BLOCKCHAIN BASED DECENTRALIZED AUTHENTICATION AND ACCESS CONTROL MODEL FOR IoT DEVICES

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Computer Science and Engineering

By

Inderpal Singh

Registration Number: 12020434

Supervised By

Dr. Balraj Singh (13075)

Department of Computer Science and Engineering (Professor)

Lovely Professional University

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

LOVELY PROFESSIONAL UNIVERSITY, PUNJAB

2025

DECLARATION

I, hereby declared that the presented work in the thesis entitled “Blockchain Based Decentralized Authentication And Access Control Model For IoT Devices” in fulfilment of degree of **Doctor of Philosophy (Ph. D.)** is outcome of research work carried out by me under the supervision of Dr. Balraj Singh, working as Professor, in the School Computer Science and Engineering of Lovely Professional University, Punjab, India. In keeping with general practice of reporting scientific observations, due acknowledgements have been made whenever work described here has been based on findings of other investigator. This work has not been submitted in part or full to any other University or Institute for the award of any degree.

Inderpal

(Signature of Scholar)

Name of the scholar: Inderpal Singh

Registration No.: 12020434

Department/school: School of Computer Science and Engineering

Lovely Professional University,

Punjab, India

CERTIFICATE

This is to certify that the work reported in the Ph. D. thesis entitled “BlockchainBased Decentralized Authentication And Access Control Model For IoT Devices” submitted in fulfillment of the requirement for the award of degree of **Doctor of Philosophy (Ph.D.)** in the Department of Computer Science and Engineering, is a research work carried out by Inderpal Singh, 12020434, is bonafide record of his/her original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.

(Signature of Supervisor)

Name of supervisor: Dr. Balraj Singh

Designation: Professor

Department/school: School of Computer Science and Engineering

University: Lovely Professional University,

Punjab, India

LIST OF PUBLICATION

[1] Singh, I., & Singh, B. (2024). LAA-D: Lightweight Authentication and Access Control Mechanism with Dual-Data Storage in Cloud-Internet of Things System Using Blockchain. Iranian Journal of Science and Technology, Transactions of Electrical Engineering. **SCI (Published) IF 2.0**

[2] Singh, I., & Singh, B. (2024). Scalable Consensus algorithm and Storage in Decentralized Blockchain (SCSB) for Heterogeneous IoT Systems. Journal of Intelligent & Fuzzy Systems. **SCI (Submitted) IF 2.0**

[3] Singh, I., & Singh, B. (2023). Access management of IoT devices using access control mechanism and decentralized authentication: A review. Measurement: Sensors, 25, 100591. **Scopus (Published)**

[4] Singh, I., Singh, B., & Rana, A. K. (2023). A Robust Remote User Authentication Scheme for Supply Chain Management Using Blockchain Technology. In International Conference on Data Science and Network Engineering. Singapore: Springer Nature Singapore. **Scopus (Published)**

[5] Singh, I., & Singh, B. (2023). Integration of Decentralized Blockchain with Cloud & IoT Based SCM. In 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT). IEEE. **Scopus (Published)**

[6] Singh, I., Singh, B., & Rana, A. K. (2024). Role and Impact of Blockchain–IoT-Enabled Supply Chain Management Model for Medical Supply. In Convergence of Blockchain and Internet of Things in Healthcare (pp. 54-67). CRC Press. **Scopus (Published)**

[7] Singh, I., Singh, B., & Agrawal, P. (2023). Decentralized Lightweight Blockchain: IoT-Based Authentication System for Cloud-Based Supply Chain Management. In Integration of Cloud Computing with Emerging Technologies (pp. 171-181). CRC Press. **Scopus (Published)**

ABSTRACT

Nowadays, smart devices have made global connectivity seamless through the application of wireless devices. Internet of Things (IoT) is a popular study area that involves a variety of real-time applications and minimizes human intervention. However, the increase in deployment of data generating devices and data users in IoT environment impose serious scalability and security issues. A system with a significant number of devices is unable to assure security due to the presence of anomalies, attackers and intruders.

To address these scalability and security issues, a LAA-D (Lightweight Authentication and Access Control Mechanism with Dual-Data Storage) framework in Cloud-Internet of Things System is developed in this work. It is a combination of authentication, access control and data storage mechanisms. A set of data owners and data users are created with protection of credentials. The credentials that are taken in account for each device are: identity, device type, IP address, signature, PUF and biometric. These credentials are securely exchanged using the Key Schedule PRESENT algorithm. The approach prefers the number of credentials for the device before authentication using a fuzzy logic algorithm. In this work, the data to be stored in the cloud by the data owner is divided into two chunks of equal sizes. If an attacker can extract a segment of the data, then it brings a possibility to extract the complete data. In order to overcome this adversity, the data is divided and employs two different lightweight algorithms for encryption: SALSA20 and PRESENT Key algorithm. The credentials of each device are managed in the decentralized blockchain so the data access and the data storage is granted only after completion of authentication in the blockchain. The improved results are achieved in terms of authentication time, storage efficiency, running time, throughput, latency, and blocksize. Due to the participation of a large number of data owners, the Cloud-IoT environment causes scalability issues in data storage. Scalable Consensus Algorithm and Storage in Decentralized Blockchain (SCSB) for Heterogeneous IoT Systems, ensures fault tolerance by employing a balanced data storage approach. It is achieved through the integration of the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm, which operates using a hybrid distance measure.

Subsequently, data is stored secured by predicting the data confidentiality using dual fuzzy logic and its categorization into low confidential level and high confidential level. The data security method used for low confidentiality level is: differential privacy and for high confidentiality level is: TWINE algorithm. The above two methods are lightweight and hence, work with low computations. For the process of validation of nodes in the blockchain, Proof-of-Authentication (PoA) consensus algorithm is used. It achieves higher performance results in terms of execution time, encryption time, decryption time, storage efficiency, throughput, latency and hit rate. ifogsim is used for the experiments and to implement the work. The designed security shows better results than the existing methods and shows better achievements in terms of security challenges and scalability issues.

ACKNOWLEDGMENTS

The author has great privilege to express his immense sense of gratitude to Dr. Balraj Singh, Professor, School of Computer Science and Engineering, Lovely Professional University, Phagwara, for his valuable guidance and untiring efforts throughout the tenure of the work. He has been an inspiring force where targets appeared to be difficult during the course of work. His timely help, construction criticism and painstaking efforts made the author capable to compile the thesis in its present form. Deep sense of gratitude is expressed to authorities of Lovely Professional University, Phagwara for permitting the author to pursue his research work and extending necessary facilities during the experimental and analysis work. I would like to thank my panel members who provided valuable suggestions during the course and all the staff members of School of Computer Science and Engineering who have been very patient and co-operative with us.

I would like to thank Dr. Arun Kumar Rana, Galgotia college of engineering, Greater Nodia for giving me opportunity to use their resource and work in such a challenging environment. I am grateful to the individuals whom contributed their valuable time towards my thesis. I humbly dedicate this work to my mother Mrs. Charanjit kaur, wife Mrs. Lovepreet kaur and colleague Ms. Ramandeep Kaur, who are the source of inspiration and encouragement behind this research work. The author sincerely acknowledges the help extended by them during the tenure of this work by sacrificing their comforts and always supported me throughout all my studies at university and encouraged me with their best wishes. About all, author is highly indebted to Great and Gracious almighty God who blessed me with spiritual support and courage at each and every stage of this work.

Inderpal

INDERPAL SINGH

Date: 17 MARCH 2025

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Internet of Things (IoT) has widespread applications and supports many real-time applications. The IoT devices such as sensors, actuators and IoT users smart mobile phones, tablets, etc. generates huge amounts of data. The data generated is transferred to the end server for analysis and processing through the various mediums. Depending upon whether the information is sensitive or non-sensitive, their security requirements vary. For the provisioning of security, blockchain is presented in decentralized access with the support of a variety of applications [1].

Security is provisioned with the incorporation of authentication and access control mechanisms in IoT using blockchain technology. The process of authentication is to validate the registered credentials that are stored in hash on blockchain. A miner will validate it and give access to the data from storage [2]. The authentication is handled using the validation of unique credentials that represent a particular device.

On the other hand, the data users will request for accessing the uploaded data which is granted depending upon the created access control policy. The access control policy mechanism is developed using attributes such as: identity, device type, IP address and signature [3]. The decentralized authentication and access control mechanism in the field of IoT assures security.

Generally, data is the heart of any network like IoT, and cloud of things. In order to ensure the security and privacy of data, numerous data security protocols have been developed in the past. Providing security is highly essential for storing and retrieving important data for business or other sensitive applications [4].

In addition, IoT devices are applied in many day to day life activities such as smart home and office, autonomous driving, smart farming and agricultural activities, disaster management, wearable devices, theft alarm systems, big data analysis etc. With the vast range of IoT applications, human efforts can be reduced many folds for managing day-to-day activities. With the aid of high speed internet, all the devices collect data and process information in real time [5].

However, in the last few decades, due to huge growth in IoT and its data flow, security vulnerability has also increased. The devices are prone to security breaches such as authentication, authorization, leakage of information, privacy breaches, verification controls, tampering the network, jamming the data traffic flow, eavesdropping, etc. [6].

Lack of sufficient network security detection techniques and inadequate measures against the attacks in the diversified networks gives attackers an access to the sensitive data. However, by accessing unauthorized information, hackers can cause damage to physical devices, and can harm the integrity of individuals in society [7].

To overcome the security breaches such as Man-In-The-Middle attack, Spoofing, Unsafe Firmware, Denial of Service attack, and Data Leakage, numerous preventive measures are available. However, the uncontrolled expansion and decentralized nature in the IoT environment compromises privacy and security. In addition, various reasons such as forgot to change password, creating simplest form of password increases the risk of cyber security in IoT.

1.2 Issues in IoT and Need of Blockchain

Detection methodology: In IoT, there are various types of attack detections: Signature-based Detection, Anomaly-Based Detection, Specification-Based Detection, Behavior-Based Detection and Hybrid Detection. These methods, however, cannot detect zero-day attacks, where signatures do not match any of the predefined rules or patterns.

Cryptography issue: For the cipher of integer values, cryptosystems are specifically designed that perform simple computations which may influence the results and even help areas where incorrect diagnosis occurs. Obtaining a safe and accurate diagnosis is one of the most difficult challenges in this field. To protect the privacy of sensors in the majority of studies, cryptography is used. The application of cryptography keeps the encryption keys maintained and secure, but it is incapable of dealing with situations where it is necessary to share data with the general users. Variance confidentiality is generally being used for different privacy concerns and works primarily to distribute query results rather than datasets to the clients.

End user's privacy: Users' concerns about breaches to their private information such as: personal data, location, and other information, have recently been raised while using facilities such as cloud computing, IoT and wireless networks. A network's capabilities may be seriously harmed if no convenient security measures are in place and it is susceptible to a variety of malicious attacks.

A Denial-of-Service (DoS) attack is a malicious cyber threat that exploits a network's vulnerabilities. This attack occurs due to the presence of multiple unauthenticated, network-connected devices, which can be leveraged to overwhelm the system and disrupt its availability.

Both fog computing and edge computing provide similar functionalities by enabling data processing and intelligence at analytic platforms positioned near the data source, including speakers, motors, screens, and sensors. These computing paradigms offer comparable capabilities in terms of data transmission and real-time analysis at the network edge.

IoT and other techniques such as fog and edge utilize the computing capabilities of a local network to perform computations.

Heterogeneity issue: Device mobility and changing application needs are likely to alter the network topology on a regular basis. The environment's fluctuation, necessitate dynamic and active system controlling based on multi-criteria resource allotment and the abnormal levels of heterogeneity in IoT. Handling dynamic behaviour's through improved and enhanced resource allocation includes multi-criteria schedulers and resource management systems. Any type of dynamic system management based on multi-criteria resource allocation is what the newly developed blockchain refers to.

Accessibility and confidentiality issues: Business and service models are also one of the challenges that need to be addressed. Accessibility challenges arise because a large number of industry stakeholders are present. Furthermore, different stakeholders from various IoT devices when combined in a specific order, the cloud infrastructure can eventually result in a situation where different areas of systems are maintained by completely dissimilar entities. It could be a scenario in a cloud where IoT devices which incorporate different stakeholders are owned by the state, whereas a cloud company may own fog nodes.

When multiple players at different levels are involved, it is difficult and quite a challenging task how IoT facilities may be linked with cloud computing and fog services, and then how they can be observed and managed to security vulnerabilities. This creates issues in arbitrating roles and permissions in IoT.

Several networking technologies, such as wired devices, mobile and wireless are used in computing systems. Networking tasks such as convenience of resources, interoperability and scalability may be partially addressed when resources are consolidated within the cloud. Moreover, fog and edge computing can help overcome network bottlenecks, latency and other issues. Smart service placement is one possible way to solve this problem that can be accomplished more specifically through data localization. This approach requires administering data closer to the required services. Addressing difficulties at the end-user and IoT is the primary goal of this research.

1.3 Importance of IoT Security

Ensuring security is important for all the environments in order to maintain highest safety of the data. To enhance the reliability and to mitigate the vulnerability in the IoT environment, IoT devices are embedded with safety and security measures [8].

IoT devices encompass many objects such as home appliances, office utilities, vehicles and smart devices. These devices are connected with sensors, they could transmit and process the data. Hence, IoT devices communicate with other devices with or without people intervention in it. However, while transferring data, all the devices are vulnerable to security threats at different layers of the network architecture. For instance, in the application layer, different messaging protocols and service discovering protocols have been implemented. Therefore, Most Common Vulnerabilities and Exposures (CVE) list have analysed ample solutions for ensuring privacy and security of the data [9].

In recent years, security plays a major role in complex IoT network architectures. It not only includes software but hardware also. Hardware in IoT also suffers from many security threats such as hardware Trojans, inserting wrong chips, illegal piracy of IP, original design could be spoofed and illegally implemented in another component [10]. However, unauthorized access could be avoided using advanced encryption systems and validation in primary designing stage onwards in the hardware [11].

In digital era, Machine-to-Machine communication has evolved with the help of interconnected devices like IoT, cloud. However, despite advancements in security technologies, they remain vulnerable to cyber threats. Consequently, attackers can exploit these vulnerabilities to breach the security chain, leading to unauthorized access and theft of sensitive information stored on the devices.

Hence, cyber attackers could destroy the potential physical infrastructure and access the private data. Some of the attacks like malware injection, phishing, hacking, SQL injection, Man-In-The-Middle, advanced persistent threats could compromise the integrity of the device and data associated with the device. To mitigate these attacks, some of the counter measures have been implemented such as: access control, encryption, authentication, regular and random security updates, physical security, IP fast hopping, back doors and login process, and intrusion detection systems to safeguard the IoT based critical infrastructure [12].

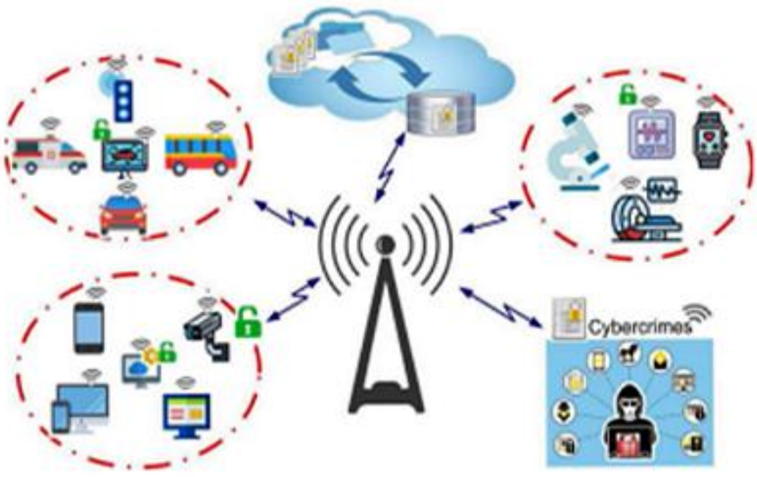


Figure 1.1. Denotes the security threats in data transfer in IoT devices

The Figure.1.1. depicts the wireless network environment, cloud of things, and IoT devices, data transferring architecture. The scenario depicts the ad-hoc and heterogeneous network environment and cyber-attacks in the internet service providers [13].

To enhance the security goals, traditionally many measures are implemented in the network functionality. The goal of security is grouped into three categories: confidentiality, Integrity of data, and availability of data. To attain the security goals c numerous security policies and protocols are implemented [14].

1.4 Traditional Methods and Its Issues in Accomplishing IoT Security

Traditional security measures include Role-based access control methods, Identity-based access control methods, and Discretionary-based access control methods.

Access control mechanisms exhibit several inherent limitations, including susceptibility to single points of failure, reduced reliability, and challenges in widespread deployment. Traditional access control frameworks are predominantly designed with centralized architectures, making scalability difficult as the system's environment expands. Additionally, these mechanisms often suffer from low throughput, further constraining their efficiency.

In the context of the Internet of Things (IoT), devices operate in heterogeneous and dynamic environments, necessitating mobility and adaptability. Consequently, conventional access control models are often inadequate for securing IoT ecosystems. The inefficiencies in these security mechanisms contribute to various cyber threats, including Denial-of-Service (DoS) attacks, spoofing, insider threats, password-guessing attacks, and data breaches [15].

However, authenticating the IoT devices or smart devices is a challenging part in the modern environment. Therefore, password authentication is not sufficient and feasible for IoT devices. Similarly, integrating the cost consuming fingerprint scanners and NFC readers are not possible for everyone and every place. These options are not suitable for inexpensive devices. In addition, IoT devices are highly decentralized, IoT devices size and shape are different. Therefore, uniform authentication processes are not suitable for all the devices. Hence, the timestamp authentication such as wearing a wristband or smart ring has been implemented in the study [16].

Authenticating and authorizing the individual plays an important role, while ensuring safety and security of the data available in IoT devices. For authorizing devices, FIWARE, OpenMTC, and AWS are already designed and implemented. However, failure in network structure or cloud servers affects the data reliability and integrity of the server. For instance, failure in authentication from the server side leads to the unavailability of the data to the connected devices [17].

Most commonly, security in the internet relies on the security protocols implemented on the network or devices. Various authentication processes are involved in different formats, but a secure and lightweight protocol implementation process is necessary for ensuring the users and confidentiality of the information. Hence, the three level security authorizations have been evolved in the study. In some mechanisms, fuzzy extraction of the user's biometrics, one-way hash function, and XOR function has been used to extend the security. However, the implementation of such three level mechanisms is suitable for a small range of IoT devices only and does not perform in the commercial environments. [18].

Cyber-attacks frequently access, alter or destroy the sensitive information stored in the servers. IoT is vulnerable to several network layers such as application layer, network layer, and sensing layer by which sensitive information could be obtained by the attackers. Furthermore, cryptosystems embedded with IoT devices are expensive, so multi-factor authentication with hash functions have been implemented to defend against the vulnerability and to provide the CIA [19].

Likely, IoT devices are deployed in known and unknown environments, which are prone to cyber-attacks. Due to vulnerable devices, many studies have focused on authenticating the IoT devices securely. Hence, the [20] study has focused on automated validation of internet security protocol, which has been robust against modification of data, session key disclosure, impersonation attacks and eves dropping attacks. The study has ensured data confidentiality and privacy. This mechanism is applied in the healthcare industry with limited resources not suitable for wide range of industrial IoT test cases. To secure the data, RFID based technology has been implemented in recent years. RFID based products contain a tag adopted with it, which are accessed by the RFID reader. The tag has encompassed the information about product details, price, colour, manufacturing date, and some more local information about the product. The advanced version of RFID facilitates the digital supply chain, detecting duplicate products, and location tracking etc. But security breaches have occurred in RFID tags also, because the keys provided to RFID are static and the spoofed keys could be reused by attackers. The problem is rectified with appending the next keys with the previous tags known as Message Authentication Code (MAC) authenticity. The suggested study has implemented secured protocol against DoS and jamming attacks [21].

Similarly, authentication and access control mechanisms have been implemented in several networks such as third generation and fourth generation networks with Authentication and Key Agreement (AKA) protocol. The 5th generation IoT devices have required a lot more security features; the study [22] has focused on implementing Slice Specific Authentication and Access Control (SSAAC) protocol, to provide better security resilience, with a considerable amount of network load. Hence, the technique has to be improvised for adopting a wide range of networks like exponentially increasing use of IoT.

IoT devices are most commonly available in heterogeneous environments. The devices are subject to harmful attacks. For instance, IoT devices are extensively affected by the various Malwares. The devices are compromised by creating botnets and Distributed Denial of Service Attack (DDoS) takes place on them. The existing cryptography solutions have only been applied to centralized network architecture. Therefore, blockchain based tamper proof security structure has been implemented in the scalable and decentralized network architecture in recent years [23].

1.5 Evolution of Blockchain and its Authentication in Achieving IoT Security

Blockchain technology has been implemented in creating the digital currency Bitcoin for the past few decades. The popularity of the digital transaction era has presented many challenges. The incorporation of blockchain technology has eradicated the double spending issues, breaching the vocal or signed contract issues faced during the non-digital era, and due to availability of data in centralized places or everywhere in the network, redundant or altered information was not presented in any case. Moreover, blockchain technology is robust against many security issues such as alteration of data or account details, Man-In-the-Middle attacks [24].

Blockchain technology ensures the reliability of data in the network and distributed in the blocks of data across the connected devices. Any entries in the data are noted as blocks of transaction. Each block is connected with another block by linking the address of the current block to the previous blocks in the network. For implementing the process, a hash algorithm is applied to ensure the integrity of the data [25].

Generally, peer-to-peer networking, distributed databases, and public key cryptography are utilized to incorporate the blockchain technology in real-time transactions without having or monitoring centralized authority or broker. However, blockchain technology has followed the energy consuming process called Proof-of-Work (PoW) [25]. PoW consists of puzzles in blocks of all the transactions carried out in the network environment. Though, if the connected IoT devices are increased, then the huge traffic flow will be generated in the network, which is susceptible to vulnerable attacks. The perceptron layers (physical Layer) of the IoT devices are monitored and information is extracted from the physical properties stored for the formation of the blocks in the blockchain. Besides, hash function and encryption function, Merkle tree and other techniques have been implemented in the blockchain [26].

Additionally, blockchain has facilitated the development of Smart Contracts (SC) which contains complete transaction histories and records. These records are securely stored over an extended period without modification. Leveraging the integrity of existing records, Smart Contracts ensure that agreements between parties, once recorded, cannot be altered or overridden in the future. Consequently, SCs autonomously execute agreements within a decentralized environment, eliminating the possibility of contract disputes and preventing the involvement of untrusted third parties [27].

Similarly, blockchain based platforms have been implemented with various programming languages in various aspects. Likewise, Ethereum smart contracts have focused on completing the contracts made by the two parties. Therefore, Ethereum based smart contract platform has been implemented widely due to its popularity and simplicity. Ethereum has generated high throughput, while implementing blockchain in the network [28].

Meanwhile, blockchain technology has utilized the distributed ledgers in it. Therefore, maintaining the ledger has provided the benefits to the organization, for the higher level of trust about the transactions. Blockchain technology has ensured the privacy and security of valid data. The Replication of data and ledger available throughout the network in all the devices ensure integrity of the data. The alteration in any one of the devices will not affect the entire transaction history or blocks are allowed any modification in the connected device without referring to the other records. The utilization of blockchain technology beyond Bitcoin and crypto currency [29].

Prior to the implementation of blockchain technology, MySQL databases were commonly used for data storage and retrieval. However, traditional databases operate in a centralized manner, where an administrator has complete control over data management, including modification and deletion. In contrast, blockchain technology is decentralized, immutable, and distributed across the network. Each transaction is stored as a block of information and secured using a robust cryptographic hashing algorithm. Furthermore, each block contains a cryptographic puzzle that must be solved to alter or delete the stored information, ensuring enhanced security and data integrity. Figure 1.2 provides a detailed representation of the blockchain architecture.

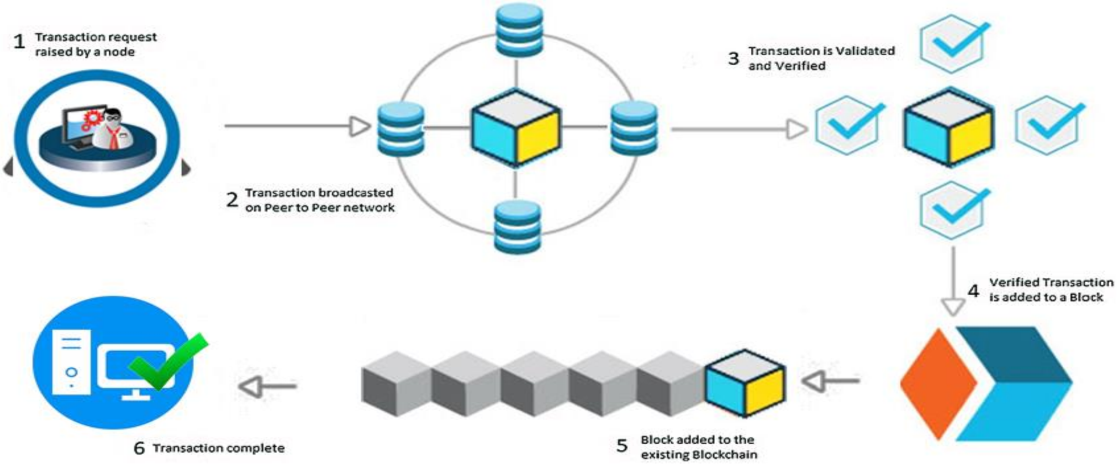

1 Transaction request raised by a node
2 Transaction broadcasted on Peer to Peer network
3 Transaction is Validated and Verified
4 Verified Transaction is added to a Block
5 Block added to the existing Blockchain
6 Transaction complete

Figure.1.2 Transaction Request Process in Blockchain

The Figure.1.2 shows the blockchain technology implementation network architecture. The structure shows that the IoT device or node raised the request for the transaction. Afterwards, the transaction has been created as blocks and blocks broadcasted to all the networked devices then the transaction validated by the other nodes in the network. The new transaction history is appended in the blockchain as a block. After completing the process the blockchain cannot be altered or deleted by anyone in the network [30].

