system. Feng et al. [157] projected a decentralized privacy enhancement approach that improves the users and systems security.

To propose a user authentication scheme and a decentralized IPFS cloud server for data storage in industrial applications that is the combination of PKI and ECC. The IPFS (InterPlanetary File System) contributes and locations the data in a disseminated file system. The proposed approach shows the results in authenticity of users, latency and throughput of the system.

5.3 Overview of User Authentication Approach

The data privacy becomes a main concern that dependents on reliability of users in industrial applications that eliminates the existing issues. To propose a user authentication approach that is combination of PKI and ECC in industrial. PKI registered the users and corresponding to that provides a digital certificate for a valid time whereas, ECC manage the certificates and keys respectively.

There are some issues occurred in PKI if users are rapidly increases as maintains certificate and key that is solved by ECC algorithm. Elliptic Curve Cryptograhy is a mathematical based cryptography developed in 1985 by Neal and Victor. As shown in Figure 5.1, the proposed approach includes several step by step processes in industrial applications.

Firstly, registration of the users and corresponding to that receives a certificate, whereas blockchain verified the authenticity of users, and then communicate through the industrial applications. If users want to enter without registration that is not possible so it provides the authenticity.

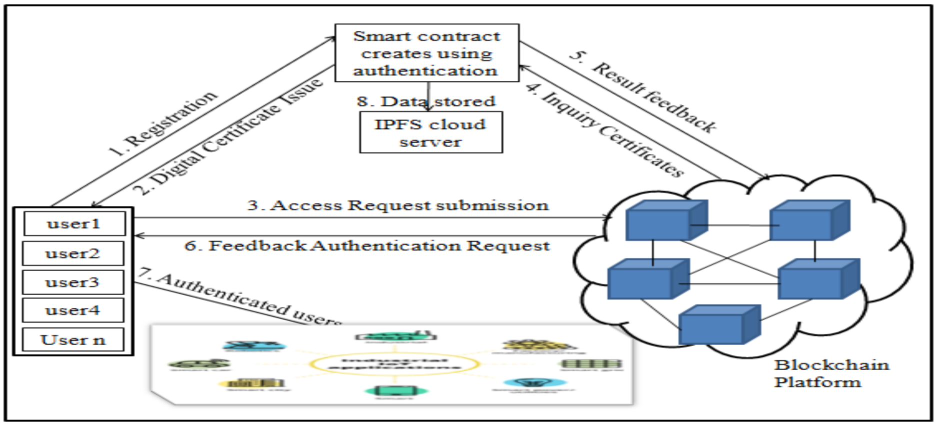


Figure 5.1: The Proposed User Authentication Approach

The proposed approach includes all the necessary components as users, blockchain, CA, key management centre [134], and IPFS server in the cloud. However, the entire proposed method is straightforward, secure, and includes all requirements for authentication in IIoT applications. The main works of these entities are designed:

- **Registered Authority:** This entity issued through the certificate authority that is trusted in IIoT applications.

- **Certificate Authority:** It is the most important and trustworthy component of the proposed approach. Furthermore, it provides a digital signature that combines the user's public key.
- **Key Management:** It is also a critical component of the proposed approach that generates and manages the key via ECC.
- **Blockchain Platform:** The contract is secure because all activities are recorded into blockchain.
- **IPFS cloud:** Large amount of data can be uploaded into it with authenticity, security, and confidential.

The proposed user authentication scheme gives services as authenticity, integrity and confidentiality.

- **Authenticity**: In industrial applications to provide the authentication of users, that carefully obtains the digital certificates and key pairs.
- **Integrity**: Blockchain technology is employed to make sure that user's data cannot be tampered with by third parties.
- **Confidentiality:** The key pairs are generated using ECC.

5.4 Flow Chart of User Authentication Approach

As shown in Figure 5.2, is the flow chart of proposed approach to overcome the existing issues of users.

1. A smart contract is created using PKI and ECC approaches.
2. If there are some ethers then compiles the contract otherwise can't compile.
3. Number of users participates in IIoT applications only authorized users are permitted to connect with industrial applications.
4. To deploy and interact the contract via Myetherwallet on the blockchain, after than no one can corrupt the data.
5. The smart contract stored on the decentralized IPFS cloud storage that returns a unique ipfs code corresponding to file.

6. The registration of the users through the registered authority as shown in Algorithm 5.1 with their address, and public key that is a trusted entity and created by certificate authority.
7. The certificate authority gives the digital certificate for a valid period.
8. Check the certificate, if it is valid after that give the permission to users to link the industrial applications.
9. To authenticate the users using the proposed approach and makes the key pairs to provide the integrity, non-repudiation, confidentiality, and authenticity of IIoT users.

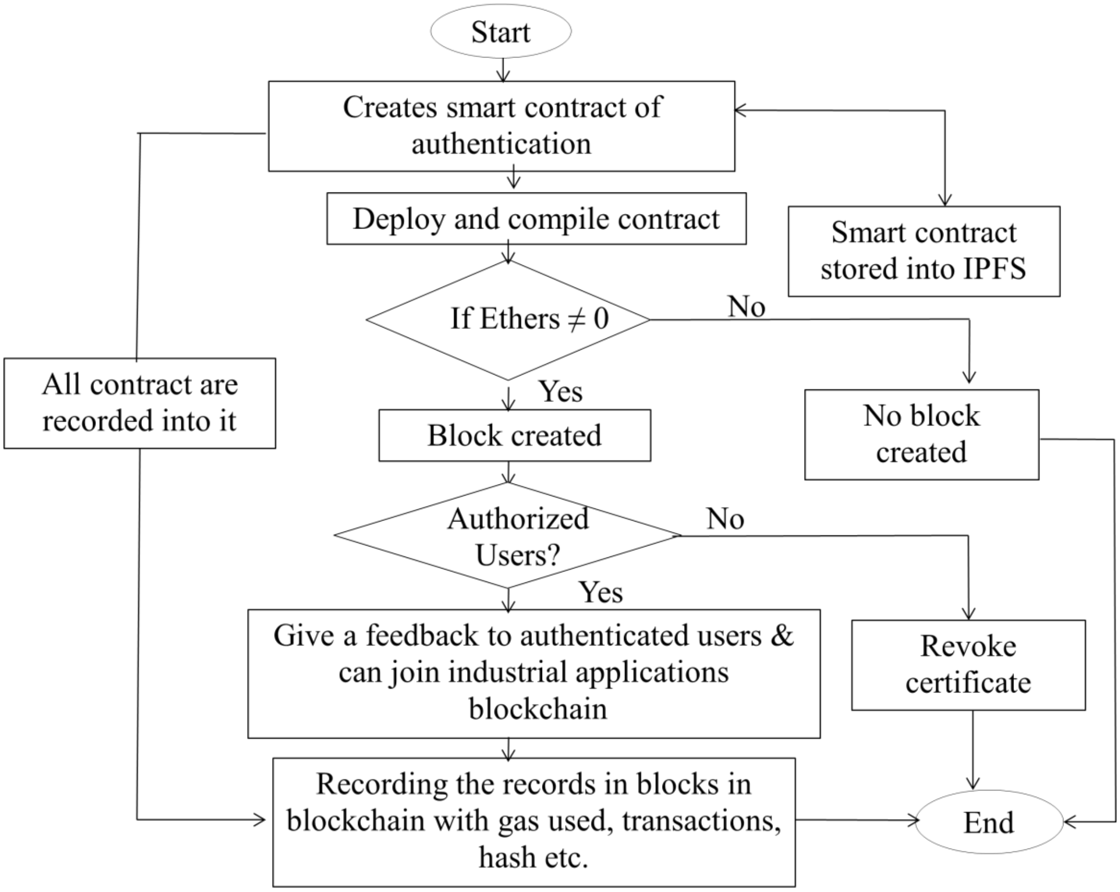

Start
Creates smart contract of authentication
Deploy and compile contract
Smart contract stored into IPFS
If Ethers ≠ 0
No
Yes
All contract are recorded into it
Block created
No block created
Authorized Users?
No
Yes
Give a feedback to authenticated users & can join industrial applications blockchain
Revoke certificate
Recording the records in blocks in blockchain with gas used, transactions, hash etc.
End

Figure 5.2: Flow chart of the User Authentication Approach

To produce the key pair for users is over a restricted field that satisfies the equations like that:

$x^3+ax+b \text{ (mod p)} = y^2 \text{ (mod p)}$ (33)

Satisfy the given equation

$4a^2+27b^2 \text{ != } 0 \text{ mod p}$ (34)

Table 5.1: The Proposed Approach Notations with explanations

Notations	**Explanations**
CA	To provide certificates to IIoT users or others
Solidity	Using the programming tool Solidity
My ether wallet	The wallet is used to deploy and interact with blockchain contracts.
Blockchain	Using the blockchain of Ethereum
RA	Registered authority of IIoT users or other entities
users	Number of users in IIoT.
Expiry	validity of the digital Certificates
revoke	In IIoT applications, if users don't act correctly, the CA should invalidate their signature
$x^3+ax+b \pmod{p} = y^2 \pmod{p}$	Using the equation, ECC
p	Prime (256 bit) number
a, b	The constants are: a and b
d	Users' unique key
k	Choose [1, n-1] random integers.
g	Generator in elliptic curve
h	Co-factor in elliptic curve
q	IIoT users' unrestricted keys

Algorithm 5.1: Create Contract of Public key Infrastructure (PKI) for Industrial Applications [134]

Inputs: number of Entity used in industrial, RA, CA, Root CA, Signature, number of users (as exposed in Table 5.1)

