DESIGN OF EFFICIENT AND SECURE TASK MATCHING TECHNIQUES IN CROWDSOURCING PLATFORM

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

ARIJITA BHOWMIK

MZU REGISTRATION NO.: 2109063

Ph.D. REGISTRATION NO.: MZU/Ph.D./1968 OF 01.09.2021



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF ENGINEERING AND TECHNOLOGY

MIZORAM UNIVERSITY

SEPTEMBER, 2025

DESIGN OF EFFICIENT AND SECURE TASK MATCHING TECHNIQUES IN CROWDSOURCING PLATFORM

BY

ARIJITA BHOWMIK

Department of Information Technology

Supervisor: Dr. Somen Debnath

Joint Supervisor: Dr. R. Chawngsangpuii

Submitted

In partial fulfilment of the requirement of the Degree of Doctor of Philosophy in Information Technology of Mizoram University, Aizawl

CERTIFICATE

This is to certify that the thesis entitled "**DESIGN OF EFFICIENT AND SECURE TASK MATCHING TECHNIQUES IN CROWDSOURCING PLATFORM**", submitted by **Arijita Bhowmik** (Registration No: *MZU/Ph.D/1968 of 01.09.2021*), for the degree of Doctor of Philosophy (Ph.D) **Department of Information Technology** at **Mizoram University** embodies the record of original investigation carried out by her under our joint supervision. She has been duly registered and the thesis presented is worthy of being considered for the award of the Ph.D degree. This work has not been submitted for any degree at any other university.

04.09.2025

Dr. Somen Debnath
Associate Professor
Deptt. of Computer Sc. & Engg.
Tripura University

Dr. Somen Debnath
Supervisor and Associate Professor
Dept. of Computer Science and Engineering
Tripura University,
Agartala-799022

Place: Agartala.
Date: 04.09.2025

Dr. R. Chawngsangpuii
Joint Supervisor and Associate Professor
Dept. of Information Technology
Mizoram University,
Aizawl-796 004

Place:
Date:

MIZORAM UNIVERSITY

SEPTEMBER,2025

DECLARATION

I, **Arijita Bhowmik**, hereby declare that the subject matter of this thesis entitled "**Design of Efficient and Secure Task Matching Techniques in a Crowdsourcing Platform** is the record of work done by me, that the contents of this thesis did not form basis of the award of any previous degree to me or to the best of my knowledge to anybody else, and that the thesis has not been submitted by me for any research degree in other University/Institute.

This is being submitted to the Mizoram University for the degree of Doctor of Philosophy (Ph.D.) in Department of Information Technology.

(ARIJITA BHOWMIK)

04.09.2025

(Dr. SOMEN DEBNATH)

Supervisor

Dr. Somen Debnath
Associate Professor
Deptt. of Computer Sc. & Engg.
Tripura University

(Dr. LALHMINGLIANA)

Head

(Dr. R. CHAWNGSANGPUII)

Joint Supervisor

Contents

Certificate i

Declaration ii

Acknowledgement iii

Abstract iv

1 Introduction 1

1.1 Overview of Task Matching in Crowdsourcing 1

1.2 Cryptographic Foundations in Tasking 3

1.2.1 Searchable Encryption (SE) 3

1.2.2 Attribute-Based Encryption (ABE) 4

1.2.3 k-Anonymous 4

1.2.4 Proxy Re-Encryption Technique (PRE): 5

1.2.5 Homomorphic Encryption Technique (HE) 6

1.2.6 Puncturable Encryption Technique (PE) 6

1.2.7 Differential Privacy Scheme (DP) 6

1.2.8 Blockchain 7

1.3 Security Issues in Task Matching 7

1.3.1 Applications of Secure Crowdsourcing 9

1.4 Motivation 10

1.5 Objectives 11

1.6 Methodology 12

1.7 Thesis Organization 13

2 Review of Literature 15

2.1 Chronological Study on Task Matching 16

2.2 Deployed Methodologies in Task Matching 18

2.2.1 Proxy Re-encryption based Task Matching 18
2.2.2 Proxy-Free Encryption-based Task Matching 19
2.2.3 Blockchain-based Task Matching 19
2.3 Challenges and Research Directions 20
2.3.1 Key Challenges 22
2.3.2 Research Directions 23

3 An Efficient Task Matching Schema with Signature-oriented Encryption 25
3.1 Overview 25
3.2 Related Work 26
3.3 Problem Formulation 28
3.3.1 Security Requirements 29
3.3.2 Design Goals 29
3.4 Detailed Schema Construction 30
3.5 Security Analysis 32
3.6 Experimental Results 34
3.6.1 Experimental Setup 34
3.6.2 Performance Comparison 35
3.7 Conclusion and Future Work 40

4 Online Blood Bank System Using Blockchain in CrowdSourcing Platform 42
4.1 Overview 42
4.2 Related Works 43
4.3 Proposed Schema 44
4.3.1 System Model 44
4.3.2 Workflow 46
4.3.3 Threat Model 46
4.3.4 Design Goals 46
4.3.5 Proposed Algorithm 48
4.4 Security Analysis 50
4.5 Performance Analysis 52
4.5.1 Experimental Setup 56
4.5.2 Comparative Analysis 56
4.6 Conclusion 58

5 Crowd-Sourced Blood Bank Management: A Secure and Efficient

Reuse-Oriented Framework **59**
5.1 Overview 59
5.2 Related Works 61
5.3 Preliminaries 62
5.3.1 System Model 62
5.3.2 Threat Model 64
5.3.3 Design Goals 64
5.3.4 Gas Fees and Computational Costs 65
5.4 Our Crowd-Sourced Blood Bank Management 65
5.4.1 System Setup 65
5.4.2 Task Publication Phase 66
5.4.3 Solution Submission Phase 66
5.4.4 Task Matching Phase 67
5.4.5 Worker Revocation Mechanism 68
5.5 Security Analysis 68
5.6 Performance Analysis 71
5.6.1 Computational Efficiency 72
5.7 Conclusion 74

6 Summary and Conclusions **75**
6.1 Future Research Directions 78

References **80**

Publication List **92**

Bio-data of the Candidate **94**

Particulars of a Candidate **95**

List of Figures

1.1 Task Matching in Crowdsourcing 2

2.1 Timeline of Task Matching Techniques 16

3.1 System Model 29
3.2 System Initialization Cost Comparison 38
3.3 Worker Revocation Cost 38
3.4 Signature Tracing Cost 39
3.5 Requirement Encryption Cost 39
3.6 Trapdoor and Signature Generation Cost 40
3.7 Matching Cost 40

4.1 Blood Donation System in Crowdsourcing Platform 45
4.2 Flow diagram of the responsive, crowd-based blockchain blood management system (without reuse policy and testing node). 47
4.3 Requester Transmission Cost 54
4.4 Worker Computation Cost 54
4.5 Computation Cost Comparison Across Blood Management Systems . 55
4.6 Transaction Latency for Blockchain Operations 56
4.7 Comparative performance analysis of existing schemes and proposed schema 57

5.1 Blood Donation System in Crowdsourcing Platform 63
5.2 Execution Time Comparison 72
5.3 Comparison of computation time 73

List of Tables

2.1 Chronological overview of privacy-preserving task matching frameworks . . . 17
2.2 Summary of Related Work on Privacy-Preserving Crowdsourcing . . 21
2.3 Comparison of notable methodologies of task matching . . . 22
2.4 Potential Developments for Improving Privacy Guarantees in Task Matching . . . 24

3.1 Notation for Setup and Cryptographic Components . . . 31
3.2 Computation Complexity . . . 35
3.3 Communication Cost . . . 36
3.4 Performance Comparison of Algorithms . . . 37

4.1 Comparison of Proposed System with Existing Works . . . 53
4.2 Computation Cost for Requesters and Workers . . . 56

5.1 Comparison between the previously used system for medical data storage and data usage . . . 72

Chapter 1

Introduction

Crowdsourcing is a way to complete a task with the help of human intelligence from a crowd of diverse individuals using open calls over the internet. This technique has become the backbone of our modern business strategies. The whole process of crowdsourcing relies on task matching. However, modern crowdsourcing platforms face security challenges in task matching, compromising sensitive data, and inviting malicious attacks like collusion and task tracking. This research investigates security and privacy in task assignments. This thesis studies the different methods used for privacy-preserving task matching. It also compares different techniques and explores their advantages, disadvantages, and computational overhead. It delves into encryption techniques and blockchain technology, emphasizing privacy-preserving work assignments for crowdsourcing platforms. The study outlines future goals to strengthen security and privacy in the task-matching process in crowdsourcing methodologies, contributing to the development of secure and efficient crowdsourced projects.

