

**PRIVACY-PRESERVING
BLOCKCHAIN-BASED VERIFIABLE
QUERY FRAMEWORK FOR SECURING
CLOUD-INTEGRATED IIOT SYSTEMS**

A PROJECT REPORT

Submitted by

BHAVADHARANI DEETCHANYA S

(2023246031)

A report for the phase-I

submitted to the faculty of

INFORMATION AND COMMUNICATION ENGINEERING

in partial fulfillment

for the award of the degree

of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY



DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY

COLLEGE OF ENGINEERING GUINDY

ANNA UNIVERSITY

CHENNAI 600 025

DECEMBER 2024

ANNA UNIVERSITY
CHENNAI - 600 025
BONAFIDE CERTIFICATE

Certified that this project report titled PRIVACY-PRESERVING BLOCKCHAIN-BASED VERIFIABLE QUERY FRAMEWORK FOR SECURING CLOUD-INTEGRATED IIOT SYSTEMS is the bonafide work of BHAVADHARANI DEETCHANYA S (2023246031) who carried out project work under my supervision. Certified further that to the best of my knowledge and belief, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or an award was conferred on an earlier occasion on this or any other candidate.

PLACE:CHENNAI

DATE:

DR.J. INDUMATHI

PROFESSOR

PROJECT GUIDE

DEPARTMENT OF IST, CEG

ANNA UNIVERSITY

CHENNAI 600025

COUNTERSIGNED

Dr. S. SWAMYNATHAN

HEAD OF THE DEPARTMENT

DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY

COLLEGE OF ENGINEERING GUINDY

ANNA UNIVERSITY

CHENNAI 600025

ABSTRACT

The rapid expansion of Industrial Internet of Things (IIoT) systems has led to an increased reliance on cloud services for managing vast amounts of data and facilitating real-time decision-making. However, current cloud-assisted IIoT systems face critical challenges in data privacy, security, and trust, as third-party CSPs often handle sensitive data, leaving it vulnerable to unauthorized access, tampering, and unverifiable integrity. These issues render the IIoT network susceptible to attacks and compromise its reliability.

This project proposes a Privacy-Preserving Blockchain-Based Verifiable Query Framework to strengthen data security, privacy, and trust in cloud-assisted IIoT systems. The framework employs a dual storage approach, storing textual data on-chain and images off-chain with secure AWS integration. A multi-signature-based query verification model ensures query reliability with blockchain nodes. Additionally, encrypted search indexes are generated without external libraries to ensure seamless integration. By incorporating hash-based integrity verification and robust privacy-preserving mechanisms, the framework addresses trust issues with CSPs and provides a scalable, efficient solution for managing IIoT data.

The outcome of the phase one project demonstrates significant advancements in securing cloud-assisted IIoT systems. The implementation of dual storage, multi-signature verification, and encrypted search indexes enhances privacy by restricting unauthorized access and ensuring data authenticity. Hash-based mechanisms effectively safeguard data integrity, leveraging blockchain's immutable ledger to establish trust in query results. These developments form a solid foundation for addressing critical challenges in IIoT networks, paving the way for further innovation and improving the overall security and reliability of cloud-assisted systems.

ABSTRACT TAMIL

இன்டஸ்ட்ரியல் இன்டர்நெட் ஆஃப் திங்ஸ் (IIoT) அமைப்புகளின் விரைவான விரிவாக்கம், பரந்த அளவிலான தரவை நிர்வகிப்பதற்கும் நிகழ்நேர முடிவெடுப்பதை எளிதாக்குவதற்கும் கிளவுட் சேவைகளை அதிகளவில் நம்புவதற்கு வழிவகுத்தது. இருப்பினும், தற்போதைய கிளவுட்-உதவி IIoT அமைப்புகள் தரவு தனியுரிமை, பாதுகாப்பு மற்றும் நம்பிக்கை ஆகியவற்றில் முக்கியமான சவால்களை எதிர்கொள்கின்றன, ஏனெனில் மூன்றாம் தரப்பு CSPகள் பெரும்பாலும் முக்கியமான தரவைக் கையாள்கின்றன, இது அங்கீகரிக்கப்படாத அணுகல், சேதப்படுத்துதல் மற்றும் சரிபார்க்க முடியாத ஒருமைப்பாடு ஆகியவற்றால் பாதிக்கப்படும். இந்த சிக்கல்கள் IIoT நெட்வொர்க்கை தாக்குதலுக்கு ஆளாக்குகிறது மற்றும் அதன் நம்பகத்தன்மையை சமரசம் செய்கிறது.

இந்தத் திட்டம் தரவுப் பாதுகாப்பு, தனியுரிமை மற்றும் கிளவுட்-உதவி IIoT அமைப்புகளில் நம்பிக்கையை வலுப்படுத்த தனியுரிமை-பாதுகாக்கும் Blockchain-அடிப்படையிலான சரிபார்க்கக்கூடிய வினவல் கட்டமைப்பை முன்மொழிகிறது. கட்டமைப்பானது இரட்டை சேமிப்பக அணுகுமுறையைப் பயன்படுத்துகிறது, பாதுகாப்பான AWS ஒருங்கிணைப்புடன் செயின் மற்றும் படங்களை ஆஃப்-செயினில் சேமிக்கிறது. பல கையொப்ப அடிப்படையிலான வினவல் சரிபார்ப்பு மாதிரியானது பிளாக்செயின் முனைகளுடன் வினவல் நம்பகத்தன்மையை உறுதி செய்கிறது. கூடுதலாக, மறைகுறியாக்கப்பட்ட தேடல் குறியீடுகள் தடையற்ற ஒருங்கிணைப்பை உறுதி செய்வதற்காக வெளிப்புற நூலகங்கள் இல்லாமல் உருவாக்கப்படுகின்றன. ஹாஷ்-அடிப்படையிலான ஒருமைப்பாடு சரிபார்ப்பு மற்றும் வலுவான தனியுரிமை-பாதுகாப்பு வழிமுறைகளை இணைப்பதன் மூலம், கட்டமைப்பானது CSPகளுடன் நம்பிக்கை சிக்கல்களை தீர்க்கிறது மற்றும் IIoT தரவை நிர்வகிப்பதற்கான அளவிடக்கூடிய, திறமையான தீர்வை வழங்குகிறது.

முதல் கட்டத் திட்டத்தின் முடிவு, கிளவுட்-உதவி IIoT அமைப்புகளைப் பாதுகாப்பதில் குறிப்பிடத்தக்க முன்னேற்றங்களைக் காட்டுகிறது. இரட்டை சேமிப்பகம், பல கையொப்ப சரிபார்ப்பு மற்றும் மறைகுறியாக்கப்பட்ட தேடல் குறியீடுகளை செயல்படுத்துவது, அங்கீகரிக்கப்படாத அணுகலைக் கட்டுப்படுத்தி, தரவு நம்பகத்தன்மையை உறுதி செய்வதன் மூலம் தனியுரிமையை மேம்படுத்துகிறது. ஹாஷ் அடிப்படையிலான வழிமுறைகள் தரவு ஒருமைப்பாட்டை திறம்பட பாதுகாக்கின்றன, வினவல் முடிவுகளில் நம்பிக்கையை ஏற்படுத்த பிளாக்செயினின் மாறாத லெட்ஜரை மேம்படுத்துகிறது. இந்த வளர்ச்சிகள் IIoT நெட்வொர்க்குகளில் உள்ள முக்கியமான சவால்களை எதிர்கொள்வதற்கான உறுதியான அடித்தளத்தை உருவாக்குகிறது, மேலும் புதுமைகளுக்கு வழி வகுக்கிறது மற்றும் கிளவுட்-உதவி அமைப்புகளின் ஒட்டுமொத்த பாதுகாப்பு மற்றும் நம்பகத்தன்மையை மேம்படுத்துகிறது.

ACKNOWLEDGEMENT

It is my privilege to express my deepest sense of gratitude and sincere thanks to **DR. J. INDUMATHI**, Professor, Project Guide, Department of Information Science and Technology, College of Engineering, Guindy, Anna University, for her constant supervision, encouragement, and support in my project work. I greatly appreciate the constructive advice and motivation that was given to help me advance my project in the right direction.