Output: validate users can communicate within the industrial applications.

```
1. By adding the trustworthy entity address and public key, users were registered in the IIoT.
    returns the entity id
      Every time entity id of users=entity id+1
          When you call the users with the entity id, then
            results in the entity id, level, and public key
        when linked the data with the ipfs
            results of certificate unique id
 A trustworthy authority signs alongside the owner's address, as well as the certificate's id & expiration date
            results sign id
  End the registered procedure or
  If users already registered, then
      evaluate the certificate id and expiration date
         if true then
              authenticated users in IIoT (gives the permission)
         else
              malicious users  (not give the permission)
2. Root certificate authority contains the address of certificate authority.
3. If a user doesn't act appropriately,
    revoke the signature of an authorized party.
```

The basic operations of ECC are the adding and doubling the points [158] as shown in Algorithm 5.2. And, m takes as a scalar point during multiplication to improve the efficiency. Takes the points on ECC are P, Q, R, whereas specified the P(x, y) curve point. And it computes k*P, a series, and the P points doubled. Let's consider P(x_1, y_1) to determine the point's doubling (2P). The curve at the location P is then calculated using the equation:

$T= ([(3x_1^2+1)/2y_1] \bmod p)$ (35)

After that, 2P coordinates of curve on R point (x_2, y_2)

$x_2= ((T^2-2x_1) \bmod p)$ (36)

$y_2= ([T(x_1-x_2)-y_1] \bmod p)$ (37)

To get 3P, we add points P and 2P, with 2P equaling Q. In this case, P has coordinates (x_1, y_1), whereas Q=2P has variables (x_3, y_3). The slope is now:

$T = [(y_3- y_1) / (x_3 – x_1)] \bmod p$ (38)

P+Q=-R

$x_2 = (T^2 – x_1 – x_3) \bmod p$ (39)

$y_2 = (T (x_1 – x_2) –y_1] \bmod p$ (40)

Due to this, we apply doubling and adding based on an order of operations chosen for 'k'. Each point (x_2, y_2) on the elliptic curve is assessed by doubling or adding points. When sign a message first of all calculates the message hash value h (m). Signature is computed using (r, v), whereas r=x modulo n and v=inverse k (m + rd).

Algorithm 5.2: Create Smart Contract of Elliptic Curve Cryptography (ECC) for Industrial Users [134]

```
Inputs: Using the ECC equations $x^3+ax+b \pmod p = y^2 \pmod p$
Output: Public and private key pairs
1. In addition, the constant values are a=0 and b=7
    p= prime 256-bit number
   g= Generator in elliptic curve
   (Cofactor) h = 1 in elliptic curve
   n is the number of points produced in the subgroup
2. Resolve the provided the formula
       $4a^2+27b^2 != 0 \bmod p$
3. Saves the address of the root certificate authority and all addresses need not be saved
4. Identifies P, Q, and R be the three distinct curve points.
```

```
5. The key pairs for both public and private keys
      Key-pairs = $[q, d]$
  private key $(d) = k \in [1, n-1]$   ($\in$ indicates the ‘ belong to’ )

      $q = d *g$   // Anywhere on the EC
                   // The generating point of EC is g.
                   // The confidential key is d.
                   // The unrestricted key is q
  cipher text = $[k*g, P(m)+k*q]$  // The encoded message is P(m)
                                   // The random positive integer decryption is referred to as k.
Let $k*g$ be the initial point and
            $P+ (k* q)$ be the subsequent concept
            $d*k*g = d*$ initial point;
            compute $P = P(m) + k*q – d*k*g$;
            So receives the original message
```

5.5 Parameter Setting

The authors analyzed the authenticity and latency of users, and system throughput of the proposed approach in industrial applications. As illustrated in Table 5.2, numbers of users are participated in IIoTs 100 to 1000, and several parameters as described in Table 5.2 are used to simulate the scenario with the existing work [135].

5.6 Experimental Outcomes

The users authenticity of the proposed, and reinforcement approach [135] is compared in this section. The proposed approach employs user authentication mechanisms as a combination of PKI and ECC. The performance of this work is evaluated by measuring the authenticity accuracy of users, latency, and system throughput. As illustrated in Figure 5.3, to give the information of all the operations gas costs in Table 5.3 that is used in industrial applications.

Table 5.2: Setting the Simulation Parameters

Parameters	Values
CA	0xac8899634aacb95c203366b36b08bfc81c530b6387ofc907af92602d691fdab
RA	0xae293b8f77fe5ebcb235e787cfc286e8455139cad7f19f5a9cadcfb83df6e9f5
IPFS	QmYvbqzZh2YDkbQCfELqJm46HLLo3WHEkQyib1MytMQsit
p	0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC2F
g	0x483ADA7726A3C4655DA4FBFFC0E1108A8FD17B448A68554199C4708FFB10D4B8
Users	[100 1000]
Expiry	365 days
a	0
b	7
d	k ∈ [1, n-1] (∈ indicates the ‘ belong to’)
k	[1, n-1]
h	1
q	d*g
Pair of keys	(q, d)

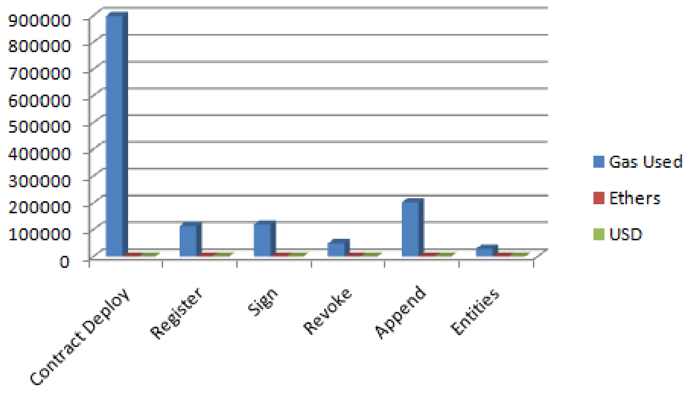


Figure 5.3: Gas used in Proposed Approach

Throughput: As illustrated in Figure 5.4 if numbers of transactions are processed in which time speed then calculate the throughput:

Throughput= number of transactions/time (41)

Latency: As illustrated in Figure 5.5, the transaction latency should be reduced then improves the system capacity. All transactions demonstrate the several things such as gas limit, gas price, contract address, nonce, and last transaction time. To calculate the delay time through the previous and current times, then calculate the latency:

Latency = current time- previous transaction time (42)

Accuracy: As illustrated in Figure 5.6, calculate the authentication user's accuracy. Assume that the possibility of unauthenticated users is equal to the number of users then

Accuracy= (1-(1/ number users)) (43)

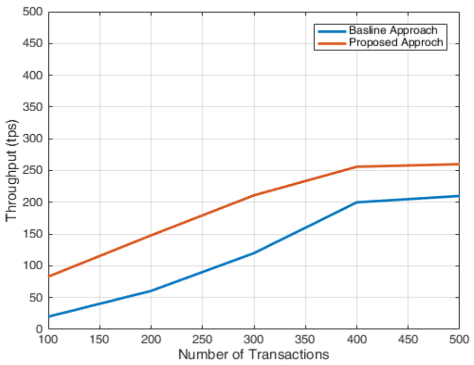


Figure 5.4: Comparison of Throughput with the Baseline and Proposed Approach

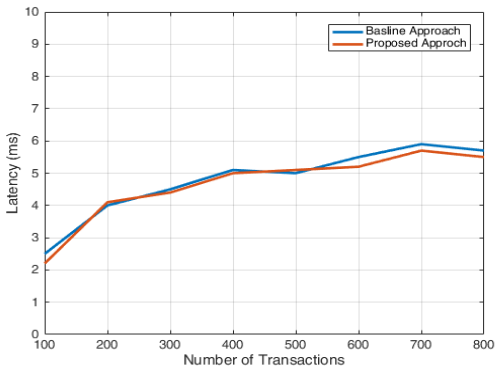


Figure 5.5: Comparison of Latency with the Baseline and Proposed Approach

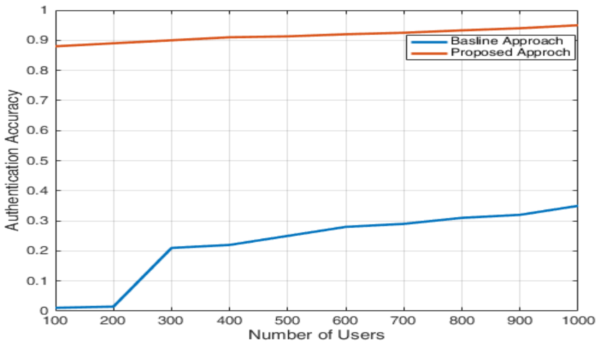
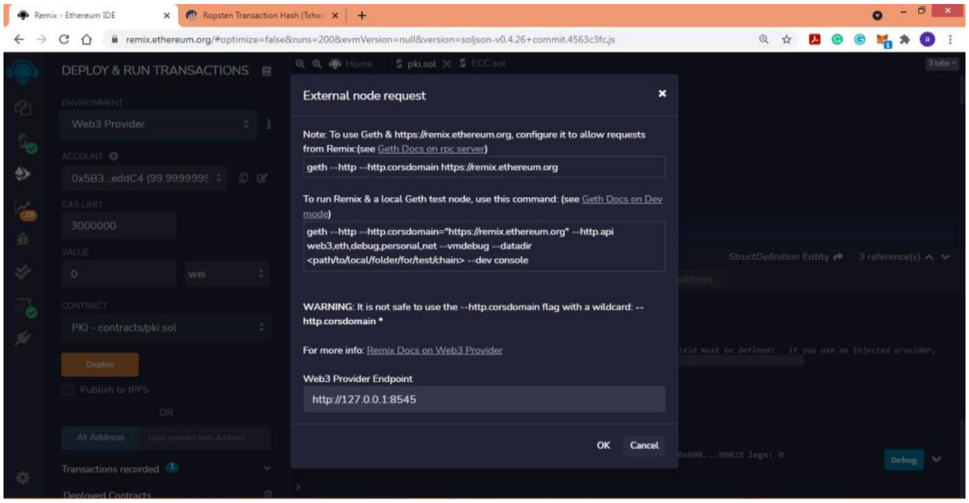