1.6 Emerging Trends in Blockchain with Decentralized Authentication for Achieving IoT Security

The incorporation of blockchain technology into IoT devices enhances security across networked systems. Blockchain operates based on Distributed Ledger Technology (DLT) with an affixed timestamp, ensuring data integrity. To further strengthen security, technologies such as Multi-Access Edge Computing (MEC), Artificial Intelligence (AI), and blockchain-enabled frameworks have been integrated into IoT ecosystems. However, as IoT devices function within decentralized networks, achieving both security and privacy in IoT and edge computing remains a significant challenge. For instance, blockchain-enabled edge intelligence faces trade-offs between security, data processing speed, and network decentralization.

Blockchain in the Financial Sector: Blockchain technology has revolutionized the financial industry due to its decentralized nature. The increasing adoption of cryptocurrency in recent years has necessitated enhanced security measures. To ensure secure and efficient financial transactions, consensus algorithms such as Proof of Participation (PoP), Paxos, and Proof of Authority and Hierarchy (PoAH) have been integrated with blockchain technology. This optimization has enabled fast and secure transactions over the internet, supported by IoT networks. Additionally, blockchain-based architectures maintain transparency, accountability, integrity, and scalability within transaction records. However, privacy and security depend on the underlying network architecture layers.

Blockchain in Healthcare: Blockchain technology has also been implemented in the healthcare industry to address real-time challenges. Although Electronic Health Records (EHRs) are widely used, advancements in Internet of Medical Things (IoMT) have introduced cost-effective and efficient tools for patient data management. Blockchain-based healthcare networks eliminate the need for intermediaries in health record transfers, thereby improving security and reliability in the digital healthcare ecosystem. Furthermore, smart contracts contribute to reducing processing time and costs, enhancing operational efficiency.

Blockchain in IoT, Drones, and Cloud Computing: Blockchain technology ensures security in decentralized networks such as IoT, drones, 5G-enabled devices, and cloud computing. To mitigate security breaches in cryptographic applications, blockchain has been employed to strengthen data privacy, confidentiality, authentication, and access control mechanisms beyond traditional security frameworks. As a result, Quality of Service (QoS) has significantly improved in drones, IoT networks, and cloud-based systems.

Blockchain in Decentralized Cab-Sharing Systems: Blockchain technology has also been applied in secure and decentralized cab-sharing systems. The increasing use of GPS tracking systems and smartphones has enabled drivers and riders to efficiently manage vacant seats in their vehicles. By leveraging blockchain, personal information remains protected, ensuring privacy while allowing transparent transactions. Additionally, the use of blockchain technology reduces travel costs and fuel consumption, distributing expenses among passengers. The inherent transparency, immutability, and verifiability of blockchain further enhance passenger security.

Blockchain in Supply Chain Management: Blockchain has expanded its applications in supply chain management, offering a decentralized ledger system that ensures secure data transfer and storage. Key benefits of blockchain in supply chain management include efficient algorithm implementation, smart contract execution, and improved traceability. Figure 1.2 illustrates the sequence of processes involved in blockchain adoption across industries. Additionally, Figure 1.3 highlights the significance of blockchain technology in various domains.

Blockchain processes consist of four key phases:

1. Pre-Transaction
2. Transaction
3. Post-Transaction
4. Monitoring

The decentralized and distributed nature of blockchain ensures the confidentiality, integrity, and availability of data across networks. As a result, digitally shared information remains immutable, safeguarding financial transactions, health records, and other critical data across industries.

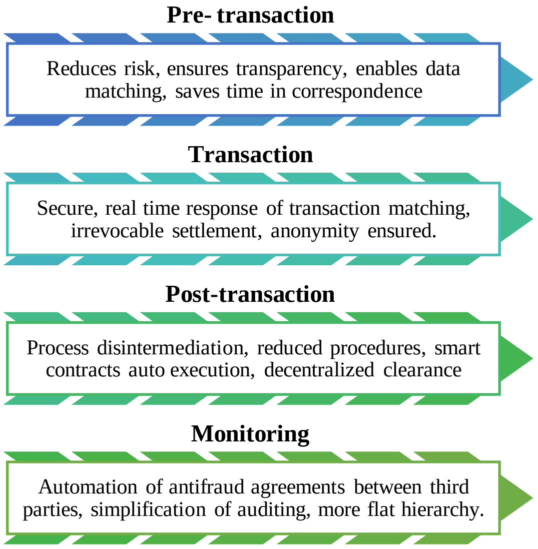

Pre- transaction
Reduces risk, ensures transparency, enables data matching, saves time in correspondence
Transaction
Secure, real time response of transaction matching, irrevocable settlement, anonymity ensured.
Post-transaction
Process disintermediation, reduced procedures, smart contracts auto execution, decentralized clearance
Monitoring
Automation of antifraud agreements between third parties, simplification of auditing, more flat hierarchy.

Figure.1.3. Processes in Blockchain Technology

In supply chain management, the blockchain has stored the information about the stocks as blocks and linked with address of the next block in previous blocks. Each block address is created with the value stored inside the blocks. Therefore, blocks could not be removed or altered which ensured the security in supply chain management [36].

1.7 Problem Identification

Blockchain platforms typically require extensive computational control, particularly when addressing the complexities of interconnecting IoT nodes. To mitigate these challenges, a decentralized model is implemented. However, the traditional centralized blockchain model, while cost-effective, imposes limitations on data flow and scalability.

Security remains a critical challenge within the IoT ecosystem. Due to the vast number of interconnected devices, IoT systems are highly susceptible to cyber threats and hacking attempts. To counteract these risks, a decentralized blockchain approach is integrated, ensuring continuous connectivity across network nodes that actively participate in the consensus process. Nevertheless, the persistent connectivity of IoT devices also introduces security vulnerabilities, increasing exposure to potential attacks.

For effective IoT deployment, reliability and scalability are essential. Conventional IoT security frameworks cannot be solely governed by a single gateway, as centralized architectures, despite their efficiency, lack robust security mechanisms. A compromised gateway could jeopardize the integrity of the entire IoT network. By adopting blockchain technology, IoT devices can securely communicate and interact without intermediary interference, enhancing traceability, improving communication security, and enabling automated workflows.

Despite its advantages, blockchain adoption in IoT faces several challenges, including technical complexity, interoperability constraints, cultural resistance, regulatory uncertainties, and coordination difficulties, which may lead to delays in implementation. Therefore, substantial modifications to existing workflows are required to ensure seamless integration and operational efficiency..

1.8 Motivation of the Study

The integration of Blockchain and Internet of Things (IoT) in Supply Chain Management (SCM) enhances transparency, security, and efficiency by enabling real-time tracking, automated validation, and tamper-proof record-keeping. This combination addresses key challenges in SCM, such as counterfeiting, inefficiencies, and lack of visibility in logistics operations.

1.9 Objectives

To achieve the enhanced security in blockchain with the combination of IoT, following objectives were set for research work:

Research Objectives:

To overcome the aforementioned gaps, following objectives are formulated:

1. To study and analyze the existing decentralized authentication and access control mechanism for IoT devices on various performance parameters.

2. To design and develop a novel decentralized authentication and access control mechanism for IoT devices on supply chain management applications for confidentiality and data privacy issue in IoT.

3. To design a novel IoT model to address heterogeneity issues and to improve the scalability of block-chain integration in IoT devices.

4. To assess the performance of the proposed method using different parameters Throughput, Latency, Efficiency, and Block Size.

1.10 Significance of the Study

Blockchain is an emerging and advanced technology that plays a crucial role in the evolution of Industry 4.0, where challenges in cloud computing and IoT applications are effectively managed with resilience and security. Bitcoin, a non-financial blockchain application built on platforms such as Ethereum and Hyperledger, addresses concerns related to transparency, trust establishment, and decentralized system availability for users.

Businesses providing blockchain services are increasingly developing non-financial applications that enhance efficiency and operational outcomes in various sectors, including oil and gas, industrial automation, and healthcare. As blockchain adoption grows, logistics and technology companies face increasing pressure to implement blockchain-based Distributed Ledger Technology (DLT) frameworks that support regional development policies and promote blockchain-driven innovation.

From a global economic perspective, countries that fail to establish legal frameworks for blockchain adoption may risk falling behind in technological advancements over the coming years. Blockchain has the potential to transform multiple industries, particularly the supply chain sector.

Blockchain in Supply Chain Management: Blockchain technology has already demonstrated its effectiveness in enhancing supply chain operations by addressing existing challenges. It significantly reduces the overall cost of tracking and managing goods throughout the supply chain while fostering trust and transparency among stakeholders, administrators, consumers, and logistics providers.

Blockchain for IoT Security: Given its numerous advantages, the current research aims to explore the advancements in blockchain technology for its adaptability in securing IoT devices. By leveraging blockchain, the study highlights its importance in ensuring security, trust, and efficiency across diverse applications.

1.11 Scope of the Study

Blockchain, integrated with smart contract technology, offers potential security solutions for IoT networks to a certain extent. A blockchain-powered centralized access control framework improves efficiency compared to conventional security techniques. While blockchain-based security mechanisms demonstrate significant potential, further advancements are required to develop comprehensive decentralized security solutions for IoT systems.

Key enhancements for achieving robust security in IoT networks using blockchain technology include:

Multi-Factor Authentication for Data Users: Implementing a multi-factor authentication (MFA) mechanism ensures that only legitimate users can participate in the system. Additionally, data owners undergo authentication, ensuring that only original and verifiable information is uploaded.

Decentralized Blockchain with Lightweight Hashing: The incorporation of lightweight hashing algorithms into decentralized blockchain networks minimizes computational overhead while maintaining security and integrity. Given the highly heterogeneous nature of IoT environments, utilizing lightweight cryptographic algorithms enhances efficiency.

Dynamic Access Control Policies: Establishing dynamic access control policies based on variable attributes ensures that data access permissions align with user-specific requirements while maintaining security and flexibility.

Trust-Aware Consensus Algorithm for Scalability: A trust-aware consensus mechanism is introduced to enhance blockchain scalability by selecting trusted nodes for block verification. The selection process relies on trust value estimation, ensuring that only reliable nodes participate in the validation process.

Cloud Scalability through Data Clustering: To address scalability challenges in cloud-based blockchain storage, a cluster-based data management approach is implemented. Data uploaded by data owners (DOs) is categorized into clusters based on attribute similarity, ensuring efficient data organization, retrieval, and storage management.

1.12 Organization of the Thesis

This section outlines the structure of the thesis, which is systematically organized as follows:

Chapter 1: Provides elaborative information on the fundamental concepts of blockchain technology, including the objectives, motivation, significance, and scope of the research.

Chapter 2: Reviews the existing solutions by examining various approaches utilized in prior research. It also discusses the classification and analysis of related works, highlighting key research gaps and associated challenges.

Chapter 3: Introduces the concept of decentralized authentication and access control, specifically designed for data owners and users in the cloud-IoT ecosystem. This chapter explores the development of lightweight cryptographic techniques and hashing algorithms to enhance scalability and security. Additionally, it examines the limitations of conventional hashing mechanisms in blockchain authentication and the constraints associated with security credentials.

Chapter 4: Introduce a priority-based lightweight authentication and access control framework for Cloud-IoT (SCSB), leveraging decentralized blockchain technology. The data owner authentication mechanism ensures secure data uploads. The cloud-stored data is efficiently clustered, optimizing storage scalability. A novel Proof-of-Authentication (PoA) mechanism is introduced to validate multiple requests by selecting a trusted node for verification. To ensure secure data transmission, the confidentiality level of the data is determined using a dual fuzzy algorithm before encryption. Additionally, the integration of lightweight cryptographic techniques and parallel processing algorithms allows for seamless operation across multiple IoT devices, addressing scalability and resource constraints.

Chapter 5: Summarizes the key findings of the research and emphasizes its significance in addressing security challenges in blockchain-integrated IoT environments. This chapter also outlines the potential future research directions.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Blockchain is a decentralized system of interconnected nodes that facilitates secure data transactions. It is increasingly utilized to enhance the security and efficiency of Internet of Things (IoT) system transactions due to its distributed architecture. Access control is a critical security challenge in IoT environments, as it is essential for ensuring data security and controlled resource sharing. However, implementing conventional access control mechanisms in IoT devices is challenging due to their resource constraints.

The IoT communication paradigm supports a growing ecosystem of interconnected devices capable of sensing, collecting, transmitting, and sharing data across diverse applications. Globally, IoT technology is being widely adopted to improve quality of life across various domains, including smart marketing, smart homes, precision agriculture, smart cities, intelligent transportation systems, industrial automation, healthcare, and education. These applications have a direct impact on human life [86].

Despite its widespread adoption, IoT security remains a critical concern, necessitating ongoing research. IoT authentication is a fundamental security mechanism required to establish trust in IoT devices [87]. Recent studies highlight the significance of blockchain technology in strengthening IoT security by enabling the development of decentralized system architectures. This approach ensures the security and authenticity of IoT nodes operating in untrusted networks without reliance on centralized third-party entities. Blockchain technology facilitates direct data exchange between entities, eliminating the need for intermediaries. Furthermore, blockchain enhances transparency, availability, and immutability, allowing users to continuously monitor and track transactions. It optimizes operations by reducing transaction complexity, accelerating processing times, and mitigating security risks.

Each transaction within a blockchain is cryptographically recorded in a block, which, upon validation, is permanently added to the blockchain ledger. This decentralized mechanism eliminates third-party involvement in transactions and removes the need to store sensitive data in centralized repositories [88].

The integration of blockchain with IoT offers multiple advantages, including decentralization, enhanced security, transparency, immutability, and autonomy. However, challenges such as data storage limitations and scalability issues persist. Several blockchain-based IoT authentication schemes have been proposed to establish secure network connections. One such approach employs a blockchain-centric authentication mechanism for IoT devices. However, this scheme introduces additional storage, computational overhead, and communication complexity due to the repetitive use of multiple devices attributes. Another proposed framework incorporates digital identity creation and management, storing IoT device credentials on a distributed ledger, though it also incurs processing overheads [89].

This chapter reviews existing research efforts aimed at securing IoT devices through centralized authentication methods.

2.2 Blockchain Based Decentralized Authentication for IoT Devices

Blockchain-based decentralized security architecture ensures mutual authentication, confidentiality, and adaptability against various threats. The proposed mutual authentication method leverages blockchain technology to provide resistance against multiple attacks. To facilitate centralized authentication for connected IoT devices, edge servers are deployed. Subsequently, a blockchain network comprising centralized edge servers is established to enable decentralized authentication and verification within heterogeneous IoT systems.

For secure communication and real-time data exchange, IoT devices are expected to function in a distributed environment with stringent low-latency requirements. The primary objective of the study [90] is to develop an authorization framework and a blockchain-based distributed authentication mechanism that enables interoperability among devices across different platforms. This framework supports secure communication between devices within the same IoT system as well as across separate IoT systems. The proposed system utilizes blockchain technology to capitalize on its decentralized structure and cryptographic capabilities while incorporating fog computing to address latency challenges. Furthermore, the attack model and security requirements are defined to evaluate the proposed approach and its effectiveness in meeting security criteria.

IoT systems increasingly operate under zero-trust conditions, where any device or system may be compromised and, therefore, cannot be inherently trusted. To minimize reliance on centralized servers, data generated by IoT devices may be processed and shared through edge computing, introducing additional security and privacy concerns. The study [91] presents a zero-trust, blockchain-enabled information-sharing method to address these issues. This approach ensures participant in centivization while maintaining fairness, entity anonymity while preserving authentication, and data privacy while upholding data integrity. By leveraging consensus mechanisms, smart contracts, and efficient voting strategies, the system prevents the dissemination of false information by filtering out unauthenticated users. The security of the proposed solution is demonstrated within a universally composable security framework, and its functionality is validated using the Ethereum blockchain platform.

As IoT systems become increasingly integrated into daily life, the proliferation of IoT devices and services necessitates secure access and communication. The study [92] introduces an approach called Bubbles of Trust (BoT), which establishes protected virtual zones to facilitate secure communication among IoT devices. BoT can be applied across various IoT scenarios and services, leveraging the security properties of public blockchain technology. Moreover, the study defines security requirements for IoT authentication and constructs a threat model. The evaluation of the proposed approach demonstrates its capability to meet security requirements and withstand potential attacks. Additionally, an extensive study on energy and time consumption has been conducted using diverse IoT devices.

Advancements in manufacturing technology have significantly improved operational efficiency and reduced costs. However, cost-cutting measures often neglect cyber security, particularly in complex environments involving multiple stakeholders. Furthermore, legacy systems and smart manufacturing processes frequently lack a security-by-design approach, making them highly vulnerable to cyber threats. The study [8] proposes a decentralized framework for IoT device integrity assurance and authentication, utilizing master nodes and private blockchains to monitor and enforce administrator-defined policies. By integrating Distributed Ledger Technology (DLT), the proposed solution enhances transparency, auditability, and decentralized consensus to verify firmware integrity and measurement values. The fully decentralized architecture eliminates centralized components that could serve as single points of failure, thereby strengthening security. The model facilitates an efficient and reliable event flow, from the initial rule-setting phase to the detection and alerting of potential malicious activities.

With the widespread adoption of intelligent and autonomous devices, seamless collaboration is crucial for improving human living standards. As the number of connected IoT devices continues to increase, identity management has become a critical requirement for edge IoT systems [9]. However, the resource-constrained nature and heterogeneity of IoT devices make conventional identity management schemes infeasible. To address this challenge, diverse application domains are adopting DLT and blockchain-based security solutions. The study proposes a distributed identity management framework for edge IoT systems, which is adaptable to various IoT applications to ensure secure and reliable device communication. The proposed model integrates distributed ledger-based identity providers near the fog layer of the IoT architecture, ensuring proximity-based identity verification. This model supports identity management for users, IoT devices, handheld devices, and edge gateways. A permissioned ledger is employed to enhance security and privacy in identity management systems.

The advancement of communication and computing technologies has led to the proliferation of sophisticated devices, such as smartphones, electric vehicles, and smart appliances. The rapid expansion of IoT has significantly increased the scale of device collaboration to provide enhanced societal benefits. However, traditional security and privacy mechanisms have become inadequate for IoT systems with decentralized or distributed topologies. Distributed Ledger Technology (DLT), an emerging digital technology, comprises various decentralized data structures that ensure data integrity through cryptographic mechanisms. DLT offers security, privacy, and decentralized computing capabilities while addressing the constraints of IoT nodes. The research aims to explore the intrinsic properties of DLT and their potential applications in overcoming security challenges in decentralized IoT environments.

Table 2.1: Summary of Related Work

Title of the paper	**Main findings or conclusion relevant to the proposed research work**
A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain [46]	This work presents a proxy re-encryption approach for data sharing in the cloud with the incorporation of Blockchain. It develops identity-based encryption and proxy re-encryption to provide security. According to this work, the Blockchain is considered a trusted authority that gives secret keys based on the user identities. In Blockchain, the traditional SHA-256 hashing algorithm is used. The data owner encrypts data based on the generated random number. **Problem Identified –** • Since the encryption is performed twice, it consumes twice the time for the conversion of cipher text. Similarly, the decryption is also conducted twice, consuming twice the time. The traditional use of the SHA-256 hashing algorithm in the Blockchain is not lightweight and cannot sustain collision attacks.
Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems [47]	The authors of this paper have proposed a hybrid centralized and blockchain-based authentication architecture. The devices are registered and authenticated using security credentials as identity and group identity. After successful authentication, the symmetric encryption key is used for encryption. Due to the use of a symmetric key, it is encrypted based on the generated public key. In this work, proof-of-work is presented to validate the blockchain transactions. **Problems Identified**: • The proof-of-work consensus algorithm could

	not support the system's scalability, which fails to operate with the increase of requests. • The Blockchain uses a traditional SHA-256 hashing algorithm, which includes multiple computations than the lightweight hashing algorithm. • Also, symmetric key cryptography requires a secure exchange of keys since the same key is used for encryption and decryption.
Integration of Blockchain and Internet of Things: Challenges and Solutions [48]	In this paper, the Blockchain-based Internet of Things (BIoT) integration is developed for provisioning security. It supports the heterogeneous system, so there occurs traffic demand. On the other hand, the common challenges are privacy, throughput, security aspects, and energy efficiency. The research direction is developing solutions for critical challenges such as adaptable security, trust framework, blockchain transaction capacity, and scalability.
Blockchain-envisioned access control for Internet of Things applications: a comprehensive survey and future directions [49]	Blockchain technology presents access control protocols in IoT for improving the countermeasures for security issues and attacks. The access control protocols are broadly classified into certificate-less, certificate-based and blockchain-based. The access control scheme operates in two processes node authentication and key establishment; it applies to multiple applications such as smart homes, industry, vehicle communication, the healthcare environment, the marine industry, and so on. The security issues in IoT are solved using Blockchain that follows hashing, decentralization, data storage, and authorization. Due to the provisioning of multiple features in

	blockchain technology, it reduces the challenges in security.
LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment [50]	In this paper, the authors have proposed a lightweight blockchain-based security scheme (LBSS) for the application of healthcare environments. The three main aspects of security integrity, confidentiality, and availability, are concentrated in this work. Data fragmentation is performed to improve data confidentiality, and the hashing scheme enables provisioning integrity. **Problem Identified:** • Data fragmentation requires combining the data again during retrieval, which needs to be accurate without any mismatch in the data.
Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV [51]	This paper proposes a blockchain-enabled data access method with attribute-based encryption offered for the Internet of Vehicles. Edge nodes are deployed in the system, which can minimize the computations. The accessibility is structured in a tree format, following the Bilinear Diffie-Hellman method. The two main entities are central and local key authorities, which are fully trusted and manage dynamic attributes, respectively. It uses local encryption and outsourced encryption in this work.
FairShare: Blockchain Enabled Fair, Accountable, and Secure Data Sharing for Industrial IoT [52]	In this paper, the authors have presented FairShare, which designs a fair, accountable, and secure data-sharing scheme for Industrial IoT. The developed system model incorporates fog nodes to reduce the computations to be performed. To assure security and privacy, proxy re-encryption is used. For the process of encryption, the AES cryptography algorithm generates

	symmetric and re-encryption keys. **Problem Identified:** The AES cryptography algorithm is a symmetric key encryption that uses the same key for encryption and decryption. So while sharing the symmetric key, it could be leaked by an intruder.

2.3 Scalable Consensus Algorithms and Storage in Decentralized Blockchain for Heterogeneous IoT System

In IoT environments, security and privacy represent significant challenges. Recently, numerous studies have sought to implement blockchain technology to enhance the security of IoT networks. However, the lightweight nature of IoT devices often fails to meet the computationally intensive requirements of blockchain-based security models. The study [93] proposes a method to address this issue by designing an IoT blockchain architecture that stores system identity data in a distributed ledger. The Blockchain of Things (BCoT) framework has been introduced to facilitate authentication transactions in the blockchain system without modifying existing system applications or hardware. Additionally, a device identification model has been proposed for blockchain-based identity authentication, employing a feature-based approach for system traffic flow. Lastly, the BCoT Sentry structure has been developed as a reference application for the proposed model. Experimental results have demonstrated the feasibility of the presented framework [141].

Over the past decade, IoT has garnered significant attention, with the number of connected IoT devices surpassing the global human population. Its widespread applications—ranging from smart cities, smart transportation, and smart homes to agriculture and environmental monitoring—have been driven by its cost-effectiveness, ease of deployment, and implementation simplicity [142]. However, IoT systems face various security and privacy challenges, particularly concerning device identification. Authentication is a fundamental process in identifying devices, yet most existing research relies on centralized systems. This study evaluates the effectiveness of a Decentralized Authentication (DecAuth) mechanism using Ethereum's blockchain framework. The results [94] indicate that IoT system authentication can be performed in a decentralized manner. Furthermore, analysis of the results confirms that the proposed method provides security against common cyber-attacks.

IoT networks consist of vast interconnected devices that require a robust and scalable security system tailored to their limited computational capabilities. Node authentication is a critical security component for IoT. Traditional authentication systems, which depend on a centralized authority, pose a single point of failure risk. Blockchain, as a decentralized and distributed network, offers an alternative approach for node authentication. However, most IoT blockchain-based applications in the literature rely on high-power devices connected to existing blockchain systems, limiting their applicability to IoT networks and reinforcing the single point of failure issue. To address these concerns, the study [95] presents a blockchain-based decentralized authentication framework that groups IoT devices into clusters based on location, computational capacity, and energy availability. A hierarchical network of interconnected blockchain authenticates devices within each cluster. A consensus protocol has been designed to verify identity-based encryption key signatures for devices and their associated clusters, thereby reducing computational overhead. Simulations of the proposed structure indicate reductions in memory and CPU loads of IoT devices. Further testing using Raspberry Pi and Docker-based networks validates a decrease in computational demand. Security and performance analysis demonstrates that the proposed framework is both scalable and lightweight while ensuring robust security protection.

Blockchain technology has been anticipated as a potential solution to address the security concerns in IoT systems, where communication security remains a critical issue. Whether transferred data involves financial transactions, sensor measurements, or authentication messages, blockchain networks verify their legitimacy and integrity before acceptance and storage. By requiring consensus among nodes for transaction validation, blockchain significantly reduces the possibility of unauthorized access or fraudulent transactions [95]. Recently, a blockchain-based authentication system has been proposed for access management in IoT devices using a distributed approach. While this protocol claims to preserve user security and privacy, the study has identified vulnerabilities related to token reuse, replay attacks, and traceability, with a success probability and complexity of one [96]. The improved blockchain-based authentication protocol, IBCbAP, has been proposed to provide enhanced security features, including secure access control and anonymity. The study has implemented IBCbAP using a local Ethereum blockchain and JavaScript programming, while formal and informal security validation was conducted using the Scyther tool. The research [96] confirms that IBCbAP offers adequate security at a reasonable computational cost.

While numerous studies focus on blockchain integration in IoT systems, many remain in their early stages. Existing research primarily explores the benefits of blockchain characteristics for IoT systems. Due to limited computational resources, IoT devices have not traditionally been considered integral components of blockchain networks. Instead, high-powered routers, gateways, or computers act as gateway nodes, serving as interfaces between IoT devices and the blockchain. Each IoT device is assigned a unique address (a pair of private and public keys). The gateway nodes, directly connected to the blockchain, facilitate communication between IoT devices and blockchain networks. Smart contracts enable automated interactions among IoT devices without human intervention. The study proposes an authentication scheme for IoT systems under decentralized authority rather than centralized control [97].