1.1 Overview of Task Matching in Crowdsourcing

Before examining secured and privacy-preserved schemes during task matching in detail, it's crucial to recognize various entities involved in crowdsourcing during the task matching process. We explain crowdsourcing with a diagram, involved entities, and several factors that can be optimized for secure and privacy-preserved task assignment purposes. The components of crowdsourcing can be defined and represented in the figure 1.1

- **Requesters**: The requesters are the people in the crowdsourcing platform who seek the solution to their specific task.

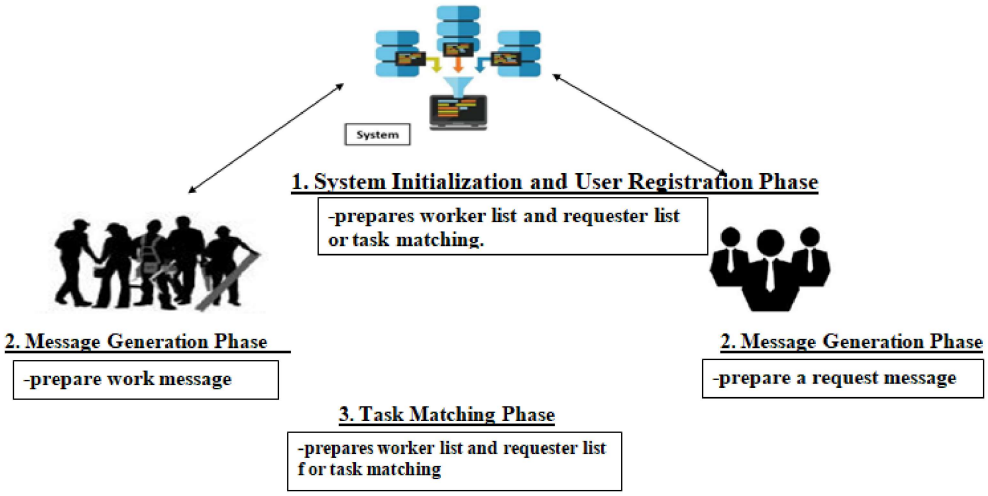


Figure 1.1: Task Matching in Crowdsourcing

- **Workers:** Workers are the people who complete the tasks on a crowdsourcing platform.
- **Crowd Server/System:** The mapping of the task requester with the workers is done here.

Task Matching matching in crowdsourcing means the matching of workers with the desired tasks through interest Hettiachchi *et al.*, 2022, location, or reputation To *et al.*, 2016b. There are two major concerns in task matching, which are discussed in Yang *et al.*, 2015:

- Task privacy:
  When a task is published by end users, they do not want the crowd server or any unauthorized participant to access their published tasks. For example, if a company needs to calculate its annual turnover, it will provide its monthly income details to the worker. This can use information. So, encryption is required in Shu, Jia, *et al.*, 2018.
- User data privacy:
  The service provider should not have access to detailed information about end users, such as their location or specific interests. For example, if a requester wants a ride, they will share their location and pickup time with the crowd server/ system. The nearest interested driver (worker) will accept the ride. Consequently, the crowd server/system will have access to the driver's sensitive geo-

graphic information Manzoor *et al.*, 2021a. There is a risk that this information could be exploited for profit, so the task data needs to be hidden.

Before communicating the task-related information with the crowd server, the worker and the requester encrypt it because the trusted crowd server may disclose the information for financial gain. But to perform a search based on the user's search query over encrypted data is a challenge Handa *et al.*, 2019a. So, a task matching technique over an encrypted channel with low communication and computation costs is required.

Different Phases of Task Matching: The task allocation is incorporated in the crowdsourcing framework comprises five phases: initialization of the system and registration by the user, where cryptographic keys are generated but risks of collusion and Sybil attacks exist Hao *et al.*, 2019; task generation, where encrypted tasks safeguard privacy yet remain vulnerable to specified tasking and location-based attacks Erlingsson *et al.*, 2014; Li, Wu, *et al.*, 2021; trapdoor generation, enabling secure queries but susceptible to inference and collusion Zhang *et al.*, 2020; identification verification, ensuring legitimacy but threatened by insider tampering and traceability leaks; and task matching, which preserves privacy yet risks manipulation or task tracing. Collectively, these phases highlight security–efficiency trade-offs in decentralized crowdsourcing.

1.2 Cryptographic Foundations in Tasking

For privacy-preserved task matching, efficient matching techniques as well as encryption techniques are used. Different encryption techniques are studied and listed below that have been used in different privacy-preserved task matching techniques. Some of the techniques that are used in this process are listed below.

1.2.1 Searchable Encryption (SE)

Searchable Encryption (SE) enables data retrieval from encrypted datasets without decryption, ensuring privacy while allowing efficient access. SE schemes include Key Generation (KEYGEN) for creating secret keys, Index Building (BUILDINDEX) for searchable encrypted indexes, Trapdoor (TRAPDOOR) for query creation, and Search (SEARCH) for comparing queries to encrypted indexes. SE techniques include Symmetric Searchable Encryption and Asymmetric Searchable Encryption, which use a single key and a public-private key pair simultaneously. SE plays a crucial role in task matching in crowdsourcing by allowing efficient search and retrieval of encrypted data

without revealing sensitive information. SE enables servers to match encrypted queries (representing tasks or data) with encrypted datasets while ensuring data privacy, facilitating secure and private task allocation, and the conversation between users and servers. Ambati *et al.*, 2011 presents a privacy-preserving decentralized task recommendation scheme using searchable symmetric encryption. Ni *et al.*, 2018 introduces a task allotment securing deduplication scheme in mobile crowdsensing systems using fog computing. The research article Pournajaf *et al.*, 2014 studies the locations in mobile crowdsensing systems. User turnover presents issues for single-user SE in the context of crowdsourcing Ma *et al.*, 2018a.

1.2.2 Attribute-Based Encryption (ABE)

ABE controls data based on attributes of the user or policies. Key-Policy ABE (KP-ABE) links encryption keys to access policies, while Ciphertext-Policy ABE (CP-ABE) links encrypted data with access policies. CP-ABE supports content-based, role-based, and multi-authority policies, making it useful for secure email, surveillance, analytics, and digital wallets. Advanced forms include Ciphertext Policy Attribute Set and Hierarchical ABE. ABE enhances privacy and security in task matching by ensuring only authorized users with matching attributes can access specific tasks or data. In crowdsourcing or collaborative environments, ABE provides flexibility in access control. Here, tasks are assigned based on user roles, qualifications, or attributes. By enforcing access policies at the encryption level, ABE ensures that only eligible participants can decrypt and view the task details, ensuring data confidentiality Debnath and Bhuyan, 2019 while facilitating secure task distribution. Hao *et al.*, 2019 used ABE along with ElGamal to design a privacy-preserved task allocation schema. Yin *et al.*, 2019 made use of a safe and tailored recommendation system for crowdsourcing, which seamlessly combines attribute-based encryption with searchable encryption to provide precise, tailored task recommendations while protecting user privacy. Yuan *et al.*, 2019 used both symmetric-key and attribute-based encryption to guarantee task matching against an untrusted server.