Figure 5.6: Comparison of Authentication Accuracy with the Baseline and Proposed Approach

As illustrated in Figure 5.7, to connect the smart contract of proposed user authentication approach with the blockchain in industrial applications. Only the authenticated users can interact with the other users, and IIoT system, whereas, user tried to misbehave then revoke certificate immediately. The smart contract can interact with blockchain where all the activities of users are recorded into it that is illustrated in Figure 5.8. As illustrated in Figure 5.9, the smart contracts stored onto the IPFS blockchain based decentralized cloud server and also gives a prefix code that begins from Qm. The performance of the proposed approach gives the better outcomes when compared to existing approach.



External node request

Note: To use Geth & https://remix.ethereum.org, configure it to allow requests from Remix:(see Geth Docs on rpc server)

```
geth --http --http.corsdomain https://remix.ethereum.org
```

To run Remix & a local Geth test node, use this command: (see Geth Docs on Dev mode)

```
geth --http --http.corsdomain="https://remix.ethereum.org" --http.api
web3,eth,debug,personal,net --vmdebug --datadir
<path/to/local/folder/for/test/chain> --dev console
```

WARNING: It is not safe to use the --http.corsdomain flag with a wildcard: --http.corsdomain *

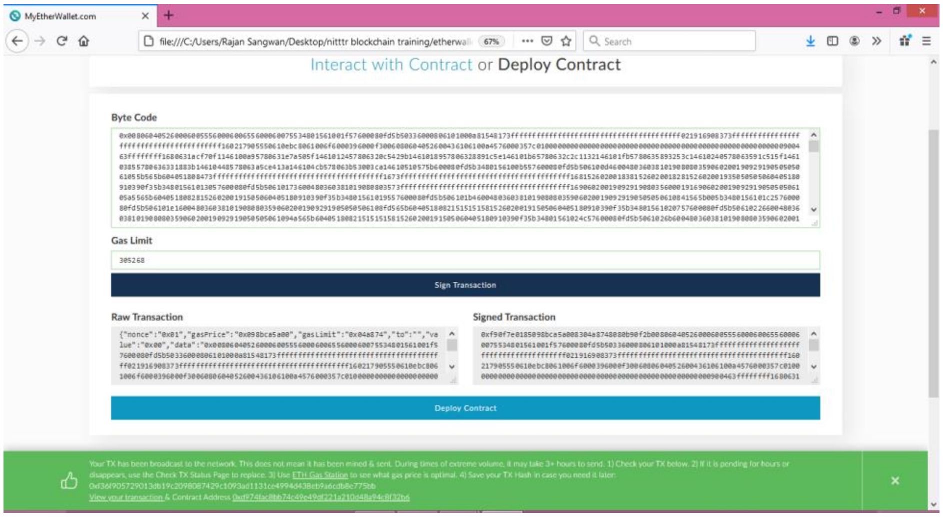
For more info: Remix Docs on Web3 Provider

Web3 Provider Endpoint

http://127.0.0.1:8545

OK Cancel

Figure 5:7 Solidity contract connected with Blockchain


MyEtherWallet.com
file:///C:/Users/Rajan Sangwan/Desktop/nitttr blockchain training/etherwall
67%
Search
Interact with Contract or Deploy Contract
Sign Transaction
Deploy Contract

Byte Code

0x008060405260006005556000600655600060075534801561001f57600080fd5b503360008061010000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffff
ffffffffffffffffffffffff16021790555061 0ebc8061006f6000396000f3006080604052600436106100a4576000357c0100000000000000000000000000000000000000000000000000000000900 4
63ffffffff1680631acf70f1146100a957806 31e7a505f14610124578063 20c5429b1461018957806328891c5e146101b65780632c2c1132146101fb5780635893253c146102405780635391c515f1461
0385578063 6331883b146104485780 63a5ce413a146104cb5780 63b53003ca14610510575b600080fd5b348015610 0b557600080fd5b5061 00d460048036038101908080359060200190929190505050
61055b565b60405180 8473ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff1681526020018381526020018281526020019350505050604051 80
910390f35b348015610130576000 80fd5b50610173600480360381019080803573ffffffffffffffffffffffffffffffffffffffff16906020019092919080356000191690602001909291905050 5061
05a5565b604051808281526020019150506040518091039 0f35b34801561019557600080fd5b506101b46004803603810190808035906020019092919050505061 084156 5b005b34801561 01c2576000
80fd5b506101e16004803603810190808035906020019092919050505061 08fd565b60405180821515151581526020019150506040518091039 0f35b348015610207576000 80fd5b506102266004 8036
0381019080803590602001909291905050506 1094a565b6040518082151515158152602001915050604051809103 90f35b348015610 24c576000 80fd5b50610 26b6004803603810190808035906 02001

Gas Limit

305268

Raw Transaction

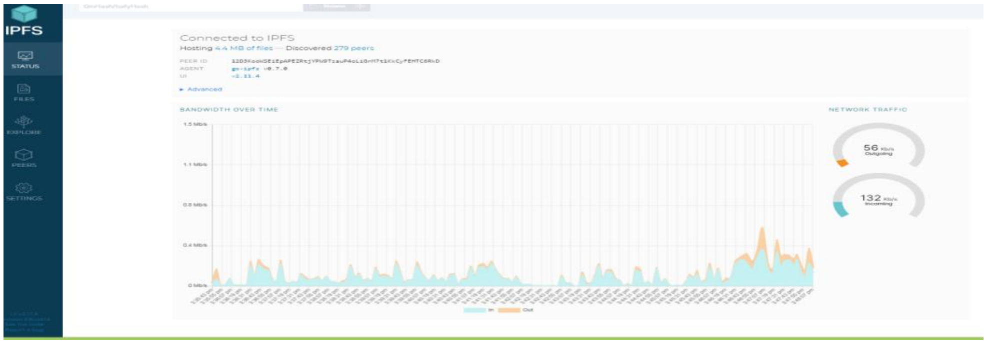
{"nonce":"0x01","gasPrice":"0x098bca5a00","gasLimit":"0x04a874","to":"","va
lue":"0x00","data":"0x008060405260006005556000600655600060075534801561001f5
7600080fd5b503360008061010000a81548173ffffffffffffffffffffffffffffffffffffff
ff021916908373ffffffffffffffffffffffffffffffffffffffff16021790555061 0ebc806
1006f6000396000f3006080604052600436106100a4576000357c010000000000000000000

Signed Transaction

0xf90f7e0185098bca5a0083 04a8748080b90f2b008060405260006005556000600655 6000 6
0075534801561001f57600080fd5b5033600080610 1000a81548173ffffffffffffffffff
ffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff160
217905550610ebc8061006f6000396000f30060806040526004361061 00a4576000357c0100
000000000000000000000000000000000000000000000000000000000900463ffffffff1680631

Your TX has been broadcast to the network. This does not mean it has been mined & sent. During times of extreme volume, it may take 3+ hours to send. 1) Check your TX below. 2) If it is pending for hours or disappears, use the Check TX Status Page to replace. 3) Use ETH Gas Station to see what gas price is optimal. 4) Save your TX Hash in case you need it later:
0xf36f905729013db19c2098087429c1093ad1131ce4994d438eb9a6cdb8e775bb
View your transaction & Contract Address 0xd974fac8bb74c49e49df221a210d48a94c8f32b6

Figure 5.8: The smart contract is deployed on the Blockchain using the wallet



Connected to IPFS
Hosting 4.4 MB of files — Discovered 279 peers

PEER ID 12D3KooWSEiEpAPEZRtjYPW9TzauP4oLiGnM7t1KkCyFEHTC6RkD
AGENT go-ipfs v0.7.0
UI v2.11.4

► Advanced

Figure 5.9: Smart contract are uploaded into IPFS cloud

Table 5.3: Gas used in Authentication Approach

(Gas=1gwei, 1 Ether= 228 USD)

Parameters	**Contract Deploy**	**Register**	**Sign**	**Revoke**	**Append**	**Entities**
Gas Used	896902	113218	118061	48463	202150	28500
Ethers	0.00089	0.00011	0.00012	0.000048	0.00020	0.00003
USD	0.20292	0.02508	0.02736	0.010944	0.0456	0.00684

5.7 Summary of the chapter

This chapter presents a user authentication mechanism that is a combination of PKI and ECC algorithms to enhance the systems throughput, improves the user's authenticity, and reduced the latency using blockchain technology in industrial applications. Every time checks the authentication of users if not authorized then revokes the certificate immediately and stops the interface with IIoTs.

The performance demonstrates that proposed approach is superior to the existing approach that increased the systems throughput and users authenticity upto 73% and 93% respectively, and reduced the latency upto 6.77% in industrial applications. The attackers became very smart that can implement another method to breach the user's authenticity, so can be further extend this approach.