In addition to blockchain integration, this study explores the convergence of edge computing and blockchain to establish decentralized security architecture for IoT systems in real-time applications. Recent studies have introduced edge nodes, gateways, and cloud-based intermediaries between blockchain networks and IoT devices [98]. The proposed study presents centralized, decentralized, and hybrid authentication architectures to provide secure and efficient IoT device authentication. The findings indicate that the model reduces IoT device power consumption by 28%

compared to blockchain-based authentication methods and by 22% compared to centralized methods [98].

The study further investigates decentralized authentication mechanisms. In large-scale IoT deployments, decentralized authentication addresses latency challenges by verifying device entities via edge nodes. Decentralized security mechanisms are essential for ensuring data integrity and authentication consistency within edge authentication services. The advent of 5G has enhanced IoT capabilities by enabling higher transmission speeds, lower latency, massive device deployment, and extensive coverage for IoT applications. The proposed study introduces A2 Chain, a decentralized authentication framework combining blockchain and blockchain alliance technology. A2 Chain facilitates secure and efficient authentication data sharing across diverse application domains [99].

Similarly, the study discusses various authentication and access control (AC) approaches for IoT devices. One solution involves integrating AC functionalities directly into IoT devices. However, due to limited memory, computational power, and policy-handling capabilities, IoT devices struggle to maintain AC lists. Consequently, alternative solutions such as client-server models have been proposed, leveraging communication protocols for resource-constrained devices. Another approach involves using blockchain as a database to store AC policies and transaction requests [100].

The study also explores a blockchain-based architecture for securing IoT systems. The proposed solution employs a multi-agent system for decentralized AC. Traditional centralized AC solutions provide easily accessible control policies but suffer from single points of failure. Blockchain, as a distributed ledger comprising cryptographically linked data records, ensures data immutability and security. The proposed framework aligns with the Confidentiality, Integrity, and Availability (CIA) security triad, making it suitable for constrained IoT devices. Blockchain Managers (BCMs) facilitate secure communication among IoT devices, fog nodes, and cloud environments. The study presents a multi-agent system that delivers decentralized IoT AC security with lightweight mechanisms [101].

Additionally, the study examines blockchain's role in securing IoT-generated big data stored in cloud computing environments. Authentication ensures that only authorized users can access cloud-stored data. The study implements the Decentralized Blockchain-based Authentication (DBA) protocol, which utilizes decentralized blockchain technology and cryptographic hash functions for authentication. The DBA protocol is validated using blockchain technology and multiple authentication credentials [102].

The study identifies a limitation in centralized delegation, wherein legal delegations may be rejected while illegal ones are permitted, and necessitating trust establishment without third-party reliance. Blockchain (BC) offers an uninterrupted delegation mechanism by maintaining a tamper-resistant distributed ledger. The Blockchain-based Permission Delegation and Access Control in IoT (BACI) architecture introduce key components such as users, devices, IoT managers, smart contracts, and application managers. Security analysis confirms the system's integrity, availability, and confidentiality, proving blockchain as a reliable, tamper-resistant security mechanism for decentralized systems [103].

Finally, the study explores blockchain's technological evolution, evaluating consensus algorithms, platforms, and trust assumptions. The authors examine blockchain's role as a distributed data repository, external authorization logic, and OAuth2-based authentication framework. The proposed decentralized smart home architecture highlights potential security threats, including single points of failure in device authentication. Security considerations for smart cities and decentralized IoT architectures are discussed [104].

Table 2.2: Summary of Related Work

Title of the paper	**Main findings or conclusion relevant to the proposed research work**
Towards Blockchain-Based Secure Storage and Trusted Data Sharing	An attribute-based access control (A-BAC) policy is presented in this paper, which incorporates the Advanced Encryption Standard for encryption and the

Scheme for IoT Environment [53]	elliptic curve Diffie-Hellman algorithm for sharing keys. The data owner uploads data in encrypted form using AES-128, and the data attributes are stored in Interplanetary File System (IPFS). Then the stored data is accessed by the data user requesting with the file location, i.e., content identifier, and the data is retrieved and decrypted. **Problem Identified –** • The data owners and users are not authenticated in this system which is a primary security risk. Since the illegitimate data owner could upload irrelevant data or occupy unnecessary resources, in contrast, the participation of illegitimate users may increase the traffic in the network, which mitigates access to legitimate data users. • The AES algorithm is a symmetric cryptography algorithm using the same key for encryption and decryption. The data owner encrypts the file using the key generated from the AES algorithm, which is not secure since the key has to be shared with all the requesting data users.
AAC-IoT: Attribute Access Control Scheme for IoT Using Lightweight Cryptography and Hyperledger Fabric Blockchain [54]	In this paper, the authors have proposed an attribute access control scheme for IoT (AAC-IoT), which incorporates Hyperledger Fabric (HLF) Blockchain. According to this work, the data owners and users are authenticated with multiple factors ad identity, certificate, signature, and physical unclonable function (PUF). The access control policy is defined, and for every user access, the number of attributes is selected using the fuzzy logic method. The credentials of the data owner are secured using a lightweight PRESENT

	algorithm. Then, the QUARK algorithm is involved in hashing in the Blockchain. For the authentication of data users, the neural network is used that enables the authentication of multiple users at a time. **Problem Identified –** • According to this work, the credentials of the data owner are only secured using lightweight cryptography. At the same time, the data user's credentials are also significant to be secured since illegitimate users may participate in the system. This work needs to provide security for the data that is to be uploaded to the cloud. The storage of raw data cannot maintain the secrecy of the confidential data.
A Blockchain-Based Privacy-Preserving Publish-Subscribe Model in IoT Multidomain Data Sharing [55]	A secure blockchain-based privacy-preserving access control (BPAC) scheme is presented in this paper. Confidentiality is assured with the Fully Homomorphic Encryption (FHE) algorithm. In this BPAC model, the certificate authority is trusted and responsible for generating private and public keys. According to this work, the subscriber requests access directly to the publisher while the publisher encrypts and sends it to the Blockchain. Then the Blockchain authorizes the access request, which again re-encrypts before forwarding it to the subscriber. The Blockchain is considered to be a private broker in this system. **Problem Identified –** • In this work, the Blockchain performs re-encryption, i.e., encryption is processed twice, which needs to decrypt twice to extract the data, which consumes time.

	The credentials considered for authentication are not unique; hence there are chances of allowing illegitimate subscribers.
Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment [56]	The authors have developed an access control-enabled Blockchain (ACE-BC) framework in this paper. The attribute-based encryption scheme is used for encryption, and the additional homomorphic encryption is for user key generation. The Blockchain is the trusted authority in this system, and it connects with a proxy server where the data owner receives the re-encryption key. The data owner performs the encryption twice, which is decrypted twice by the data user. **Problem Identified –** • In this work, the Blockchain performs re-encryption, i.e., encryption is processed twice, which needs to decrypt twice to extract the data, which consumes time. • Using a homomorphic encryption algorithm has the traditional problem of slowness, and it requires a more significant amount of resources for processing.

2.4 Authentication and Access Control and access control mechanism with dual data storage in Cloud-IoT Using Blockchain

Access Control (AC) refers to a set of policies and rules that define whether a specific user is permitted to access services, users, other mechanisms, or procedures to interact with data resources. Blockchain (BC) is a decentralized public ledger and a Peer-to-Peer (P2P) distributed network. Its structure incorporates functionalities such as authentication, AC for IoT devices, and registration, all of which are linked to a smart contract to verify user validity. A token is generated for access authorization upon successful authentication. The authentication process varies due to diverse environments and heterogeneous architectures supporting IoT devices. The primary objective of BC is to securely transfer access tokens while enforcing user access rights, authorization checks, and transaction tracing. The study has highlighted the limitations of traditional AC methods for IoT and has examined the feasibility of employing BC systems for AC management [106].

Similarly, the study has investigated existing BC-based AC and authentication methods across various application domains, including resource sharing, cloud computing, IoT, telecommunications, and healthcare. It has provided a taxonomy categorizing existing approaches and compared them based on security capabilities, cost efficiency, and computational overhead [140]. BC has been utilized as an immutable, distributed, and secure storage mechanism for user credentials and identity verification. AC mechanisms are categorized into three primary models: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Access Control List (ACL) methods, such as Discretionary Access Control (DAC). Each approach has been applied in specific contexts. The study has demonstrated how integrating smart contracts into BC can enhance identity management across multiple websites [107].

As observed in prior research, BC treats IoT interactions as distinct transactions and facilitates programming logic execution through smart contracts. This integration enhances AC performance, confidentiality, authentication in Blockchain IoT (BIoT), and overall security. The decentralization of IoT systems through BC technology has been explored in this study. Due to the lack of standardization, an accepted IoT reference model has yet to be established. IoT is characterized by resource constraints, device heterogeneity, lack of infrastructure, security vulnerabilities, context awareness, and spontaneous interactions [139]. Middleware, a software layer positioned between the network communication layer, operating system, and application, has been introduced to facilitate process coordination and integration. Additionally, a general framework has been proposed for BIoT, incorporating system design principles [108].

Currently, authentication involves various processes, including password-based, certificate-based, and biometric-based identification methods, such as facial recognition, fingerprint scanning, and voice authentication. Traditional IoT systems, which rely on centralized architectures, present significant security and operational challenges. This issue has been addressed through blockchain-based identity authentication schemes, such as BlockAuth. BlockAuth leverages edge devices to construct blockchain nodes, providing a decentralized, secure, and efficient authentication solution. This method possesses several key features: each edge device functions as an independent node within the blockchain, and all nodes operate on an equal footing within the decentralized network. In the event of node failure, other nodes can compensate, eliminating single-point failures common in traditional systems. Unlike conventional centralized authentication units, validation occurs within the blockchain nodes, reducing risks associated with centralized validation centers, particularly in high-load scenarios. The proposed method has demonstrated improved reliability and efficiency in authentication processes [109].

Previous studies have introduced BlockAuth for authentication, whereas the current research explores an alternative, more efficient authentication mechanism [137]. This method integrates IoT devices with blockchain technology to enhance security. The study examines the challenges of device authentication in IoT and assesses the benefits of combining blockchain technology with IoT security solutions. Specifically, the study introduces an Ethereum blockchain-based authentication technique for IoT devices. To ensure secure communication between IoT devices and miner nodes, an intelligent contract-based authentication algorithm has been proposed. This method compares the proposed authentication technique with existing blockchain-based IoT authentication solutions in terms of communication overhead, financial costs, and computational efficiency [136]. The proposed model has been rigorously validated through formal modeling, Hierarchical Petri Nets (HLPN) analysis, and Z3 solver verification. Given the growing adoption of decentralized applications, Ethereum blockchain—comprising numerous Ethereum Virtual Machines (EVMs)—has been analyzed, modeled, and validated to demonstrate the accuracy of the proposed authentication method [110].

Earlier studies have utilized Ethereum blockchain for IoT authentication. In contrast, the present research [111] introduces a novel authentication scheme based on the RSA dynamic accumulator and Unspent Transaction Output (UTXO) verification method.

This approach employs a decentralized blockchain-based storage system to securely store IoT-related data, eliminating the need for third-party management. The advantages of blockchain-based storage have been assessed in terms of privacy, reliability, and security. The RSA dynamic accumulator mechanism has been incorporated to enhance security [135]. Additionally, the UTXO-based verification technique, utilizing the RSA accumulator, provides proof of participation while filtering out lightweight nodes, thereby improving transaction validation efficiency. This research proposes a decentralized storage system leveraging blockchain technology to address data reliability, privacy, and security concerns in IoT data management [134].

Previous authentication mechanisms have relied on RSA accumulators and UTXO-based verification for IoT security. However, the present study [112] introduces a multi-layered security framework tailored for IoT applications [133]. The research addresses privacy and security concerns across three fundamental IoT layers: the terminal layer, the network layer, and the application layer. Due to the diversity of terminal devices, security vulnerabilities arise when these devices connect to the network [132]. Furthermore, additional security risks are associated with network transmission and remote cloud interactions.

Table 2.3: Summary of Related Work

Title of the paper	**Main findings or conclusion relevant to the proposed research work**
A decentralized lightweight blockchain-based authentication mechanism for IoT systems [57]	This paper proposes a decentralized authentication and access control mechanism in the IoT environment. The proposed system architecture is designed with two layers as device layer and the fog layer. The communication is categorized into three such device-to-fog, fog-to-fog, and device-to-device. Initially, the device registers with the Blockchain so that it can be authenticated each time. The key and signature generation is performed using Elliptic Curve Digital Signature Algorithm (ECDSA). Each device registers with a certificate and a unique

	system identity. According to this work, the blockchain-enabled fog is presented for certificate verification and encryption. The security credentials are encrypted and then authenticated by the Blockchain. **Problem identified**: • This work presents only a limited number of verification credentials (system identity and certificate).
Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain [58]	In this paper, the authors have proposed a privacy-preserving that presents an attribute-based access control scheme using blockchain technology in the supply chain. The Blockchain manages multiple attributes such as phone number, identification, affiliation, and email according to the user. This process is carried out in system setup, key generation, encryption, decryption, and revoke and update. A public key and the private key are generated for both the data owner and data user, using which the data encryption and decryption are performed. **Problem Identified:** This work uses a conventional cryptography algorithm vulnerable to quantum attacks. It fails to provide security in such occurrence of attackers into the system.
Securing the access control policies to the Internet of Things resources through permissioned Blockchain [59]	This paper is designed to integrate Blockchain with an IoT environment with the assurance of overwhelming different types of attacks. IoT nodes and users are the two main entities involved in the IoT system. In this paper, Networked Bright Object (NOS) plays an essential role in distributed management, along with lightweight security for information. The Blockchain

	consists of an identifier, a set of transactions, timestamps, hashes, and smart contracts. After verification, the hashing is conducted using on SHA-256 algorithm. **Problem identified:** • The traditional SHA-256 algorithm is vulnerable to collision attacks due to the similar hashes construction. This is not a lightweight hashing algorithm. Hence it requires performing multiple computations. • All the devices are allowed to verify access control policies, while the devices could be illegitimate and participate in the system.
A formally verified blockchain-based decentralized authentication scheme for the Internet of Things [60]	A decentralized blockchain-based authentication is presented in this paper that operates authentication using a token mechanism. A formally verified blockchain-based decentralized authentication scheme for the Internet of Things. The process that is involved in this work is user registration, miner registration, token generation, and token verification. The token is generated using ID and address. The signature is generated using Elliptic Curve Digital Signature Algorithm (ECDSA), and the hashing is performed using the SHA-256 algorithm. The user's signature is considered a token, which is verified and allows access. **Problem identified:** The traditional SHA-256 algorithm is vulnerable to collision attacks due to the similar hashes construction. This is not a lightweight hashing algorithm. Hence it requires performing multiple computations.

Blockchain Technologies in Logistics and Supply Chain Management: A Bibliometric Review [61]	The paper proposes reviewing supply chain management (SCM) to identify research gaps. The influence of this research area is demonstrated in the paper by predicting the number of published papers. As a result, the increase in the year, the number of publications increases gradually every year. The importance of Blockchain is also studied in this work.
Blockchain-Based Access Control Techniques for IoT Applications [62]	This paper demonstrates blockchain-based access control in the IoT environment. It expands the partially decentralized and fully decentralized system setup. The issue of using trusted third parties in IoT is highlighted as the reason behind the elimination of third-party for access control.
Securing Fog Computing with a Decentralised User Authentication Approach Based on Blockchain [63]	This paper presents a decentralized user authentication system that considers multiple authentication credentials. The credentials for authentication are username, password, Ethereum address, email, and biometric. The fog server is the blockchain node connecting cloud and edge devices/sensors. The authentication credentials are hashed using the SHA-256 algorithm. According to the incorporation of Blockchain, it is responsible for the authentication of the registered user devices.
Borderchain: Blockchain-Based Access Control Framework for the Internet of Things Endpoint [64]	The authors have proposed a Borderchain that composes of the following entities as IoT owners, IoT gateways, IoT vendors, IoT services, IoT users, and internet service providers. Authentication is performed for the gateway, user devices, and owners. The authentication is performed based on the generated unique signature. The system's trusted devices are allowed access, and the untrusted ones are revoked. The signature is verified, and the authentication is completed for the device.
Decentralized blockchain-	This paper proposed a Decentralized Blockchain-based

based authentication for secure data sharing in Cloud-IoT [65]	Security (DeBlock-Sec) scheme that comprises three main phases: authentication, data encryption, and data retrieval. It presents a Decentralized-based Authentication (DBA) protocol that considers multiple factors as credentials for authenticating. The data encryption is performed using a lightweight SALSA20 algorithm. The credentials evaluated are identity, password, finger vein, and location.

2.5 IoT-Cloud Architecture Authentication Schemes

The Authentication and Authorization (A&A) protocol for IoT-enabled smart grid authentication has been analyzed in this study [113], which also explores the integration of blockchain technology within smart grids. The primary objective of this research is to assess the limitations of existing smart grid infrastructures and propose an enhanced access control mechanism. The proposed method employs the Elliptic Curve Cryptography (ECC) algorithm to secure communications within the smart grid system. Additionally, blockchain technology eliminates the need for a central authority or third-party intermediaries [131]. The introduced approach enhances grid security and ensures non-repudiation through the implementation of smart contracts. Identification rules have been established to verify user identity, facilitate secure data transfer within the grid, and enroll smart meters. Performance evaluations indicate that the proposed method is both efficient and cost-effective in terms of communication and computation. Furthermore, security analyses demonstrate that this approach reduces communication overhead while mitigating potential cyber threats [114].

While the previously discussed study focused on the ECC algorithm for smart grid applications, the current research [115] explores blockchain implementation in IoT devices, specifically Ethereum wallets. This method introduces a decentralized validation approach leveraging Ethereum's blockchain ecosystem, bridging the gap between off-chain and on-chain resources [130]. Ethereum wallets, considered as IoT applications, enable secure interactions between Ethereum accounts. These wallets can be classified as either hardware or software-based. Hardware wallets, such as USB devices, store private keys externally, whereas software wallets store keys within a computer or mobile phone memory [128].

To generate an Ethereum wallet address, a private key is first created. A 128-character hexadecimal string is extracted from the private key, and the KECCAK-256 algorithm is applied to derive a 64-character hexadecimal string. The final wallet address is generated by selecting the last 40 characters of this string and prefixing it with "0x." This method strengthens security against phishing attacks by incorporating improved security measures and cautionary mechanisms to prevent unauthorized access [129].

While prior research has examined blockchain applications in Ethereum wallets, this study [116] focuses on blockchain-based decentralized authentication for smart homes. In the IoT ecosystem, smart homes rely on network connectivity and remote access via mobile devices, which interact with various sensors. IoT devices transmit data to secure blockchain ledgers, ensuring the integrity of tamper-resistant transaction records [126]. The primary objective of this research is to introduce an authentication mechanism leveraging intelligent contracts within blockchain-enabled IoT networks. This approach provides lightweight, scalable, and privacy-preserving security solutions.

In smart home environments, multiple interconnected devices communicate with each other and the cloud through a centralized hub [127]. The proposed method incorporates Ethereum blockchain technology to implement smart contracts, thereby enhancing security and efficiency. One of the key advantages of this approach is its ability to deliver highly secure services without reliance on third-party entities, thereby eliminating external security threats. The system ensures robust data protection and privacy, making it a reliable authentication solution for smart home applications.

Table 2.4: Summary of Related Work

Paper Title	Method	Limitations
Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple servers to server architecture [66]	Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple server architecture.	The user tracking attack could affect the multiserver framework.
An enhancement of a smart card authentication scheme for multiserver architecture [67]	Using an improved smart card authentication scheme.	Vulnerable to offline password-guessing attacks.
An efficient and anonymous chaotic map-based authenticated vital agreement for multiserver architecture [68]	Applying the anonymous-based authentication key agreement in the multiserver architecture.	Vulnerable to user tracking and insider attack.
An enhanced multiserver authentication protocol using password and smart-card: cryptanalysis and design [69]	Employing password and smart card: cryptanalysis and design.	Vulnerable to offline guessing and user tracking attack.
A lightweight authentication protocol for IoT-enabled devices in a distributed cloud computing environment [70]	A lightweight authentication protocol for IoT- enabled devices in a distributed computing environment.	Vulnerable to the offline guessing attack and does not satisfy audit property.

Lightweight IoT-based authentication scheme in cloud computing circumstance [71]	Employing a lightweight two-factor authentication scheme that consists of a one-way hash function and exclusive-or operation with cloud assistance.	Vulnerable to user tracking and insider attack.

2.6: Security Mechanism based on Blockchain

Blockchain technology has emerged as a revolutionary solution for enhancing security across various domains, including IoT, cloud computing, smart grids, healthcare, and financial services. Its decentralized, immutable, and cryptographic nature provides robust protection against unauthorized access, data tampering, and cyber threats. The following are key security mechanisms based on blockchain:

Decentralized Authentication and Authorization: Blockchain eliminates the reliance on centralized authentication authorities by distributing identity management across multiple nodes. Smart contracts facilitate secure authentication protocols, ensuring that only verified users and devices can access specific resources.

Data Integrity and Immutability: Blockchain ensures data integrity by storing records in cryptographically linked blocks. Any alteration in a single block invalidates the entire chain, making data tampering virtually impossible.

Secure Key Management: Traditional Public Key Infrastructure (PKI) systems rely on central authorities, which are vulnerable to attacks. Blockchain-based PKI distributes key management, enhancing security and resilience.

Blockchain-Based Secure Communication: Blockchain enhances communication security by providing encrypted, decentralized messaging and secure transaction validation.

Blockchain for IoT Security: IoT devices are highly vulnerable to cyber threats due to their limited computational power and security features. Blockchain secures IoT networks by Decentralized Device Authentication: Uses blockchain to verify and register IoT devices securely. Lightweight Consensus Mechanisms: Energy-efficient algorithms such as Proof-of-Authority (PoA) optimize performance in IoT environments.

Table 2.5: Summary of Related Work

Paper Title	Method	Limitation
Blockchain and smart contracts for the Internet of Things [72]	Integrating blockchain and intelligent contracts simplify sharing IoT services and resources and cryptographically authorizes automation.	No discussion of IoT security improvement.
Cloud-based commissioning of constrained devices using permissioned blockchains [73]	A privacy-preserving method called Chain Anchor is used for cloud and IoT device integration.	It cannot support identification.
Blockchain infrastructure for the semantic web of things [74]	Proposing a framework for a semantic web of things by a semantic-based resource discovery layer and an essential blockchain infrastructure combination.	Using a private blockchain limits its usage.
Blockchain for IoT security and privacy: the case study of a smart home [75]	Developing an architecture that consists of a local blockchain per use case, a shared blockchain, and an overlay blockchain.	The local blockchains limit availability as they are centralized. Moreover, there is an identification issue and communication enhancement because of the high activity of nodes.

Towards a novel privacy-preserving access control model based on blockchain technology in IoT [76]	Proposing a framework for IoT (FairAccess) that stores the policies in a private blockchain.	Handling just policy-based systems makes it infeasible for IoT.

2.7: Existing Surveys on DLT-based Supply Chain

Blockchain technology presents an innovative approach to managing data systems throughout the supply chain, ensuring transparency, security, and trust among stakeholders. It enforces accountability among participants by maintaining an immutable and cryptographically secured record of all transactions within a decentralized network [121]. The reliance on Distributed Ledger Technology (DLT) enables a shared, tamper-proof ledger across all participants, offering significant advantages in fostering collaboration and trust.

One of the key benefits of blockchain in supply chain management is its ability to prevent unauthorized modifications or deletions of records. This ensures that all stakeholders possess identical copies of the ledger, providing a comprehensive and verifiable view of the entire supply chain network. Various studies highlight blockchain’s effectiveness in enhancing cooperation and trust, positioning it as a fundamental solution to challenges in supply chain management. The technology serves as a "truth mechanism," preventing fraudulent activities and ensuring data integrity [122].

Blockchain has been implemented in several pilot projects and Proof-of-Concept (PoC) initiatives aimed at improving traceability and transparency within supply chain operations. However, despite its advantages, blockchain faces scalability and performance limitations in dynamic supply chain environments. Unlike conventional centralized supply chain models, decentralized supply chains introduce additional complexities as they evolve alongside blockchain integration. Addressing these scalability challenges is critical to ensuring the seamless functionality of DLT-based supply chains [123].

This study explores the scalability challenges and advancements in supply chain management, both in traditional frameworks and blockchain-enabled systems. Several initiatives aim to integrate blockchain with supply chain management to mitigate existing inefficiencies and leverage its decentralized capabilities. However, due to blockchain's inherent scalability constraints, supplementary technologies are being incorporated to bridge these gaps and prevent potential disruptions in supply chain operations. This study focuses on these auxiliary technologies and evaluates their impact on enhancing the scalability and efficiency of blockchain-based supply chains.

Table 2.6: Summary of Related Work

Title of the paper	Main findings or conclusion relevant to the proposed research work
Blockchain Technology for Supply Chain Management: A Comprehensive Review [77]	In this paper, the authors have concentrated on the growth of utilizing blockchain technology (BCT) in supply chain management. The analysis is conducted on the SCOPUS database to identify the importance of BCT. The evolution of BCT is BCT 1.0 (Bitcoin), BCT 2.0 (Ethereum), CT 3.0 (Hyperledger), and BCT 4.0 (Industry 4.0). According to the growth of BCT, it can improve the number of transactions processed per second.
Blockchain Technologies in Logistics and Supply Chain Management: A Bibliometric Review [78]	The paper proposes reviewing supply chain management (SCM) to identify research gaps. The influence of this research area is demonstrated in the paper by predicting the number of published papers. As a result, the increase in the year, the number of publications increases gradually every year. The importance of Blockchain is also studied in this work.
Understanding Blockchain	Reviews industrial applications across different

Technology for Future Supply Chains: a Systematic Literature Review and Research Agenda [79]	domains.
How the Blockchain Enables and Constrains Supply Chain Performance." International Journal of Physical Distribution & Logistics Management [80]	Surveys the enabling and constraining technology roles from a business/management-oriented perspective.
Blockchain Applications in Supply Chains, Transport, and Logistics: a Systematic Review of the Literature [81]	Organizes the theoretical implications of adopting Blockchain in supply chains.
Exploring the Impact of Blockchain on Digitized Supply Chain Flows: A Literature Review [82]	Analyzes the impact of DLT on different supply chain flows through case studies.
Supply Chain Management Based on Blockchain: A Systematic Mapping Study [83]	It offers a systematic mapping study focusing on the research aspect of Blockchains and recognizes challenges that remain unsolved.
Blockchains in Operations and Supply Chains: A Model and Reference Implementation [84]	Conducts a brief literature review to introduce Blockchain technology and utilization.