1.2.3 k-Anonymous

k-Anonymity, first introduced by Latanya Sweeney in 1998, is a widely used technique for encryption purposes to minimize the re-identifying problem in anonymized datasets. The principle ensures indistinguishability from at least $k-1$ other records, thereby making re-identification significantly harder. This is typically achieved through

two mechanisms: *generalization*, which reduces the granularity of data attributes, and *suppression*, which removes certain data values altogether. By grouping records with similar characteristics, k-anonymity safeguards individual privacy while still maintaining the utility of the dataset, making it particularly valuable in contexts involving sensitive data such as healthcare or demographics.

In crowdsourcing and task-matching environments, k-anonymity plays an essential role in protecting participant privacy. Sensitive attributes like location, skill set, or demographic information are anonymized so that each task request or worker profile is not distinguishable from those of minimum k other participants. So, identity protection while enabling efficient and fair task allocation. To enhance privacy further, researchers have explored combining k-anonymity with *differential privacy* Chi *et al.*, 2017, which provides stronger guarantees against inference attacks. Liu *et al.*, 2017 proposed a task assignment strategy in spatial crowdsourcing that incorporates k-anonymity to protect workers' location information. Similarly, Wang et al. Wang *et al.*, 2018 demonstrated that applying differential privacy-based methods can incentivize worker participation in crowdsourcing platforms by ensuring stronger protection of sensitive attributes.

1.2.4 Proxy Re-Encryption Technique (PRE):

(PRE) is an approach that is based on a trusted proxy to convert the data into a ciphertext using the key, without exposing the underlying plaintext. This property makes PRE particularly valuable in task-matching frameworks where secure and flexible data sharing among multiple participants is required. PRE schemes can operate in two modes: *simplex* (one-directional) and *duplex* (bi-directional). Over the years, several extensions have been developed to address different application needs, including private PRE, identity-based PRE, conditional PRE, attribute-based PRE, time-bound PRE, threshold PRE, and matrix decomposition-based PRE.

In task matching, PRE enhances security by allowing encrypted task data to be securely transformed and shared across different parties without exposing the underlying data. For instance, tasks encrypted under one key can be re-encrypted to be accessible by another party with a different key, facilitating secure collaboration and data sharing. Duplex PREs, capable of two-way transformation, enable bidirectional data sharing between multiple users or systems. This ensures that tasks can be matched and managed securely while maintaining the confidentiality of sensitive information. Shu, Jia, *et al.*, 2018 Hao *et al.*, 2019Alamer *et al.*, 2017 used proxy- re encryption schema.

1.2.5 Homomorphic Encryption Technique (HE)

HE ensures that the outcomes are kept private at all times. This approach comprises types such as partly, moderately, gradually, and totally HE and allows operations on encrypted data using arithmetic or Boolean circuits. Even with its safe processing capabilities, HE has drawbacks including computational complexity and restricted multiplication depth, which limit its scalability for large-scale crowdsourcing applications because it requires expensive ciphertext operations. Although they are more precise, advanced forms like Paillier HE still have scaling issues. Methods such as server-assigned jobs, which optimize task allocation by allowing workers to define job preferences, help to increase scalability. Overall, HE ensures that privacy is maintained while still allowing necessary computations for effective task matching. Some of the methodologies using this technique are as follows: Shen *et al.*, 2015 proposed a privacy-preserved schema for crowdsourcing using additive HE, and Xiong *et al.*, 2019 Liu *et al.*, 2018 used HE.

1.2.6 Puncturable Encryption Technique (PE)

Green and Miers first introduced PE in 2015, which is a public-key cryptographic technique allowing a decryption key to be punctured to exclude specific data or values from decryption. This mechanism supports fine-grained data management by enabling the selective exclusion of data from being decrypted without altering the encryption scheme. The decryption key can be updated by the receiver to reflect changes, while the sender remains unaware of these updates. This flexibility is beneficial for scenarios where data access needs to be controlled or modified over time without re-encrypting the entire dataset. In task matching, Puncturable Encryption (PE) enhances security and flexibility by allowing specific data or values to be excluded from decryption dynamically. Overall, PE supports adaptable and secure task matching in dynamic environments. A schema based on attribute keys and punctured was proposed by Affum *et al.*, 2022.

1.2.7 Differential Privacy Scheme (DP)

DP is a method for preserving privacy while sharing information about groups rather than individuals. It works by introducing small, random adjustments to each data point, ensuring that the changes do not significantly impact the overall statistics. This approach helps to obscure details about specific individuals, making it difficult to infer private information from the data. Differential privacy sets a formal boundary on the

disclosure of private information in aggregate data, allowing statistical insights while protecting individual privacy. This technique is especially useful for sharing sensitive data in databases or research while minimizing risks to personal privacy In task matching, Differential Privacy plays a crucial role in protecting individual privacy while enabling the analysis and sharing of group-level data.Overall, differential privacy ensures that task matching processes can leverage group data effectively while safeguarding individual privacy. To *et al.*, 2014 and To *et al.*, 2016b proposed schema relying on DE.

1.2.8 Blockchain

Blockchain technology is a distribute, decentralized, and transparent system that logs transactions across multiple computers. It operates without a central authority, using cryptographic techniques to ensure data integrity and prevent tampering. Blockchain is commonly used in cryptocurrencies, smart contracts, and secure data sharing, offering transparency, security, and trust in digital interactions.

Centralized Architectures: In centralized crowdsourcing platforms (e.g., Amazon Mechanical Turk), a single crowd server is responsible for task allocation, user management, and reputation control. Fast response time, efficient matching, and reduced system complexity are its advantages, and single point of failure, potential data leakage, and susceptibility to insider threats are its disadvantages.

Decentralized: Decentralized models leverage blockchain and distributed ledgers to eliminate the need for trusted intermediaries. Smart contracts can enforce transparent task allocation policies. Tamper-resistance, auditability, and removal of central authority are the advantages. High latency, limited scalability, and costly consensus protocols are disadvantages.

Hybrid Architectures: Hybrid systems attempt to balance the benefits of both models. For example, the crowd server may perform fast task assignment, while blockchain ensures transparency and immutability of assignments. Combining efficiency with trustworthiness is the advantage. Added design complexity, synchronization overhead are disadvantages.

1.3 Security Issues in Task Matching

According to the above discussion, the design goals of a secure task assignment system are as follows:

- Privacy-preservation:

The confidentiality of employees and job-related information is needed. To learn more about a worker or task, an adversarial node must be unable to decipher the encrypted data used for matching Wu *et al.*, 2019.

- Anonymity:
  The majority of crowdsourcing websites need anonymity since it safeguards both workers' and requesters' personal information. In particular, it is impossible to detect the identity of a worker who submits a query, and a requester can't identify the identity of a task they have submitted Yang *et al.*, 2015.

- Soundness:
  Soundness is achieved through several validations. The service provider is unable to falsify or deliver incomplete results, and the result is truthful according to this thesis's assertion Wu *et al.*, 2019.