I am grateful to **Dr. S. SWAMYNATHAN**, Professor and Head, Department of Information Science and Technology, College of Engineering Guindy, Anna University for providing us with the opportunity and necessary resources to do this project.

I would also wish to express my deepest sense of gratitude to the Members of the Project Review Committee: **Dr. S.SRIDHAR**, Professor, **Dr. G.GEETHA**, Associate Professor, **Dr. D.NARASHIMAN**, Teaching Fellow Department of Information Science and Technology, College of Engineering Guindy, Anna University, for their guidance and useful suggestions that were beneficial in helping me improve my project.

I also thank the faculty member and non teaching staff members of the Department of Information Science and Technology, Anna University, Chennai for their valuable support throughout the course of our project work.

BHAVADHARANI DEETCHANYA S
(2023246031)

TABLE OF CONTENTS

ABSTRACT	iii
ABSTRACT TAMIL	iv
ACKNOWLEDGEMENT	v
LIST OF FIGURES	ix
LIST OF TABLES	x
LIST OF ABBREVIATIONS	xi
1 INTRODUCTION	1
1.1 INDUSTRIAL INTERNET OF THINGS (IIoT)	1
1.2 PRIVACY-PRESERVING MECHANISMS	2
1.3 BLOCKCHAIN-BASED SECURITY	3
1.4 VERIFIABLE QUERY FRAMEWORK	4
1.5 INTEGRATION WITH CLOUD SYSTEMS	4
1.6 ORGANIZATION OF THE REPORT	6
2 LITERATURE SURVEY	8
2.1 OVERVIEW	8
2.2 PRIVACY-PRESERVING MECHANISMS IN ENCRYPTED DATA SEARCH AND IOT SYSTEMS	8
2.3 BLOCKCHAIN SECURITY AND PRIVACY CHALLENGES IN DECENTRALIZED SYSTEMS	9
2.4 DATA ENCRYPTION IN BLOCKCHAIN SYSTEMS	11
2.5 QUERY PROCESSING IN BLOCKCHAIN SYSTEMS	12
2.6 MULTISIGNATURE SECURITY ENHANCEMENTS	13
2.7 CLOUD-ASSISTED SYSTEMS AND BLOCKCHAIN INTEGRATION	13
2.8 OBJECTIVE OF THE PROPOSED SYSTEM	16
3 SYSTEM DESIGN	18
3.1 GENERATION OF ENCRYPTED ON-CHAIN DATABASE	18
3.2 GENERATION OF ENCRYPTED OFF-CHAIN DATABASE	19
3.3 GENERATION OF ENCRYPTED SEARCH INDEX	19
3.4 PRIVACY-PRESERVING SEARCH OPERATION	20
3.5 MULTISIGNATURE-BASED QUERY	20

	vii
3.6	HARDWARE REQUIREMENTS 21
3.7	SOFTWARE REQUIREMENTS 21
4	DESIGN AND IMPLEMENTATION 22
4.1	BLOCKCHAIN DEVELOPMENT AND DEPLOYMENT 22
4.1.1	Initialize the Truffle Project 22
4.1.2	Edit the truffle-config.js File 23
4.1.3	Deploy to Ganache 23
4.2	STORING TEXT DATA ON-CHAIN 23
4.2.1	Receive User Input 24
4.2.2	Encrypt Data 24
4.2.3	Hashing and Conversion to Bytes32 Format 24
4.2.4	Store Data and Return Confirmation 25
4.3	STORING IMAGE DATA OFF-CHAIN 25
4.3.1	Receive and Upload Image to S3 25
4.3.2	Convert and Store Metadata on the Smart Contract 25
4.3.3	Return Confirmation with Metadata 26
4.4	Performing Search Operation 26
4.4.1	Receive and Encrypt Search Term 26
4.4.2	Generate Numeric Search Key and Convert to Bytes32 26
4.4.3	Retrieve Data and Validate Integrity 27
4.4.4	Return Search Results 27
4.5	IMPLEMENTATION OF MULTISIGNATURE QUERY VERIFICATION 27
4.5.1	Privacy-Preserving Search Operation 27
4.5.2	Multisignature-Based Query Verification 28
5	RESULTS AND DISCUSSION 29
5.1	HOME PAGE 29
5.2	STORE ON - CHAIN DATA 29
5.3	BLOCK CREATION IN GANACHE 30
5.4	STORE OFF - CHAIN DATA 31
5.5	AWS S3 BUCKET PAGE 31
5.6	SEARCH OPERATION 31
5.7	MULTISIGNATURE RESULT 32
5.8	DISCUSSION 32

6	CONCLUSION AND FUTURE WORK	34
6.1	CONCLUSION	34
6.2	FUTURE WORK	34
	REFERENCES	36

LIST OF FIGURES

3.1	Architecture diagram for the proposed system	19
4.1	Initialize the truffle project	23
4.2	Truffle-config.js File	23
4.3	Deploy to ganache	24
5.1	Home page	29
5.2	Store on - chain data	30
5.3	Block creation in ganache	30
5.4	Store off - chain data	31
5.5	AWS S3 bucket page	31
5.6	Search operation	32
5.7	Multisignature result	32

LIST OF TABLES

2.1	Summary of Existing System	17
-----	----------------------------	----

LIST OF ABBREVIATIONS

<i>IIoT</i>	Industrial Internet of Things
<i>AI</i>	Artificial Intelligence
<i>ML</i>	Machine Learning
<i>QoP</i>	Quality of Protection
<i>QoS</i>	Quality of Service
<i>Iot</i>	Internet of Things
<i>UAV</i>	Unmanned Aerial Vehicles
<i>PoW</i>	Proof of Work
<i>PoS</i>	Proof of Stake
<i>DApps</i>	Decentralized Applications
<i>OPE</i>	Order-Preserving Encryption
<i>AWS</i>	Amazon Web Services

CHAPTER 1

INTRODUCTION

1.1 INDUSTRIAL INTERNET OF THINGS (IIoT)

The Industrial Internet of Things (IIoT) is at the heart of industry digital transformation, which offers seamless connectivity between machines, sensors, and humans. With the development of these technologies, such as AI, ML, and big data analytics, IIoT systems can extract meaningful insights from the huge data that they collect. For example, predictive maintenance in manufacturing uses IIoT data to predict where equipment is likely to fail even before it happens, meaning less downtime and cost. In logistics, IIoT devices can track real-time shipments, making transactions transparent and efficient. With cloud platforms being used as the storage and processing base for data, there remain vulnerabilities, especially when this industrial data is sensitive in nature. The data, critical operational information, is prone to breaches, unauthorized modifications, and misuse by third-party providers. Such vulnerabilities make a secure and privacy-preserving solution imperative.

The Privacy-Preserving Blockchain-Based Verifiable Query Framework addresses these challenges by integrating blockchain's decentralized and tamper-proof nature with advanced cryptographic methods. Blockchain ensures that data integrity is maintained while providing an immutable audit trail for all transactions. Encryption and query privacy mechanisms, which are basically cryptographical techniques, ensure further security of the sensitive information. This framework not only protects the data lifecycle but also helps to build confidence in the minds of all IIoT stakeholders. Since this solution bridges the gap between cloud scalability and blockchain security, it has the

capability to empower the industries to make use of the IIoT system without compromising their data confidentiality and reliability.

1.2 PRIVACY-PRESERVING MECHANISMS

Privacy-preserving mechanisms refer to a set of techniques and strategies designed to protect sensitive data from unauthorized access, while enabling its legitimate use. These mechanisms ensure that personal, financial, or industrial data is kept confidential, secure, and used only by authorized entities. Common privacy-preserving techniques include data encryption, anonymization, access control, and secure multi-party computation. The goal is to balance the need for privacy with the need for data accessibility and usability, especially in environments like cloud computing and the Industrial Internet of Things (IIoT), where vast amounts of sensitive data are generated and stored.