2.8 Research Gap

1. The existing communication models for IoT devices suffer from various serious security threats due to the various kinds of security attacks. From the extensive review of the existing techniques, following gaps have been identified.
2. The authentication is conducted using one or two security credentials which is not sufficient due to increase in the threats.
3. Decentralized blockchain enables security, while the traditional use of SHA-256 algorithm is vulnerable to collision attack and also has a larger number of computations when compared with lightweight hashing algorithms.
4. Authentication is concentrated only on the data user side, however there is no assurance that only legitimate data owners take part into the system. The upload of fake information is also possible.
5. The access control policies are defined statically in defining the number of attributes that lengthens the attributes and policies respectively.
6. Decentralized blockchain enables security, while the traditional use of SHA-256 algorithm is vulnerable to collision attack and also has a larger number of computations when compared with lightweight hashing algorithms. The increase in computation fails to operate for large scale systems that are composed of numerous devices.
7. The concept of using re-encryption for data security increases the computation time, due to the performance of encryption twice and decryption twice by the data owner as well as data user and hence it creates scalability issues.
8. The security for uploaded data is provided by the use of a cryptography algorithm which is common for all the data. However the data requires being stored securely, it consumes the same computations for all the data that are to be uploaded.

2.9 Summary

This chapter provides a comprehensive review of the literature on blockchain-based decentralized authentication in the Internet of Things (IoT). With the widespread adoption of IoT devices, ensuring robust security mechanisms has become a critical requirement. The integration of blockchain technology for authentication enhances the security and reliability of IoT networks by mitigating vulnerabilities associated with centralized systems. Even though a substantial amount of solutions exist and a lot of research work has been done, still the IoT devices suffer from authentication mechanisms, single point failure, scalability issues, access control policies, heterogeneity issues and low computational power.

CHAPTER 3

LAA-D: Lightweight Authentication and Access Control Mechanism with Dual-Data Storage in Cloud-Internet of Things System Using Blockchain

3.1. Introduction

This chapter introduces a novel Blockchain-based decentralized authentication and access control system. The process of authentication is conducted for the data owner and data user by considering identity, device type, IP address and signature, PUF, and biometric respectively. SALSA20 and PRESENT are encryption algorithms used in the proposed system to encrypt data chunks. SALSA20 is a stream cipher that generates a key stream to encrypt data, while PRESENT is a block cipher that encrypts data in fixed-size blocks. These authentication credentials are managed in the blockchain. The credentials are stored in encrypted form using the Key Schedule PRESENT algorithm. In the authentication of data users, the number of credentials is selected using fuzzy logic that improves security [143].

The concept of decentralized authentication and access control mechanism is built for data owners and data users in the cloud-IoT environment. The development of lightweight cryptography and hashing enriches the scalability as well as the security of the environment. The challenges associated with employing conventional techniques in blockchain, along with the consideration of the number of credentials, contribute to the improvement of this work. The main contributions of this chapter are as follows:

1. The process of registration and authentication of the owner and user credentials are encrypted using the Key schedule PRESENT algorithm. This assures security for the submitted credentials, to mitigate the attackers who steal legitimate credentials.
2. The selection of the number of credentials is determined using fuzzy logic in the consideration of previous authentication success, and access status.
3. To make the system scalable, the hashing in the blockchain is performed using a lightweight QUARK algorithm. The lightweight hashing is used for minimizing the computations that could support multiple devices.

4. To improve security, the chunks are divided into two and it is applied with two different encryption algorithms for each division. A division of chunks uses SALSA 20 encryption and the other division of chunks uses the PRESENT algorithm.

3.2. Authentication and Access Control Mechanism with Dual-Data Storage in Cloud-Internet of Things System Using Blockchain

The Blockchain-based decentralized authentication and access control system is designed. This system design consists of a data owner, decentralized blockchain, attribute authority, data user, and cloud server. The key concept of this work is to develop an authentication and access control for the data users to utilize the stored data. The two common processes of Data Owner (DO) and Data User (DU) are registration and authentication, while the registration is a one-time process only. The Data Owner (DO) uploads the data and the Data User (DU) gives only a query to extract data. In this proposed system, the processing is handled by the attribute authority, which has sufficient resources. So the energy consumption of the proposed system does not reach a threshold.

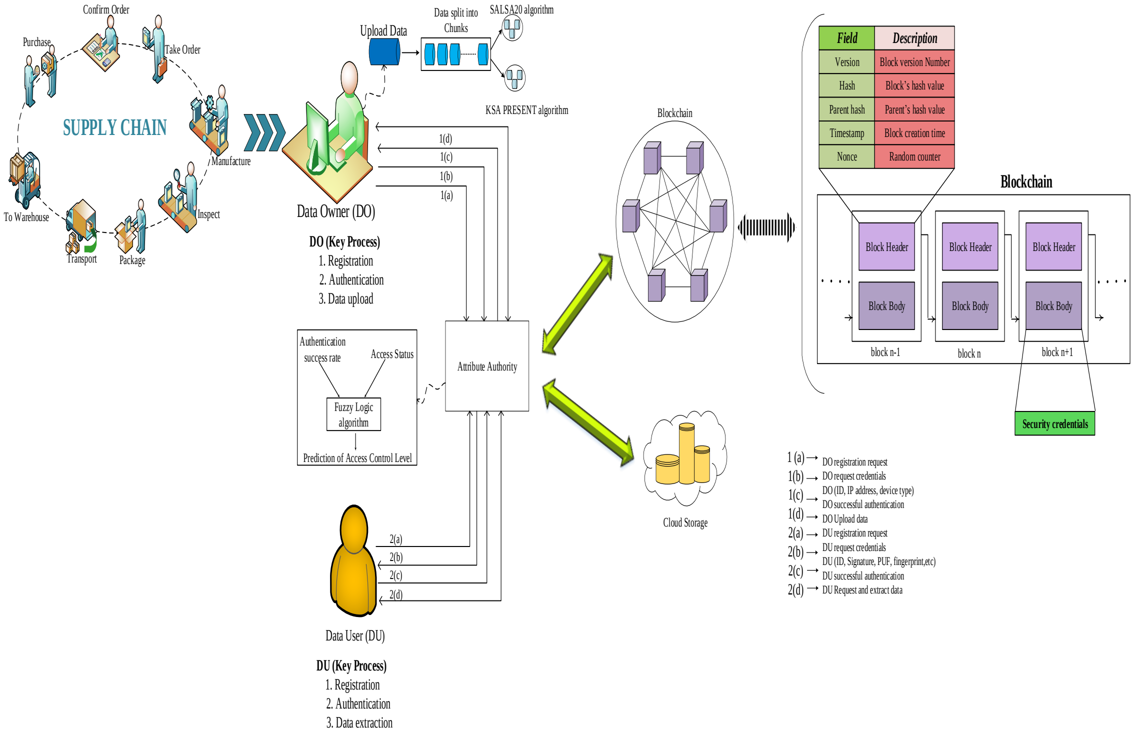


Figure 3.1: Lightweight Authentication and Access Control Mechanism

3.3 Cloud –IoT System Model

1) Data Owner (DO)

DO gather the supply chain information that can include details about purchase, order, manufacturing, package, transportation, and so on. The gathered data is uploaded into the storage for access. Each DO has to be registered in the system so that he/she can upload the data. Let D_i be the total number of DOs and $i = 0,1,2, \ldots .n, D_i = \{D_0,\ D1, D_2, \ldots \ldots ..dn\}$.

2) Data User (DU)

DU is the mobile device that is defined as an IoT device in this system. DU is allowed to access the uploaded data from the storage on passing the authentication and access control policies. The DU also registers with the system, still, there are chances for the involvement of illegitimate DUs. Since the uploaded is confidential for some services, security is strengthened for DU. Let d_j be the total number of DOs and j=0,1,2,…..n $d_j = \{d_0, d_1, d_2, \ldots \ldots ..dn\}$.

3) Attribute Authority (AA)

The deployed attribute authority is trustable; hence it is non-convincible by the attackers. It is connected to the blockchain for authentication and access control. According to the importance of the data, the attributes are set and the policies are defined.

4) Decentralized Blockchain

The decentralized blockchain is accessed by the DU and DO from anywhere at any time. Blockchain composes of blocks with hash values and other credentials; it enables to improve the level of security. The key role of blockchain is to manage the security credentials and validate during each login of DU and DO. It is unable to alter or edit the data in any way which assures to be improving security. It is decentralized and hence it allows access from anywhere to access the data after authentication.

5) Cloud Server

The cloud is used for data storage, which stores data that are uploaded by the DO. Each authenticated data is uploaded into the cloud. The storage efficiency of the cloud server can be increased as per the arrival of users and the requirement of storage to store the data. The cloud server can manage huge data without any loss.

The decentralized blockchain uses a lightweight QUARK algorithm for hashing the block's information and user details. In the QUARK algorithm sponge construction involves three steps: initialization, absorbing phase, and squeezing phase [32]. Based on the performance of these three steps, the information is hashed and then it is stored in the blocks of the blockchain [143].

3.4 Registration of Data User (DU) and Data Owner (DO)

In the IoT system, the Data Users (DU) and Data Owners (DO) are initially registered through a multi-credential authentication mechanism, ensuring enhanced security and identity verification. First of all, the DO registration is carried out by considering identity, device type i.e. used for data upload, and unique IP address. The credentials are submitted to attribute authority and it has been stored in the blockchain. The credentials are transferred via a secure channel and also these credentials are encrypted using the Key schedule PRESENT algorithm. Here are the steps followed for DO registration,

Step 1:D_1 is a DO requesting registration with ID_1, andIP_1, where D_1 denotes one of the DO devices, ID_1 is DO's identity, and IP_1 is DO’s IP address. The request is submitted to AA, which validates the credentials.

Step 2: After validation of DO’s credentials, the AA requests for DT of DO, where DT is the device type that is used by the DO to upload the aggregated data into the server.

Step 3: Then the DO sends DT to the AA in encrypted. The AA updates DO credentials to the blockchain and stores DO’s information in a separate block.

Algorithm 3.1: DO Registration

```
Input: DO's credentials – Identity, IP address, and device type
Output: Successful DO registration
1. Start
2. $D_1(Req) \rightarrow AA$ // Registration Request
3. $AA(Res) \rightarrow D_1(ID, IP)$ // Response from AA
4. $D_1$ Computes $e(ID_1, IP_1)$ and sends to $AA$ // Determines encrypted Credentials using KSA PRESENT algorithm
5. $AA$Receives $e(ID_1, IP_1)$, decrypts it and validates.
6. If $e(ID_1,\ IP_1) = valid$
    {
        $AA(Req) \rightarrow D_1(DT)$
    Else
        Discard $D_1$
    }
  End if
7. $AA$ Receives $DT$ of $D_1$ and updates in the blockchain. // Use of decentralized blockchain
8. $AA$ Reports → $D_1$(Successful authentication)
9. $D_1$ → Ready to upload data
10. End
```

According to the above algorithm the DO registers in the system and then it authenticates each time to upload its data into the server. In similar, DU registration is performed whereas the consideration of credentials is different.

The credentials that are taken into account are identity, signature, IMEI number of the device, fingerprint, e-mail, and Physically Unclonable Function (PUF). The biometric i.e. fingerprint used for security assures the integrity of the system since the fingerprint is unique for each user and so it is complex to be forged. Also, PUF is one of the best solutions that provide higher security, and it enables predicting original device participation in the system. The PUF stands unique for each device and will not replicate with any other device [143].

The steps that are followed in the process of registration are illustrated sequentially.

Algorithm 3.2: DU Registration

Input: DU's credentials – Identity, signature, IMEI, Fingerprint, e-mail, and PUF

Output: Successful DU registration

```
1. Start
2. $d_1(Req) \rightarrow AA$ // Registration Request
3. $AA(Res) \rightarrow d_1(Id, IM)$ // Response from AA
4. $d_1$ Computes $e(Id_1, IM)$ and sends to $AA$ // Determines encrypted Credentials using KSA
5. $AA$ Receives $e(Id_1, IM)$, decrypts it and validates.
6. If $e(Id_1, IM) = valid$
     {
                          $AA(Req) \rightarrow d_1(Sig, Fp_1)$
      Else
        Discard $d_1$
      }
   End if
7. $AA$ Receives encrypted $e(Sig, Fp_1)$of $d_1$ and updates in blockchain. // Use of decentralized blockchain
8. If $e(Sig, Fp_1) = valid$
     {
                          $AA(Req) \rightarrow d_1(E_1, PUF_1)$
      Else
        Discard $d_1$
      }
   End if
9. $AA$ Receives encrypted $e(E_1, PUF_1)$of $d_1$ and updates in blockchain. // Use of decentralized blockchain
10. $AA$ Reports → $d_1$(Successful authentication)
11. $d_1$ → Ready to access data
12. End
```

Step 1: d_1 be a DU requesting for registration with Id_1, and IM_1, where d_1 denotes one of the DU devices, Id_1 is DU's identity, $and\, IM_1$ is DU's unique IMEI number. The request is submitted to AA, which validates the credentials.

Step 2: After validation of DU's credentials, the AA requests for Sig and $Fp_1$of d_1, where Sig is the signature and Fp_1 is the finger print of the d_1 which takes into account of 8-bit binary. The credentials Sig and $Fp_1$of d_1 are sent to AA and are encrypted.

Step 3: Then AA validates the credentials and it again requests for E_1 and PUF_1 of d_1. These two credentials are submitted to AA.

Step 4: Upon receiving all the credentials from d_1, it is validated and stored in the blockchain in an encrypted format.

Step 5: After successful registration, the DU can access the uploaded data based on the access control policies.

Algorithm 3.3: Secure DO and DU Credentials

Input: DO's and DU's credentials

Output: encrypted credentials stored in the blockchain

```
1. Start
2. Storing of the secret key
3. The key is divided into four blocks each having 32 bits. The four blocks perform XOR operation, S-box, and two reverse processes.
4. Combine all the four blocks
5. Perform shifting of 61 bits
6. Apply XOR operation in the LSB
7. End
```

In this proposed system, the DO's and DU's credentials are stored in the blockchain in encrypted form using a key schedule algorithm (KSA) developed in the PRESENT block cipher method. The credentials play a significant role during authentication; in case it is stolen then the illegitimate user could access the data from cloud storage [143].

The KSA PRESENT-128 is executed 31 times to create 31 round keys for processing. Initially, in the 1st round 64-bit is considered a round key. Then, after storage of the secret key, 61-bits are shifted in the register. Next, S-box substitution from the two sets of the leftmost four bits is performed.

3.5 Intelligent Selection of Credentials

In this proposed system, the number of credentials is chosen for authenticating DU. Fuzzy logic is to improve DU authentication with respect to the number of credentials. The fuzzy logic algorithm is presented for determining the number of security credential counts to be considered for authentication of DU. It reflects on the provisioning of DU authentication based on the validation of specified number of credentials [143].

According to the DU’s level of confidentiality, the number of credentials for authentication is selected using the fuzzy logic algorithm. The metrics that are considered for credential selection are previous authentication success, and access status. The fuzzy logic works with a rule-based corresponding to the input metrics. It enables one to analyze the problem and make decisions based on the truth value obtained from the statements. Fuzzy logic operates with three key components such as fuzzifier, interference engine, and defuzzifier.

1) Fuzzifier

It handles the process of receiving input parameters and converts the crisp values into fuzzy sets. The parameters previous authentication success(S_A), and access status(A_S) are the two input parameters. Authentication success is defined as the number of successful authentications into the system to access the DO's data. The access status is defined as accessibility that is given to each DU as views and downloads.

2) Inference Engine

In this engine, the rules are applied and operate as per the degree of membership function. The rules are generated using IF-THEN-ELSE as shown in table 3.1. The input values are processed and the output from the membership rules. The membership value is given between 0 and 1.

3) Defuzzifier

The obtained outcome from the engine is in the form of fuzzy sets, which are converted into crisp values. It gives the outcome for the given input.

TABLE 3.1: FUZZY RULES

S_A	A_S	Output
H	*H*	*H*
H	*L*	*M*
L	*H*	*M*
L	*L*	*L*

H - High, L - Low, M - Medium

Fuzzy logic systems can perform human reasoning and decision-making efficiently. Based on the fuzzy logic, the numbers of credentials that are required for authenticating the DU. Not all the DU are illegitimate in the system, so a different number of credentials are considered for the authentication of DU.

3.6. Authentication of DU and DO

The process of authentication is performed for DO and DU during data upload and data access respectively. According to the registered credentials the DU and DO are authenticated. Authenticating the DU computes the number of credentials to be used for authentication and based on the fuzzy result the number of credentials is validated in AA. The authentication of DO before data upload is conducted based on the below steps,

Step 1: Initially, let DO submit an authentication request to AA for uploading data into the cloud server.

Step 2: After approval from AA, the DO submits the encrypted identity and IP address along with the timestamp for validation.

Step 3: The timestamp is verified by AA and then it checks the identity and IP address from the stored blockchain, if the credentials are true then it requests for the data type.

Step 4: Next as per the request from AA, the DO submits the data type, which is used to upload the data. This credential is also responded to with a timestamp.

Step 5: AA verifies the timestamp and checks the data type of the DO and if all three credentials are valid, it gives permission for data upload.

Step 6: On completion of authentication, the data is uploaded to the cloud server.

Then the access attributes are extracted from the data by the AA. Using the extracted attributes, the access policies for the particular data are structured and validated during the access of DU. On the other hand; the DU is authenticated based on the predicted number of credentials as depicted in the previous section. Here are the steps that are involved in DU authentication with the consideration of all six security credentials,

Step 1: Initially, the DU submits an authentication request to AA for accessing data from the cloud server.

Step 2: The AA approves the request and computes the number of credentials to be taken into account for authentication. Based on the result, it prefers a selective number of credentials. Let's assume all the credentials need to be checked.

Step 3: On receiving approval the DU submits the encrypted identity and IMEI number along with the timestamp for validation.

Step 4: The timestamp is verified by AA and then it checks identity and IMEI from the stored blockchain, if the credentials are true then it requests for Sig and Fp_1.

Step 5: Next as per the request from AA, the DU submits encrypted Sig and Fp_1. This credential is also responded to with a timestamp.

Step 6: AA verifies the timestamp and then it checks encrypted Sig and Fp_1 of the DU and if the credentials are true then it requests for E and PUF for final verification.

Step 7: Then again DU sends encrypted E and PUF to AA with the timestamp.

Step 8: The last two credentials of DU are checked after validation of the timestamp. With these credentials, the authentication of DU is completed.

Step 9: If all the credentials are checked, it allows to access data from the cloud.

3.7. Secure Data Storage

The data uploaded by the DO is securely stored in the cloud environment. The data is split into two chunks and encrypted before storage. The data is divided, and it ensures to increase in the provisioning of security to the system. One part of the data is transformed into ciphertext using SALSA20 and the other part is encrypted using the PRESENT algorithm. SALSA20 algorithm is a stream cipher method that uses a pseudorandom function.

The dual-storage mechanism divides data into two chunks, which are then encrypted using different algorithms—SALSA20 and PRESENT. This approach increases the security of the stored data. If an attacker compromises one chunk of the data, the second chunk remains secure because it cannot be decrypted using the same key. This method ensures that sensitive data is not exposed unless both chunks are accessed and decrypted together.

The proposed research incorporates lightweight cryptography (SALSA20 and PRESENT algorithms) to enhance the security and efficiency of data storage. These algorithms are designed to be efficient in terms of computation, making them suitable for IoT devices with limited resources. This approach not only secures the data but also ensures that the encryption and decryption processes do not consume excessive computational power, which is crucial for maintaining performance in IoT environments. The dual-storage mechanism is integrated with blockchain technology to store metadata and security credentials securely. Blockchain ensures that the records of data storage and access are immutable and tamper-proof. This integration further strengthens data security by providing a decentralized and transparent method for tracking data access and modifications, preventing unauthorized access or alterations.

The four main functions that are performed in this lightweight cryptography are quarter round, row round, column round, and double round. This function works on the add-rotate XOR operator. The size of the input and output are the same and the size is 64 bytes. The hash function in this algorithm is operated 10 times in the process of a counter. The key parameters that are used for processing are constant value in the size of 16 bytes, count at 8 bytes, input key of 32 or 6 bytes, and nonce value of 8 bytes.

Let y=(y_0,y_1,y_2,y_3), in which the y is about 32 bits in size. Initially, the quarter round function is performed and it is given as y=(z_0,z_1,z_2,z_3), and each element is illustrated below,

$$z_1 = y_1 \oplus ((y_0 + y_3) <<< 7)$$

$$z_2 = y_2 \oplus ((z_1 + y_0) <<< 9)$$

$$z_3 = y_3 \oplus ((z_2 + z_1) <<< 13)$$

$$z_0 = y_0 \oplus ((z_3 + z_2) <<< 18) \qquad (1)$$

The operators that are involved in the above expressions represent$<<<$ rotation, $+$ denotes arithmetic addition and $\oplus$ XOR bitwise operation.

$$(z_0, z_1, z_2, z_3) = QR(y_0, y_1, y_2, y_3)$$

$$(z_5, z_6, z_7, z_4) = QR(y_5, y_6, y_7, y_4)$$

$$(z_{10}, z_{11}, z_8, z_9) = QR(y_{10}, y_{11}, y_8, y_9)$$

$$(z_{15}, z_{12}, z_{13}, z_{14}) = QR(y_{15}, y_{12}, y_{13}, y_{14}) \qquad (2)$$

The sequence of 16 input elements ranging $(from\, y_0, y_1, y_2, \dots, y_{15})$ is arranged in a square matrix. After applying the row round function, a single row is modified in a quarter round i.e. QR.

The row round (y) = $(z_0, z_1, z_2, z_3, \dots\dots, z_{15})$is the function defines row round.

$$\begin{bmatrix} y_0 & y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 & y_7 \\ y_8 & y_9 & y_{10} & y_{11} \\ y_{12} & y_{13} & y_{14} & y_{15} \end{bmatrix} \quad (3)$$

Let

$column\,round\,(x) = (y_0, y_1, y_2, \ldots., y_{15})$, and $x = (x_0, x_1, x_2, x_3 \ldots\ldots., x_{15})$ in which x is a 16-element structure that consists of 32 bits each. A similar construction of 16 elements and 32 bits each is defined in column round (x).

$$(y_0, y_4, y_8, y_{12}) = QR(x_0, x_4, x_8, x_{12})$$

$$(y_5, y_9, y_{13}, y_1) = QR(x_5, x_9, x_{13}, x_1)$$

$$(y_{10}, y_{14}, y_2, y_6) = QR(x_{10}, x_{14}, x_2, x_6)$$

$$(y_{15}, y_3, y_7, y_{11}) = QR(x_{15}, x_3, x_7, x_{11}) \qquad (4)$$

Similar to the column round, the input elements $(x_0, x_1, x_2, x_3 \ldots.., x_{15})$ are given in a square matrix and then it performs the column round function that alters a single column in each QR as given below.

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix} \qquad (5)$$

Finally, the double round(DR) function is used which is executed by considering column round (CR) and row round (RR) as follows,

$$DR(x) = RR(CR(x)) \qquad (6)$$

The second part of the chunk is encrypted using the PRESENT algorithm. It is a lightweight block cipher algorithm that works with a key size of 80-bit or 128-bit. This algorithm makes use of a 64-bit block size and activates a non-linear layer. The non-linear layer operates in S-boxes parallel using an optimal property of non-linearity. The functions that are involved in this algorithm are bytes substitution, shifting rows, multiplication of columns, and addition of keys.

The S-box layer is a nonlinear substitution block that creates information from the original information. The default size of information processed is 64-bit input in addition to 16 nibbles.

```
Generate RoundKeys()
For i = 1 to 31
Do
AddRound Key (State, $K_i$)
SBoxLayer (State)
Player (State)
end for
AddRound Key (State, $K_{32}$)
```

The around keys operate with an 80-bit key that is represented as a vector K. In this add round key, the input key bit rotation is performed as follows,

$$[K_{79}K_{78} \ldots\ldots K_0] = [K_{18}K_{17} \ldots\ldots K_{20}K_{19}] \qquad (7)$$

From this process of adding round keys, the bits in the constructed key go in rotation and create a new key, which is used for the next round. The rotation usually takes place as below,

$$K_i = K_{63}K_{62} \ldots K_0 = K_{79}K_{78} \ldots K_0 \qquad (8)$$

Then according to the S-Box layer results,

$$[K_{79}K_{78}K_{77}K_{76}] = S[K_{79}K_{78}K_{77}K_{76}] \qquad (9)$$

Next, the XOR operator is incorporated for the mixing of keys and the expression is given as,

$$[K_{19}K_{18}K_{17}K_{16}K_{15}] = [K_{19}K_{18}K_{16}K_{15}]XORCounter \qquad (10)$$

The process of adding a round key is executed for converting the original information into cipher; hence this is performed in the required number of rounds. During the reverse process i.e. conversion of original information, it is essential to consider all the keys K_i.

3.7.1 Experimental Evaluation and Simulation Specification

The presented implementation is worked on the iFogSim simulation tool. It is an open-source simulator tool that enables the prediction of resource management, storage, utilization of cloud resources, and so on. The iFogSim simulator is a framework specifically designed for modeling and simulating fog computing environments. Fog computing, also known as edge computing, extends cloud computing by bringing computation, storage, and networking resources closer to end devices, reducing latency and improving the efficiency of data processing. The proposed system majorly concentrates on the provisioning of security. The software that is used for implementation is JDK 12.0.2, NetBeans IDE 8.2, and MySQL-5.7.36 (WAMP SERVER 3.2.6).

Table 3.2: Simulation Specifications

Entity	Specification
Data Owner	2
Data User	6
Fog Nodes	2
Attribute Authority	1

For experimental evaluation, we have used a supply chain dataset that is collected from the company of DataCo Global. This dataset enables an analysis of the proposed system with the provisioning of security. The dataset is in '. CSV format and it composes of multiple details about the shipment, benefits, delivery status, customer details, and so on.