CHAPTER 6
CONCLUSION AND FUTURE SCOPE

Blockchain technology is decentralized, immutable, security, privacy, anonymous, confidential, and transparent. This work is concentrated on the security of the network in different phases along with various applications.

The first chapter of the thesis provides the fundamental knowledge of blockchain technology along with its types and also discussed the architecture of blockchain with its benefits, applications, problem statements and research objectives.

The chapter second is described the literature review in different network phases as device, data, and user to concern the security in different applications.

The third chapter of the thesis focuses on the primary goal of employing blockchain technology to protect the Internet of vehicles (devices) by using incentive mechanisms. DPSO and MITA incentive approaches are used in which a number of miners participate, but miners are selected on the basis of high data quality, trust through the MITA approach. Further, the selected miners verify and validate the block by using the DPSO when several blocks are present. The miners get a reward for validating the blocks and at the same time if their behavior is not appropriate then a great penalty can also be imposed. The proposed approach illustrate the better result in quality, enhance the detection rate of malevolent nodes, increase trust, and decrease the DoS attack and compromised miners as compared to existing approach.

The fourth chapter of the thesis is discussed a major goal of employing blockchain technology to secure data transmission and storage using the CP-ABE (ciphertext policy attribute-based encryption) and IPFS storage server. The encryption and decryption time is reduced, so the possibility of eavesdropping and man-in-middle attacks can be reduced. The outcome illustrates that the proposed approach has better performance compared to the existing approach that demonstrated through simulation.

The fifth chapter focuses on the objective in user phase through blockchain in industrial applications with PKI (Public Key Infrastructure) and ECC (elliptic curve cryptography) techniques. PKI gives the electronic certificate only to the legitimate users after registration, whereas ECC distributes and manages the keys. If the user misbehaves, then immediately revoke its certificate and disconnects the users from the industrial applications. The performance of the proposed approach is found to be better than the existing approach. in case of throughput, user accuracy, and authentication.

The sixth chapter of the thesis gives the summary of all the chapters and also discussed the conclusion and future work.

6.1 Conclusion

In the present era, concerns about data, device and user's security and privacy have escalated significantly. Many approaches are proposed to eliminate issues like centralization, authenticity, efficiency, and complexity to maintain security.

To propose incentive mechanisms that is a combination of DPSO and M-ITA algorithms to verify miners and blocks using blockchain technology in vehicular networks. The vehicles on the road share a lot of information through communication that ensures driver safety and service quality. The DPSO algorithm validates the block whereas the MITA algorithm to check the miner's is trustworthiness. The proposed work increased the trust and utility of miner's upto 65% and 20% respectively whereas the compromised miners are reduced upto 44%.

A CP-ABE blockchain-based encryption technique is proposed to secure the data in the untrusted environment by employing IPFS cloud storage to minimize user effort. The decentralized approach of this work reduces the encryption and decryption time by 23% and 37% respectively when compared with the existing approach. The proposed approach helps to eliminate many attacks which are possible due to the high computational complexity of algorithms.

A user authentication mechanism that are a combination of PKI and ECC algorithms to enhance the systems throughput, improves the user's authenticity, and reduced the latency using blockchain technology in industrial applications. Every time checks the authentication of users if not authorized then revokes the certificate immediately and stops the interface with IIoTs.

The performance demonstrates that proposed approach is superior to the existing approach that increased the systems throughput and users authenticity upto 73% and 93% respectively, and reduced the latency upto 6.77% in industrial applications. Some of the applications like IoTs, mobile crowdsensing, industrial, and healthcare where the proposed approach more efficiently used as compared to existing approaches.

6.2 Future Scope

This work can be extended as followings:

- Devices are rapidly increasing in various applications with different capacity in terms of computation and power then the security of devices can be ensured with better optimized approaches.
- Blocks are getting increases in the network, therefore, the Holochain technology can be used to reduce the complexity issues in the future.

References

[1] K. Ashton, “That Internet of Things thing, “RFID, Jun 2009.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system, “2008.

[3] https://www.ibm.com/in-en/topics/what-is-blockchain.

[4] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter, “ACMSIGSAC Conf. Comput. Commun. Secur, pp.254-269, 2016, doi: http://dx.doi.org/10.1145/2976749.2978309.

[5] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, “Blockchain challenges and opportunities A survey, “International Journal of Web and Grid Services, vol. 14, no. 4, pp.352-375, 2016.

[6] N. Mohamed and J. AI-Jaroodi, “Applying blockchain in industry 4.0 applications, “2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 14 March, 2019, doi: 10.1109/CCWC.8666558.

[7] F. Tschorsch and B. Scheuermann, “A technical survey on decentralized digital currencies, “IEEE Communications Surveys & Tutorials, 2 March, 2016, vol-18, issue-3, thirdquarter, pp.2084-2123

[8] P. McCorry, S. F. Shahandashti, and F. Hao, “A smart contract for boardroom voting with maximum voter privacy, “International Conference on Financial Cryptography and Data Security, Springer, Switzerland, pp.357-375, 2017.

[9] K. Rabah, “Challenges & opportunities for blockchain powered healthcare systems a review, “Journal Medicine Health Science, vol-1, issue-1, pp.45-52, 2017.

[10] F. Lombardi, L. Aniello, S. Angelis, A. Margheri, and V. Sassone, “A blockchain-based infrastructure for reliable and cost-effective IoTaided smart grids, “Living Internet Things Cybersecurity IoT, isbn: 978-1-78561-843-7, pp. 1-6, March 2018, DOI: 10.1049/cp.2018.0042.

[11]A. Yasin and L. Liu, “An online identity and smart contract management system, “2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), IEEE, , vol. 2, August 2016, doi: 10.1109/COMPSAC.2016.2

[12] A. Cohn, T. West and C. Parker, “Smart after all: Blockchain, smart contracts, parametric insurance and smart energy grids, “Georgetown Law Technology, Rev, vol.1, no.2, pp.273-304, 2017.

[13] G. Zhang, X. Chen, B. Feng, X. Guo, X. Hao, H. Ren, C. Dong, and Y. Zhang, "BCST-APTS: Blockchain and CP-ABE Empowered Data Supervision, Sharing, and Privacy Protection Scheme for Secure and Trusted Agricultural Product Traceability System, "Security and Communication Networks, Wiley, vol.2022, article id.2958963, https://doi.org/10.1155/2022/2958963, 15 January, 2022.

[14] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An Overview of Blockchain and 5G Networks, "27 January 2022, https://arxiv.org/abs/2201.11385.

[15] M. A. Khan, K. Salah, "IoT security: Review, blockchain solutions, and open challenges, "Future Generation Computer Systems 82 (2018), Elsevier, pp. 395–411, 26 November,2017, https://doi.org/10.1016/j.future.2017.11.022.

[16] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A Blockchain-empowered Access Control Framework for Smart Devices in Green Internet of Things, "ACM Transactions on Internet Technology, vol.21, no.3, article.80, https://doi.org/10.1145/3433542, June 2021.

[17] M. Pincheira, M. Antonini and M. Vecchio, "Integrating the IoT and Blockchain Technology for the Next Generation of Mining Inspection Systems, "Sensors, 25 January, 2022, https://doi.org/10.3390/s22030899

[18] S. Sun, R. Du and S. Chen, "A Secure and Computable Blockchain-Based Data Sharing Scheme in IoT System, "Information, 12, 47, 20 January, 2021, https://doi.org/10.3390/info12020047.

[19] T. Li, W. Liu, A. Liu, M. Dong, K. Ota, N. N. Xiong, and Q. Li, "BTS: A Blockchain-based Trust System to Deter Malicious Data Reporting in Intelligent Internet of Things, "IEEE internet of things journal, 3 July, 2021 doi:10.1109/JIOT.2021.3085004.

[20] N. Andola, Raghav, V. K. Yadav, S. Venkatesan and S. Verma, "SpyChain: A Lightweight Blockchain for Authentication and Anonymous Authorization in IoD, "Wireless Personal Communications, Springer, 26 February, 2021, https://doi.org/10.1007/s11277-021-08214-8.

[21] P. Li, H. Xu, and T. Ma, "An efficient identity tracing scheme for blockchain-based Systems, "Information Sciences 561 (2021), Elsevier, pp.130–140, 5 February, 2021, https://doi.org/10.1016/j.ins.2021.01.081.

[22] P. Kamboj, S. Khare and S. Pal, "User authentication using Blockchain based smart contract in role-based access control, "Networking and Applications, Springer, 28 April, 2021, https://doi.org/10.1007/s12083-021-01150-1.

[23] N. Fotiou and G. C. Polyzos, “Decentralized name-based security for content distribution using blockchains, “2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 415–420, 8 September, 2016, doi: 10.1109/INFCOMW.2016.7562112,

[24] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of IoT data, “CCSW '17: Proceedings of the 2017 on Cloud Computing Security Workshop, pp. 45–50, November 2017, doi: https://doi.org/10.1145/3140649.3140656.

[25] B. Dickson, “Blockchain Has the Potential to Revolutionize the Supply Chain, “Tech Crunch, San Francisco Bay Area, CA, USA, November 2016, doi: https:// techcrunch.com/2016/11/24/blockchain-has-the-potential-to-revolutionize-the-supply-chain.

[26] R. Guo, H. Shi, Q. Zhao, and D. Zheng, “ Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, “IEEE Access, vol 6, pp.11676–11686, 2 February, 2018, doi: 10.1109/ACCESS.2018.2801266.