The proposed framework incorporates robust mechanisms that address the challenges arising from data security and privacy in cloud-integrated systems of IIoT, such as protecting sensitive data against unauthorized access while ensuring smooth operations. These mechanisms combine encryption techniques and a dual storage model, balancing privacy, scalability, and operational efficiency. The framework ensures that sensitive industrial data is not compromised and is only accessed by authorized entities, even when the storage or processing infrastructure may not be trusted.

The framework stresses that encryption should be a foundational layer of security. All sensitive data is encrypted before being sent or stored, preventing third parties from accessing the data. This ensures that transmitted data remains confidential and does not include sensor readings or inventory levels. Additionally, the application of advanced cryptographic techniques enables secure querying of encrypted data, facilitating access to relevant

information without exposing the actual content to cloud service providers.

Given the enormous and heterogeneous nature of IIoT data, the framework employs a hybrid storage approach to optimize both performance and security. Critical data, such as metadata and key attributes, is stored on the blockchain to leverage its immutability and transparency. At the same time, larger data files, such as multimedia content, are stored off-chain in cloud systems to ensure scalability and reduce computational overhead on the blockchain network. This dual storage model links off-chain data to the blockchain using cryptographic hashes, ensuring data integrity while managing IIoT data securely and efficiently.

1.3 BLOCKCHAIN-BASED SECURITY

Blockchain technology is the bedrock of the framework, addressing a couple of critical security issues: data integrity and centralized control. The decentralized architecture of this blockchain ensures that data is tamper-proof and highly resilient against single points of failure. By replicating data across multiple nodes, the framework guarantees availability and reliability, even in the event of potential disruptions.

The immutability of blockchain records ensures that data integrity is preserved. Cryptographic hashes secure each transaction, preventing unauthorized modifications and enabling stakeholders to audit the data's history. This is particularly significant in IIoT systems, where the authenticity and accuracy of data directly impact decision-making processes.

Decentralization has the added benefit of trust among various stakeholders. Manufacturers, distributors, and other participants in an IIoT ecosystem can behave as nodes of a blockchain network. Thus, reliance

on a centralized controlling element is removed while encouraging an open, accountable, and shared governance culture in the same ecosystem

1.4 VERIFIABLE QUERY FRAMEWORK

A Verifiable Query Framework (VQF) is a cryptographic and computational model designed to ensure that queries executed on a distributed system, such as a blockchain network, return accurate and authenticated results. It allows users to verify the correctness of the query results without relying solely on the trustworthiness of the data provider. The framework typically incorporates cryptographic mechanisms such as digital signatures, hashing, and multi-party computation (MPC) to authenticate data and verify its integrity.

In such a framework, query results are not only encrypted to preserve privacy but also signed by multiple parties (e.g., blockchain nodes), enabling the user to confirm the authenticity of the data before acting on it. This creates a secure and transparent process for accessing data in environments like Industrial Internet of Things (IIoT) systems, where data integrity and privacy are critical for real-time decision-making.

For example, in supply chain management applications, a verifiable query framework ensures that the information retrieved for tracking and monitoring is not tampered with, even when stored with untrusted third-party providers. By ensuring privacy-preserving query operations and providing mechanisms for authenticating query results, the framework reduces risks related to data manipulation and enhances the overall trustworthiness of the system. This promotes higher levels of transparency and accountability, as stakeholders can independently verify the data's authenticity before using it in decision-making processes.

1.5 INTEGRATION WITH CLOUD SYSTEMS

The integration of blockchain with cloud systems provides a hybrid solution that combines the strengths of both technologies. Cloud systems offer scalability, cost-effectiveness, and high-performance capabilities for managing large amounts of data and performing complex computations. Blockchain, on the other hand, ensures data integrity, transparency, and security through decentralized consensus and cryptographic mechanisms. By integrating these two systems, the proposed framework leverages the cloud for efficient data storage and processing, while maintaining the trust and immutability provided by blockchain.

The proposed system combines blockchain platforms with cloud infrastructure to form a unified ecosystem designed to optimize the security, scalability, and efficiency of Industrial Internet of Things (IIoT) systems. The core objective of the system is to provide secure data management and real-time analytics through a distributed ledger, while utilizing the cloud's scalability and computational power for data processing and storage.

In this system, non-sensitive data is hosted on cloud platforms, which allows IIoT operators to take advantage of the cloud's ability to handle large datasets and perform computational tasks efficiently. Real-time analytics are performed in the cloud, providing actionable insights for operators to proactively address potential issues such as equipment failures or supply chain disruptions.

Blockchain serves as the primary source of trust in this framework, ensuring the integrity and authenticity of data through cryptographic hashing and the storage of secure metadata on-chain. Interactions between the blockchain and cloud systems are streamlined by a verification protocol,

designed to interface seamlessly with the blockchain. This enables smooth data exchange and verification between the two systems.

By integrating blockchain with cloud systems, the framework improves the overall performance, security, and reliability of IIoT ecosystems. It ensures that data is managed securely and transparently, while also enabling efficient, scalable operations that can handle large volumes of real-time data. This integrated approach enhances the capabilities of IIoT systems, ensuring they can operate securely and efficiently at scale.

1.6 ORGANIZATION OF THE REPORT

This report is organized into 6 chapters, describing each part of the project with detailed illustrations and system design diagrams.

CHAPTER 2: Literature Review reviews existing research, studies, and relevant literature related Autonomous Driving. Discusses the background, theories, and methodologies used by other researchers

CHAPTER 3: System Design describes the design of the project. Explains the architecture, components, algorithms, and any other technical details.

CHAPTER 4: Implementation provides details about how the project was implemented. Discusses the tools, technologies, programming languages, and frameworks used.

CHAPTER 5: Result and Analysis presents the results of the project. Analyzes the outcomes, compare them with expectations, and discuss any challenges faced during implementation.

CHAPTER 6: Conclusion and Future Work summarizes the findings and draws conclusions. Discusses the significance of your work and its implications

CHAPTER 2

LITERATURE SURVEY

2.1 OVERVIEW

Blockchain technology has emerged as a transformative solution for securing Cloud-Assisted IIoT systems by addressing critical challenges such as data privacy, integrity, and trust. Existing literature highlights the limitations of centralized cloud services, including data breaches and unauthorized access, which threaten the security of sensitive industrial data. Blockchain's decentralized architecture and cryptographic mechanisms enhance data protection by eliminating single points of failure and enabling tamper-proof records. Additionally, techniques like smart contracts and multi-signature models ensure automated and verifiable query processing, reducing reliance on third-party cloud providers. This foundation provides a robust framework for privacy-preserving query verification and secure data management in IIoT environments.

2.2 PRIVACY-PRESERVING MECHANISMS IN ENCRYPTED DATA SEARCH AND IOT SYSTEMS

B. Wang et al. [1] emphasize the need for secure and efficient multi-keyword fuzzy searches on encrypted cloud data, enabling users to retrieve relevant information even with minor input inaccuracies. Their proposed framework ensures privacy preservation while maintaining data security and search precision. However, the study identifies challenges, such as computational overhead and the trade-off between search accuracy and efficiency, particularly in large-scale datasets. Similarly, Qiuyun et al.

[2] introduce VPSL, a verifiable privacy-preserving data search framework for cloud-assisted IoT systems. By integrating searchable encryption with verifiable mechanisms, this solution ensures secure searches on encrypted data while preserving data integrity. Despite its efficiency in resource-constrained environments, challenges like scalability and the complexity of implementing verifiable search operations remain open areas for further research.

Zhang et al. [3] focus on privacy and security in mobile healthcare (mHealth) networks, proposing a Quality of Protection (QoP) framework to safeguard sensitive patient data while optimizing system performance. Their approach includes lightweight cryptographic algorithms and context-aware authentication for resource-constrained devices, addressing challenges such as energy consumption and diverse privacy requirements. Zheng et al. [4] tackle privacy concerns in IoT data linkage by employing advanced encryption and anonymization techniques, balancing data utility with privacy protection. In social networks, Zaobo et al. [5] present a privacy-preserving mechanism combining data perturbation and utility models to enable secure data sharing without compromising data quality. Additionally, Han et al. [6] propose a privacy-aware influence maximization method for GPS-enabled networks, leveraging differential privacy and secure aggregation to protect sensitive user data while optimizing influence spread. These frameworks underscore the critical importance of addressing privacy and efficiency trade-offs in modern interconnected systems.