The Dataco Supply Chain dataset is a comprehensive collection of data that provides insights into the operations of a global supply chain. It typically includes various data points related to supply chain activities, such as procurement, inventory management, logistics, and transportation.

3.7.1.1 Key Features of the Dataco Supply Chain Dataset

i. **Product Information**: Details about the products being moved through the supply chain, including product IDs, descriptions, categories, dimensions, weights, and unit costs.

ii. **Order Details**: Information about individual orders, including order IDs, dates, quantities, order statuses, and pricing details. This can help analyze order patterns, fulfillment rates, and sales trends.

iii. **Supplier Data**: Information about suppliers, including supplier IDs, locations, lead times, and pricing terms. This data can be crucial for evaluating supplier performance and understanding sourcing dynamics.

iv. **Inventory Records**: Data on stock levels at various points in the supply chain, such as warehouses, distribution centers, and retail locations. It often includes stock keeping unit (SKU) details, inventory levels, reorder points, and stock movements.

v. **Transportation and Logistics**: Information on shipping and transportation, including carrier details, shipping routes, transit times, shipping costs, and delivery statuses. This data helps analyze the efficiency of logistics operations and optimize transportation networks.

vi. **Customer Information**: Data on customers, including customer IDs, locations, purchase histories, and preferences. This can be used to analyze customer demand patterns and improve customer service.

vii. **Financial Metrics**: Financial information related to supply chain operations, such as costs (procurement, transportation, storage), revenue from sales, profit margins, and cost savings from optimization efforts.

viii. **Geographical Data**: Location-based data on suppliers, warehouses, customers, and transportation routes, which can be used for geographic analysis and optimizing supply chain networks.

The dataset is uploaded via the created data owner, and it is accessed by the data users. Based on the proposed system model, the algorithms are incorporated as per the specification in table 2. The proposed system architecture is depicted in Figure 3.2.

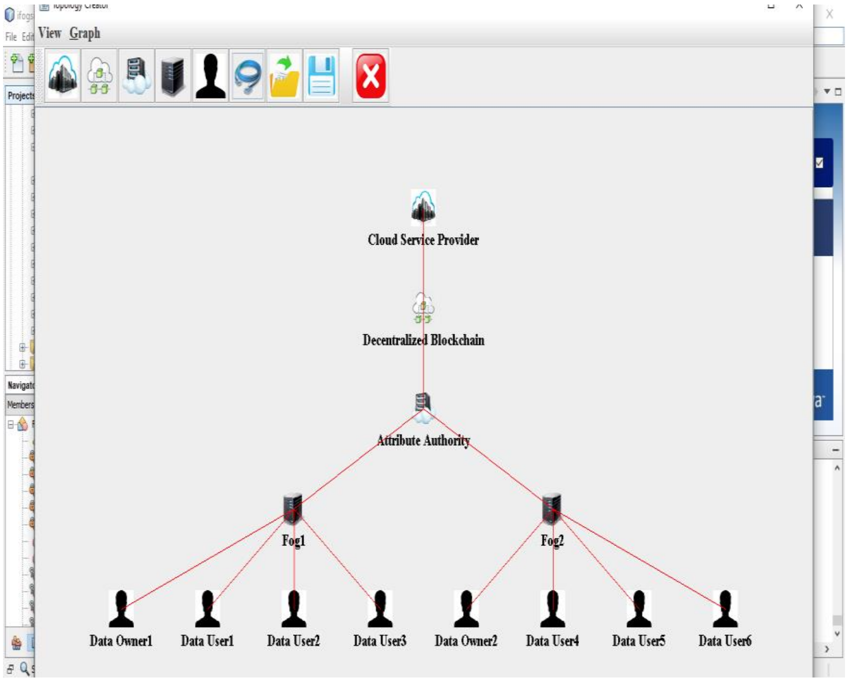


Figure 3.2: Proposed System Model

3.7.2 Comparative Results

The performance metrics are assessed based on authentication time, storage efficiency, execution time, throughput, latency, and block size.

1) Authentication Time

Authentication time quantifies the duration required to authenticate devices based on their credentials. A reduced authentication time indicates an efficient authentication mechanism. In this context, devices function as data users, submitting requests to access the data.

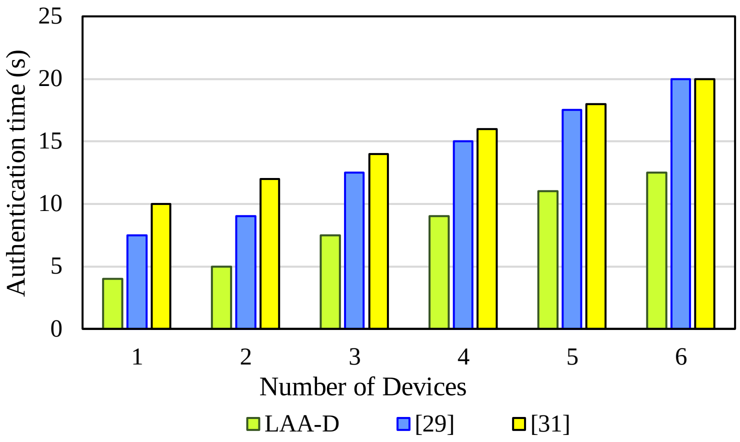


Figure 3.3.: Comparison of Number of Devices vs. Authentication Time

Figure 3.3 presents a comparative analysis of authentication time between the proposed model and the existing system. The proposed model achieves an average authentication time of approximately 8 seconds, whereas the existing system requires 14 seconds. In the existing system, user authentication is performed using common credentials without incorporating a lightweight cryptographic algorithm, resulting in higher authentication latency.

2) Storage Efficiency

Storage efficiency is a critical factor in this model, as data is stored on a cloud server. In the context of supply chain management applications, data is uploaded and maintained in the cloud. To assess this efficiency, storage efficiency is quantified based on cloud storage utilization.

Storage efficiency is analyzed by plotting it against the data size occupied by uploaded information. In the proposed model, the cloud infrastructure stores and manages only data chunks, whereas user and owner credentials, along with their transaction records, are securely maintained within a decentralized blockchain network.

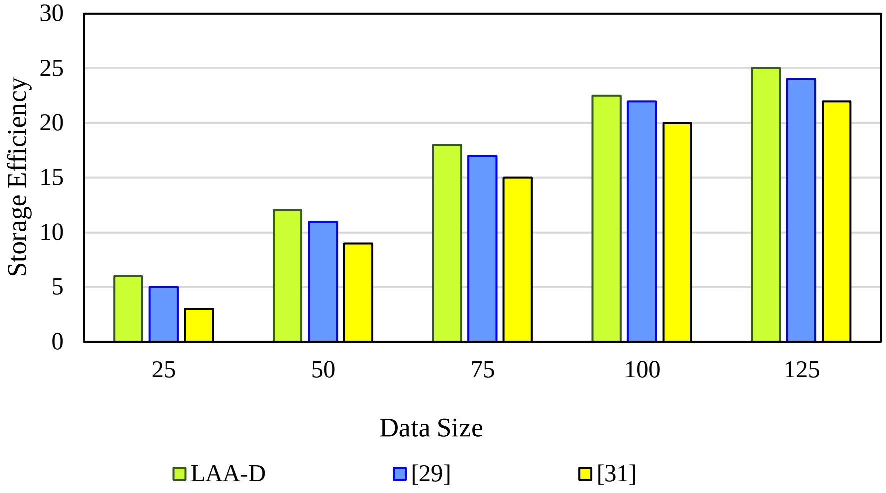


Figure 3.4.: Comparison of Data Size vs. Storage Efficiency

The evaluation of storage efficiency is presented in Figure 3.4. The lower storage efficiency observed in the existing system, compared to the proposed model, demonstrates the effectiveness of the proposed approach in managing uploaded data. In the proposed model, raw data is partitioned into smaller chunks before storage, optimizing space utilization. Conversely, in the existing system, storing raw data directly results in suboptimal storage efficiency due to increased data size requirements.

3) Execution Time

This research primarily focuses on security and proposes an access control mechanism. The execution time is estimated based on various access attributes, with a shorter execution time indicating an efficient access control design. The access attributes are extracted from the uploaded data by the Authorization Authority (AA) and are used to determine data access permissions for users. As the number of access attributes increases, the time required for data encryption and decryption also rises due to the higher computational overhead associated with attribute validation.

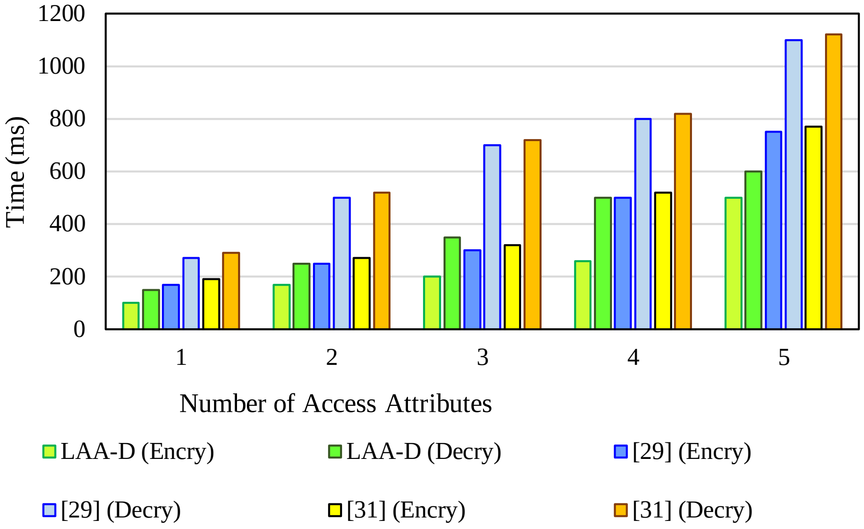


Figure 3.5: Comparison of Number of Access Attributes vs. Execution Time

Figure 3.5 presents the measured execution time for encryption and decryption as a function of the number of access attributes. The proposed system model demonstrates lower encryption and decryption times compared to the existing system due to the implementation of lightweight cryptographic techniques, which enhance computational efficiency even as the number of access attributes increases.

4) Throughput

Throughput refers to the volume of data transmitted from the source to the destination within a specified time interval. It represents the rate of message delivery, where higher throughput corresponds to faster message transmission. In this research, throughput is evaluated based on the transmission of messages for authentication and data access processes.

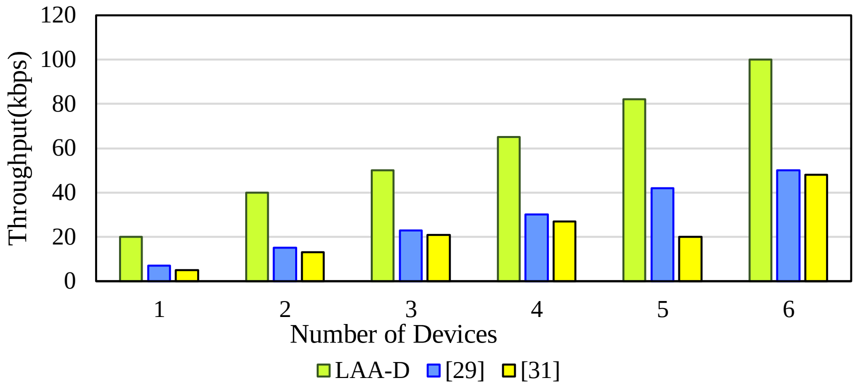


Figure 3.6: Comparison of Number of Devices vs. throughput

The graphical representation of throughput is depicted in Figure 3.6, comparing the performance of the proposed and existing systems. The results indicate that the proposed system achieves a higher throughput than the existing system, with an average throughput of approximately 60 kbps, compared to 28 kbps in the existing system, yielding an improvement of 32 kbps. This enhancement in throughput ensures more efficient data transmission and maintains optimal performance as the number of devices increases. Consequently, the proposed system demonstrates superior operational efficiency compared to the existing system.

5) Latency

Latency refers to the delay in message transmission from data users to other network entities. Lower latency indicates a more efficient system design compared to previous models. As the number of users increases, latency must remain within acceptable limits to prevent system failures.

This metric plays a crucial role in assessing the performance improvements of the proposed system. A system with high latency fails to support scalability, leading to inefficiencies. To evaluate performance, latency is measured and plotted against the increasing number of network devices. The results demonstrate that latency is significantly higher in the existing system compared to the proposed model. The reduced latency in the proposed system is attributed to the implementation of the lightweight KSA-PRESENT algorithm, which enhances credential security while minimizing computational overhead. Reduced computational complexity enables faster device authentication. In contrast, while previous approaches ensured secure authentication, they introduced higher latency due to the extensive computations required for credential validation.

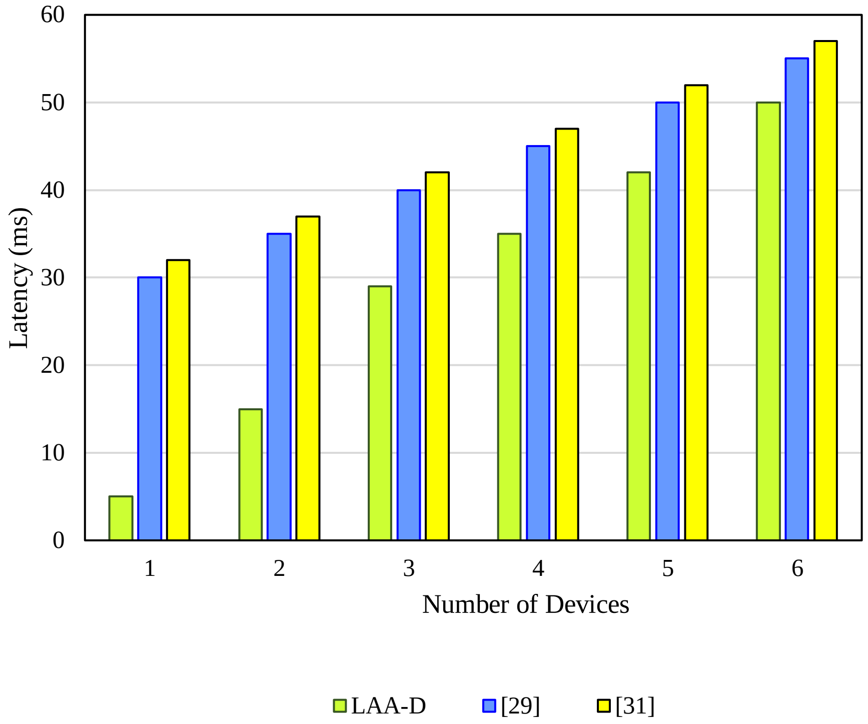


Figure 3.7: Comparison of Number of Devices Vs Latency

Figure 3.7 presents a comparative analysis of latency between the proposed and existing systems. The proposed system achieves an average latency of 29 ms, whereas the existing system exhibits a latency of 42.5 ms. These results demonstrate that the proposed system significantly reduces latency compared to the existing approach. The lower latency ensures improved system performance and supports scalability, making it more efficient for handling an increasing number of network devices.

6) Hit Rate

In this research, blockchain technology is integrated, necessitating the measurement of block size. As the number of user devices increases, the blockchain expands sequentially, leading to a corresponding growth in block size. The increase in block size impacts the time required for credential validation; therefore, validation efficiency is assessed concerning the hit rate.

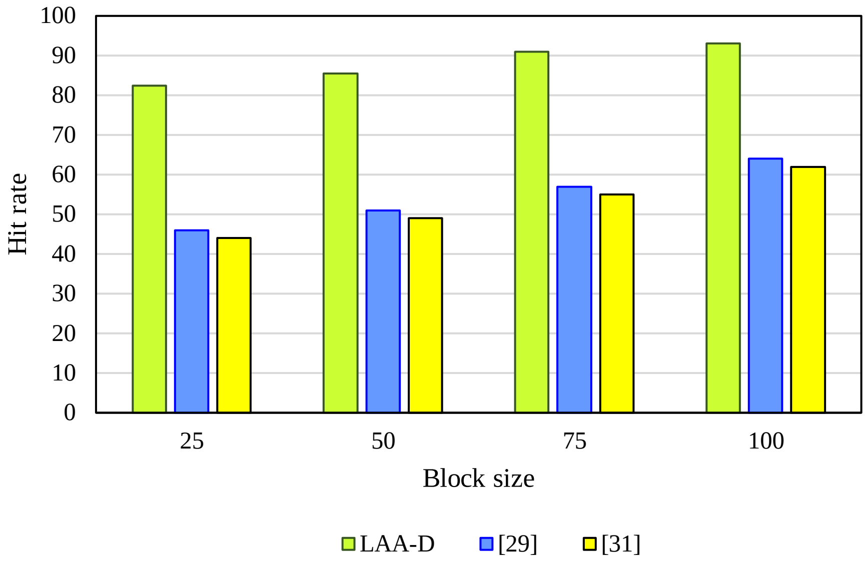


Figure 3.8: Comparison of Block Size vs. hit rate

Figure 3.8 illustrates the relationship between block size and hit rate, demonstrating that an increase in block size leads to a higher hit rate. The proposed system achieves a significantly higher hit rate compared to the existing system. This comparative analysis indicates that the proposed model enhances the hit rate more effectively than the existing approach. The improvement in hit rate reflects the enhanced utilization of blockchain technology, ensuring better security and efficient credential management.

3.8 Summary

This chapter presents a lightweight authentication and access control framework with a dual-data storage approach. The proposed system ensures authentication for both data owners (DOs) and data users (DUs). Data owners are authenticated based on identity, device type, and IP address, whereas data users are authenticated using a fuzzy logic algorithm that evaluates multiple credentials, including identity, signature, IMEI number, biometric data, email, and physically unclonable function (PUF). For enhanced security, data uploaded by the owner is partitioned into two chunks and encrypted using lightweight SALSA20 and PRESENT cryptographic algorithms. Additionally, the credentials of both data owners and data users, along with data usage records, are managed within a decentralized blockchain secured by the lightweight QUARK algorithm. The proposed system assures security with the designed strong authentication of DO and DU to upload data and access data respectively. However, the increase in the DOs and DUs at a particular period may tend to increase processing time.

Chapter 4

Scalable Consensus algorithm and Storage in Decentralized Blockchain (SCSB) for Heterogeneous IoT Systems

4.1. Introduction

Heterogeneity in the Internet of Things (IoT) refers to the capability of supporting a diverse range of devices through the integration of various technologies for internet connectivity. This communication is ubiquitous, extending across multiple applications. Typically, IoT devices operate with limited power and computational capabilities, where heterogeneous IoT systems utilize appropriate protocols, standards, and technologies to ensure seamless interoperability. These heterogeneous devices include sensors, actuators, thermostats, and other smart components.

The IoT with heterogeneous devices gathers a huge amount of data that differs in the severity based on the application. For instance, a healthcare environment composed of sensors that collect patient's data which can be either sensitive or non-sensitive.

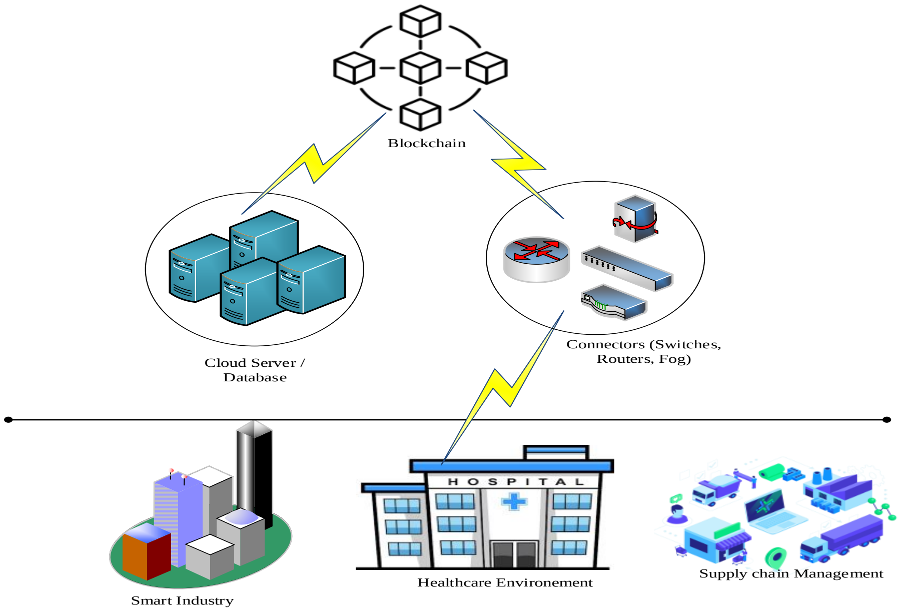


Figure 4.1: Architecture of integrated heterogeneous cloud-IoT with blockchain technology.

Blockchain is one of the popular solutions incorporated in the integration of heterogeneous IoT with cloud. The development of this type of architecture is challenging since it needs to be flexible to support any type of application. The combination of heterogeneous cloud IoT with blockchain technology architecture is depicted in figure 4.1. It assists with the solution in providing security risks as well as multiple real-time applications.

4.2. Contributions of the Chapter

- The exchange of security credentials during authentication is secured in decentralized blockchain with the incorporation of lightweight QUARK algorithm.
- In a decentralized blockchain, the Proof-of-Authentication (PoAH) protocol performs node authentication by calculating trust values based on predefined criteria and metrics.
- The collected data is uploaded by the data owner which determines the confidentiality level of the data before it is uploaded. The confidentiality level is computed using dual fuzzy logic algorithm.
- From the confidential level prediction as low and high different methods are used such as Laplace based differential privacy and lightweight TWINE algorithm respectively.
- The proposed system operates within a heterogeneous IoT environment; data in the cloud is clustered and stored efficiently. A hybrid distance metric is utilized in the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm to optimize data organization and management.

A secure Blockchain-based Privacy-Preserving Access Control (BPAC) scheme is introduced in this study [37]. Data confidentiality is ensured through the implementation of the Fully Homomorphic Encryption (FHE) algorithm. In the BPAC model, a trusted Certificate Authority (CA) is responsible for generating private and public key pairs. According to this framework, a subscriber directly requests access from the publisher, who then encrypts the data and transmits it to the blockchain. The blockchain subsequently authorizes the access request and performs re-encryption before forwarding the data to the subscriber. Within this system, the blockchain functions as a private broker. To address these concerns, the authors proposed an Access Control Enabled Blockchain (ACE-BC) framework [38], integrating Attribute-Based Encryption (ABE) for data encryption along with Homomorphic Encryption (HE) for user key generation. In this model, the blockchain serves as a trusted authority and is linked to a proxy server, which provides re-encryption keys to the data owner. The data owner encrypts the information twice, and the data user performs double decryption to access the content. The proxy re-encryption approach for cloud-based data sharing, incorporating blockchain technology [39]. This framework employs Identity-Based Encryption (IBE) and proxy re-encryption to enhance security. In this model, the blockchain acts as a trusted authority, issuing secret keys based on user identities. The system utilizes the traditional SHA-256 hashing algorithm for blockchain security. Data encryption is carried out by the data owner using a randomly generated number. Additionally, a hybrid centralized and blockchain-based authentication architecture was proposed [40]. In this system, devices are registered and authenticated using security credentials, including identity and group identity. Following successful authentication, symmetric encryption is applied using a generated public key. This framework implements the Proof-of-Work (PoW) consensus mechanism for blockchain transaction validation. However, the following key challenges are identified:

- The blockchain performs re-encryption, requiring double encryption and decryption processes, which significantly increases computational overhead and processing time.
- The authentication mechanism relies on non-unique credentials, potentially allowing unauthorized subscribers to gain access.
- The blockchain performs re-encryption, resulting in a doubled computational burden for both encryption and decryption processes.
- The use of the homomorphic encryption algorithm introduces significant processing delays and demands extensive computational resources.
- Since encryption and decryption are performed twice, the system requires double the processing time for ciphertext conversion.

- The SHA-256 hashing algorithm, traditionally employed in blockchain, is computationally intensive and susceptible to collision attacks, making it less efficient for lightweight applications.
- The PoW consensus algorithm lacks scalability, resulting in performance degradation as the number of requests increases.
- The reliance on the SHA-256 hashing algorithm introduces excessive computational overhead compared to lightweight cryptographic techniques.
- Symmetric key cryptography necessitates a secure key exchange process, as the same key is used for both encryption and decryption.

Summary of Key Issues in Existing Research:

While decentralized blockchain technology enhances security, the traditional use of SHA-256 hashing is vulnerable to collision attacks and incurs high computational costs. Increased computational complexity limits the feasibility of large-scale systems with numerous connected devices.

Cryptographic encryption techniques ensure data security; however, a uniform encryption approach for all data types results in redundant computations, increasing processing time and resource consumption.

The absence of robust security mechanisms exacerbates scalability issues, as illegitimate devices infiltrate the system, leading to increased traffic and potential data access vulnerabilities.

4.3 Scalable Consensus algorithm and Storage in Decentralized Blockchain (SCSB) Heterogeneous IoT System

The SCSB heterogeneous IoT system is designed to work in a scalable environment as shown in figure 4.2. This is a heterogeneous system that composes of a variety of devices into a system. It submits different types of information for processing and storage. The deployment of decentralized blockchain into this system assures in secure data storage and elimination of illegitimate devices.