[27]J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, “Consortium blockchain-based malware detection in mobile devices, “IEEE Access, vol 6, pp.12118–12128, 13 February, 2018, doi: 10.1109/ACCESS.2018.2805783.

[28] M. C. K. Khalilov, A. Levi, “A survey on anonymity and privacy in Bitcoin like digital cash systems, “IEEE Communication Surveys and Tutorials, vol 20, issue3, pp-2543–2585, 26 March, 2018.

[29] David W. Kravitz and Jason Cooper, “Securing user identity and transactions symbiotically: IoT meets blockchain, “Global Internet things summit (GIoTS), IEEE, pp.1-6, 24 August, 2017, doi: 10.1109/GIOTS.2017.8016280.

[30] R. Shrestha, and S. Y. Nam, “Regional Blockchain for Vehicular Networks to Prevent 51% Attacks, “IEEE Access, vol 7, 2019, https://ieeexplore.ieee.org/abstract/document/8763943.

[31]D. Zheng, C. Jing, R. Guo , S. Gao, and L. Wang, “A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs, “IEEE Access, vol 7, 2019, https://ieeexplore.ieee.org /abstract/ document/8808923.

[32]S. Bao, P. Asuquo, H. Cruickshank, Z. S. Y. Cao, A. Lei, Z. Sun, and M. Huth, "Pseudonym Management Through Blockchain: Cost-Efficient Privacy Preservation on Intelligent Transportation Systems, “IEEE Access, 2019, doi: https://ieeexplore.ieee.org/abstract/document /8732988/IEEE Access, 2921605.

[33]S. Hong, “P2P networking based internet of things (IoT) sensor node authentication by Blockchain, “Springer, Korea, 5March, 2019, doi: https://doi.org/10.1007/s12083-019-00739-x.

[34] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, “The Role of Blockchain to Fight against COVID-19, “IEEE engineering management review, 8 August, 2020, doi: 10.1109/EMR.2020.3014052.

[35] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, S. Salman, “Blockchain technology in the healthcare industry: Trends and opportunities, “Journal of Industrial Information Integration, 4 March, 2021, doi: https://doi.org/10.1016/j.jii.2021.100217, 2452-414x.

[36] A. Devi, G. Rathee and H. Saini, “Secure Blockchain-Internet of Vehicles (B-IoV) Mechanism using DPSO and M-ITA Algorithms, “Journal of Information Security and Applications, Elsevier, 10 December, 2021, doi: https://doi.org/10.1016/j.jisa.2021.103094, 2214-2126.

[37] E. Tan, S. Mahula and J. Crompvoets, “Blockchain governance in the public sector: A conceptual framework for public management, “Government Information Quarterly, Elsevier, vol.39, issue.1, January 2022, doi: https://doi.org/10.1016/j.giq.2021.101625.

[38]D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. (Sherman) Shen, “Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain, “IEEE Transactions on Industrial Informatics, vol.15, issue.6, June 2019, doi: https://ieeexplore.ieee.org/abstract/ document/8640264.

[39]F. Yang, W. Zhou, Q. Wu, R. Lung, N. N. Xiong, and M. Zhou, “Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism, “IEEE access, China, vol.7, 2019, doi: https://ieeexplore.ieee.org/ abstract/document/ 8798621.

[40]. Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran,” Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment, “IEEE Internet of things journal, vol. 6, no. 3, June 2019, doi: https://ieeexplore.ieee.org/abstract/ document/8668426.

[41] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, P. Zeng, “Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism, “IEEE Transactions on Industrial Informatics, 2018, doi: https://ieeexplore.ieee.org /abstract/ document/8661654.

[42] E. K. Wanga, Z. Liang, C. Chen, S. Kumari, and M. K. Khan, “PoRX: A reputation incentive scheme for blockchain consensus of IIoT, “Elsevier, 9 August, 2019, https://doi.org/ 10.1016/ j.future.2019.08.005.

[43] R. Asif, K. Ghanem and J. Irvine, “Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy, “Sensors 2021, 23 December 2020, doi: https://dx.doi.org/10.3390/s21010028.

[44] M. Tayseer A. Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, ”Hierarchical blockchain structure for node authentication in IoT networks, “Egyptian Informatics Journal, 19 February, 2022, doi: https://doi.org/10.1016/j.eij.2022.02.005.

[45] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao and S. Liu, “Blockchain-Based Data Preservation System for Medical Data, “Journal Medical System (2018) Springer, 28 June, 2018, doi: https://doi.org/10.1007/s10916-018-0997-3.

[46] W. Dai, C. Dai, K. R. Choo, C. Cui, D. Zou, and H. Jin, “SDTE: A Secure Blockchain-based Data Trading Ecosystem, “IEEE Transactions on Information Forensics and Security, 2019, doi: 10.1109/TIFS.2019.2928256.

[47] W. Liang, M. Tang, J. Long, X. Peng, J. Xu and K. C. Li, *“*A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things, “IEEE Transactions on Industrial Informatics, 2019, doi:10.1109/TII.2019.2907092.

[48] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, “BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control, “Special Section on Blockchain-enabled Trustworthy Systems, IEEE Access, 21 May, 2020, doi: 10.1109/ACCESS.2020.2992649.

[49] M. M. Arcinas, “A Blockchain Based Framework for Securing Students Educational Data, “Linguistica Antverpiensia, issn: 0304-2294, 22 May, 202, issue-2, www.hivt.be.

[50] Z. Chen, W. Xu, B. Wang and H. Yu, “A blockchain-based preserving and sharing system for medical data Privacy, “Future Generation Computer Systems, Elsevier, page no.338–350, 17 May, 2021, doi: https://doi.org/10.1016/j.future.2021.05.023.

[51] M. Ha, S. Kwon, Y. J. Lee, Y. Shim, J. Kim, “Where WTS meets WTB: A Blockchain-based Marketplace for Digital Me to trade users’ private data, “Pervasive and Mobile Computing, Elsevier, August 2019, doi: https://doi.org/10.1016/j.pmcj.2019.101078.

[52] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, “A Blockchain Privacy Protection Scheme Based on Ring Signature, “Special Section on Blockchain Technology: Principles and Applications, IEEE Access, 14 April, 2020, doi:10.1109/ACCESS.2020.2987831.

[53] D. C. Nguyen, P. N. Pathirana, M. Ding, A. Seneviratne,” Privacy-Preserved Task Offloading in Mobile Blockchain with Deep Reinforcement Learning, “IEEE Transactions on Network and Service Management, 26 July, 2020, doi:10.1109/TNSM.2020.3010967.

[54] X. Qin, Y. Huang, Z. Yang, and X. Li, “LBAC: A lightweight blockchain-based access control scheme for the internet of things, “Information Sciences, Elsevier, pp.222–235, 20 December, 2020, doi: https://doi.org/10.1016/j.ins.2020.12.035.

[55] G. Lax, A. Russo, and L. S. Fascì, “A Blockchain-based approach for matching desired and real privacy settings of social network users, “Information Sciences, Elsevier, page no. 220-235, 26 January, 2021, doi: https://doi.org/10.1016/j.ins.2021.01.004.

[56] T. Ahsan, F. Z. khan, Z. Iqbal, M. Ahmed, R. Alroobaea, A. M. Baqasah , I. Ali and M. A. Raza, “IoT Devices, User Authentication, and Data Management in a Secure, Validated Manner through the Blockchain System, “Wireless Communications and Mobile Computing, Wiley, article id.8570064, 8 February, 2022, doi: https://doi.org/10.1155/2022/8570064.

[57] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, “Blockchain-based decentralized trust management in vehicular networks,” IEEE Internet of Things Journal, vol.6, issue.2, pp.1495-1505, 14 May, 2018, doi: 10.1109/JIOT.2018.2836144.

[58] W. Hu, Y. Hu, W. Yao, and H. Li, ”A Blockchain-Based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles, ”IEEE Access, vol.7, 16 September,2019, doi: 10.1109/ACCESS.2019.2941507.

[59] H. Chai, Supeng, K. Zhang, and S. Mao,” Proof-of-Reputation Based-Consortium Blockchain for Trust Resource Sharing in Internet of Vehicles,” IEEE Access, vol.7, 2 December, 2019, doi: 10.1109/ACCESS.2019.2956955.

[60] H. Wang, Q. Wang, D. He, Q. Li, Z. Liu,” BBARS: Blockchain-Based Anonymous Rewarding Scheme for V2G Networks,” IEEE Internet of Things, vol.6, pp.3676-3687, 1 January, 2019, doi: 10.1109/JIOT.2018.2890213.

[61] C. Xu, H. Liu, P. Li, and P. Wang, “ A Remote Attestation Security Model based on Privacy-Preserving Blockchain for V2X,” IEEE Access, vol.6, pp.67809-67818, 9 November, 2018, doi: 10.1109/ACCESS.2018.2878995.

[62] C. Chen, J. Wu, H. Lin, W. Chen, Z. Zheng, “A Secure and Efficient Blockchain-based Data Trading Approach for Internet of Vehicles,” IEEE Transactions on Vehicular Technology, vol. xx, 2020.

[63] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, J. Zhao, “Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory, “IEEE Transactions on Vehicular Technology, vol.68, no.3, 23 January, 2019, doi: 10.1109/TVT.2019.2894944.

[64] Y. Wang, Z. Cai, Z. H. Zhan, Y. J. Gong, and X. Tong, “An Optimization and Auction-Based Incentive Mechanism to Maximize Social Welfare for Mobile Crowdsourcing,” IEEE Transactions On Computational Social Systems, vol.6, issue.3, pp.414-429, 11 April, 2019, doi: 10.1109/ TCSS.2019.2907059.