2.3 BLOCKCHAIN SECURITY AND PRIVACY CHALLENGES IN DECENTRALIZED SYSTEMS

The integration of blockchain technology across various sectors has brought to light several security and privacy concerns that must be addressed to unlock its full potential. Fernández-Caramés et al. [7] explore the synergy

between UAVs (Unmanned Aerial Vehicles) and blockchain for enhancing inventory management and traceability in Industry 4.0 warehouses. Their work emphasizes the role of decentralization in improving data protection and monitoring efficiency, although issues like high UAV costs, scalability, and data privacy concerns remain significant challenges in large-scale industrial applications. In a broader context, Joshi et al. [8] survey the fundamental security and privacy issues surrounding blockchain, pinpointing vulnerabilities such as consensus mechanism attacks, privacy leakage, and scalability limitations. The authors highlight promising solutions like homomorphic encryption, zero-knowledge proofs, and sharding to address these issues, though the need for further research remains in balancing transparency with confidentiality for wider blockchain adoption.

Blockchain's security challenges extend to various aspects of decentralized systems, including the integrity of transactions and the protection of sensitive data. Joshi et al. [9] examine data integrity, confidentiality, and authentication concerns in blockchain, stressing the importance of cryptographic techniques such as zero-knowledge proofs and homomorphic encryption to improve privacy. They explore solutions for scalability, such as sharding and off-chain storage, which are essential to managing large-scale transactions. Similarly, Lin and Liao [10] focus on blockchain vulnerabilities like 51% attacks and smart contract weaknesses, proposing enhanced consensus algorithms and secure smart contract frameworks. Wang et al. [11] explore blockchain's potential in industries like finance and healthcare but acknowledge significant challenges like energy consumption and privacy issues. They propose hybrid consensus mechanisms and integration with emerging technologies like IoT and AI to overcome these hurdles. Li et al. [12] provide a comprehensive analysis of blockchain security, categorizing threats across various layers such as consensus mechanisms, data integrity, and network security. They emphasize the importance of privacy-preserving

techniques, such as zero-knowledge proofs and ring signatures, and highlight the ongoing challenge of balancing security, performance, and decentralization in blockchain systems. These surveys collectively underscore the need for advanced solutions to enhance blockchain security and privacy while ensuring scalability for widespread adoption.

2.4 DATA ENCRYPTION IN BLOCKCHAIN SYSTEMS

Rakesh Agrawal et al. [13] focus on developing an encryption scheme that preserves the order of numeric data, allowing range queries on encrypted databases without decrypting the data. The objective is to establish an order-preserving encryption (OPE) scheme that facilitates database operations such as sorting and comparisons while maintaining data confidentiality. However, the literature highlights a critical limitation: the leakage of order information inherent in OPE, which can expose encrypted data to potential inference attacks. Though the scheme shows efficiency for specific operations, it lacks robust security guarantees, particularly in scenarios where adversaries can conduct statistical analysis based on the ciphertext sequence.

Dawn Xiaoding Song et al. [14] address the challenge of conducting secure searches on encrypted data, ensuring that neither the data nor search queries are revealed to untrusted servers. Their aim is to create practical cryptographic techniques that support keyword-based searches on encrypted data, enabling users to perform searches while ensuring confidentiality and security. A key limitation discussed is the trade-off between security and performance. While the proposed techniques ensure security, they introduce significant computational overhead, especially with large datasets. Additionally, these methods often depend on precise keyword matches, limiting their flexibility and usability in real-world scenarios where fuzzy or adaptable search functionalities are needed.

Boldyreva et al. [15] introduce Order-Preserving Symmetric Encryption (OPE), a cryptographic method that maintains the order of plaintext values in their encrypted form. This allows comparison operations on encrypted data without decryption, making it suitable for secure database queries and range queries. The proposed OPE scheme is based on rigorous theoretical foundations, ensuring security under specific conditions and balancing computational efficiency. However, the authors acknowledge challenges such as the potential leakage of order information, scalability issues for large datasets, and the trade-offs between security and performance in practical applications.

2.5 QUERY PROCESSING IN BLOCKCHAIN SYSTEMS

Przytarski et al. [16] explore the growing need for effective query processing in decentralized and immutable data environments, noting that traditional database query methods are insufficient. They examine existing techniques for query processing within blockchain settings, evaluate their effectiveness and limitations, and suggest areas for future research to improve performance, scalability, and adaptability, particularly for complex queries. One significant limitation identified in the literature is the inherent trade-off between query efficiency and the decentralized architecture. Maintaining data consistency and executing complex queries across distributed nodes leads to considerable performance bottlenecks. Additionally, the immutable nature of blockchain data creates challenges in modifying and enhancing query execution plans, limiting the system's ability to support real-time or extensive analytics.

2.6 MULTISIGNATURE SECURITY ENHANCEMENTS

Harn et al. [17] explored enhancements to the efficiency and security of identity-based multi-signature schemes, enabling multiple signers to endorse a single document collaboratively through a streamlined identity-based framework. The goal is to create a multi-signature scheme utilizing the Guillou-Quisquater (GQ) signature framework, focusing on reducing computational complexity and communication overhead. This approach aims to be effective in resource-constrained environments, including wireless sensor networks and mobile systems. Nonetheless, as highlighted in existing studies, a drawback of this method is its susceptibility to specific security threats, including forgery or replay attacks, especially in dynamic networks where managing keys and coordinating signers can prove to be complex. Moreover, although the framework minimizes overall computational demands, the identity-centric design raises significant concerns about key escrow and reliance on a central authority, potentially resulting in privacy challenges.

2.7 CLOUD-ASSISTED SYSTEMS AND BLOCKCHAIN INTEGRATION

Hossain and Muhammad [18] propose a cloud-assisted Industrial Internet of Things (IIoT) framework tailored for health monitoring, focusing on real-time data collection, analysis, and decision-making. This framework leverages IIoT devices to continuously monitor patients' physiological data and cloud computing for efficient storage and advanced analytics. The approach enhances the scalability and flexibility of health monitoring systems while ensuring timely responses to critical health events. Challenges identified include ensuring data privacy and security within the cloud, managing the high volume of data generated by IIoT devices, and addressing latency concerns to enable real-time monitoring. This work highlights the potential of integrating IIoT

and cloud technologies to transform traditional healthcare systems into more proactive and data-driven models.

Wu et al. [19] present an innovative approach to efficient B-tree-based indexing tailored for cloud data processing environments. The paper addresses the limitations of traditional indexing techniques in distributed and scalable cloud infrastructures, where data is often partitioned and replicated across multiple nodes. The authors propose a cloud-optimized B-tree indexing framework that enhances performance by incorporating features like workload-aware partitioning, dynamic node allocation, and efficient query processing. The framework balances load distribution and minimizes the overhead of maintaining index consistency across distributed systems. Experimental evaluations demonstrate significant improvements in query latency and index maintenance costs compared to existing methods. However, the study notes challenges in handling highly dynamic workloads and ensuring fault tolerance in large-scale cloud systems. This research serves as a foundation for developing scalable and efficient indexing techniques for modern cloud-based applications.

Li et al. [20] present a novel approach for secure and verifiable multi-key image search in cloud-assisted edge computing environments. The paper addresses the growing need for efficient and privacy-preserving image retrieval systems, especially in scenarios where sensitive image data is stored in cloud systems and processed through edge computing nodes. The authors propose a secure image search framework that employs advanced encryption techniques and a multi-key search mechanism to ensure both the privacy of the data and the integrity of search results. By utilizing homomorphic encryption, the framework enables secure search operations on encrypted image data, preventing unauthorized access while maintaining the ability to perform queries. Additionally, the paper introduces a verifiable search process, where

the correctness of the search results is guaranteed through cryptographic proofs, ensuring that users can trust the results without compromising their data's privacy. The proposed system also addresses challenges such as communication overhead and computational efficiency, which are critical in edge computing environments with resource-constrained devices. While the solution provides promising results in terms of security and privacy, the authors acknowledge that the scalability of the system and its integration with existing cloud-edge infrastructures remain areas for further investigation.