- Zero Proxy:
  In the proxy-based SE technique, the identity of the task requester or the worker may be compromised. Moreover, the interaction costs are inadequate for the proxy-based task matching schema (Shu, Jia, *et al.*, 2018).

- Transparency:
  Maintainence of the transparency is required. Transparent communication builds trust among users (Pang *et al.*, 2020).

- Accuracy and Efficiency:
  Design algorithms that ensure accurate and efficient task matching despite privacy-preserving measures. Focus on optimizing the matching process to deliver relevant tasks to workers and suitable workers to requesters in a timely manner.

- Usability:
  Create user-friendly interfaces and experiences that allow users to easily configure their privacy preferences. Enable users to customize their privacy settings and understand the implications of their choices in the task matching context.

- Compliance:
  Design of schema in a way that aligns with legal requirements and industry best practices to protect users' rights and privacy Diamantopoulou *et al.*, 2018.

- Robustness:
  Build a schema that can withstand various attacks and attempts to compromise

privacy. Conduct rigorous testing and validation to identify and address potential vulnerabilities in the privacy-preserving mechanisms Ma and Olshevsky, 2020.

1.3.1 Applications of Secure Crowdsourcing

Privacy-preserving task matching is critical in domains where sensitive data is involved. Applications include:

Healthcare Crowdsourcing:

Patients or healthcare organizations may outsource tasks such as medical data annotation or disease monitoring. Privacy-preserving task assignment ensures that medical records remain confidential while enabling collaborative research.

Smart Transportation and Ride-Sharing:

Platforms like Uber or Ola rely on real-time location-based task assignment. Without strong privacy mechanisms, workers (drivers) and requesters (passengers) risk exposure of sensitive location data. Cryptographic task matching prevents misuse of geographic information.

Security Auditing and Bug Bounties:

Organizations often crowdsource vulnerability assessments to ethical hackers. Task matching in such cases must prevent adversarial participants from exploiting sensitive system information while ensuring that valid workers receive appropriate rewards.

Disaster Management and Crisis Response:

During natural disasters or emergencies, tasks such as relief distribution and volunteer coordination can be matched securely. Privacy-preserving task allocation protects the identities and locations of vulnerable populations.

Data Annotation:

Large-scale AI training relies heavily on crowdsourced data labeling. Privacy-preserving schemes allow sensitive datasets (e.g., medical images, financial records) to be annotated without exposing raw data, thus maintaining compliance with data protection laws.

1.4 Motivation

Crowdsourcing is an innovative technique using human intelligence to solve problems across diverse areas like business, healthcare, transportation, and artificial intelligence. By enabling task requesters to connect with distributed workers through open calls on the internet, crowdsourcing ensures cost-effectiveness, scalability, and faster execution. However, as the reliance on crowdsourcing grows, so do the concerns about **data privacy**, **authenticity**, and **transparency** in the task matching process.

Need for Secure Task Matching

Task matching forms the core of any crowdsourcing system, determining how workers relate tasks based on their interests, requirements, and location. Unfortunately, their current practice of transmitting task-related information through centralized servers exposes both requesters and workers to serious risks. Sensitive requester data (e.g., financial records, medical details) may be disclosed to untrusted intermediaries, leading to data leakage. Worker information, such as location, preferences, and skills, can be exploited for profiling and unauthorized surveillance. A compromised or malicious crowd server may misallocate tasks, manipulate reputation systems, or sell confidential data for profit.

Gaps in Existing Solutions

Although encryption, reputation models, and blockchain technologies have been introduced in crowdsourcing, most existing platforms suffer from one or more limitations:

- High computational and communication overhead caused by heavy cryptographic operations such as homomorphic encryption.
- Trade-off between **privacy** and **efficiency**, where stronger privacy guarantees result in slower task allocation.
- Vulnerability to insider attacks, collusion, and inference attacks, even in semi-trusted settings.
- Limited applicability of decentralized methods due to scalability and latency challenges.

Research Motivation

The motivation of this study is driven by the urgent need to design **privacy-preserving, efficient, and scalable task matching mechanisms** for crowdsourcing platforms. Specifically:

- To ensure that sensitive task and user information remains confidential even in the presence of untrusted servers.
- To provide fair and secure task allocation resistant to collusion, Sybil attacks, and malicious manipulation.
- To explore modern cryptographic tools (searchable encryption, attribute-based encryption, ring signatures) and emerging technologies (blockchain) for building next-generation crowdsourcing frameworks.
- To establish a balance between **strong security guarantees** and **practical deployment**, ensuring low computational and communication overhead.

Thus, the central motivation of this research lies in strengthening the security and privacy foundations of task matching in crowdsourcing systems, thereby contributing to the development of reliable, transparent, and efficient platforms for future large-scale human-computation projects.

1.5 Objectives

In light of the aforementioned security concerns and difficulties, the research work's objectives are broken down into the following sections for the proposed work: The main objective of this thesis is to create and implement a secure, efficient framework for task matching in crowdsourcing platforms. The particular aims of the research are as follows:

1. **To undertake a systematic study of the existing task-matching schemes in crowdsourcing with a focus on security and privacy features.**
   This objective involves an in-depth literature review and comparative analysis of current task matching mechanisms. The goal is to evaluate how existing schemes address security vulnerabilities and privacy concerns, identify their limitations, and highlight the gaps that need to be addressed in the context of modern crowdsourcing platforms.

2. **To develop a robust and efficient task matching scheme incorporating privacy-preserving encryption techniques.**
   Building upon the insights gained from the initial analysis, this objective focuses on the design of a novel task-matching framework. The proposed system will incorporate lightweight encryption methods to ensure user anonymity, data confidentiality, and protection against data inference attacks during task allocation.

3. **To deploy blockchain technology to enhance transparency and reduce storage requirements in crowdsourcing task matching mechanisms.**
   This objective seeks to leverage the decentralized, immutable, and transparent nature of blockchain technology. By integrating blockchain into the task matching framework, the system aims to ensure auditable task transactions, decentralized data storage, and minimized reliance on central authorities, thereby improving trust and efficiency.

4. **To strike a balance between system performance and the level of security provided, with particular emphasis on resource-constrained environments.**
   This objective is to evaluate and optimize the proposed framework to achieve an effective trade-off between security strength and performance, particularly in environments with limited computational power, bandwidth, or energy availability, such as mobile or edge devices.

1.6 Methodology

Phase 1: Study of Existing Schemes The first phase of this research involves a comprehensive study of existing task-matching schemes with a particular emphasis on privacy-preserving and secure computation techniques. An extensive literature review is conducted to analyze cryptographic mechanisms such as searchable encryption, attribute-based encryption, ring signatures, and homomorphic encryption, each offering distinct trade-offs between efficiency and privacy. The comparative analysis highlights key limitations, including high computational overheads in large-scale settings, vulnerability to collusion attacks that compromise fairness, and scalability challenges that restrict practical deployment. These findings provide the foundation for identifying research gaps and motivating the design of an enhanced privacy-preserving task matching framework.

Phase 2: Development of Privacy-Preserving Task Matching Scheme In the second

phase, a novel framework is developed to address the shortcomings identified in prior works. The proposed scheme integrates lightweight cryptographic primitives with privacy-preserving search algorithms to ensure secure and efficient task matching. Specifically, searchable encryption enables secure task query processing without exposing sensitive details, while ring signatures guarantee worker anonymity and provide unforgeability against malicious actors. Additionally, trapdoor generation mechanisms allow workers to query tasks in a privacy-preserving manner, preventing adversaries from linking user identities with task preferences. The resulting system ensures confidentiality of requester data, strong anonymity for workers, and robust resistance to inference and profiling attacks.