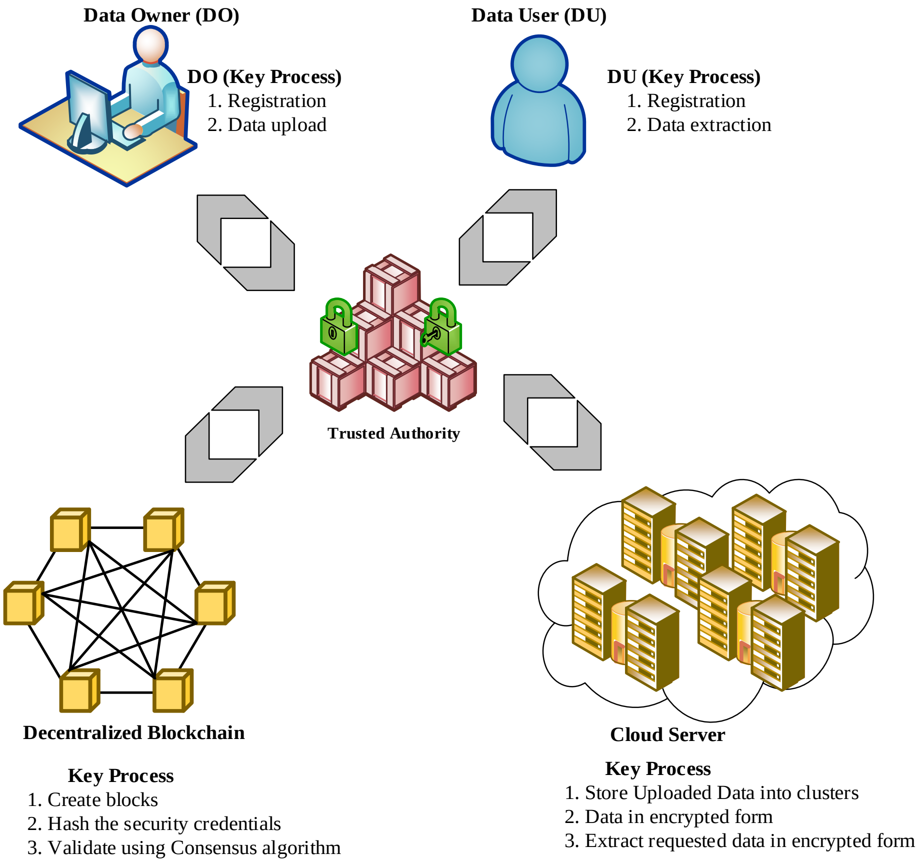


Figure 4.2: SCSB Work Process

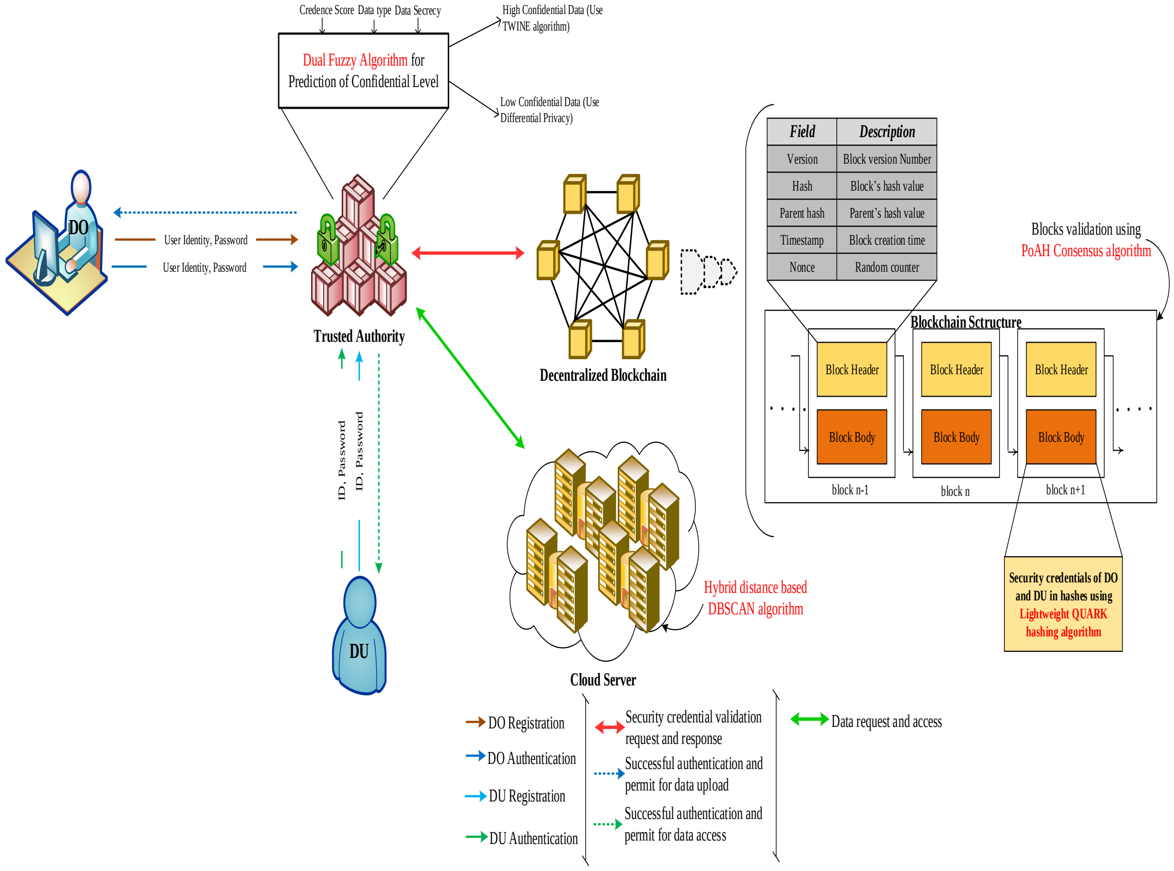
4.3.1 System Model

The SCSB is developed to improve scalability issues and support heterogeneity in IoT environment based on the incorporation of decentralized blockchain. There are five key entities in this system and they are data owner, data user, trusted authority, decentralized blockchain and cloud server. The work natures of each entity in this system are illustrated below.

(i) Data Owner (DO): The DOs collect information from IoT devices and upload the data into cloud server. There are multiple DO participating in the system, where each DO have individual login.

(ii) Data User (DU): The DU participates in the system to access the cloud and extract uploaded data. Each DU requests to cloud via trusted authority. The DUs are validated with basic credential of Identity and password.

(iii) Trusted Authority (TA) : This entity in the system is trusted and hence it is responsible to validate credentials for authentication. It maintains the attributes for each data when the DO uploads the data. The TA connects with blockchain for assuring security. The credentials are stored in hashes into blockchain.


Credence Score
Data type
Data Secrecy
Dual Fuzzy Algorithm for Prediction of Confidential Level
High Confidential Data (Use TWINE algorithm)
Low Confidential Data (Use Differential Privacy)
DO
User Identity, Password
User Identity, Password
Trusted Authority
ID, Password
ID, Password
DU
Decentralized Blockchain
Blocks validation using PoAH Consensus algorithm
Blockchain Sctructure
Block Header
Block Body
Block Header
Block Body
Block Header
Block Body
block n-1
block n
block n+1
Security credentials of DO and DU in hashes using Lightweight QUARK hashing algorithm
Hybrid distance based DBSCAN algorithm
Cloud Server
DO Registration
DO Authentication
DU Registration
DU Authentication
Security credential validation request and response
Successful authentication and permit for data upload
Successful authentication and permit for data access
Data request and access

Field	Description
Version	Block version Number
Hash	Block’s hash value
Parent hash	Parent’s hash value
Timestamp	Block creation time
Nonce	Random counter

Figure 4.3: SCSB Architecture Model

(iv) Decentralized Blockchain: Blockchain is decentralized which is able to provide access for all DOs and DUs. The blockchain is composed of blocks that enable to manage credentials secrecy.

(v) Cloud Server: Cloud server is responsible to store the encrypted data uploaded by the DO. The data is accessed from cloud by the DU after completion of authentication.

The constructed SCSB heterogeneous IoT system model is depicted in figure 4.3. As per the developed system model, the processes in blockchain, and cloud are executed.

4.3.2. DO and DU Authentication and Blockchain Consensus algorithm

Let the system composes of *L* and *M* number of DOs and DUs that are represented as $\{DO_1, DO_2, DO_3, \ldots DO_L\}$ and $\{DO_1, DO_2, DO_3, \ldots DO_M\}$. The DO and DU have unique identity and password using which the DO and DU is identified in the system. On completion of successful authentication, the DO uploads the data and DU accesses the required data. The credentials are stored in decentralized blockchain. The blockchain stores security credentials in the form of hashes using lightweight QUARK algorithm. For each authentication, the security credentials are verified and then it allows access.

The lightweight QUARK algorithm constructs sponge based on three phases as initialization, absorbing phase and squeezing phase. Assume the identity and password are denoted as *sc*. The size of sponge will be of $b=r+c>=n$, where c is the capacity and n is the length of output. Hereby the process performed in sponge construction is depicted below,

(i) Initialization phase: In this phase, the *sc* is the security credential which is padded with '1' bit. This padding is presented with the addition of '0' until it reaches the length of *r* that is multipliable. The term *r* is the block length which is one of the parameter used in QUARK algorithm.

(ii) Absorbing phase: Let the *r* bits of blocks involve XOR function with the last *r* bit of $Y_{b/2-r}, \ldots, Y_{b/2-1}$ that represents the state. It is inserted along the application of permutation *P*.

(iii) Squeezing phase: In this phase, *r* bits in the state is obtained as output along with the application of permutation *P*, this is performed until *n* bit are obtained as output.

Based on this hashing the DO's and DU's security credentials are hashed by itself before sending request for authentication. In blockchain, the blocks are equipped with hashes in each block which is used for authentication. This algorithm is able to overwhelm multiple attacks as collision, differential, etc. It resists from stealing of security credentials of DO and DU which enables to mitigate illegitimate device participation into the system.

The heterogeneity IoT composes of numerous devices which submits a huge number of requests for processing, hence a lightweight Proof-of-Authentication (PoAH) consensus algorithm is presented in blockchain. Using this consensus algorithm, a trusted validator is selected among the nodes for validation in blockchain. The incorporated PoAH is suitable for resource constrained device and it is able to support scalability of the system. At the time of validation of blocks, the authentication of node is performed based on the estimation of trust values of the node. The transactions in the blocks are signed using traditional digital signature algorithm.

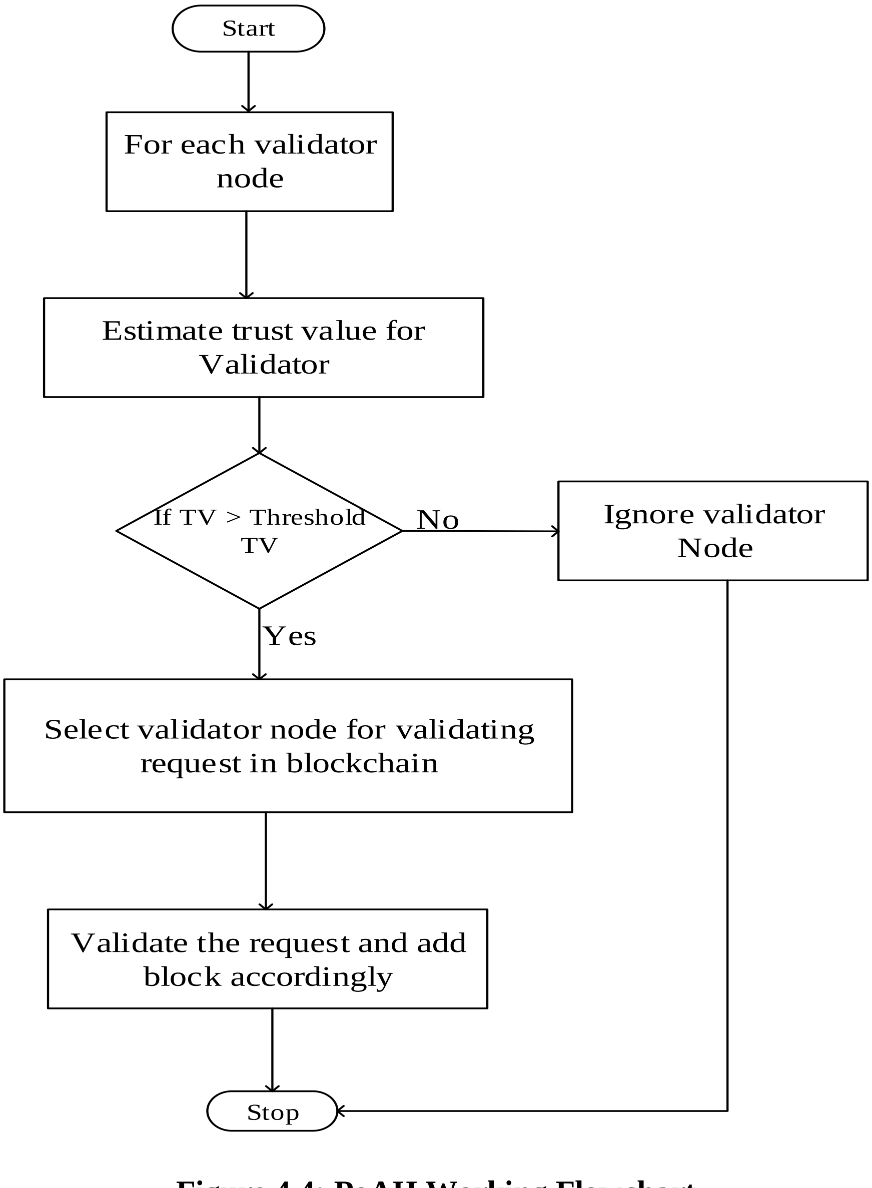

Start
For each validator node
Estimate trust value for Validator
If TV > Threshold TV
No
Ignore validator Node
Yes
Select validator node for validating request in blockchain
Validate the request and add block accordingly
Stop

Figure 4.4: PoAH Working Flowchart

The trust value represented as TV is estimated from the summation of node's behaviour and number of successful authentication. The node behaviour is defined as the participation in the system with the neighbour nodes. The use of lightweight hashing algorithm in blockchain enables to perform faster validation and maintains same level of security. The presented consensus algorithm works with the validation of security credentials of DU and DO using the selected trusted node. On receiving the request for validation, the node is selected and then it determines the public key for the verification of signature of the block. After the validation of signature, the hash values are computed.

Algorithm 4.1 Proposed lightweight PoAH

Input: Lightweight QUARK hash, private (*PK*) and public (*PuK*) key for each node.

Output: Validated blocks with trusted nodes

```
1. Begin
2. Blockchain receives request for validation
3. The validating nodes signs the block using private key
   and broadcast the request
4. Nodes check with the signature and submits trust values.
5. If (TV>Threshold)
     {
        Select as validator node and then add blocks
   Else
        Estimate trust value for next node
     }
   End if
6. End
```

4.4 Data Storage in Cloud

On completion of authentication of DO based on the registered credentials, it is allowed to upload the collected data. The confidentiality level of the data is predicted using dual fuzzy logic algorithm that takes in account of data type, credence score and data secrecy. The confidentiality level is categorized into high and low. The high confidential data is encrypted using lightweight TWINE algorithm [41] while the low confidential data is secured using Laplace based differential privacy. In this process of data storage initially the dual fuzzy logic is applied for determining the confidentiality level.

The dual fuzzy logic algorithm is constructed with two fuzzy logic blocks shown in figure 4.5. Each fuzzy logic block composes of three entities as fuzzifier, interference engine and defuzzifier.

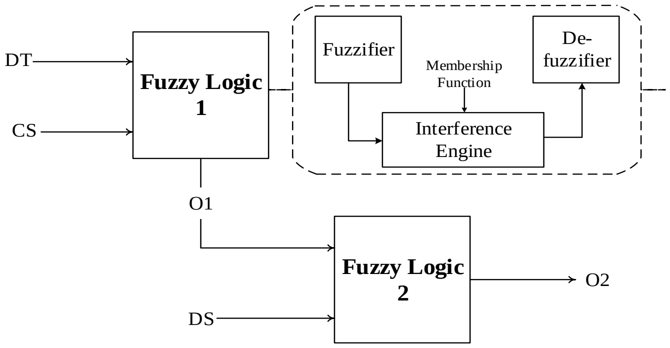


Figure 4.5: Dual fuzzy logic

The fuzzy logic method is operated based on the prediction of degree of truth which uses Boolean logic to determine outcome as true or false in 1 or 0. It is operated with the defined set of rules based on the fed input parameters. The work process of each entity is illustrated in the following.

(i) *Fuzzifier*: The fuzzifier is the initial block which performs fuzzification that receives input values. According to the proposed dual fuzzy logic, the first fuzzy logic considers data type and credence score. Then the second fuzzy considers data secrecy and output 1 as its input. The input is in crisp values and it is converted as fuzzy set for further processing.

(ii) *Inference Engine*: This engine is fed with knowledge base fuzzy rules which works on 'IF-THEN' rules defined for the submitted input. For the given two input values a set of four rules are developed. The input are presented in High, Low values that are defined as a range of values. From the input values, the degree of membership function is designed.

(iii) *Defuzzifier*: The extracted outcome based on the membership functions is in the form of fuzzy set. In this block, it is converted into crisp values.

The data type is categorized into two as normal data and emergency data. It is predicted based on the static threshold value for each measurement. Then, the credence score is determined based on the number of successful authentication and amount of data uploaded. The increase in these two metrics assures to result with the higher credence score. The data secrecy is the importance of data storage in the cloud. For example, it could be more sensitive and hence it requires high data secrecy. It could include specifications in the data as company agreements, income tax information, transactions, account details and others. According to these three parameters the dual fuzzy logic determines the high confidential level and low confidential level of data storage in cloud. The fuzzy rules for the prediction of confidential level are illustrated in table 4.1 and table 4.2.

Table 4.1: Fuzzy Logic 1 Rules Set

DT	**CS**	**O1**
H	H	H
H	L	H
L	H	L
L	L	L

Table 4.2: Fuzzy Logic 2 Rules Set

DS	**O1**	**O2**
H	H	H
H	L	H
L	H	L
L	L	L

If the dual fuzzy logic method results with high, then the data follows lightweight TWINE algorithm else Laplace based differential privacy is used. The TWINE algorithm is a 64-bit lightweight block cipher. It uses bitwise exclusive OR operator. The three key processes followed are encryption, key schedule and decryption. The reverse of encryption is performed in decryption. Let the plain text be in the size of 64-bit, round key *RK* which is generated from the secret key. Initially, round function is applied that is based on nonlinear layer using 4-bit S-boxes. Along with this diffusion layer is used to permute 16 blocks. Then, the S-box mapping is performed for specified number of bits and it shuffles the block. Next step is key schedule the round keys are produced and processed. Further, the inverse process of encryption is presented for decryption.

If the output consists of low-sensitivity data, the Laplace-based differential privacy method is applied to ensure data protection. The differential privacy is enabled to provide security for the data. It is a mechanism that adds noise to secure the data from attackers. The differential privacy is developed using two numeric values as epsilon and delta that are represented as ε and δ. The value of δ is included as the multiplicative bound. If the value is set low, then the risk is also smaller. In Laplace mechanism based differential privacy adds Laplacian noise to the function. It computes function *f*, then it adds noise from Laplace distribution. The noise to be added is determined as follows.

$$N=[\text{Sensitivity of } f \,/\, \varepsilon] \text{ , where } \delta=0 \qquad (1)$$

The mathematical formulation for Laplace mechanism is given as,

$$[D] = f[D] + \varepsilon \qquad (2)$$

Let D be the data to be stored into the cloud from data owners. Based on the use of differential privacy the data is secured.

4.4.1. Data Clustering

The data is clustered in cloud for assuring scalability in storage due to the arrival of huge amount of data that are collected from heterogeneous data. The clustering of data is presented using Hybrid distance with Density-based spatial clustering of applications with noise algorithm (H-DBSCAN). This algorithm uses two key parameters such as minPts and eps i.e. epsilon. The minPts denotes minimum number of points which clusters a dense region, on the other hand the eps defines the distance measurement which is measured using the points that are located. In this work hybrid distance is used which takes in account of Manhattan distance and Euclidean distance. The formulation for Manhattan and Euclidean distance measure is given as,

$$d_1 = \sum_{i=1}^{n} |x_i - y_i| \tag{3}$$

Then the Euclidean distance formula is measured as follows,

$$d_2 = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{4}$$

where $x_i$and y_i are the data points in the cloud based on which the clusters are constructed. In this work, hybrid distance is used that estimates $d_1$and d_2 for the same set of data points and then it predicts average for it. The hybrid distance measure D is given as below,

$$D = \frac{d_1 + d_2}{2} \tag{5}$$

Initially, identifying the neighbouring point present within eps, then predict the core points. In case if the predicted core point is already in a cluster ignore it else consider it in cluster construction. On identifying the density connected points with respect to the core points, the data are clustered. The data points that covered within minPts in the radius eps. All the neighbouring points are considered to be in same cluster. The process of clustering enables to improve scalability of data storage.

Algorithm 4.2 H-DBSCAN algorithm

Input: Owner’s Data, eps, minPts

Output; Clusters (C)

```
1. Start
2. Let C=1
3. For each non-visited point p
     {
         Assign p as visited point
         Determine neighbours N using D
     if |N| ≥ minPts
    N = N∪ N’
    }
4. if (p’is not included in any cluster)
     {
        add p’to C
    else
       ignore
      }
5. Stop
```

As per the above pseudo code, the H-DBSCAN algorithm is developed. Based on the clustering of data in cloud, the scalability of heterogeneous data is achieved. The use of hybrid distance measure enables to improve the perfect identification of neighbouring data points that enhances clustering.

4.5 Experimental Evaluation

The SCSB IoT heterogeneous system is implemented using a simulation framework to evaluate its performance. This section is structured into two parts: the simulation setup and the comparative analysis.

4.5.1 Simulation Setup

In this section, the SCSB IoT heterogeneous system is modeled and implemented using the iFogSim simulation tool. The system is designed to simulate n number of Data Owners (DOs) and Data Users (DUs), facilitating data upload and access from the cloud. The number of IoT devices and fog nodes within the fog computing environment is determined based on application requirements, network topology, data processing needs, and performance objectives.

The heterogeneous nature of the system is represented by configuring various device types with differing computational capabilities (CPU, memory, and storage) and functional roles (data generation, processing, and storage), accurately reflecting real-world fog computing environments. iFogSim provides a comprehensive framework for modeling devices, networks, applications, and resource management strategies, enabling efficient scheduling of tasks within the fog environment. By supporting heterogeneous devices and dynamically scalable architectures, iFogSim facilitates the design of efficient, responsive, and robust fog computing systems.

The integration of IoT with blockchain in iFogSim involves simulating a decentralized architecture where blockchain technology enhances the security, privacy, and reliability of IoT-based operations. This combination leverages fog computing for localized data processing and storage, thereby reducing latency and bandwidth consumption, while blockchain ensures data integrity and secure transactions across the network.

Heterogeneity is effectively managed through adaptive resource allocation, multi-protocol communication support, and decentralized blockchain mechanisms, ensuring secure and scalable operations. To strengthen security, a decentralized blockchain framework is incorporated for authentication and node validation. Additionally, one of the key challenges in IoT heterogeneous systems—scalability—is addressed through the implementation of lightweight cryptographic algorithms and efficient data clustering in the cloud server.

Figure 4.6 illustrates the sequence diagram of the proposed SCSB system, depicting the interaction between various entities involved in the architecture. The system operations follow this defined sequence, where, upon successful authentication, data is stored based on its confidentiality level. Figure 4.7 presents the simulated SCSB system in iFogSim, showcasing the connectivity between fog nodes, DOs, and DUs. In this model, fog nodes function as intermediary entities, establishing communication links between network nodes. Their primary role is to receive data access requests and forward them to the trusted authority for validation and further processing.