[65] X. F. Liu, Z. H. Zhan, J. D. Deng, Y. Li, T. Gu and J. Zhang, “An energy efficient ant colony system for virtual machine placement in cloud computing, ”IEEE Transactions on Evolutionary Computation, vol. 22, no.1, pp.113–128, Feb. 2018, doi: 10.1109/TEVC.2016.2623803.

[66]Y. Hu, Y. Wang, Y. Li, and X. Tong, “An incentive mechanism in mobile crowdsourcing based on multiattribute reverse auctions,” Sensors, vol.18, no.10, p. 3453, 14 October 2018, https://doi.org/10.3390/s18103453.

[67] Y. H. Jia, W. N. Chen, T. Gu, H. Zhang, H. Q. Yuan, S. Kwong and J. Zhang, “Distributed Cooperative Co-Evolution With Adaptive Computing Resource Allocation for Large Scale Optimization, “IEEE Transactions on Evolutionary Computation, vol.23, issue.2, April 2019, doi: 10.1109/TEVC.2018.2817889.

[68] X. Zhang, Z. Yang, Y. J. Gong, Y. Liu and S. Tang, “SpatialRecruiter: Maximizing sensing coverage in selecting workers for spatial crowdsourcing, ”IEEE Transactions on Vehicular Technology, vol. 66, no. 6, pp. 5229–5240, June 2017, doi: 10.1109/TVT.2016.2614312.

[69] H. To, C. Shahabi, and L. Kazemi, “A server-assigned spatial crowdsourcing framework, ”ACM Transactions on Spatial Algorithms and Systems, vol. 1, no. 1, pp. 1–28, August 2015, doi: https://doi.org/10.1145/2729713.

[70] X. F. Liu, Z. H. Zhan, Y. Gao, J. Zhang, S. Kwong and J. Zhang, “Coevolutionary particle swarm optimization with bottleneck objective learning strategy for many-objective optimization, ”IEEE Transactions on Evolutionary Computation, vol.23, issue.4, Aug. 2019, doi: 10.1109/TEVC.2018.2875430.

[71] J. Wang, Mengruli, Y. He, H. Li, K. Xiao, and C. Wang, “A Blockchain based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications, ”IEEE Access, vol. xx, 2018, doi: 10.1109/ ACCESS. 2018. 2805837.

[72] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, ”A Blockchain-Based Location Privacy Protection Incentive Mechanism in Crowd Sensing Networks, ”Sensors 2018, doi:10.3390/s18113894, 2018.

[73] N. Malik, P. Nanda, X. He and R. P. Liu, “Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology,” Springer, 20 April 2020, doi: https://doi.org/10.1007/s11276-020-02325-z.

[74] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang,” Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks, ”Hindawi Mobile Information Systems, 2018, ID 6874158, https://doi.org/10.1155/2018/6874158.

[75] M. Sivaram, G. Rathee, R. Rastogi, M. T. Quasim, and H. Saini, ”A resilient and secure two-stage ITA and blockchain mechanism in mobile crowdsourcing, ”Springer, 3 March 2020, doi: https://doi.org/ 10.1007/ s 12652-020-01800-x.

[76] C. Chen, L. Chen, L. Liu, S. He, X. Yuan, D. Lan, and Z. Chen, “Delay-Optimized V2V-Based Computation Offloading in Urban Vehicular Edge Computing and Networks,” IEEE Access, vol.8, 2020, doi: 10.1109/ACCESS.2020.2968465.

[77] G. Tsaousoglou, K. Steriotis, N. Efthymiopoulos, P. Makris, and E. Varvarigos, “Truthful, Practical and Privacy-aware Demand Response in the Smart Grid via a Distributed and Optimal Mechanism,” IEEE Transactions on Smart Grid, 2019, doi: 10.1109/TSG.2020.2965221.

[78] X. Huang, Y. Zhang, D. Li, L. Han,” An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains, “Future Generation Computer Systems (2018), 2018, doi: https://doi.org/ 10.1016/ j.future.2018.09.046.

[79] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, “Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks, ”IEEE Transactions on Parallel and Distributed Systems, 2019, doi: org/10.1109/TPDS.2019.2900238.

[80] S. Thakur, B. P. Hayes, and G. Breslin, “Distributed Double Auction for Peer to Peer Energy Trade using Blockchains,” IEEE, 2018, doi: 978-1-5386-5517-7/18.

[81] A. Choubey, S. Behera, Y. S. Patel, K. Mahidhar and R. Misra, “EnergyTradingRank Algorithm for Truthful Auctions among EVs via Blockchain Analytics of Large Scale Transaction Graphs,”

2019 11th International Conference on Communication Systems & Networks (COMSNETS), 2019, doi: 978-1-5386-7902-9/19/IEEE.

[82] T. Liu, J. Wu, L. Chen, Y. Wu and Y. Li, “Smart Contract-Based Long-Term Auction for Mobile Blockchain Computation Offloading,” IEEE Access, 2974750, vol.8, February 2020, doi: 10.1109/ACCESS.

[83] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong and G. Wu, “An incentive mechanism with privacy protection in mobile crowdsourcing systems,” Computer Networks, vol. 102, pp. 157–171, June 2016.

[84] M. Macdonald, L. Thorrold, and R. Julien, “The blockchain: A comparison of platforms and their uses beyond bitcoin”, Work pp.1-8, 2017.

[85] T. T. Kuo, H. Z. Rojas and L. Machado, “Comparison of blockchain platforms: a systematic review and healthcare examples, “Journal of the American Medical Informatics Association, vol.26, issue.5, pp.462-478, March 2019, doi: https://doi.org/10.1093/jamia/ocy185

[86] M. J. M. Chowdhury, MD. S. Ferdous, K. Biswas, N. Chowdhury, A. S. M. Kayes, M. Alazab and P. Watters, “A comparative analysis of distributed ledger technology platforms”, IEEE Access, vol.7, pp.167930-943, 15 November, 2019, doi: 10.1109/ACCESS.2019.2953729.

[87] Y. Yahiatene, M. A. Riahla, A. Rachedi, D. E. Menacer, and F. N. Abdesselam,” A blockchain-based framework to secure vehicular social Networks,” Wiley, 2 May, 2019, doi: 10.1002/ett.3650.

[88] J. Noh, S. Jeon and S. Cho, ’’Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles, ”www.mdpi.com/journal/electronics, Electronics 2020, 9, 74; doi:10.3390/ electronics 9010074, 2020.

[89] P. K. Sharma, S. Y. Moon and J. H. Park,’’ Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City”, Journal of Information Process System, vol.13, no.1, pp.184-195, February 2017.

[90] Y. T. Yang, L. D. Chou, C. W. Tseng, F. H. Tseng, and C. C. Liu”, Blockchain-based Traffic Event Validation and Trust Verification for VANETs”, IEEE Access, vol.xx, 2017, doi: 10.1109/2017, 2017.

[91] K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li, and Y. Yang, ”A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks, ”IEEE Transactions on Vehicular Technology, 2019, doi: 10.1109/TVT.2020.2968094.

[92] Y. Park, C. Sur, H. Kim, and K. H. Rhee,” A Reliable Incentive Scheme Using Bitcoin on Cooperative Vehicular Ad Hoc Networks, “The Development of a Secure Framework and Evaluation Method for Blockchain, vol- 5, pp-34-41, 2017.

[93] Z. Yang, K. Yang, Lei, K. Zheng, and C. Victor and M. Leung, “Blockchain-based Decentralized Trust Management in Vehicular Networks”, IEEE Internet of Things Journal, 2018, doi: 10.1109/JIOT.2018.2836144.

[94] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu,” A Privacy-preserving Trust Model based on Blockchain for VANETs”, IEEE Access, vol.xx, 2017, doi: 10.1109/2864189.

[95] G. Baldini, J. L. H. Ramos, G. Steri, and S. N. Matheu, ”Zone Keys Trust Management in Vehicular Networks based on Blockchain, ”IEEE, 2019, doi: 978-1-7281-2171-0/19.

[96] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang,” CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles, “IEEE transactions on intelligent transportation systems, 2017, doi: 10.1109/TITS.2017.2777990.

[97] F. Knirsch, A. Unterweger, and D. Engel,” Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions”, Springer, 4 sept, 2017, doi: 10.1007/s00450-017-0348-5.

[98] A. Ijaz, and N. Javaid,” Reward and Penalty based Mechanism in Vehicular Network using Decentralized Blockchain Technology, “26 July, 2019, doi: https://www.researchgate.net/publication/ 334644810.

[99] H. Zheng, J. Shao, and G. Wei, ”Attribute-based encryption with outsourced decryption in blockchain, ”Peer-to-Peer Networking and Applications, Springer, 14 April 2020, https://doi.org/10.1007/s12083-020-00918-1.

[100] H. Cui, Z. Wan, X. Wei, S. Nepal, and X. Yi,” Pay as You Decrypt: Decryption Outsourcing for Functional Encryption Using Blockchain, “IEEE Transactions on Information Forensics and Security, vol. 15, 2020.

[101] C. Lin, D. He, X. Huang, X. Xie, and K. K. R. Choo,” Blockchain-based system for secure outsourcing of bilinear pairings, “Elsevier, 2018, doi: https://doi.org/10.1016/j.ins.2018.12.043.