Phase 3: Blockchain-Enabled Transparency and Storage Optimization The third phase incorporates blockchain technology into the task-matching process to achieve decentralized trust and transparency. Smart contracts are employed to enforce automated and transparent task allocation without reliance on centralized servers, while the blockchain ledger ensures tamper-proof and auditable task records. To address the storage limitations of blockchain, an off-chain storage mechanism is adopted, where task data is stored externally while hash references are maintained on-chain for integrity verification. This hybrid model significantly reduces on-chain storage overhead, enhances system scalability, and ensures trustworthy task assignment while preserving transparency and accountability for all participants.

Phase 4: Efficiency and Security Analysis The final phase of the methodology involves validating the proposed framework through extensive experimental analysis under different computational and network constraints. A prototype implementation is developed using Pairing-Based Cryptography (PBC) libraries along with blockchain frameworks to test the practical feasibility of the design. The evaluation considers execution time, communication cost, and scalability under varying workloads, benchmarking results against existing approaches. The outcomes demonstrate that the proposed framework achieves an optimized solution for crowdsourcing in areas like online blood bank systems.

1.7 Thesis Organization

This thesis is structured into the following chapters:

Chapter 1 establishes the research challenge and framework, introducing concepts like crowd sourcing, task matching, task data privacy, and data recovery. It emphasizes the roles of secured task matching challenges, verification methods, and different

framework studies in cloud data integrity.

Chapter 2 reviews existing literature on privacy-preserving task matching schemes, establishing a foundation for understanding different approaches and methodologies. The concept of this chapter is based on the journal paper titled "A Survey on Secure and Privacy-Aware Task in Crowdsourcing Platforms", which is communicated in the *Distributed Computing*(SCIE) Journal.

Chapter 3 proposes a signature-oriented privacy-preserving task matching schema. The approach enhances user anonymity and data integrity without relying on proxy re-encryption. It addresses privacy risks associated with exposing sensitive user data. The solution aims to balance security, efficiency, and performance in crowdsourced task matching. The concept of this chapter is based on the journal paper titled "An Efficient Task Matching Schema with Signature-Oriented Encryption Technique," which was published in the *Utilitas Mathematica*(Scopus) Journal. A part of this chapter is also published at the International Conference on Recent Advances in Science, Technology, and Engineering (ICRASTE) with the title "A secure and efficient schema by integrating blockchain and crowd-sourcing in online language learning platforms".

Chapter 4 introduces blockchain technology within a crowdsourcing framework to enhance transparency, traceability, privacy, and efficiency in blood donation and distribution. The integration of blockchain ensures tamper-proof records, real-time verification, and decentralized access, while crowdsourcing enables community participation. This work is published in Proceedings of the International Conference on Advanced Communications and Machine Intelligence (MICA 2023) titled "Online Blood Bank System Using Blockchain in Crowdsourcing Platform".

Chapter 5 integrates searchable encryption and blockchain to optimize donor-recipient matching. By leveraging crowdsourcing and a fine-grained reuse mechanism, the system reduces redundancy, improves match efficiency, and lowers transaction costs. It enhances transparency and data integrity through blockchain, while protecting the privacy of donors and recipients without relying on centralized intermediaries. Security and performance analysis demonstrate the system's resilience, scalability, and suitability for real-time emergency healthcare scenarios. We communicated this paper with the title "Crowd-Sourced Blood Bank Management: A Secure and Efficient Reuse-Oriented Framework" in *Utilitas Mathematica*(Scopus) journal.

Chapter 6 provides a conclusion to the research, summarizing achievements, reflecting on goals, and suggesting future directions, followed by a list of references at the end.

Chapter 2

Review of Literature

The research in this domain has focused heavily on the development of cryptographic tasking methods. These methods ensure that task requesters and workers can exchange sensitive information without revealing underlying data to third parties. Subsequent studies extended this line of work by introducing advanced schemes such as proxy re-encryption and differential privacy, which enhance flexibility and resilience against inference attacks.

In parallel, reputation- and trust-based systems have been widely adopted to improve reliability in task allocation. However, these approaches introduce new privacy concerns by recording detailed behavioral logs that may leak sensitive worker or requester information. To address these shortcomings, blockchain-based solutions have recently gained prominence, offering transparency, immutability, and decentralized trust. While blockchain has shown promise, its deployment in crowdsourcing systems raises challenges related to storage overhead, transaction costs, and scalability.

The foundational works highlight their contributions, limitations, and suitability for real-world deployment in this literature review. By synthesizing research across cryptography, task-matching methodologies, and blockchain integration, the chapter establishes the groundwork for identifying research gaps and motivating the development of a novel, efficient, and privacy-preserving task-matching framework tailored to sensitive applications such as online blood bank management. By focusing on these design goals, developers and researchers can create privacy-preserving task matching schemas that safeguard user data, maintain user trust, and ensure the seamless functioning of crowdsourcing platforms. Privacy-preserved task matching is a critical concern in various domains such as crowdsourcing, IoT, and cloud computing, where user and task data confidentiality must be maintained. To ensure both efficient matching and pri-

vacy protection, a range of encryption and matching techniques has been explored. HE allows computation on encrypted data without revealing its content, enabling privacy-preserved operations during task matching. Attribute-Based Encryption (ABE) and Functional Encryption offer fine-grained access control and matching based on encrypted attributes. In addition, indexing and filtering methods like secure k-nearest neighbors (kNN) and Bloom filters have been integrated with encryption schemes to enhance the efficiency of matching. Various studies have proposed hybrid approaches that combine encryption with machine learning or heuristic algorithms to balance privacy, accuracy, and computational performance, making task matching both secure and scalable.

In task matching, blockchain ensures transparency, security, and decentralization. Using smart contracts, tasks are automatically assigned and rewards are released upon completion without intermediaries. The immutable ledger records task assignments and payments, preventing disputes and fraud. Blockchain enables secure collaboration by protecting user data with encryption and supporting reputation systems that provide tamper-proof ratings for workers and employers. Additionally, blockchain's incentive mechanisms allow for fair distribution of rewards, often in cryptocurrency. This trustless environment makes blockchain ideal for crowdsourcing, freelancing, and collaborative platforms, ensuring privacy and efficiency in task matching. Agrawal *et al.*, 2023; Li *et al.*, 2024; Liu *et al.*, 2023 used block chain. The major technological changes for the year can be seen in the Figure 2.1.

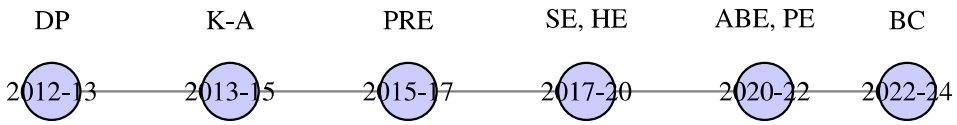


Figure 2.1: Timeline of Task Matching Techniques

2.1 Chronological Study on Task Matching

To analyze the methodology adopted for privacy-preserving task matching, we conducted a chronological survey of different approaches. This survey highlights the progressive evolution of privacy-aware techniques and the threat vectors that have been addressed over time, such as location privacy leakage. The timeline of task matching frameworks with privacy safeguards is summarized in Table 2.1.