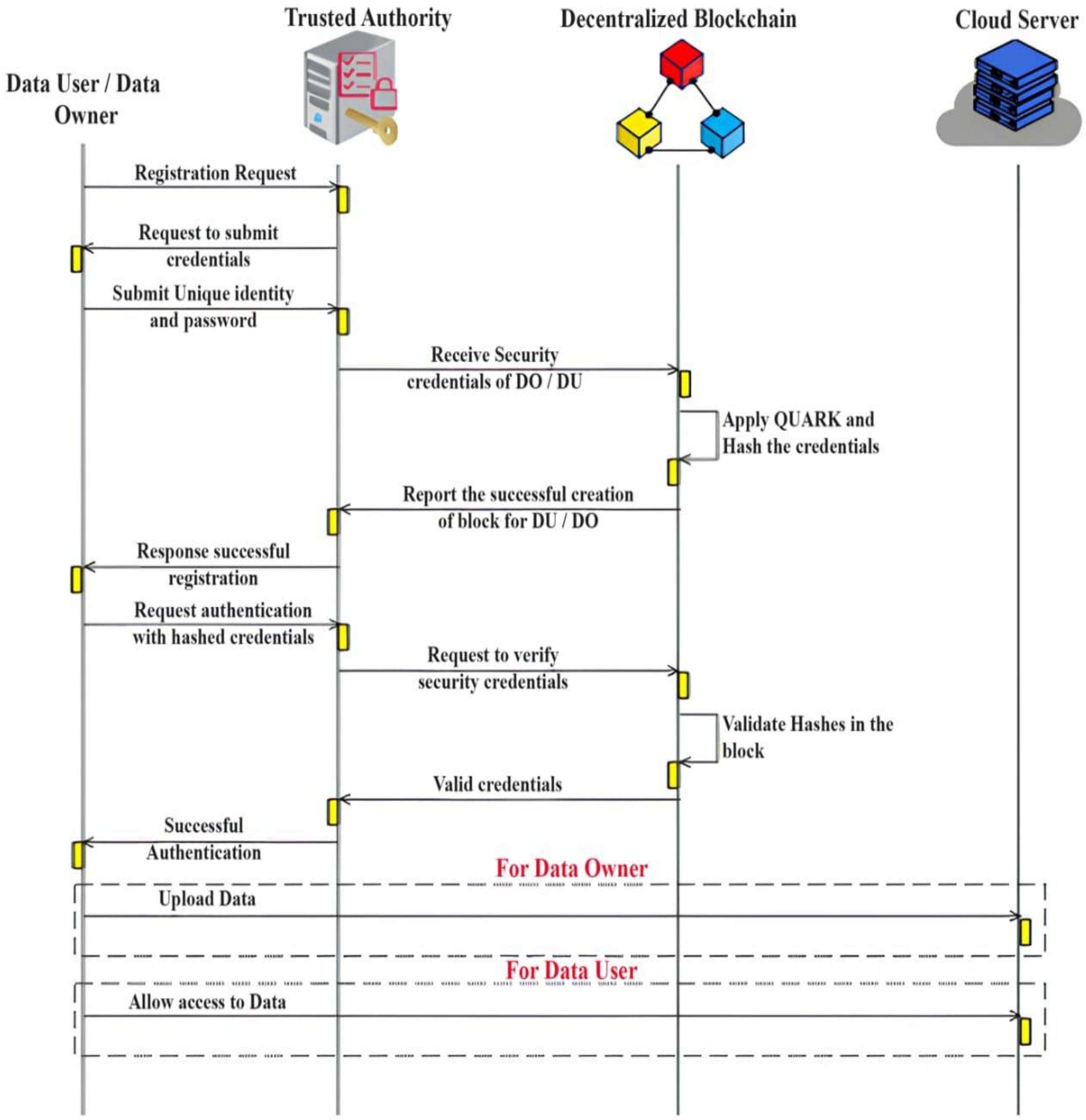

Trusted Authority
Decentralized Blockchain
Cloud Server
Data User / Data Owner
Registration Request
Request to submit credentials
Submit Unique identity and password
Receive Security credentials of DO / DU
Apply QUARK and Hash the credentials
Report the successful creation of block for DU / DO
Response successful registration
Request authentication with hashed credentials
Request to verify security credentials
Validate Hashes in the block
Valid credentials
Successful Authentication
For Data Owner
Upload Data
For Data User
Allow access to Data

Figure 4.6: SCSB Sequence Diagram

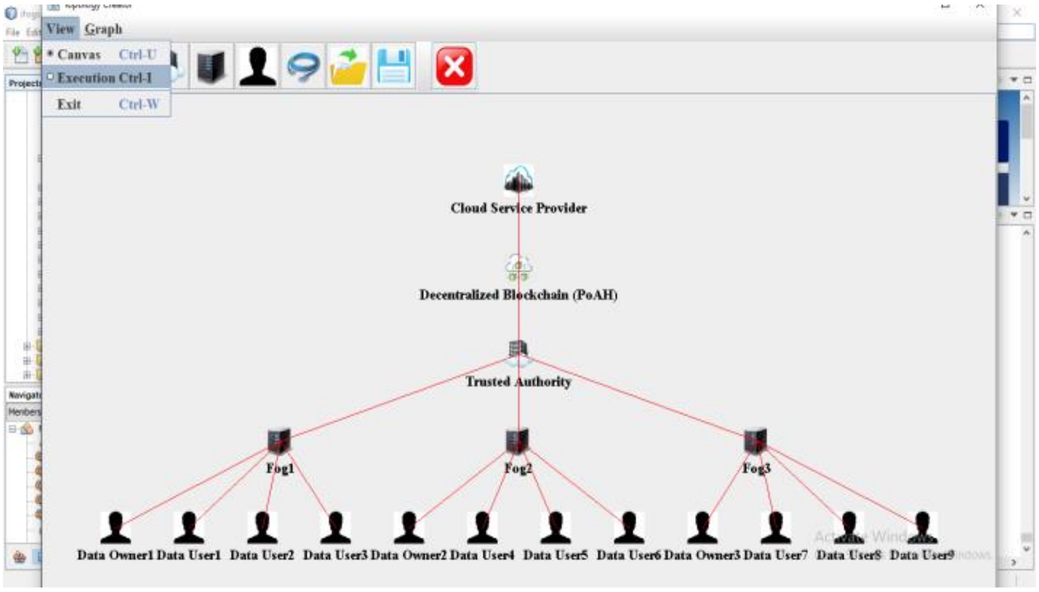
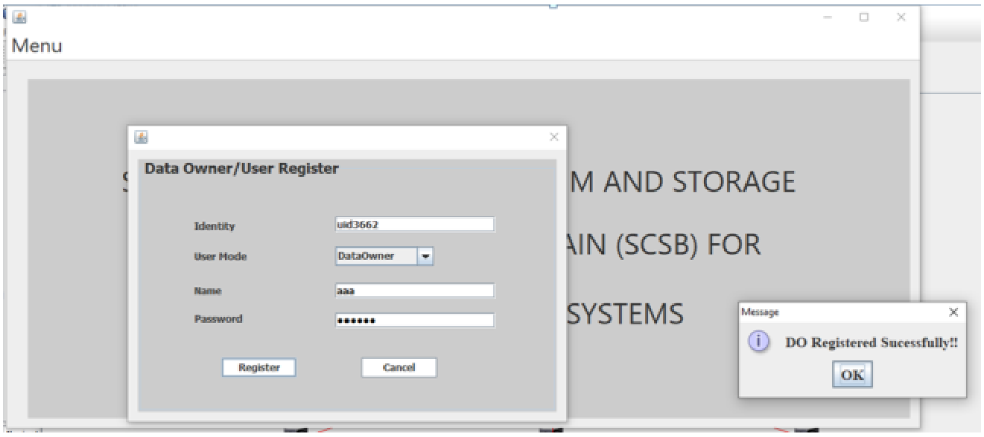


Figure 4.7: iFogSim SCSB System Model



Data Owner/User Register

Identity: uid3662

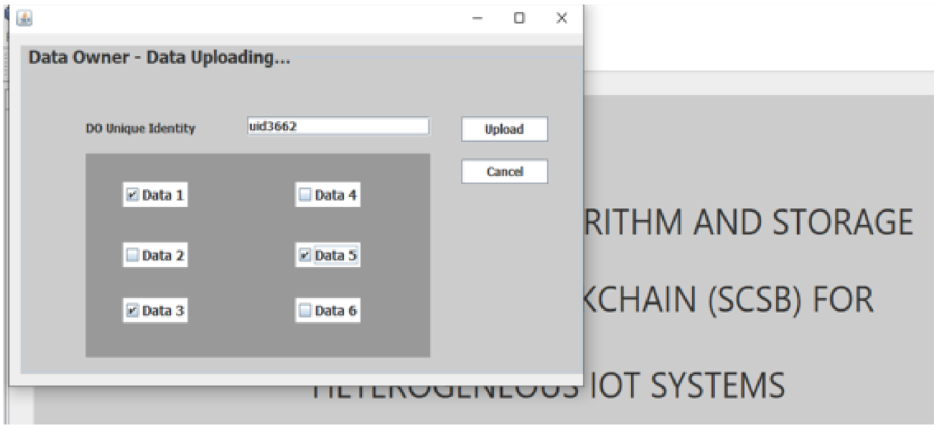
User Mode: DataOwner

Name: aaa

Password: ••••••

DO Registered Sucessfully!!

Figure 4.8: DO and DU Registration



Data Owner - Data Uploading...

DO Unique Identity: uid3662

☑ Data 1 □ Data 4

□ Data 2 ☑ Data 5

☑ Data 3 □ Data 6

Figure 4.9: DO data upload

The process of registration and data upload is depicted in Figure 4.8 and Figure 4.9. Each Data Owner (DO) has the privilege to upload multiple data files simultaneously, with no restrictions on data type. The proposed implementation has been developed and executed using the iFogSim simulation tool.

iFogSim is an open-source simulation framework specifically designed for modeling and simulating fog computing environments. It facilitates the evaluation of resource management strategies, storage optimization, and cloud resource utilization. Fog computing, also referred to as edge computing, extends traditional cloud computing by bringing computational, storage, and networking resources closer to end devices, thereby reducing latency and enhancing data processing efficiency.

The iFogSim simulation environment is configured using JDK 12.0.2, NetBeans IDE 8.2, and MySQL 5.7.36 (WAMP SERVER 3.2.6), all installed on a Windows 10 operating system. Table 4.3 provides a detailed overview of the system specifications utilized for the SCSB implementation.

Table 4.3: Simulation Specifications

Entity	**Specification**
Data Owner	3
Data User	9
Fog Nodes	3
Trusted Authority	1
Cloud Service Provider	1

4.5.2 Comparative Analysis

The comparative analysis is performed based on key performance parameters, including execution time, encryption time, decryption time, storage efficiency, throughput, latency, and hit rate. The proposed SCSB IoT heterogeneity system is evaluated against existing research methodologies, including ACE-BC, proxy re-encryption, and blockchain-based authentication.

Additionally, Table 4.4 and Table 4.5 present a detailed comparison of the proposed system with previous research approaches, highlighting its improvements in security, efficiency, and scalability.

Table 4.4: Comparison on Existing and Proposed Process

Reference	**DO Authentication**	**DU Authentication**	**Blockchain**	**Data Storage Confidentiality**
[30]	×	✓	✓	×
[31]	×	✓	✓	×
[32]	×	✓	✓	×
[34]	×	✓	×	×
[35]	✓	✓	✓	✓
[36]	✓	✓	✓	✓
[38]	✓	×	✓	✓
[39]	×	×	✓	✓
Proposed (SCSB)	✓	✓	✓	✓

Table 4.5: Comparison on Existing Method

Reference	DO Authentication	DU Authentication	Blockchain Technology	Consensus algorithm	Hashing algorithm in blockchain	Data storage security algorithm	Application Supported
[30]	-	Mutual authentication (ECC based authentication protocol)	Smart Contracts	Proof of Stake	SHA-256 algorithm	-	Decentralized application
[31]	-	Majority-based verification	Smart Contracts	-	SHA-256 with ECC algorithm	Data stored without security	Not mentioned
[33]	-	Blockchain-based token requesting mechanism	Smart Contracts	-	SHA-256 algorithm	-	Not mentioned
[34]	-	Identity based authentication	-	-	-	-	IoT based Agriculture
[35]	-	-	Ethereum smart contract	Proof-of-Authority	Collision resistant hash function	AES-128 encryption	Not mentioned
[36]	Hashing credentials using QUARK algorithm	Artificial neural network	Hyperledger fabric blockchain	Not mentioned	QUARK hashing algorithm	PRESENT algorithm	Any Sensitive IoT application

[38]	Identity authentication	-	Distributed blockchain	Not mentioned	SHA-256 algorithm	Attribute encryption mechanism	Cyber security in IoT0
[39]	-	-	Decentralized blockchain	Proof-of-Work	SHA-256 algorithm	Proxy re-encryption	Emergency IoT applications
Proposed (SCSB)	Lightweight QUARK algorithm	Lightweight QUARK algorithm	Decentralized blockchain	Proof-of-Authentication	Lightweight QUARK algorithm	TWINE algorithm and differential privacy	Heterogeneous IoT

-: ***Represents the not implemented.***

1. Execution time

Execution time is defined as the duration required for the Data User (DU) to process a request and obtain access from the cloud. An increase in execution time indicates degraded system performance. Figure 4.10 illustrates the comparative analysis of execution time among SCSB, ACE-BC, proxy re-encryption, and blockchain-based authentication mechanisms. The proposed SCSB system achieves a lower execution time compared to prior research methodologies, primarily due to the integration of a lightweight consensus algorithm.

Furthermore, the presence of illegitimate devices contributes to increased execution time by generating high network traffic, submitting fake requests, and occupying computational resources, thereby adversely affecting system efficiency.

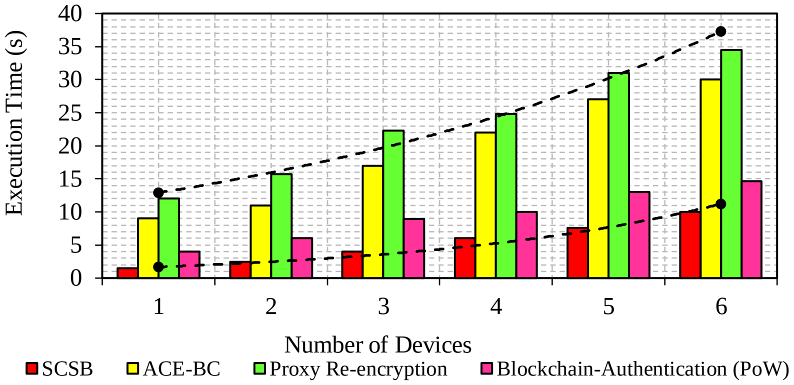


Figure 4.10: Comparison on Execution time

Blockchain technology has been utilized with the SHA-256 algorithm, which requires multiple computational processes, resulting in longer execution times. Additionally, while re-encryption mechanisms enhance security, they also contribute to higher execution time due to the necessity of performing encryption and decryption operations twice.

The proposed SCSB system achieves an average execution time of 5.3 seconds, whereas the maximum execution time observed in prior research is 23 seconds. In the SCSB system, execution time gradually increases as the number of connected devices grows, demonstrating the system's scalability under increasing workloads.

2. Encryption time and Decryption time

Encryption and decryption time refer to the duration required for a device to encrypt and decrypt a message using private and public keys. The efficiency of this process is influenced by the complexity of the cryptographic algorithm employed. Algorithms with minimal computational overhead effectively reduce encryption and decryption time, thereby enhancing system performance and responsiveness.

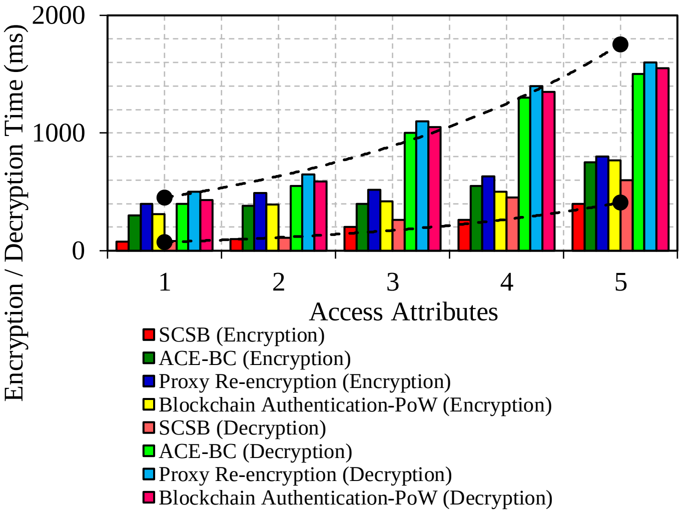


Figure 4.11: Comparison on Encryption and Decryption time

The encryption and decryption time is evaluated based on the increase in the number of access attributes. The comparative analysis of this parameter is presented in Figure 4.11 demonstrating that the proposed SCSB system achieves a lower encryption and decryption time compared to existing research methodologies. This improvement is attributed to the adoption of lightweight cryptographic algorithms, which optimize computational efficiency.

Table 4.6: Average Encryption and Decryption time

Methods used	Encryption Time (ms)	Decryption Time (ms)
SCSB	207	300
ACE-BC	476	950
Proxy Re-encryption	568	1050
Blockchain based authentication (PoW)	478	994

The integration of a lightweight consensus algorithm and blockchain with lightweight hashing enhances encryption and decryption efficiency by reducing computational overhead. This optimization significantly improves the scalability of heterogeneous systems by minimizing processing complexity. Table 4.6 presents a comparative analysis highlighting the time differences between the proposed and existing algorithms. Therefore, the adoption of lightweight cryptographic techniques serves as an effective approach to minimizing processing time and ensuring scalability in resource-constrained environments.

3. Storage Efficiency

Storage efficiency refers to the cloud server's capability to store heterogeneous data effectively. The storage of diverse data types introduces scalability challenges due to the continuous influx of large volumes of data from multiple data owners. In the proposed SCSB system, data is clustered using H-DBSCAN before being stored in the cloud. The clustering-based storage approach enhances scalability by efficiently organizing and managing data, thereby optimizing storage efficiency and improving system performance.

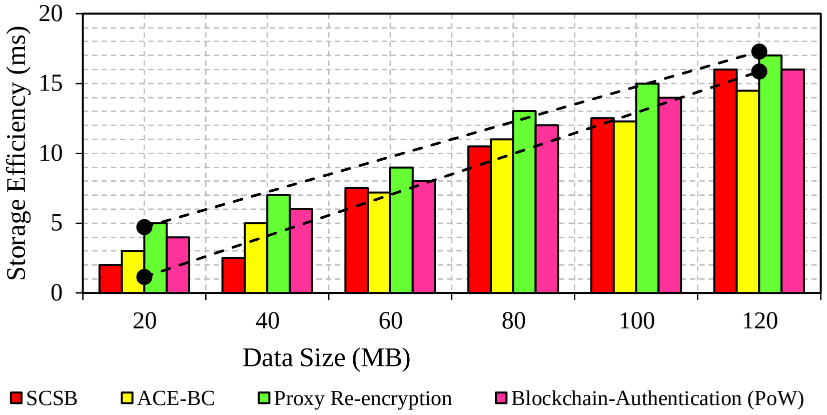


Figure 4.12: Comparison on Storage Efficiency

The results for storage efficiency are illustrated in Figure 4.12. In previous research works, data validation was performed, and all raw data were directly stored, leading to inefficient storage management and increased data redundancy. In contrast, the proposed system demonstrates higher storage efficiency by employing clustering techniques. The clustering process organizes data into specific groups, categorizing it into distinct classes within the cloud server, thereby optimizing storage utilization and enhancing scalability.

4. Throughput

Throughput is a significant network parameter that measures the amount of data transferred to the end server within the given amount of time.

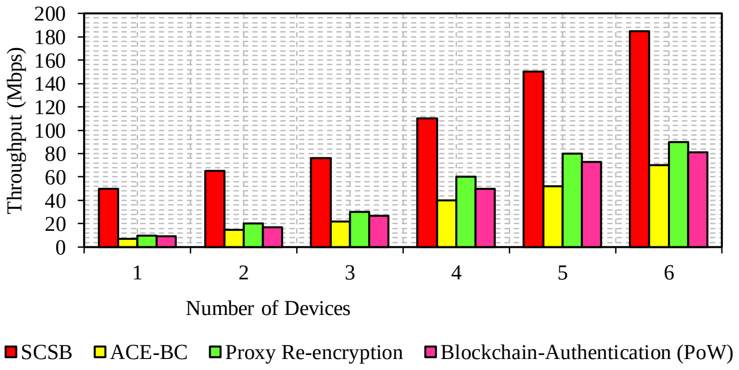


Figure 4.13: Comparison on Throughput

The throughput is analyzed as a function of the increasing number of devices, which leads to a higher volume of processing requests. Each device can generate multiple requests; including data uploads or access requests. Regardless of the request type, authentication and validation are essential before providing the required service. The graphical representation of throughput is illustrated in Figure 4.13, demonstrating that the SCSB system achieves higher throughput compared to previous research methods.

The proposed system attains an average throughput of 106 Mbps, with a minimum recorded throughput of 34 Mbps. The increase in throughput ensures efficient message transmission between devices. The significant gap between the throughput of the proposed and existing methods highlights the enhanced efficiency of data storage and access in the SCSB system.

4. Latency

Latency is the time delay encountered during data transmission from the source to the destination. An increase in latency indicates prolonged data transfer duration, leading to reduced system efficiency. Higher latency adversely impacts system performance by increasing response time and degrading real-time data processing capabilities.

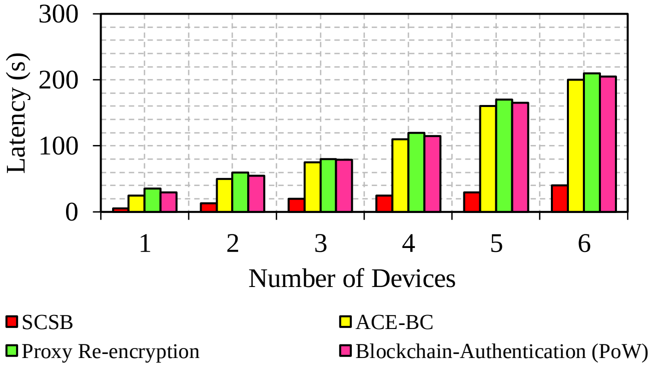


Figure 4.14: Comparison on Latency

The performance evaluation of latency is illustrated in Figure 4.14, presenting a comparative analysis between the proposed SCSB system and existing methodologies. The results indicate that the proposed system achieves lower latency compared to existing approaches, such as proxy re-encryption and blockchain-based authentication.

Table 4.7: Average Latency

Methods used	**Latency (s)**
SCSB	22.15
ACE-BC	103.4
Proxy Re-encryption	112.5
Blockchain based authentication (PoW)	108.15

The average latency achieved for each method is presented in Table 4.7. As indicated in the table, the proxy re-encryption method exhibits higher latency due to the dual encryption and decryption process for each data transmission from the device. Conversely, the integration of lightweight algorithms minimizes computational complexity, effectively reducing latency. Furthermore, the adoption of lightweight algorithms enhances system scalability and is well-suited for resource-constrained IoT devices, ensuring efficient processing and improved performance.

5. Hit rate

The performance evaluation of the hit rate concerning the increase in block size is illustrated in Figure 4.15. The hit rate parameter represents the percentage of successful device requests processed within the blockchain network. In the proposed SCSB system, the integration of a lightweight consensus algorithm enhances the hit rate by leveraging trusted nodes for block validation, thereby improving the overall efficiency and reliability of the system.

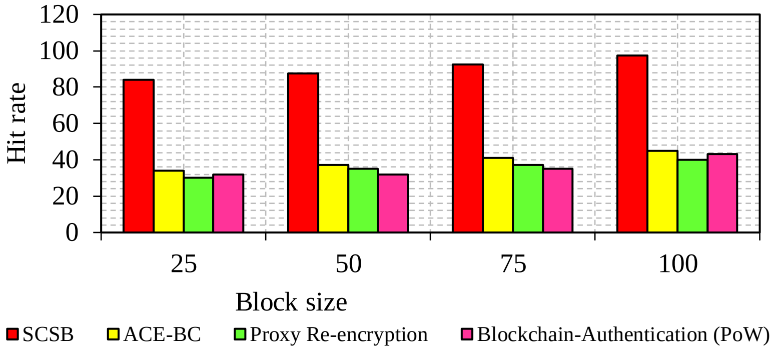


Figure 4.15: Comparison on Hit rate

Previous research methods exhibit a lower hit rate due to the lack of a trusted node selection mechanism for validation. When validation is performed by an untrusted or illegitimate node, it compromises the integrity of the process, leading to inefficient management and a reduced hit rate.

Summary

A priority-based lightweight authentication and access control mechanism is developed for Cloud-IoT, specifically addressing scalability challenges in heterogeneous IoT environments. The system begins with the registration and authentication of data owners (DOs) and data users (DUs) using user ID and password credentials. The transmission of these security credentials is secured using the lightweight QUARK algorithm, which is also integrated into the decentralized blockchain framework to enhance security while reducing computational overhead.

Upon authentication, the data owner uploads data to the cloud after determining its confidentiality level using a dual fuzzy algorithm. Low-confidential data is encrypted using the lightweight TWINE algorithm, whereas high-confidential data is secured with differential privacy techniques. To manage scalability efficiently, the uploaded data is clustered using the H-DBSCAN algorithm, mitigating the challenges posed by excessive heterogeneous data storage.

For blockchain-based security and validation, a lightweight Proof-of-Authentication (PoAH) consensus algorithm is employed. This algorithm prioritizes trusted nodes for validation, effectively eliminating illegitimate nodes from the process. As a result, the proposed SCSB system demonstrates enhanced performance in terms of security and scalability.

Future work will focus on extending the security framework by incorporating decentralized blockchain mechanisms for improved protection of cloud-stored data.

CHAPTER 5

CONCLUSION AND FUTURE WORK

The main contribution of this research is concluded in this chapter. A detailed study is done in the area of the Internet of Things (IoT) with its application, key issues, architecture and research challenges. IoT is a widespread research topic that makes communication easier with the involvement of the internet and things. The number of IoT devices is increasing day by day and hence different data collection from a variety of applications has become simpler. However, the challenging issue is the provisioning of security, to give protection for sensitive information. The technology of Blockchain is introduced to solve all the critical challenges faced in IoT security. From the analysis of state-of-the-art security approaches, it is observed that an increase in computational complexity leads to higher latency, resulting in scalability challenges. To address these issues, lightweight cryptographic and hashing algorithms are designed and integrated into blockchain frameworks, ensuring both enhanced security and improved scalability.

The proposed framework introduces lightweight authentication and access control in a decentralized blockchain. In this work, the authentication metrics that are taken into account are identity, device type, IP address and signature, Physical Unclonable Function (PUF), and biometrics. The credentials are protected during the registration and authentication process due to threats such as password attacks, man-in-middle-attacks, eavesdropping attacks, and hijacking attacks. The SALSA20 and PRESENT block cipher algorithms are proposed to ensure the protection of credentials. As there is a higher density of arriving requests, the number of credentials for authentication is chosen using fuzzy logic.

The efficiency of providing security to the data storage is based on the prediction of the required data confidentiality. This prediction is conducted using a dual fuzzy algorithm, followed by classification of high confidential level and low confidential level incorporating lightweight TWINE algorithm and differential privacy. The issue of scalability in storage is balanced using Density-based Spatial Clustering

Applications in Noise (DBSCAN) with hybrid distance measure. In blockchain, the nodes are validated with a Proof-of-Authentication (PoA) consensus algorithm that is designed to validate created nodes and manage security in the designed decentralized blockchain. The proposed approach has been analyzed through the iFogsim simulator. The experimental results have been compared and analyzed with the existing approaches. The obtained results represent that the proposed approaches outperform the existing approaches.

This chapter concludes the research work done in this thesis by highlighting its main contributions. It also discussed about the authentication, access control and data storage in Internet of Things.

5.1 Conclusion

The main contributions of this chapter are.

- The process of registration and authentication of the owner and user credentials are encrypted using the Key schedule PRESENT algorithm. This assures security for the submitted credentials, to mitigate the attackers who steal legitimate credentials.
- The selection of the number of credentials is determined using fuzzy logic in the consideration of previous authentication success, and access status. To make the system scalable, the hashing in the blockchain is performed using a lightweight QUARK algorithm. The lightweight hashing is used for minimizing the computations that could support multiple devices.
- To improve security, the chunks are divided into two and it is applied with two different encryption algorithms for each division. A division of chunks uses SALSA 20 encryption and the other division of chunks uses the PRESENT algorithm.
- The exchange of security credentials during authentication is secured in a decentralized blockchain with the incorporation of a lightweight QUARK algorithm. In decentralized blockchain Proof-of-Authentication (PoAH) performs node authentication based on the computation of trust values.

- The collected data is uploaded by the data owner which determines the confidentiality level of the data before it is uploaded. The confidentiality level is computed using dual fuzzy logic algorithm.
- From the confidential level prediction as low and high different methods are used such as Laplace based differential privacy and lightweight TWINE algorithm respectively.
- As the proposed system is heterogeneity IoT the data in cloud is clustered and stored. A hybrid distance in Density-based Spatial clustering of applications is applied.

5.1.1 Limitations of this work

- Due to the increase in the number of requests the scalability issue becomes common in the network. The key limitations are depicted in the following.
- The main focus of the study is to ensure protection for the credentials and the data to be stored. It is presented using lightweight cipher algorithms; however, the balancing of arriving requests is not considered.
- The implementation is done on the iFogsim Simulator with a specified and limited number of data owners, data users and number of requests. The outcome brings better security provisioning, whereas the results can vary in real-time applications and scenarios.
- The proposed framework can be deployed at any type of application such as healthcare, supply chain, industry and others.