[102]. R. M. A. Latif, K. Hussain & N. Z. Jhanjhi, A. Nayyar, and O. Rizwan,” A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology,

"Multimedia Tools and Applications, Springer, 10 November, 2020, doi: https://doi.org/10.1007/s11042-020-10087-1.

[103] P. Giungato, R. Rana, A. Tarabella and C. Tricase," Current Trends in Sustainability of Bitcoins and Related Blockchain Technology, "www.mdpi.com/journal/sustainability, 30 November 2017, doi:10.3390/su9122214.

[104] G. Zyskind, O. Nathan and A. 'Sandy' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data, "2015 IEEE CS Security and Privacy Workshops, IEEE Computer Society, 2015, doi: 10.1109/SPW.2015.27.

[105] Huan Chen, Yijie Wang, "SSChain: A full sharding protocol for public blockchain without data migration overhead, "Pervasive and Mobile Computing, Elsevier, https://doi.org/10.1016/j.pmcj.2019.101055, 17 July, 2019.

[106] C. H. Liu, Q. Lin and S. Wen, "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning, "IEEE Transactions on Industrial Informatics, 2018, doi: 10.1109/TII.2018.2890203.

[107] https://en.wikipedia.org/wiki/InterPlanetary_File_System.

[108] S. Wang, X. Wang, and Y. Zhang, "A Secure Cloud Storage Framework with Access Control Based on Blockchain", IEEE Access, vol 7, 2019, doi:10.1109/ ACCESS. 2019. 2929205.

[109] J. T. Hao, Y. Sun, and H. Luo, "A Safe and Efficient Storage Scheme Based on BlockChain and IPFS for Agricultural Products Tracking, "Journal of Computers, vol.29, no.6, 2018, doi: 10.3966/199115992018122906015.

[110] F. Li, C. Shang, L. Zhang, and J. Liu," TFBO: A Trusted Framework based on Blockchain for Outsourcing Data Entry, "2020 IEEE International Conference on Smart Internet of Things (SmartIoT), 20 September, 2020, doi: 10.1109.

[111] S. R. Lashkami, R. E. Atani, A. Arabnouri, and G. Salemi," A Blockchain Based Framework for Complete Secure Data Outsourcing with Malicious Behavior Prevention", 28th Iranian Conference on Electrical Engineering (ICEE), 2020, IEEE, 978-1-7281-7296-5/2020.

[112] H. Wang, X. A. Wang, S. Xiao, and J. S. Liu," Decentralized data outsourcing auditing protocol based on blockchain", Journal of Ambient Intelligence and Humanized Computing, Springer, 25 July 2020, doi.org/10.1007/s12652-020-02432-x.

[113] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, “Blockchain based Efficient and Robust Fair Payment for Outsourcing Services in Cloud Computing”, Information Sciences, 7 June 2018, doi: 10.1016/j.ins.2018.06.018.

[114] Y. Zhang, R. H. Deng, Ximeng Liu, and Dong Zheng,” Outsourcing Service Fair Payment based on Blockchain and its Applications in Cloud Computing”, IEEE Transactions on Services Computing, doi:10.1109/TSC.2018.2864191, vol. XX, 2018.

[115] K. Fan, Z. Bao, M. Liu, A. V. Vasilakos and W. Shi, “Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT”, Future Generation Computer System, 2019, doi: https://doi.org/10.1016/j.future.2019.10.014.

[116] S. Jiang, and J. Liu, and L. Wang, and S. Yoo, ”Verifiable Search Meets Blockchain: A Privacy-Preserving Framework for Outsourced Encrypted Data”, IEEE, 2019, 978-1-5386-8088-9.

[117] S. Wang, Y. Wang, and Y. Zhang,” Blockchain-based fair payment protocol for deduplication cloud storage system “, IEEE Access, 2019, doi: 10.1109.

[118] J. Sun, X. Yao, S. Wang, and Y. Wu,” Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS, ”IEEE Access, September 3, 2020, doi:10.1109/ACCESS.2020.3018816.

[119] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, ”FADB: A Fine-Grained Access Control Scheme for VANET Data based on Blockchain, “IEEE Access, vol 4, 2016, doi: 10.1109.

[120] C. Lin, D. He, X. Huang, M. K. Khan, and K. R. Choo,” DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain, “IEEE Transactions on Information Forensics and Security, vol. 15, 2020.

[121] C. Lin, D. He, X. Huang, X. Xie, and K. R. Choo,” PPChain: A Privacy-Preserving Permissioned Blockchain Architecture for Cryptocurrency and Other Regulated Applications”, IEEE Systems Journal, 25 August, 2020, doi: 10.1109/JSYST.2020.3019923.

[122] P. Pandey & R. Litoriya,” Securing and authenticating healthcare records through blockchain technology”, Cryptologia, 30 Jan 2020., doi: 10.1080/01611194.2019.1706060.

[123] G. Tripathi, M. A. Ahad, and S. Paiva, “S2HS- A blockchain-based approach for smart healthcare system” ,https://doi.org/10.1016/j.hjdsi.2019.100391, Elsevier, 5 November 2019.

[124] C. Rupa, and D. Midhunchakkaravarthy,” Preserve Security to Medical Evidences using Blockchain Technology, “Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020), IEEE Xplore, 24 June 2020, ISBN: 978-1-7281-4876-2.

[125] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Ghalib, A. Shankar, and X. Cheng, “Secure smart contracts for cloud-based manufacturing using Ethereum blockchain”, 18 August 2020, doi: 10.1002/ett.4129, Wiley.

[126] K. Hao, J. Xin, Z. Wang, K. Cao and G. Wang, “Blockchain-based Outsourced Storage Schema in Untrusted Environment, “IEEE Access, vol 4, 2016, doi:10.1109/ ACCESS.2019.2938578.

[127] K. Hao, J. Xin, Z. Wang and G. Wang, “Outsourced data integrity verification based on blockchain in untrusted environment, “World Wide Web, Springer, 4 March, 2020, doi: https://doi.org/10.1007/s11280-019-00761-2.

[128] E. B. Sifah, Q. Xia, K. O. O. Agyekum, H. Xia, A. Smahi and J. Gao, “A Blockchain Approach to Ensuring Provenance to Outsourced Cloud Data in a Sharing Ecosystem, “IEEE systems journal xplore, 26 May, 2021.

[129] T. Benil and J. Jasper, “Cloud based security on outsourcing using blockchain in E-health systems, “Computer Networks, Elsevier, 3 June, 2020, doi: https://doi.org/10.1016/j.comnet.2020.107344.

[130] https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT.

[131] Q. Fan, J. Chen, L. J. Deborah, and M. Luo, “A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain, “Journal of systems architecture, Elsevier, 26 March, 2021, doi: https://doi.org/10.1016/j.sysarc.2021.102112.

[132] Y. Wu, H. N. Dai, and H. Wang, “Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0, “IEEE Internet of Things Journal, vol. xx, no. x, August, 2020, doi:10.1109/JIOT.2020.3025916.

[133] J. Wang, L. Wu, K. K. R. Choo, and D. He, “Blockchain Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure, ”IEEE Transactions on Industrial Informatics, 2019, doi: 10.1109/TII.2019.2936278.

[134] D. Tao, P. Ma, M. S. Obaidat, “Anonymous identity authentication mechanism for hybrid architecture in mobile crowd sensing networks”, Int J Commun Syst. 2019, e4099, 21 June 2019, https://doi.org/10.1002/dac.4099.

[135] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, “Enabling Secure Authentication in Industrial IoT with Transfer Learning empowered Blockchain”, IEEE Transactions on Industrial Informatics, vol.17, issue.11, pp.7725-7735, 28 May, 2021, doi: 10.1109/TII.2021.3049405.

[136] J. T. Hao, Y. Sun, and H. Luo, “A Safe and Efficient Storage Scheme Based on BlockChain and IPFS for Agricultural Products Tracking, ”Journal of Computers, vol. 29 no. 6, 2018, pp. 158-167, 2018, doi: 10.3966/199115992018122906015.

[137] H. Zareen, S. Awan, M. B. E. Sajid, S. M. Baig, M. Faisal, and N. Javaid, “Blockchain and IPFS based Service Model for the Internet of Things, “April 2021, https://www.researchgate.net/publication/351134391.

[138] S. Zhao, S. Li, and Y. Yao, “Blockchain Enabled Industrial Internet of Things Technology, ”IEEE Transactions on computational social systems, 10 June, 2019, doi:10.1109/TCSS.2019.2924054.

[139]. T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage, I. Ahmad, M. Liyanage, An Braeken, and Mika Ylianttila,” BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks”, IEEE Access, vol. 4, 2016, doi: 10.1109/ACCESS.2020.3017891.

[140] K. Huang, X. Zhang, Y. Mu, X. Wang, G. Yang, X. Du, F. Rezaeibagha, Q. Xia, and M. Guizani, “Building Redactable Consortium Blockchain for Industrial Internet-of-Things, “IEEE Transactions on Industrial Informatics, 2019, doi: 10.1109/TII.2019.2901011.

[141] M. Sharma, S. Pant, D. K. Sharma, K. D. Gupta, V. Vashishth, and A. Chhabra, “Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions, “Wiley, Trans Emerging Tel Tech, 16 September 2020, doi: 10.1002/ett.4137.

[142] K. Yu, L. Tan, M. Aloqaily, H. Yang, Y. Jararweh, “Blockchain-Enhanced Data Sharing with Traceable and Direct Revocation in IIoT”, IEEE Transactions on Industrial Informatics, 2020, doi: 10.1109/TII.2021.3049141.