Park and Park [21] examine the application of blockchain technology in enhancing the security of cloud computing environments, focusing on use cases, challenges, and potential solutions. The paper outlines various scenarios where blockchain can address key security concerns such as data integrity, access control, and authentication in cloud systems. The authors highlight how blockchain's decentralized, immutable ledger can provide enhanced transparency and traceability of cloud-based transactions, thus mitigating risks associated with data tampering and unauthorized access. They also discuss the challenges of implementing blockchain in cloud environments, including scalability issues, energy consumption, and integration complexity with existing cloud architectures. Moreover, the paper explores several solutions to these challenges, such as the use of hybrid blockchain models and consensus algorithms that balance security with efficiency. The authors conclude by emphasizing the need for further research into blockchain's potential for securing cloud computing, particularly in terms of performance optimization and addressing the interoperability of blockchain systems with various cloud platforms.

2.8 OBJECTIVE OF THE PROPOSED SYSTEM

- Develop a blockchain-enabled privacy-preserving verifiable query framework for securing cloud-assisted IIoT systems.
- Protection of data stored and accessed from Cloud Service Providers, that is, through encryption and blockchain integration.
- Use multi-signature verification techniques to maintain user data privacy during query operations.
- Implement mechanisms to validate the integrity and authenticity of query results returned from cloud storage.
- Combine blockchain for on-chain storage of critical textual attributes with off-chain storage for multimedia data.

Table 2.1: Summary of Existing System

Author(s) and Paper Title	Technique Used	Feature Advantages	Limitations
Fernández-Caramés et al. , <i>Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applications in Big Data-Driven Supply Chain Management</i>	Integration of UAVs and Blockchain for real-time inventory tracking and traceability in supply chain management	Enhances inventory management, traceability, and data security using UAVs and blockchain	High cost of UAVs, scalability issues in blockchain, and privacy concerns in large-scale implementations
Rakesh Agrawal et al. , <i>Order Preserving Encryption for Numeric Data</i>	Order-Preserving Encryption (OPE) scheme for range queries on encrypted databases	Supports sorting and comparison operations on encrypted data while preserving confidentiality	Leakage of order information and vulnerability to inference attacks
Dawn Xiaoding Song et al. , <i>Practical Techniques for Searches on Encrypted Data</i>	Cryptographic techniques for keyword-based searches on encrypted data	Maintains data confidentiality and allows secure searches over encrypted data	Performance overhead and limited to exact keyword matches
B. Wang et al. , <i>Privacy-Preserving Multi-Keyword Fuzzy Search Over Encrypted Data in the Cloud</i>	Multi-keyword fuzzy search mechanism for flexible search over encrypted cloud data	Flexible searches tolerant to minor input errors, ensuring data security and accuracy	Increased complexity and computational overhead
Przytarski et al. , <i>Query Processing in Blockchain Systems: Current State and Future Challenges</i>	Analysis of current query processing methods in blockchain systems	Evaluates blockchain-based query efficiency and proposes future enhancements for complex queries	Performance bottlenecks and difficulty in updating query plans for large-scale analytics
Harn et al. , <i>Efficient Identity-Based GQ Multisignatures</i>	Identity-based multi-signature scheme using the Guillou-Quisquater (GQ) framework	Reduces computational complexity and communication overhead in constrained environments	Vulnerable to forgery and replay attacks, and key escrow issues
Guo and Yu , <i>A Survey on Blockchain Technology and its Security</i>	Survey of blockchain foundations and security challenges	Identifies vulnerabilities and explores cryptographic solutions such as homomorphic encryption and zero-knowledge proofs	Consensus mechanism attacks, scalability issues, and privacy concerns
Li et al. , <i>Order-Revealing Encryption: File-Injection Attack and Forward Security</i>	Analysis of an order-revealing encryption scheme with improved forward security	Mitigates file-injection attacks while maintaining efficiency	Vulnerability to leakage under specific adversarial models
Hossain and Muhammad , <i>Cloud-Assisted Industrial Internet of Things (IIoT) Framework for Health Monitoring</i>	Real-time data collection and analysis using IIoT devices and cloud computing	Improves scalability and flexibility for health monitoring systems	Data privacy and latency challenges in cloud environments
Joshi et al. , <i>Security and Privacy Challenges in Blockchain Systems</i>	Survey on blockchain security and privacy	Identifies vulnerabilities and discusses solutions like homomorphic encryption and zero-knowledge proofs	Challenges include consensus mechanism attacks and privacy leakage
Boldyreva et al. , <i>Order-Preserving Symmetric Encryption for Secure Data Querying</i>	Order-Preserving Symmetric Encryption (OPE)	Enables secure comparison and range queries on encrypted data	Potential leakage of order information and scalability issues
Zhang et al. , <i>Security and Privacy Challenges in Mobile Healthcare Networks</i>	QoP-driven framework for mHealth networks	Balances security, efficiency, and user satisfaction in health monitoring systems	Trade-offs between security and system performance

CHAPTER 3

SYSTEM DESIGN

The system design introduces a blockchain-enabled privacy-preserving framework for securing cloud-assisted Industrial Internet of Things (IIoT) systems. It combines on-chain and off-chain data management, using blockchain for secure, immutable storage of sensitive data and cryptographic techniques for query verification. Large data files are stored off-chain to optimize performance, while ensuring data integrity and privacy. This hybrid approach enables secure querying without exposing sensitive information, offering a scalable and secure solution for IIoT ecosystems.

3.1 GENERATION OF ENCRYPTED ON-CHAIN DATABASE

This module focuses on securing textual data by employing a two-layer encryption process. Initially, the plain text input from the user interface undergoes Caesar cipher encryption, where each character is shifted by a predefined key to produce ciphertext. The ciphertext is subsequently hashed using the SHA-256 algorithm, generating a unique, tamper-proof hash value. This hash value is recorded on the blockchain as a transaction, ensuring data immutability and integrity. To complete the process, a transaction ID is generated, providing the user with confirmation that the encryption and storage on-chain were successful. This ensures both security and traceability for sensitive textual data.