5.2 Future Work

This work has developed a lot of possibilities for future research. The lightweight algorithms are developed to resolve the security issues in the Internet of Things environment. It also focuses on scalability issues and data storage in the cloud.

The following are the possible future work.

- The proposed work is tested only for the supply chain data that includes details of the manufacturer, customer, and seller. In future. Other similar attributes and applications involving sensitive data can be considered such as healthcare etc..
- The utilization of resources for the arriving requests can be handled using load balancing techniques that shall manage overloaded conditions.
- Incorporation of artificial intelligence techniques that process in parallel to minimize the latency.
- The efficiency of the proposed security has to be tested in the presence of different attackers.
- The number of fog nodes used in the experimental setup can be increased to observe the response of the proposed work on a large scale.
- The performance of the proposed system can be tested against scalability by increasing the number of devices.

REFERENCES

[1] C. M. d. Morais, D. Sadok, and J. J. J. o. t. B. C. S. Kelner, "An IoT sensor and scenario survey for data researchers," vol. 25, pp. 1-17, 2019.

[2] T. de Vass, H. Shee, S. J. J. O. Miah, and S. C. M. A. I. Journal, "IoT in supply chain management: Opportunities and challenges for businesses in early industry 4.0 context," vol. 14, pp. 148-161, 2021.

[3] A. J. I. o. T. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," vol. 15, p. 100420, 2021.

[4] K. R. J. I. I. o. T. J. Sollins, "IoT big data security and privacy versus innovation," vol. 6, pp. 1628-1635, 2019.

[5] N. S. Himanshu and R. Singh, "Evolution of IoT to IIoT: Applications & Challenges."

[6] A. D. Jurcut, P. Ranaweera, and L. J. I. s. a. i. a. Xu, "Introduction to IoT security," pp. 27-64, 2020.

[7] R. Patil, P. P. Ruhin Patel, M. Patil, and R. Ganager, "A Supervised Machine Learning Approach for Smart Home IoT Devices."

[8] G. J. I. J. o. T. Ahmed, Innovation and Management, "Improving IoT privacy, data protection and security concerns," vol. 1, 2021.

[9] H. F. Atlam, G. B. J. D. t. t. Wills, and s. cities, "IoT security, privacy, safety and ethics," pp. 123-149, 2020.

[10] G. Nebbione and M. C. J. F. I. Calzarossa, "Security of IoT application layer protocols: Challenges and findings," vol. 12, p. 55, 2020.

[11] S. Sidhu, B. J. Mohd, T. J. J. o. S. Hayajneh, and A. Networks, "Hardware security in IoT devices with emphasis on hardware trojans," vol. 8, p. 42, 2019.

[12] D. Resul and M. Z. J. I. J. o. I. S. S. Gündüz, "Analysis of cyber-attacks in IoT-based critical infrastructures," vol. 8, pp. 122-133, 2020.

[13] A. A. Abd El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, et al., "Providing end-to-end security using quantum walks in IoT networks," vol. 8, pp. 92687-92696, 2020.

[14] H. A. Abdul-Ghani, D. J. J. o. S. Konstantas, and A. Networks, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," vol. 8, p. 22, 2019.

[15] H. Liu, D. Han, and D. J. I. A. Li, "Fabric-IoT: A blockchain-based access control system in IoT," vol. 8, pp. 18207-18218, 2020.

[16] X. Li, F. Yan, F. Zuo, Q. Zeng, and L. Luo, "Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices," 2019.

[17] H. Kim, E. Kang, D. Broman, and E. A. J. A. T. o. I. o. T. Lee, "Resilient authentication and authorization for the Internet of Things (IoT) using edge computing," vol. 1, pp. 1-27, 2020.

[18] B. H. Taher, S. Jiang, A. A. Yassin, and H. J. I. A. Lu, "Low-overhead remote user authentication protocol for IoT based on a fuzzy extractor and feature extraction," vol. 7, pp. 148950-148966, 2019.

[19] A. A. Ahmed and W. A. J. S. Ahmed, "An effective multifactor authentication mechanism based on combiners of hash function over internet of things," vol. 19, p. 3663, 2019.

[20] A. Adeel, M. Ali, A. N. Khan, T. Khalid, F. Rehman, Y. Jararweh, et al., "A multi- attack resilient lightweight IoT authentication scheme," vol. 33, p. e3676, 2022.

[21] B. Mbarek, M. Ge, and T. Pitner, "Self-adaptive RFID Authentication for Internet of Things."

[22] S. Behrad, E. Bertin, S. Tuffin, and N. J. F. G. C. S. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," vol. 108, pp. 46-61, 2020.

[23] M. Mukhandi, F. Damiao, J. Granjal, and J. P. Vilela, "Blockchain-based Device Identity Management with Consensus Authentication for IoT Devices."

[24] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. J. F. I. Ishfaq, "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing," vol. 14, p. 341, 2022.

[25] N. J. A. N. Satoshi, "Bitcoin–Open Source P2P Money," 2019.

[26] H. Tian, X. Ge, J. Wang, C. Li, and H. J. I. C. Pan, "Research on distributed blockchain‐based privacy‐preserving and data security framework in IoT," vol. 14, pp. 2038-2047, 2020.

[27] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, A. J. P.-t.-p. N. Bani-Hani, and Applications, "Blockchain smart contracts: Applications, challenges, and future trends," vol. 14, pp. 2901-2925, 2021.

[28] Z. Wang, H. Jin, W. Dai, K.-K. R. Choo, and D. J. F. o. C. S. Zou, "Ethereum smart contract security research: survey and future research opportunities," vol. 15, pp. 1-18, 2021.

[29] U. Khalid et al., "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," Cluster Computing, vol. 23, no. 6, pp. 2067–2087, 2020.

[30] J. Lanaky et al., "BcmECC: A Lightweight Blockchain-Based Authentication and Key Agreement Protocol for Internet of Things," Mathematics, vol. 9, no. 24, 2021.

[31] Y. Deng et al., "A Secure and Efficient Access Control Scheme for Shared IoT Devices over Blockchain," Mobile Information Systems, vol. 2022, 2022.

[32] Q. Zhou et al., "A novel privacy protection scheme for internet of things based on blockchain and privacy set intersection technique," Journal of Cloud Computing, vol. 11, no. 93, 2022.

[33] B. Chai et al., "BHE-AC: a blockchain-based high-efficiency access control framework for Internet of Things," Personal and Ubiquitous Computing, pp. 971–982, 2022.

[34] B. Hassan et al., "A Cost Effective Identity-Based Authentication Scheme for Internet of Things-Enabled Agriculture," Wireless Communications & Mobile Computing, 2022.

[35] Z. Ullah et al., "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," IEEE Access, vol. 10, pp. 36978–36994, 2022.

[36] S. Alshehri and O. Bamasag, "AAC-IoT: Attribute Access Control Scheme for IoT Using Lightweight Cryptography and Hyperledger Fabric Blockchain," Applied Sciences, vol. 12, no. 16, 2022.

[37] Z. Liu et al., "A Blockchain-Based Privacy-Preserving Publish-Subscribe Model in IoT Multidomain Data Sharing," Wireless Communication and Mobile Computing, vol. 2022, 2022.

[38] A. Alharbi, "Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System," Sensors, vol. 23, no. 6, 2023.

[39] K. O.-B. O. Agyekum et al., "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," IEEE Systems Journal, vol. 16, no. 1, pp. 1685–1696, 2021.

[40] A. Raja Santhi and P. J. L. Muthuswamy, "Influence of blockchain technology in manufacturing supply chain and logistics," vol. 6, p. 15, 2022.

[41] Y. Du, Z. Wang, and V. C. J. F. I. Leung, "Blockchain-enabled edge intelligence for IoT: Background, emerging trends and open issues," vol. 13, p. 48, 2021.

[42] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. J. C. C. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," vol. 24, pp. 2841-2866, 2021.

[43] S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar, and R. A. J. I. A. Khan, "A systematic analysis on blockchain integration with healthcare domain: scope and challenges," vol. 9, pp. 84666-84687, 2021.

[44] T. Han, I. d. L. Ribeiro, N. Magaia, J. Preto, A. H. F. N. Segundo, A. R. L. de Macêdo, et al., "Emerging drone trends for blockchain-based 5G networks: Open issues and future perspectives," vol. 35, pp. 38-43, 2021.

[45] S. Namasudra and P. J. I. T. o. I. T. S. Sharma, "Achieving a decentralized and secure cab sharing system using blockchain technology," 2022.

[46] K. O. B. O. A. Agyekum et al., "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," IEEE Systems Journal, vol. 16, no. 1, pp. 1685-1696, 2021.

[47] O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 2, pp. 726-739, 2023.

[48] S. Zafar et al., "Integration of blockchain and Internet of Things: challenges and solutions," Annals of Telecommunications, Springer, pp. 13-32, 2022.

[49] P. Bagga et al., "Blockchain-envisioned access control for internet of things applications: a comprehensive survey and future directions," Telecommunications Systems, Springer, pp. 125-173, 2022.

[50] O. Said, "LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment," Sensors, MDPI, vol. 22, no. 20, 2022.

[51] Y. Zhang et al., "Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV," Journal of King Saud University - Computer and Information Science, vol. 34, no. 10, pp. 9216-9227, 2022.

[52] J. Sengupta et al., "FairShare: Blockchain Enabled Fair, Accountable and Secure Data Sharing for Industrial IoT," IEEE Transactions on Network and Service Management, 2023.

[53] Z. Ullah et al., "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," IEEE Access, vol. 10, pp. 36978-36994, 2022.

[54] S. Alshehri and O. Bamasag, "AAC-IoT: Attribute Access Control Scheme for IoT Using Lightweight Cryptography and Hyperledger Fabric Blockchain," Applied Sciences, vol. 12, no. 16, 2022.

[55] Z. Liu et al., "A Blockchain-Based Privacy-Preserving Publish-Subscribe Model in IoT Multidomain Data Sharing," Wireless Communication and Mobile Computing, Hindawi, 2022.

[56] Z. Ullah et al., "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," IEEE Access, vol. 10, pp. 36978-36994, 2022.

[57] U. Khalid et al., "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," Cluster Computing, Springer, pp. 2067-2087, 2020.

[58] C. Liu et al., "Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain," Security and Communication Networks, Hindawi, 2022.

[59] A. Rizzardi et al., "Securing the access control policies to the Internet of Things resources through permissioned blockchain," Concurrency and Computation Practice and Experience, Wiley Online Library, 2022.

[60] K. Hameed et al., "A formally verified blockchain based decentralized authentication scheme for the internet of things," The Journal of Supercomputing, pp. 14461-14501, 2021.

[61] A. Rejeb et al., "Blockchain Technologies in Logistics and Supply Chain Management: A Bibliometric Review," Logistics, MDPI, vol. 5, no. 4, 2021.

[62] S. Namane and I. B. Dhaou, "Blockchain-Based Access Control Techniques for IoT Applications," Electronics, MDPI, vol. 11, no. 14, 2022.

[63] O. Umoren et al., "Securing Fog Computing with a Decentralised User Authentication Approach Based on Blockchain," Sensors, MDPI, vol. 22, no. 10, 2022.

[64] Y. E. Oktian and S. G. Lee, "BorderChain: Blockchain-Based Access Control Framework for the Internet of Things Endpoint," IEEE Access, vol. 9, pp. 3592-3615, 2020.

[65] S. Alshehri et al., "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4239-4256, 2022.

[66] Y. Zhang, W. Wang, and J. Liu, "Flexible and password-authenticated key agreement scheme based on chaotic maps for multiple servers to server architecture," International Journal of Information Security, vol. 19, no. 3, pp. 233-245, 2020. Available: https://doi.org/10.1007/s10207-019-00482-7.

[67] C. Chen and J. Huang, "An enhancement of a smart card authentication scheme for multiserver architecture," Journal of Network and Computer Applications, vol. 134, pp. 1-10, 2019. Available: https://doi.org/10.1016/j.jnca.2019.02.004.

[68] M. K. Khan and K. S. Alghathbar, "An efficient and anonymous chaotic map-based authenticated key agreement for multiserver architecture," Computers & Security, vol. 79, pp. 56-67, 2018. Available: https://doi.org/10.1016/j.cose.2018.07.004.

[69] A. K. Das and A. Goswami, "An enhanced multiserver authentication protocol using password and smart-card: cryptanalysis and design," The Journal of Supercomputing, vol. 73, no. 3, pp. 1428-1452, 2017. Available: https://doi.org/10.1007/s11227-016-1855-5.

[70] D. He, N. Kumar, and N. Chilamkurti, "A lightweight authentication protocol for IoT-enabled devices in a distributed cloud computing environment," Future Generation Computer Systems, vol. 89, pp. 555-562, 2018. Available: https://doi.org/10.1016/j.future.2018.06.042.

[71] X. Li, Y. Zhang, and W. Wang, "Lightweight IoT-based authentication scheme in cloud computing circumstance," Journal of Information Security and Applications, vol. 55, 102654, 2020. Available: https://doi.org/10.1016/j.jisa.2020.102654.

[72] Y. Zhang and Y. Wang, "Blockchain and smart contracts for the Internet of Things," Journal of Network and Computer Applications, vol. 144, 102682, 2020. Available: https://doi.org/10.1016/j.jnca.2019.102682.

[73] X. Liu and J. Chen, "Cloud-based commissioning of constrained devices using permissioned blockchains," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8935-8946, 2019. Available: https://doi.org/10.1109/JIOT.2019.2934567.

[74] S. Lee and J. Park, "Blockchain infrastructure for the semantic web of things," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4185-4194, 2020. Available: https://doi.org/10.1109/TII.2019.2959782.

[75] H. Kim and N. Park, "Blockchain for IoT security and privacy: The case study of a smart home," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5535-5545, 2019. Available: https://doi.org/10.1109/JIOT.2019.2895913.

[76] L. Zhang and Z. Yu, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," Computers & Security, vol. 104, 102312, 2021. Available: https://doi.org/10.1016/j.cose.2021.102312.

[77] M. Chen and X. Zhang, "Blockchain technology for supply chain management: A comprehensive review," Computers & Industrial Engineering, vol. 142, 106561, 2020. Available: https://doi.org/10.1016/j.cie.2020.106561.

[78] N. Kshetri, "Blockchain technologies in logistics and supply chain management: A bibliometric review," Logistics, vol. 2, no. 1, 18, 2018. Available: https://doi.org/10.3390/logistics2010018.

[79] H. Treiblmaier, "Understanding blockchain technology for future supply chains: A systematic literature review and research agenda," Supply Chain Management: An International Journal, vol. 23, no. 6, pp. 545-563, 2018. Available: https://doi.org/10.1108/SCM-03-2018-0142.

[80] Y. Wang and M. L. Singgih, "How the blockchain enables and constrains supply chain performance," International Journal of Physical Distribution & Logistics Management, vol. 49, no. 4, pp. 320-339, 2019. Available: https://doi.org/10.1108/IJPDLM-03-2018-0134.

[81] M. M. Queiroz and S. F. Wamba, "Blockchain applications in supply chains, transport, and logistics: A systematic review of the literature," International Journal of Production Research, vol. 58, no. 7, pp. 2063-2081, 2019. Available: https://doi.org/10.1080/00207543.2019.1650976.

[82] K. Francisco and D. Swanson, "Exploring the impact of blockchain on digitized supply chain flows: A literature review," Journal of Supply Chain Management, vol. 54, no. 1, pp. 23-44, 2018. Available: https://doi.org/10.1111/jscm.12194.

[83] F. Tian, "Supply chain management based on blockchain: A systematic mapping study," International Journal of Computer Applications, vol. 153, no. 5, pp. 50-56, 2016. Available: https://doi.org/10.5120/ijca2016914152.

[84] A. Gurtu and J. Johny, "Blockchains in operations and supply chains: A model and reference implementation," Journal of Manufacturing Technology Management, vol. 30, no. 3, pp. 497-522, 2019. Available: https://doi.org/10.1108/JMTM-01-2018-0018.

[85] D. Dujak and D. Sajter, "Blockchains and the supply chain: Findings from a broad study of practitioners," Logistics, vol. 3, no. 1, pp. 1-17, 2019. Available: https://doi.org/10.3390/logistics3010015.

[86] A. Raj and S. D. Shetty, "IoT Eco system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey," Wireless Personal Communications, vol. 130, no. 3, pp. 1481-1517, 2022.

[87] F. Corno, L. De Russis, and L. Mannella, "Helping novice developers harness security issues in cloud-IoT systems," Journal of Reliable Intelligent Environments, vol. 8, no. 4, pp. 261-283, 2022.

[88] I. Gupta, A. K. Singh, C.-N. Lee, and R. Buyya, "Secure Data Storage and Sharing Techniques forData Protection in Cloud Environments

Systematic Review, Analysis, and Future Directions," IEEE Access, vol. 10, pp. 71247-71277, 2022.

[89] M. N. Jahantigh, A. M. Rahmani, N. J. Navimirour, and A. Rezaee, "Integration of Internet of Things and cloudcomputing: a systematic survey," IET Communications, vol. 14, no. 5, pp. 497-512, 2020.

[90] I. Ali, I. Ahmedy, A. Gani, M. U. Munir, and M. H. Anisi, "Data Collection in Studies on Internet of Things (IoT),Wireless Sensor Networks (WSNs), and Sensor

Cloud (SC): Similarities and Differences," IEEE Access, vol. 10, pp. 33909-33931, 2022.

[91] O. R. Devi et al., "The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence," Scientific Programming, vol. 2022, 2022.

[92] C. Hahn et al., "Efficient IoT Management with Resilience to Unauthorized Access to Cloud Storage," IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 1008-1020, 2020.

[93] A. Abdelmaboud et al., "Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions," vol. 11, p. 630, 2022.

[94] A. I. Abdi et al., "Blockchain Platforms and Access Control Classification for IoT Systems," Symmetry, vol. 12, no. 10, 2020.

[95] S. Namane and I. B. Dhaou, "Blockchain-Based Access Control Techniques for IoT Applications," electronics, vol. 11, no. 14, 2022.

[96] T. Sultana et al., "Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices," Applied Sciences, vol. 10, no. 2, 2020.

[97] A. (J.) Chang et al., "Blockchain Technology for Supply Chain Management: A Comprehensive Review," FinTech, vol. 1, no. 2, 2022.

[98] L. Cruz-Piris et al., "Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources," Sensors, vol. 18, no. 3, 2018.

[99] S. Pal and Z. Jadidi, "Protocol-Based and Hybrid Access Control for the IoT: Approaches and Research Opportunities," Sensor, 2021.

[100] K. Zala et al., "On the Design of Secured and Reliable Dynamic Access Control Scheme of Patient E-Healthcare Records in Cloud Environment," 2022.

[101] V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, "Blockchain-based trust management and authentication of devices in smart grid," Cleaner Engineering and Technology, vol. 8, 2022.

[102] X. Li, "A Blockchain-Based Verifiable User Data Access Control Policy for Secured Cloud Data Storage," Computational Intelligence and Neuroscience, 2022.

[103] U. Narayanan, V. Paul, and S. Joseph, "Decentralized blockchain based authentication for secure data sharing in Cloud IoT," Journal of Ambient Intelligence and Humanized Computing, pp. 769-787, 2022.

[104] P. Zhai, J. He, and N. Zhu, "Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing," Applied Sciences, vol. 2, no. 7, 2022.

[105] S. Algarni et al., "Blockchain-Based Secured Access Control in an IoT System," Applied Sciences, vol. 11, no. 4, 2021.

[106] H. Truong et al., "Enabling Decentralized and Auditable Access Control for IoT through Blockchain and Smart Contracts," Security and Communication Networks, 2022.

[107] N. Sivaselvan et al., "SUACC-IoT: secure unified authentication and access control system based on capability for IoT," Cluster Computing, 2022.

[108] Y. Deng et al., "A Secure and Efficient Access Control Scheme for Shared IoT Devices over Blockchain," Mobile Information Systems, 2022.

[109] J.-P. Aumasson et al., "Quark: a lightweight hash," Journal of Cryptography, pp. 313-339, 2013.

[110] S. Wang et al., "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38437-38450, 2018.

[111] M. Noaman et al., "Challenges in Integration of Heterogeneous Internet of Things," in Intelligent Mobile Edge Computing for Smart Internet of Things: Architecture, Algorithm, and Application, Hindawi, 2022.

[112] C. Parmar et al., "Middleware to Address Heterogeneity Problem in IoT," International Journal of Advances Research in Science, Communication and Technology, vol. 2, no. 3, 2022.

[113] V. Nguyen et al., "Versatile Network Codes: Energy Consumption in Heterogeneous IoT Devices," IEEE Access, 2020.

[114] S. Chen et al., "Edge AI for Heterogeneous and Massive IoT Networks," in 19th IEEE International Conference on Communication Technology, 2019.

[115] L. Hang and D.-H. Kim, "Design and Implementation of an Integrated IoT Blockchain platform for Sensing Data Integrity," Sensors, vol. 19, no. 10, 2019.

[116] L. H. Al-Farhani et al., "IoT and Blockchain-Based Cloud Model for Secure Data Transmission for Smart City," in Recent Advances in IoT and Blockchain-Based Security/Privacy in Advent Technology, Hindawi, 2023.

[117] W. Rafique et al., "SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things," in Advances of Intelligent Sensory Data Processing and Protection in IoT, Hindawi, 2023.

[118] M. Tcholakian et al., "Self-Sovereign Identity for Consented and Content-Based Access to Medical Records Using Blockchain," in Recent Advances in IoT and Blockchain-Based Security/Privacy in Advent Technology, Hindawi, 2023.

[119] A. S. Rajasekaran et al., "FHAAPS: Efficient Anonymous Authentication with Privacy Preservation Scheme for Farm-to-Home Communication," in Security Hardened and Privacy Preserved Vehicle-to-Everything (V2X) Communication, Hindawi, 2023.

[120] S. Bhattacharyya et al., "An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System," in Blockchain-Assisted Secure Smart Cities Communication, Hindawi, 2023.

[121] M. T. AI Ahmed, F. H. Hashim, S. J. Hashim, and A. Abdullah, "Authentication-Chains: Blockchain-Inspired Lightweight Protocol for IoT Networks," Electronics, vol. 12, no. 4, 2023.

[122] S. M. Hosseini, J. Ferreira, and P. C. Bartolomeu, "Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations," Electronics, vol. 12, no. 6, 2023.

[123] C. Nartey et al., "Blockchain-IoT peer device storage optimization using an advanced time-variant multi-objective particle swarm optimization algorithm," EURASIP Journal on Wireless Communications and Networking, no. 1, 2022.

[124] P. Bagga et al., "Blockchain-envisioned access control for internet of things applications: a comprehensive survey and future directions," Telecommunication Systems, pp. 125-173, 2022.

[125] Y. Mezquita et al., "Blockchain-Based Supply Chain Systems, Interoperability Model in a Pharmaceutical Case Study," Sensors, vol. 23, no. 4, 2023.

[126] N. Kumar et al., "A Blockchain-Oriented Framework for Cloud-Assisted System to Countermeasure Phishing for Establishing Secure Smart City," in Blockchain-Assisted Secure Smart Cities Communication, Hindawi, 2023.

[127] D. Chatziamanetoglou and K. Rantos, "Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus," in Advances in Cyber Threat Intelligence, Hindawi, 2023.

[128] S. Zhou et al., "A systematic Review of Consensus Mechanisms in Blockchain," Mathematics, vol. 11, no. 10, 2023.

[129] A. Guru et al., "A Survey on Consensus Protocols and Attacks on Blockchain Technology," Applied Sciences, MDPI, 2023.

[130] N. Shi et al., "BacS: A blockchain-based access control scheme in distributed internet of things," Peer-to-Peer Networking and Applications, Springer, pp. 2585-2599, 2021.

[131] F. Jeribi et al., "An Efficient trust Management Technique Using ID3 Algorithm With Blockchain in Smart Buildings IoT," IEEE Access, vol. 11, pp. 8136-8149, 2022.

[132] R.-K. Sheu et al., "Autonomous Mutual Authentication Protocol in the Edge Networks," Sensors, vol. 22, no. 19, 2022.

[133] A. I. Abdi et al., "Hierarchical Blockchain-Based Multi-Chaincode Access Control for Securing IoT Systems," Electronics, vol. 11, no. 5, 2022.

[134] J. Lanaky et al., "BcmECC: A Lightweight Blockchain-Based Authentication and Key Agreement Protocol for Internet of Things," Mathematics, vol. 9, no. 24, 2021.

[135] P. Gangwani et al., "IoT Device Identity Management and Blockchain for Security and Data Integrity," International Journal of Computer Applications, vol. 184, no. 42, 2023.

[136] Q. Zhou et al., "A novel privacy protection scheme for internet of things based on blockchain and privacy set intersection technique," Journal of Cloud Computing, Springer, vol. 11, no. 93, 2022.

[137] B. Chai et al., "BHE-AC: a blockchain-based high-efficiency access control framework for Internet of Things," Personal and Ubiquitous Computing, Springer, pp. 971-982, 2022.

[138] B. Hassan et al., "A Cost Effective Identity-Based Authentication Scheme for Internet of Things-Enabled Agriculture," Wireless Communications & Mobile Computing, 2022.

[139] A. Alharbi, "Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System," Sensors, vol. 23, no. 6, 2023.

[140] T. Suzaki et al., "TWINE: A Lightweight, Versatile Block Cipher," in ECRYPT Workshop on Lightweight Cryptography, 2011.

[141] L. Jiang, "A fast and accurate circle detection algorithm based on random sampling," Future Generation Computer Systems, vol. 123, pp. 245-256, 2021.

[142] M. Vijarania et al., "Energy Efficient Load-Balancing Mechanism in Integrated IoT-Fog-Cloud Environment," Electronics, vol. 11, 2023.

[143] I. Singh etal., "LAA-D: Lightweight Authentication and Access Control Mechanism with Dual-Data Storage in Cloud-Internet of Things System Using Blockchain," Iranian Journal of Science and Technology, Transactions of Electrical Engineering, vol. 48, no. 1, pp. 1-7, Sep. 2024.