Mobile platforms allow rewards, enabling users to participate in crowdsourcing through their devices. However, most task allocation mechanisms struggle to main-

Reference	**Core Concept**	**Technique Used**	**Evaluation Approach**
Huang *et al.*, 2017	Vehicular crowdsourcing privacy	Pseudonyms, location cloaking	Prototype, simulation
Shu, Liu, *et al.*, 2018	Anonymous task assignment	Attribute-based encryption, anon. authentication	Security proofs, experiments
Dai and Qiao, 2018	Differential privacy for location	Laplace noise, grid cloaking	Prototype, privacy-utility tradeoff
Wang *et al.*, 2018	Location protection with k-anonymity	Cloaking, dummy injection	Prototype, analysis
Xiong *et al.*, 2019	Incentive-aligned assignment	Geometric perturbation, encrypted matching	Theoretical + simulations
Zhai *et al.*, 2019	Secure truthful allocation	VCG auction + cloaking	Security study, experiments
Hao *et al.*, 2019	Interest-aware matching	Searchable encryption, garbled circuits	Security study, synthetic data
Yin *et al.*, 2019	Personalized task suggestion	Identity-based encryption, preference modeling	Proofs, real dataset
Tang *et al.*, 2020	Privacy + incentives	Paillier cryptosystem, economic modeling	Proofs, real data evaluation
Zhao *et al.*, 2020	Blockchain-assisted FL for IoT	Gradient masking, blockchain consensus	Prototype, IoT case study
Zhang *et al.*, 2020	Fog-enabled allocation	Cloaking, encrypted indices, SE	iFogSim prototype
Li, Wu, *et al.*, 2021	Decentralization of matching technique	Encrypted match, cloaked locations	Android prototype, evaluation
Zou *et al.*, 2021	Hybrid blockchain framework	Incentives, reputation, location cloaking	Hyperledger prototype
Wang *et al.*, 2022	Obfuscated location matching	Planar Laplace distribution (graph-based)	Real dataset evaluation
Zhou *et al.*, 2022	Location-privacy guarantee	Additive secret sharing	Real-world dataset
He *et al.*, 2023	Worker-task-location privacy	Fuzzy logic + cryptography	Real-world dataset
Jiang *et al.*, 2024	Fine-grained task reuse	Blockchain, smart contracts	Ethereum testbed analysis

Table 2.1: Chronological overview of privacy-preserving task matching frameworks

tain both efficiency and privacy while also providing fair incentives to participants. Cryptography-driven models address these issues. For instance Ning *et al.*, 2017 introduced a win–win incentive mechanism using dual-policy attribute-based encryption, allowing workers and requesters to set access policies and achieve bipartite matching. Similarly, Tang *et al.*, 2020 emphasized incentive-compatible models while preserving task privacy.

Fog computing has been leveraged to reduce computational costs while preserving task and worker confidentiality. Zhang *et al.*, 2020 proposed a model using threshold secret sharing to verify worker eligibility and resist malicious attacks. The authors in Zhao *et al.*, 2020 proposed learning system.

Decentralization is very important for data preservation. Li, Wu, *et al.*, 2021 presented a distributed system using homomorphic encryption to prevent location leakage, whereas Zou *et al.*, 2021 designed CrowdHB, a hybrid blockchain solution with location privacy guarantees and performance optimization. Other works applied differential privacy Wang *et al.*, 2018, k-anonymity Sun *et al.*, 2017, or auction-based assignment Zhai *et al.*, 2019 to strengthen task-worker privacy.

Later schemes adopted blockchain-backed privacy-preserving task matching Wu *et al.*, 2019, searchable encryption-based task recommendations Yin *et al.*, 2019, and geometry-aware range query protection Yuan *et al.*, 2019. More recent proposals combine cryptography, machine learning, and distributed ledgers to balance efficiency, privacy, and fairness. Overall, this progression shows a clear shift from centralized, computation-heavy methods toward distributed, incentive-compatible, and cryptographically hardened frameworks for secure task matching.

2.2 Deployed Methodologies in Task Matching

In this section, we explain different deployment strategies that are used in a privacy-preserved task matching technique. The major deployment strategies are proxy re-encryption-based, proxy-free, and blockchain-based. The working strategy, along with the advantages and disadvantages, is explained below.

2.2.1 Proxy Re-encryption based Task Matching

These cryptographic methods enable a third party to transform data into ciphertexts using the key so that it cannot be decrypted by another party. A requester encrypts a task using their public key, resulting in a ciphertext. This encrypted task is then sent to the proxy server. By utilizing PRE, the proxy can re-encrypt this ciphertext with

the public key of a specific worker, allowing that worker to decrypt and access the task details securely. To *et al.*, 2016b presented a schema to achieve attributes and data security. Shu and Jia, 2016 Shu, Liu, *et al.*, 2018 also used a proxy cryptosystem. Proxy-free encryption-based task matching enhances privacy by removing centralized trust, allowing direct interactions between requesters and workers for quicker task assignments and efficient workflows. However, it introduces challenges such as increased complexity in key management and complications in key revocation. Additionally, as the number of users grows, managing direct connections may become cumbersome, potentially impacting overall system efficiency.

2.2.2 Proxy-Free Encryption-based Task Matching

Proxy-free encryption based task matching enhances security and privacy by removing the need for a central proxy, allowing direct interactions between requesters and workers. Requesters encrypt task details with their public keys and share them directly, enabling workers to independently search and match tasks. Each worker has a unique key pair, ensuring they decrypt only authorized tasks, minimizing sensitive data exposure. Proxy-free encryption-based task matching eliminates centralized trust, enhancing privacy through direct interactions between requesters and workers. This leads to quicker task assignments and a more efficient workflow. However, it introduces challenges, including increased complexity in key management and complications in key revocation. Additionally, managing direct connections may become cumbersome as the number of users grows. Shu, Liu, *et al.*, 2018 and To *et al.*, 2016a used proxy free technique.

2.2.3 Blockchain-based Task Matching

Blockchain-based task matching utilizes decentralized ledger technology to improve transparency, security, and efficiency in task assignments between requesters and workers. Tasks are recorded as immutable transactions on the blockchain, allowing requesters to post tasks while workers browse and accept assignments in a trustless environment, eliminating intermediaries. Smart contracts automate agreement execution, ensuring secure management of payments and task completion, thereby enhancing data integrity and fostering trust among participants in the process. Blockchain-based task matching offers several advantages, including enhanced transparency and security through immutable records, fostering trust among participants. Smart contracts play a vital role in automating the tasking process, ensuring fair task allocation, timely

completion, and transparent payment without requiring intermediaries. Despite these benefits, challenges remain, including scalability limitations, high computational and energy costs associated with certain blockchain frameworks, and the steep learning curve that can hinder adoption by non-technical users.

Several studies have explored blockchain as a promising solution for secure and efficient task management. For instance, Manzoor *et al.*, 2021a employed blockchain to enhance proxy re-encryption mechanisms, thereby ensuring secure task delegation. Li *et al.*, 2018 Implemented an architecture that used blockchain. Wu *et al.*, 2013 also developed their technique. Guo *et al.*, 2020 proposed FedCrowd, a federated crowdsourcing platform incorporating privacy-preserving techniques to protect participant data. Lin and Zhang, 2020b designed a blockchain-based scheme to mitigate Sybil attacks in crowdsourcing voting systems.

Furthermore, evolving tasking schemas in crowdsourcing environments have been systematically analyzed, as summarized in Table 2.2. A comparative evaluation of technologically diverse schemes, highlighting trade-offs in privacy, efficiency, and scalability, is presented in Table 2.3. Together, these works underline blockchain's potential while emphasizing the need for optimization to address its inherent limitations.

2.3 Challenges and Research Directions

The preceding analysis clearly highlights that several significant challenges remain unresolved despite ongoing efforts in privacy-protected task matching. To develop task management systems that prioritize privacy, these research challenges must be addressed effectively. This section outlines some key issues in the field.