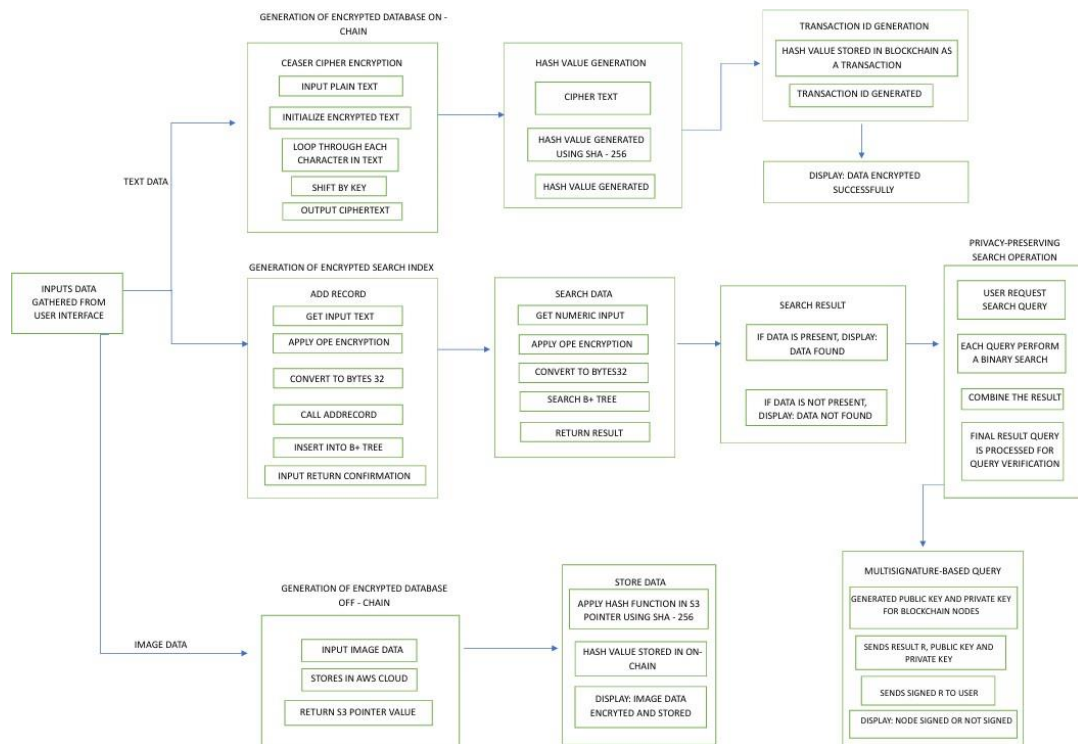


Figure 3.1: Architecture diagram for the proposed system

3.2 GENERATION OF ENCRYPTED OFF-CHAIN DATABASE

For large data files such as images, this module optimizes performance by leveraging off-chain storage in AWS S3. The image data is securely stored, and a pointer value (such as an S3 URI) is generated. To maintain data integrity, the pointer is hashed using the SHA-256 algorithm, and the resulting hash is stored on the blockchain. This hybrid approach not only ensures scalability but also maintains a secure link between on-chain records and off-chain data. The blockchain serves as a trusted ledger to verify the authenticity and integrity of the off-chain image data while reducing storage overhead.

3.3 GENERATION OF ENCRYPTED SEARCH INDEX

This module enables efficient and privacy-preserving search capabilities by encrypting the input data using Order-Preserving Encryption (OPE). OPE allows encrypted data to retain its order, which is crucial for performing range queries. The encrypted values are converted into a standardized 32-byte format and added to a B+ tree data structure. The B+ tree enables quick indexing and retrieval of encrypted records. Once the record is successfully added to the index, the system confirms the operation to the user. This mechanism ensures that data remains secure while still being searchable, providing an efficient balance between privacy and functionality.

3.4 PRIVACY-PRESERVING SEARCH OPERATION

The search operation is designed to protect user privacy during data retrieval. Input queries are first encrypted using the same OPE mechanism to maintain consistency with the encrypted search index. The encrypted query is then processed across multiple nodes of the blockchain network, each performing a binary search on its segment of the B+ tree index. Partial results from the nodes are securely combined to produce the final output. This result is further verified using cryptographic techniques to ensure its accuracy. The modularity and decentralization of the search process guarantee both privacy and scalability in the query handling.

3.5 MULTISIGNATURE-BASED QUERY

To further strengthen security, the system employs a multi-signature approach for query result validation. Each blockchain node involved in processing the query generates a public and private key pair. After processing

the query, the nodes use their private keys to sign the results. These signed results are sent to the user, who uses the public keys to verify their authenticity. This multi-signature process ensures that only authorized nodes contribute to the query results, making the responses tamper-proof and trustworthy. By requiring multiple signatures for validation, the system enhances trustworthiness and mitigates the risk of unauthorized data manipulation.

3.6 HARDWARE REQUIREMENTS

- Processor: 3.0 GHz Intel Scalable Processor or above
- RAM: 8 GB (minimum)
- Storage: SSD with at least 10 GB of free space

3.7 SOFTWARE REQUIREMENTS

- Ethereum: Ethereum network (testnet) for blockchain deployment and testing.
- Ganache: For local Ethereum blockchain testing and development.
- Truffle: For smart contract development, testing, and deployment.
- Solidity: Programming language for writing smart contracts.
- Node.js: JavaScript runtime environment for backend services and npm package management.
- Web3.js/ethers.js: JavaScript libraries for interacting with the Ethereum blockchain from the frontend.
- AWS: Amazon Web Services (AWS) for hosting, deployment, and management of blockchain nodes and decentralized applications.

CHAPTER 4

DESIGN AND IMPLEMENTATION

The implementation of the Privacy-Preserving Blockchain-Based Verifiable Query Framework for Securing Cloud-Integrated IIoT Systems focuses on integrating blockchain technology with cloud services to ensure secure, verifiable, and privacy-preserving data access in Industrial Internet of Things (IIoT) environments. The system architecture incorporates a permissioned blockchain (such as Ethereum) for storing sensitive data, while non-sensitive data is stored in a cloud environment (e.g., AWS S3). Privacy-preserving techniques, including encryption and hashing are employed to maintain data confidentiality and integrity during query execution. A multi-signature scheme ensures the verifiability of query results. This approach enables secure data querying from IIoT devices, with the blockchain providing authentication and verification mechanisms to guarantee data privacy. The cloud infrastructure offers scalability and resilience, supporting the seamless integration of IIoT systems.

4.1 BLOCKCHAIN DEVELOPMENT AND DEPLOYMENT

4.1.1 Initialize the Truffle Project

Before proceeding with the Truffle setup, make sure Node.js is installed on your machine. Node.js is needed to run Truffle and other JavaScript-based tools. Truffle is a framework for Ethereum smart contract development, deployment, and testing. Initializing a Truffle project in your directory integrates it with the Truffle suite and enables you to interact with

the Ganache environment, which is essential for local Ethereum blockchain simulation.

```
Compiling your contracts...
=====
> Compiling .\contracts\DataStore.sol
> Artifacts written to C:\Users\deetc\Desktop\flask-ethereum-app\blockchain-flask\build\contracts
> Compiled successfully using:
  - solc: 0.8.0+commit.c7dfd78e.Emscripten.clang
```

Figure 4.1: Initialize the truffle project

4.1.2 Edit the truffle-config.js File

Once Truffle is initialized, a truffle-config.js (or truffle-config.json in some versions) file is automatically created. This file contains the configuration details about various networks, including the Ganache network. You'll need to edit this file to specify how the smart contracts will connect to the Ganache blockchain.

```
module.exports = {
  networks: {
    development: {
      host: "127.0.0.1",
      port: 7545,
      network_id: "*",
    },
  },
  compilers: {
    solc: {
      version: "0.8.0",
    },
  },
}
```

Figure 4.2: Truffle-config.js File

4.1.3 Deploy to Ganache

Ganache serves as a local Ethereum blockchain that simulates a real blockchain environment. This allows you to deploy smart contracts and test transactions with preloaded Ether, without interacting with a live network.

```

2_deploy_contracts.js
=====
Replacing 'DataStore'
-----
> transaction hash: 0x3a2cf4d704daf877fa9ddd4fce9c02865e65a2b22d628af6897a5baac93b0857
> Blocks: 0
> contract address: 0x71f7295fc5531CEE5F2c4cb7d330E546f6DA2aE9
> block number: 1
> block timestamp: 1735667956
> account: 0x73CcE3c5c12d6f981a798D86E12Dd73F0Fe497fa
> balance: 99.99610780825
> gas used: 1153242 (0x1198da)
> gas price: 3.375 gwei
> value sent: 0 ETH
> total cost: 0.00389219175 ETH

> Saving artifacts
-----
> Total cost: 0.00389219175 ETH

Summary
=====
> Total deployments: 1
> Final cost: 0.00389219175 ETH

```

Figure 4.3: Deploy to ganache

4.2 STORING TEXT DATA ON-CHAIN

4.2.1 Receive User Input

The user sends a POST request to the server with the text data they want to store. This data is retrieved from the request using the appropriate method for form data.

4.2.2 Encrypt Data

The text data is then encrypted using a Caesar cipher, which works by shifting each character in the text by a fixed value (in this case, the shift is set to 3).