[143] J. Huang, L. Kong, G. Chen, M. Y. Wu, X. Liu, P. Zeng,” Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism, ”IEEE Transactions on Industrial Informatics, 2019, doi:10.1109/TII.2019.2903342.

[144] J. Wan, J. Li, M. Imran, D. Li, and F. Amin, “A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory, “IEEE Transactions on Industrial Informatics, 2019, doi: 10.1109/TII.2019.2894573.

[145] L. Vishwakarma, and D. Das, “SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain, “Journal of Parallel and Distributed Computing, Elsevier, pp.94–105, 10, April 2021.

[146] S. Iqbal, R. M. Noor, A. W. Malik and A. U. Rahman, “Blockchain-enabled adaptive learning-based resource sharing framework for IIoT environment, “IEEE Internet of Things Journal, 16 June, 2021, doi: 10.1109/JIOT.2021.3071562.

[147] X. Cai, S. Geng, J. Zhang, D. Wu, Z. Cui, W. Zhang, and J. Chen,” A Sharding Scheme based Many-objective Optimization Algorithm for Enhancing Security in Blockchain-enabled Industrial Internet of Things, “IEEE Transactions on Industrial Informatics, vol.14, no.8, 15 June, 2021, doi: 10.1109/TII.2021.3051607.

[148] S. F. Lorenzo, J. Anorga, and S. Arrizabalaga, “Methodological performance analysis applied to a novel IIoT access control system based on permissioned blockchain, “Information Processing and Management, 102558, Elsevier, 9 March, 2021.

[149] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, “Blockchain-enabled Federated Learning Data Protection Aggregation Scheme with Differential Privacy and Homomorphic Encryption in IIoT, “IEEE Transactions on Industrial Informatics, 30 June, 2021, doi:10.1109/TII.2021.3085960.

[150] C Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, “Blockchain-Based Software-Defined Industrial Internet of Things: A Dueling Deep *Q*-Learning Approach, “IEEE internet of things Journal, vol. 6, no. 3, June 2019, doi:10.1109/JIOT.2018.2871394.

[151] J. Wang, B. Wei, J. Zhang, X. Yu, P. K. Sharma, “An optimized transaction verification method for trustworthy blockchain-enabled IIoT, “Ad Hoc Networks 119 (2021) 102526, Elsevier, 7 May, 2021,doi: https://doi.org/10.1016/j.adhoc.2021.102526.

[152] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, Z. Zou, “A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things, “Journal of Industrial Information Integration 21 (2021) 100190, Elsevier, 8 December, 2020, doi: https://doi.org/10.1016/j.jii.2020.100190.

[153] K. Singh, O. Dib, C. Huyart, and K. Toumi, “A novel credential protocol for protecting personal attributes in blockchain, “Computers and Electrical Engineering, Elsevier, 12 February, 2020, doi: https://doi.org/ 10.1016/ j. compeleceng.2020.106586 0045-7906.

[154] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi and K. Salah, “A User Authentication Scheme of IoT Devices using Blockchain-enabled Fog Nodes, “IEEE, 2018, 978-1-5386-9120-5.

[155] R. Mu, B. Gong, Z. Ning, J. Zhang, Y. Cao, Z. Li, W. Wang and X. Wang, “An identity privacy scheme for blockchain-based on edge computing, ”Concurrency ComputatPract Exper.2021, e6545, 21 May, 2021, doi: https://doi.org/10.1002/cpe.6545.

[156]K. Kostal, R. Bencel, M. Ries, P. Truchly and I. Kotuliak, “Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain, “IEEE, 2019, 978-1-7281-0945-9.

[157]T. Feng, X. Chen, C. Liu, and X. Feng, “Research on privacy enhancement scheme of blockchain transactions, “Wiley, 2 September, 2019, doi: 10.1002/spy2.89.

[158] S. M. C. Vigila, and K. Muneeswaran, “Implementation of Text based Cryptosystem using Elliptic Curve Cryptography, ”ICAC 2009, 978-1-4244-4787-9/09.

[159] M. M. Rana, W. Xiang, E. Wang, X. Li, and B. J. Choi, “Internet of Things Infrastructure for Wireless Power Transfer Systems, “IEEE Access, vol.6, pp. 19295-19303, 24 January, 2018, doi: 10.1109/ACCESS.2018.2795803.

[160] G. Rathee, A. Sharma, R. Iqbal, N. Jaglan and R. Kumar, “A Blockchain Framework for Securing Connected and Autonomous Vehicles, “Sensors 2019, vol.19, 18 July 2019, 3165;, doi: https://doi.org/10.3390/s19143165.

[161] M. S. Raniyal, I. Woungang, and S. K. Dhurandher, “An RSA-Based User Authentication Scheme for Smart-Homes Using Smart Card, “Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, ISDDC 2018, Springer, Lecture Notes in Computer Science, vol 11317, doi: https://doi.org/10.1007/978-3-030-03712-3_2

[162] A. Kunwar, A. Gautam, and B. K. Kamaujia, “Inverted L-slot triple-band antenna with defected ground structure for WLAN and WiMAX applications, “International Journal of Microwave and Wireless Technologies, Volume 9 Issue 1,pp. 191- 196, February 2017, doi: https://doi.org/10.1017/S1759078715001105.

[163] M. Kumar, H. K. Verma, and G. Sikka, “A secure data transmission protocol for cloud-assisted edge-Internet of Things environment, “Transactions on Emerging Telecommunications Technologies, 22 March 2020, doi: https://doi.org/10.1002/ett.3883.

[164]N. R. Patel, S. Kumar, and S. K. Singh, “Energy and Collision Aware WSN Routing Protocol for Sustainable and Intelligent IoT Applications, “IEEE Sensors Journal, 31 May, 2021, doi:10.1109/jsen.2021.3076192.

[165] S. K. Biswash, and C. Kumar, “Multi home agent and pointer-based (MHA–PB) location management scheme in integrated cellular-WLAN networks for frequent moving users, “Computer Communications, Elsevier,vol.33,issue.18, pp. 2260-2270, December 2010, doi: https://doi.org/10.1016/j.comcom.2010.07.028.

[166] P. Meena, P. Sharma and K. Sharma, "Optimizing Control of IOT Device using Traditional Machine Learning Models and Deep Neural Networks," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2022, pp. 445-451, doi: 10.1109/ICCMC53470.2022.9753943.

[167] C. A. Kerrache, A. Lakas, N. Lagraa and E. Barka, “UAV-assisted technique for the detection of malicious and selfish nodes in VANETs, “Vehicular Communications, Elsevier, vol.11, pp.1-11, January 2018.

[168] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar and M. S. Obaidat "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops, Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644088.

[169] A. Makkar, T. W. Kim, A. K. Singh, J. Kang and J. H. Park, "Secure IIoT Environment: Federated Learning Empowered Approach for Securing IIoT From Data Breach, "IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6406-6414, September, 2022, doi: 10.1109/TII.2022.3149902.

List of Publication

Published Papers in Journals

- A. Devi, G. Rathee, H. Saini, “Secure Blockchain-Internet of Vehicles (BIoV) Mechanism using DPSO and M-ITA Algorithms, “Journal of Information Security and Applications, Elsevier, **Impact factor. 5.6**, vol.64, February, 2022, doi: https://doi.org/10.1016/j.jisa.2021.103094. (**SCIE Indexed**)
- A. Devi, A. Kumar, G. Rathee, H. Saini, “User Authentication of Industrial Internet of Things (IIoT) through Blockchain, “Multimedia Tools and Applications, Springer, **Impact Factor. 3.6**, pp. 19021–19039, 9 December, 2022, doi: https://doi.org/10.1007/s11042-022-14154-7**. (SCIE Indexed)**

Communicated Paper in Journal

- Devi, A. Kumar, G. Rathee, H. Saini, “Secure Information Transfer and Sharing using IPFS and Encryption through Blockchain”, International Journal of Sensor Networks, **Impact Factor- 1.1,** ISSN: 1748-1287 **(SCIE Indexed)**

Published Book Chapter

- A. Devi, G. Rathee, H. Saini, “Secure Information Transmission in Intelligent Transportation Systems Using Blockchain Technique, “Internet of Things, Intelligent cyber physical systems for autonomous transportations, Springer, Switerzerand, 2021, ISBN 978-3-030-92053-1, doi: https://doi.org/10.1007/978-3-030-92054-8.

Published Conferences

- A. Devi, G. Rathee and H. Saini, "Using Optimization and Auction Approach: Security provided to Vehicle network through Blockchain Technology, “2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 476-480, doi:10.1109/PDGC50313.2020.9315804.
- A. Devi, G. Rathee, H. Saini, “Security Concerns at Various Network Phases Through Blockchain Technology, “A. Choudhary, A.P. Agrawal, R. Logeswaran, Unhelkar B. (eds) Applications of Artificial Intelligence and Machine Learning. Lecture Notes in

Electrical Engineering, Springer, vol. 778, 31 July, 2021, Singapore, doi: https://doi.org/10.1007/978-981-16-3067-5_45.

- A. Devi., G. Rathee, H. Saini, “Industrial IoT with Secure Authentication Mechanism through Blockchain Technology, “Lecture notes in networks and systems, 3rd Doctoral symposium on computational intelligence (DOSCI 2022), Springer, Singapore, 2022, isbn: ISBN 978-981-19-3147-5, doi: https://doi.org/10.1007/978-981-19-3148-2.

Workshop Attended

- Attended Workshop on “Blockchain Technology” (March 2-7, 2020) jointly organized by National Institute of Technical Teachers Training & Research (NITTR), Chandigarh.