Recently, blockchain technologies have advanced considerably, becoming suitable for various applications due to their inherent accountability, transparency, and redundancy. However, with the rapid growth of quantum computing, the threats that could target these systems are also increasing. Additionally, the exponential growth of data generation and analysis in commercial and governmental applications underscores the necessity for robust big data processing solutions. This situation emphasizes the urgent need for new security technologies to safeguard extensive data processing systems. By enhancing security, applications can leverage big data analytics without the constant threat of cyberattacks compromising sensitive information.

Reference	**Core Concept**	**Technique Used**	**Evaluation Approach**
Huang *et al.*, 2017	Vehicular crowdsourcing privacy	Pseudonyms, location cloaking	Prototype, simulation
Shu, Liu, *et al.*, 2018	Anonymous task assignment	Attribute-based encryption, anon. authentication	Security proofs, experiments
Wang *et al.*, 2018	Location protection with k-anonymity	Cloaking, dummy injection	Prototype, analysis
Xiong *et al.*, 2019	Incentive-aligned assignment	Geometric perturbation, encrypted matching	Theoretical + simulations
Zhai *et al.*, 2019	Secure truthful allocation	VCG auction + cloaking	Security study, experiments
Hao *et al.*, 2019	Interest-aware matching	Searchable encryption, garbled circuits	Security study, synthetic data
Yin *et al.*, 2019	Personalized task suggestion	Identity-based encryption, preference modeling	Proofs, real dataset
Tang *et al.*, 2020	Privacy + incentives	Paillier cryptosystem, economic modeling	Proofs, real data evaluation
Zhao *et al.*, 2020	Blockchain-assisted FL for IoT	Gradient masking, blockchain consensus	Prototype, IoT case study
Zhang *et al.*, 2020	Fog-enabled allocation	Cloaking, encrypted indices, SE	iFogSim prototype
Li, Wu, *et al.*, 2021	Decentralization of matching technique	Encrypted match, cloaked locations	Android prototype, evaluation
Zou *et al.*, 2021	Hybrid blockchain framework	Incentives, reputation, location cloaking	Hyperledger prototype
Wang *et al.*, 2022	Obfuscated location matching	Planar Laplace distribution (graph-based)	Real dataset evaluation
Zhou *et al.*, 2022	Location-privacy guarantee	Additive secret sharing	Real-world dataset
He *et al.*, 2023	Worker-task-location privacy	Fuzzy logic + cryptography	Real-world dataset
Jiang *et al.*, 2024	Fine-grained task reuse	Blockchain, smart contracts	Ethereum testbed analysis

Table 2.2: Summary of Related Work on Privacy-Preserving Crowdsourcing

Schema	Advantage	Disadvantage
Shu, Yang, *et al.*, 2018a	The crowd server cannot reveal task information as task matching is done between cipher text and trapdoor.	If the authority is not fully trusted, they can register malicious users. Malicious users may in turn break the task privacy. Moreover, it is centralized.
Shu, Jia, *et al.*, 2018	The privacy details like location details etc. of the worker and requester along with the task privacy is maintained.	Re-encryption key leaking is a possibility is there by the server breaking the whole privacy.
Li *et al.*, 2018	Data is stored in distributed database. So, it is more secure.	Miners are honest but may fork a chain with dishonest workers. There is a chance of 51% attack.
Zhu *et al.*, 2019	Distributed authority for agreement management is more secure.	Considered secure, but might face challenges in managing consensus among distributed parties, especially with dishonest nodes.

Table 2.3: Comparison of notable methodologies of task matching

2.3.1 Key Challenges

- **Privacy-utility trade-off:** Balancing privacy preservation with task matching utility is a fundamental challenge.
- **Scalability:** Many privacy-preserving algorithms face scalability issues when dealing with large-scale crowdsourcing platforms. Developing efficient algorithms that can handle a massive number of tasks and workers while preserving privacy is a significant challenge.
- **Adversarial attacks:** Adversaries may attempt to exploit vulnerabilities in privacy-preserving mechanisms. Research is needed to develop robust algorithms that can withstand various adversarial attacks and maintain privacy under malicious attempts to undermine the system.
- **Regulatory compliance:** Ensuring that privacy-preserving task matching systems comply with regulations while maintaining their effectiveness is a challenge.
- **User acceptance and trust:** Convincing workers and requesters to trust and adopt privacy-preserving mechanisms is essential. Designing systems that are transparent, easy to understand, and trustworthy is critical for user acceptance.

- **Real-time constraints:** Many crowdsourcing applications require real-time or near-real-time task assignments. Meeting these constraints while preserving privacy poses a significant challenge and requires innovative solutions.

Addressing these challenges and exploring the mentioned research directions will be instrumental in advancing the field of privacy-preserving task matching in crowdsourcing.

2.3.2 Research Directions

- Explore advanced differential privacy mechanisms to ensure robust privacy protection while maintaining task matching efficiency and utility. Develop algorithms that provide meaningful task assignments without compromising individual workers' data privacy.
- Investigate into task assignments without revealing their private inputs. Develop efficient protocols for task matching while preserving privacy.
- Research on integrating HE schemes into task-matching algorithms. This would allow computations on encrypted data, ensuring privacy during the processing of task assignment algorithms.
- Data applications will require the development of secure techniques. Privacy-preserving task matching in crowdsourcing remains a crucial research area, yet it presents several challenges that must be addressed.
- Explore blockchain technology for secure and transparent task matching. Develop smart contracts to facilitate trustless task assignments while preserving privacy.
- Design task matching algorithms that consider the context of tasks and workers to preserve privacy effectively. Context-aware algorithms can provide personalized task recommendations without revealing sensitive information.
- Develop a platform allowing worker to understand and control their privacy settings during task matching. Empower workers with granular control over the information they share while ensuring a seamless user experience.

Potential developments for improving privacy guarantees is shown in Table 2.4.

Technique	Key Idea	Benefits	Challenges
Federated Learning (FL)	Decentralized training of models on user devices without sharing raw data	• Preserves local data privacy • Supports personalization • Lessens data leakage	• Needs secure aggregation • High communication overhead • Model drift
Post-Quantum Cryptography (PQC)	Use of quantum-resistant algorithms (e.g., lattice-based cryptography)	• Guarantees long-term data confidentiality	• Larger key sizes • Expensive computation
Blockchain-based Auditability	Leveraging blockchain's immutability for task assignment and logging	• Ensures transparent, tamper-proof records • Enables dispute resolution and verification	• Transaction fees (gas costs) • Latency
Hybrid Privacy Models	Combining techniques like HE and FL or DP and Blockchain	• Balances performance and privacy • Increases defense-in-depth	• Scalability issues • Complex system integration • Expensive development cost
Edge-based Secure Computation	Processing on mobile/-fog based system	• Lessens latency and bandwidth usage • Increases local privacy	• Resource constraints • Integration complexity

Table 2.4: Potential Developments for Improving Privacy Guarantees in Task Matching

Chapter 3

An Efficient Task Matching Schema with Signature-oriented Encryption

Crowdsourcing platforms have revolutionized the way tasks are outsourced and completed by the use of internet. Central to their effectiveness is the ability to match workers with tasks. However, the exchange of sensitive information of the entities poses significant risks to data security. Traditional encryption methods and proxy re-encryption techniques face limitations in maintaining both scalability and privacy. In this thesis, we introduce ring signatures in the tasking process to ensure anonymity of the user along with data integrity. Our proposed system addresses the weaknesses of conventional approaches of Shu, Liu, *et al.*, 2018 by eliminating reliance on proxy re-encryption and offering robust protection against identity inference. We present the design, implementation, and analysis it's security maintaining privacy in dynamic and large-scale crowdsourcing environments.