Algorithm 4.1 Caesar Cipher Encryption

Plaintext string P , Shift value S Encrypted string E

$E \leftarrow$ Empty String

character c in P c is an uppercase letter $E \leftarrow E + \text{chr}(((\text{ord}(c) - \text{ord}('A') + S) \bmod 26) + \text{ord}('A'))$ c is a lowercase letter $E \leftarrow E + \text{chr}(((\text{ord}(c) - \text{ord}('a') + S) \bmod 26) + \text{ord}('a'))$

$E \leftarrow E + c$

return E

4.2.3 Hashing and Conversion to Bytes32 Format

After the encryption, the resulting text is hashed using the SHA-256 algorithm to generate a unique numeric value. This numeric value is then converted into a bytes32 format, which serves as a unique identifier for the data and is compatible with the smart contract for on-chain storage.

4.2.4 Store Data and Return Confirmation

The encrypted text and its corresponding bytes32 hash are stored on the Ethereum blockchain by calling a smart contract's storage function. The transaction is sent to the Ethereum network, and upon receiving the transaction receipt, the system confirms the successful storage. After validating the signatures, the server responds with a success message, including the status of the node signatures.

4.3 STORING IMAGE DATA OFF-CHAIN

4.3.1 Receive and Upload Image to S3

Upon receiving a POST request from the user with an image file, the server retrieves the image using the request method. The image is then uploaded to AWS S3 using the designated upload function, and it is stored in the preconfigured S3 bucket named 2024bucket-blockchain. A unique file name is generated by hashing the content of the image using the SHA-256 algorithm, ensuring that each file is identified and stored securely with a distinct name.

4.3.2 Convert and Store Metadata on the Smart Contract

The S3 file pointer is hashed using SHA-256 to create a unique numeric value that serves as a reference to the image stored off-chain. This generated metadata hash is then converted into a bytes32 format, making it compatible for on-chain storage. The storeData() function of the smart contract is called to store this metadata (the S3 pointer) on the Ethereum blockchain, effectively linking the off-chain image data to an on-chain reference.

4.3.3 Return Confirmation with Metadata

Once the metadata is successfully stored on the blockchain, the server responds with the S3 pointer, along with a success message and confirmation that the image has been securely stored off-chain and linked to the blockchain reference.

4.4 Performing Search Operation

4.4.1 Receive and Encrypt Search Term

The user submits a POST request with the search term, which is retrieved by the server. The search term is then encrypted using the Caesar cipher, ensuring it matches the format of the encrypted data stored previously.

4.4.2 Generate Numeric Search Key and Convert to Bytes32

The encrypted search term is hashed using the SHA-256 algorithm and converted into a numeric value. This numeric search key is then

transformed into a bytes32 format, making it compatible with the smart contract's requirements for on-chain interaction.

4.4.3 Retrieve Data and Validate Integrity

The `getData()` function of the smart contract is invoked with the encrypted search key to fetch the metadata pointer of the stored data. After retrieving the data, the system ensures its integrity by verifying the signatures of all blockchain nodes, confirming the validity of the retrieved data.

4.4.4 Return Search Results

If the data is found, the response includes the S3 pointer and the status of the signatures, confirming the successful retrieval of the data. If no matching data is found, the response indicates that the search term does not exist on the blockchain.

4.5 IMPLEMENTATION OF MULTISIGNATURE QUERY VERIFICATION

4.5.1 Privacy-Preserving Search Operation

- **Binary Search in Smart Contract:** The smart contract performs a binary search within the B+ tree index structure for each query, retrieving matching metadata.
- **Query Verification:** The aggregated search results are verified on-chain for correctness and consistency.

Algorithm 4.2 Privacy-Preserving Search Performed in Blockchain:

Privacy-preserving search query Q , Search indexes for on-chain data SIB A set of records R

Initialization: $R \leftarrow \emptyset, RB \leftarrow \emptyset$

$Q_i \in Q$ $RB_i \leftarrow \text{binarySearch}(Q_i, SIB_i)$ where $SIB_i \in SIB$

if nextOperator = "" **then** $RB \leftarrow RB \cup RB_i$ nextOperator = "" $RB \leftarrow RB \cap RB_i$

$R \leftarrow \text{append}(RB, RC)$ $R \leftarrow \text{verifyQueryResult}(R, PK, S)$

return R

4.5.2 Multisignature-Based Query Verification

- **Key Pair Generation:** Blockchain nodes generate cryptographic key pairs for signing queries during initialization.
- **Query Signing:** Each node signs the query using its private key and the R value. This signed result is returned to the user.
- **Signature Validation:** The smart contract verifies that multiple nodes have signed the query and aggregates their signatures into a final response.

CHAPTER 5

RESULTS AND DISCUSSION

This chapter presents the results obtained in implementing the proposed work.

5.1 HOME PAGE

Blockchain Data Storage System

Store Data On-Chain

Product name:

Search Data On-Chain

Product name:

Store Image Off-Chain

Select Image: No file chosen

Figure 5.1: Home page

This Output represents a Blockchain Data Storage System with three functionalities: 1. Store Data On-Chain: Input and store product names on the blockchain. 2. Search Data On-Chain: Search for product names stored on the blockchain. 3. Store Image Off-Chain: Upload and save images off-chain.

5.2 STORE ON - CHAIN DATA

This output showcases a user interface where data has been successfully encrypted and stored on the blockchain, with confirmation displayed as "Data encrypted and stored on-chain."

Store Data On-Chain

Product name:

Data encrypted and stored on-chain.

Figure 5.2: Store on - chain data

5.3 BLOCK CREATION IN GANACHE

This output demonstrates the creation of Block 1, which is part of the process of deploying a smart contract and recording the encrypted data transaction on the blockchain.

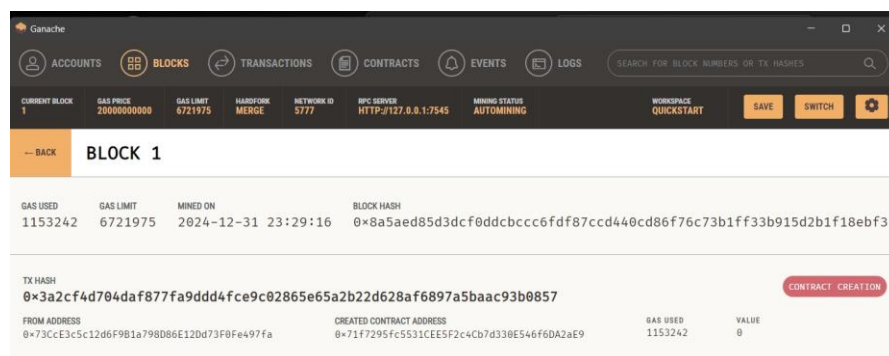


Figure 5.3: Block creation in ganache

5.4 STORE OFF - CHAIN DATA

This output screenshot displays a web interface that confirms the successful off-chain storage of an image file. It provides a visual indication that the image has been securely stored in the cloud, with a reference to its location on the blockchain.



Figure 5.4: Store off - chain data

5.5 AWS S3 BUCKET PAGE

This output screenshot shows an AWS S3 bucket named 2024bucket-blockchain containing image files with details like name, size, and last modified timestamps.

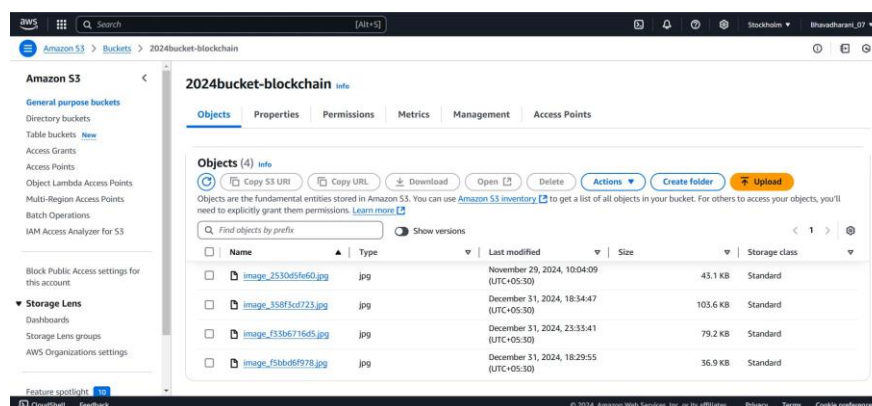
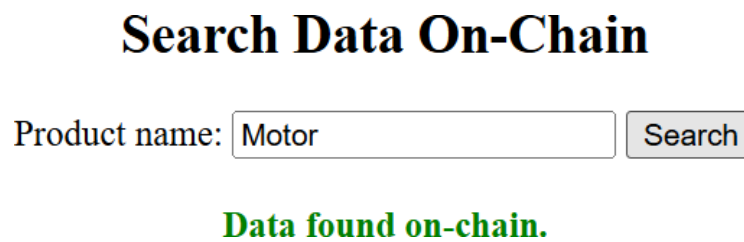


Figure 5.5: AWS S3 bucket page

5.6 SEARCH OPERATION

This output screenshot shows a web interface for searching on-chain data, where the product name was queried, and the system confirmed with the message "Data found on-chain".



Search Data On-Chain

Product name:

Data found on-chain.

Figure 5.6: Search operation

5.7 MULTISIGNATURE RESULT

This output demonstrates a successful multisignature process, where multiple nodes have contributed their signatures. Each signature serves as a confirmation of the nodes' consensus, ensuring the validity and integrity of the data.

```
All nodes signed the data.
0xC2f674cC68261ea0736FC300E68eF6d4E688c479: Node signed the data
0x7b95E23A886A19aD087c19CF440de9A5d65600Ef: Node signed the data
0x7354BF2120d66B9201CfB42399D08e0886FA2bc3: Node signed the data
127.0.0.1 - - [31/Dec/2024 18:55:36] "POST /store text ope HTTP/1.1" 200 -
```

Figure 5.7: Multisignature result

5.8 DISCUSSION

The performance analysis of the proposed Systems focuses on evaluating the framework's efficiency in terms of data integrity, query verification, and scalability in real-world applications. The integration of

blockchain and multi-signature-based query verification ensures high levels of security while maintaining transparency and decentralization. However, while the framework enhances data privacy and trust, it introduces some overhead due to the cryptographic operations and signature verification processes, potentially affecting query response times.

The use of dual storage—on-chain for textual data and off-chain for multimedia—optimizes performance by minimizing the load on the blockchain, but the reliance on cloud storage for large datasets may introduce latency when querying off-chain data. Despite these challenges, the system demonstrates significant improvements in securing IIoT systems, ensuring verifiable query results, and offering a decentralized approach to data verification, which enhances trust and accountability in cloud-assisted IIoT environments. The scalability of the system is also evident as it can handle large volumes of data through the efficient use of blockchain and cloud resources, although further optimization may be required to reduce latency and improve processing speeds.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

This thesis proposed a blockchain-enabled privacy-preserving verifiable query framework to bridge the gap in critical security and privacy concerns in a cloud-assisted Industrial Internet of Things system. It is built by integrating blockchains with a dual storage approach, maintaining sensitive textual attributes on-chain, and multimedia off-chain using AWS. It incorporates multi-signature-based query verification and encrypted search indexes to ensure data integrity, secure access, and privacy-preserving search capabilities. A demonstration of this implementation will illustrate that the blockchain can indeed enable better trust and reduce potential third-party CSP-related risk exposures. This approach will certainly present a strong foundation toward IIoT data management being secure and transparent for those handling it, while countering a few major scalability efficiency concerns and user privacy risks.

6.2 FUTURE WORK

Future work will therefore be directed in some such areas for further enhancement towards the framework. It goes without saying that cryptography aspects like homomorphic encryption can be integrated to achieve functionality of computations on encrypted data so that privacy is never exposed. The performance regarding its query handling and generating appropriate search indexes for large IIoT systems is another point still to be improved. The third reason leads to the improvement in the operational efficiency of IIoT networks, involving AI/ML algorithms for anomaly detection and predictive analytics in

the framework. The final enhancement of the framework would be support for interoperability between various blockchain platforms, thereby allowing this technology to penetrate a larger industrial ecosystem. These advances will be helpful in establishing robust, secure, and privacy-preserving solutions for next-generation IIoT systems.

REFERENCES

- [1] Bing Wang, Shucheng Yu, Wenjing Lou, and Y Thomas Hou. Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. In *IEEE INFOCOM 2014-IEEE conference on computer communications*, pages 2112–2120. IEEE, 2014.
- [2] Qiuyun Tong, Yinbin Miao, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H Deng, and Hongwei Li. Vpsl: Verifiable privacy-preserving data search for cloud-assisted internet of things. *IEEE Transactions on Cloud Computing*, 10(4):2964–2976, 2020.
- [3] Kuan Zhang, Kan Yang, Xiaohui Liang, Zhou Su, Xuemin Shen, and Henry H Luo. Security and privacy for mobile healthcare networks: from a quality of protection perspective. *IEEE Wireless Communications*, 22(4):104–112, 2015.
- [4] Xu Zheng, Zhipeng Cai, and Yingshu Li. Data linkage in smart internet of things systems: a consideration from a privacy perspective. *IEEE Communications Magazine*, 56(9):55–61, 2018.
- [5] Zaobo He, Zhipeng Cai, and Jiguo Yu. Latent-data privacy preserving with customized data utility for social network data. *IEEE Transactions on Vehicular Technology*, 67(1):665–673, 2017.
- [6] Meng Han, Ji Li, Zhipeng Cai, and Qilong Han. Privacy reserved influence maximization in gps-enabled cyber-physical and online social networks. In *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud)*, pages 284–292. IEEE, 2016.
- [7] Tiago M. Fernández-Caramés, Oscar Blanco-Novoa, Iván Froiz-Míguez, and Paula Fraga-Lamas. Towards an autonomous industry 4.0 warehouse: A uav and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors*, 2019.
- [8] Huaqun Guo and Xingjie Yu. A survey on blockchain technology and its security. *Blockchain: research and applications*, 3(2):100067, 2022.
- [9] Archana Prashanth Joshi, Meng Han, and Yan Wang. A survey on security and privacy issues of blockchain technology. *Mathematical foundations of computing*, 1(2), 2018.
- [10] Iuon-Chang Lin and Tzu-Chun Liao. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, 19(5):653–659, 2017.

- [11] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, 14(4):352–375, 2018.
- [12] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. *Future generation computer systems*, 107:841–853, 2020.
- [13] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Order preserving encryption for numeric data. In *Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data*. Association for Computing Machinery, 2004.
- [14] Dawn Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. pages 44–55, 02 2000.
- [15] Yuan Li, Xing-Chen Wang, Lin Huang, and Yun-Lei Zhao. Order-revealing encryption: File-injection attack and forward security. *Journal of Computer Science and Technology*, 36(4):877–895, 2021.
- [16] D Przytarski, C Stach, C Gritti, and B Mitschang. Query processing in blockchain systems: Current state and future challenges. *future internet* 2022, 14, 1, 2022.
- [17] Lein Harn, Jian Ren, and Changlu Lin. Efficient identity-based gq multisignatures. *International Journal of Information Security*, 8:205–210, 2009.
- [18] M Shamim Hossain and Ghulam Muhammad. Cloud-assisted industrial internet of things (iiot)-enabled framework for health monitoring. *Computer Networks*, 101:192–202, 2016.
- [19] Sai Wu, Dawei Jiang, Beng Chin Ooi, and Kun-Lung Wu. Efficient b-tree based indexing for cloud data processing. *Proceedings of the VLDB Endowment*, 3(1-2):1207–1218, 2010.
- [20] Yingying Li, Jianfeng Ma, Yinbin Miao, Liming Liu, Ximeng Liu, and Kim-Kwang Raymond Choo. Secure and verifiable multikey image search in cloud-assisted edge computing. *IEEE Transactions on Industrial Informatics*, 17(8):5348–5359, 2020.
- [21] Jin Ho Park and Jong Hyuk Park. Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 9(8):164, 2017.
- [22] Kevin Werbach. *The Blockchain and the New Architecture of Trust*. Mit Press, 2018.