3.1 Overview

Crowdsourcing is fueled by the growth of the internet, this model has seen rapid expansion over the past decade, giving rise to well-known platforms like Upwork, Amazon Mechanical Turk, and CrowdFlower. These platforms act as intermediaries, connecting individuals who post tasks referred to as requesters with workers willing to complete them in exchange for payment. A key element in the success of these platforms is how effectively they match tasks with workers whose skills and preferences align.

Task matching is an important feature of crowdsourcing systems. It's the process that enables the backend, often referred to as the crowd-server, to connect workers with relevant job postings. However, this matching process typically involves the sharing

of personal information such as identity, location, or professional background which raises serious concerns about user privacy and data security.

3.2 Related Work

This paper explores three key research areas: 1) secured task matching; 2) searchable encryption (SE) methods; and 3) ring signature techniques

Secured Task Matching in crowdsourcing:

Crowdsourcing enables cost-effective task distribution. The rise of mobile Internet and Online-To-Offline (O2O) models has driven the need for efficient crowdsourcing task assignments Song *et al.*, 2017. A task-matching approach leveraging worker preferences to enhance efficiency and engagement has been proposed in Yuen *et al.*, 2011. However, privacy and security risks in crowdsourcing have become a major concern, leading to research on privacy-preserving mechanisms in data aggregation Zhang *et al.*, 2016. Various approaches aim to protect user and data privacy while maintaining efficiency in task matching. A crowdsourcing schema that enables multi-keyword matching while preserving task and worker privacy using polynomial functions, proxy re-encryption, and asymmetric scalar-product-preserving encryption(ASPE) Shu, Jia, *et al.*, 2018. To overcome the inefficiency of proxy-based schema, proxy-free schema have been developedShu, Yang, *et al.*, 2018a. A decentralized blockchain approach is proposed in Guo *et al.*, 2020,Li, Bai, and Wei, 2021. Recent work ensuring fine-grained worker selection for efficient task matching has been proposed in Li *et al.*, 2024.

Searchable encryption:

Searchable Encryption (SE) ensures secure data retrieval in crowdsourcing by supporting single-user and multi-user models Ma *et al.*, 2018b. The SE framework includes KEYGEN for key generation, BUILDINDEX for index creation, TRAPDOOR for query formulation, and SEARCH for retrieving matching documents Handa *et al.*, 2019b. Searchable Encryption (SE) is widely used to enable privacy-preserving data retrieval in crowdsourcing, allowing users to search encrypted data without revealing sensitive information. Various SE-based approaches have been proposed for secure task matching and worker participation. Traditional methods, including symmetric and asymmetric searchable encryption, offer different trade-offs between efficiency and security. However, the dynamic nature of crowdsourcing, where workers frequently join and leave the system, presents challenges in ensuring privacy, access control, and computational efficiency. Many existing schemes rely on proxy-based architectures, which

introduce computational overhead and security risks Wei *et al.*, 2019. Additionally, centralized key management models pose a single point of failure, while some SE-based solutions fail to provide adequate privacy guarantees, such as worker anonymity and protection against query-linking attacks Ambati *et al.*, 2011, Ni *et al.*, 2018.

Several approaches have been explored to address these challenges. Searchable Symmetric Encryption (SSE) offers efficient search operations but struggles with key distribution and revocation issues Wu *et al.*, 2019. Asymmetric Searchable Encryption (ASE) overcomes key distribution challenges by using public-key cryptography but incurs higher computational costs Shu and Jia, 2016. Proxy-based SE solutions enhance scalability by offloading search computations to a third-party entity, yet they introduce security vulnerabilities related to trust assumptions Singh, 2013. More recently, blockchain-based SE frameworks have emerged to decentralize trust; however, they face challenges in query efficiency and on-chain storage costs and anonymity Jiang *et al.*, 2024. Yang et al. Yang *et al.*, 2019 proposed a privacy-preserving crowdsourcing system based on blockchain that exploits the anonymity property of blockchain and private blockchain to protect workers' privacy. Lin et al. Lin *et al.*, 2020 presented a secure blockchain-based crowdsourcing system named SecBCS by group signatures and ciphertext-policy attribute-based encryption. Despite these advancements, maintaining worker anonymity while ensuring secure and efficient task matching remains an open problem in crowdsourcing.

To address these limitations, our approach integrates ring signatures into SE-based crowdsourcing frameworks to enhance privacy protection and eliminate anonymity concerns. Unlike traditional SE schemes, which often expose user identities to the central server or rely on trusted intermediaries, our method ensures that task requester and workers remain anonymous while participating in the system.

Ring signature:

Ring signatures represent a significant advancement in digital signature technology, enhancing both security and anonymity, which is particularly beneficial in crowdsourcing contexts. These signatures allow a member of a group to sign a message without revealing their identity, making it difficult to ascertain who the signer is. One prominent approach to preserving anonymity in task matching is using ring signatures. This cryptographic technique allows a user within a group to sign a message without revealing their identity. first introduced ring signatures Rivest *et al.*, 2001, leading to extensive research into their security and efficiency. Bresson *et al.*, 2002 strengthened ring signatures by addressing security assumptions. Further advancements include Xu *et al.*, 2004, who developed a bilinear pairing-based ring signature, and Bender *et al.*, 2006, who proposed stronger security models. Boneh *et al.*, 2003

and Shacham and Waters, 2007 improved the efficiency of ring signatures by reducing computational overhead. Chandran *et al.*, 2007 introduced a sub-linear-sized ring signature without random oracles, whereas Zhang *et al.*, 2007 designed a traceable ring signature scheme. More recent studies by Chang *et al.*, 2009 and Wu, 2017 focused on certificateless ring signatures to eliminate the need for trusted third parties. Ring Signatures in Crowdsourcing and Multi-User Cryptography. With the increasing importance of multi-user cryptography, ring signatures have become vital for privacy preservation in crowdsourcing platforms. Malina *et al.*, 2018 demonstrated how ring signatures can be utilized in blockchain-based e-voting systems. Malina *et al.*, 2018 developed lightweight ring signatures for decentralized transactions, emphasizing efficiency in large-scale applications. Melchor *et al.*, 2011 proposed a threshold ring signature scheme for distributed task execution, while Tso, 2013 introduced universal ring signatures that allow flexible group formation without a predefined structure. By integrating ring signatures into task-matching protocols, we address key limitations in previous works, including privacy leakage, task attribution risks, and computational inefficiencies. Furthermore, our scheme enhances accountability without sacrificing anonymity, offering a balanced solution for privacy-preserving task matching.

3.3 Problem Formulation

This section will provide the theoretical workflow of our proposed schema. A crowdsourcing system that allows any requester to post encrypted tasks on an unprotected crowdsourcing server and match them with workers looking for projects that interest them has been considered. Malicious users may expose private information by examining the connections between their uploaded data and identification information. Therefore, we propose a secure ring signature-based crowdsourcing schema.

Four components make up our system: 1) a key generator (KG); 2) a crowdsourcing service provider (crowd-server); 3) many requesters; and 4) several employees. The system model diagram is shown in 3.1

The Key Generator (KG) initializes the system, registers users, issues public keys for requesters to encrypt task requirements, and provides each worker a unique secret key for trapdoor generation, keeping the master key confidential for signature verification. Requesters encrypt tasks, while workers create trapdoors to query relevant tasks securely. Task matching is done by the derver.

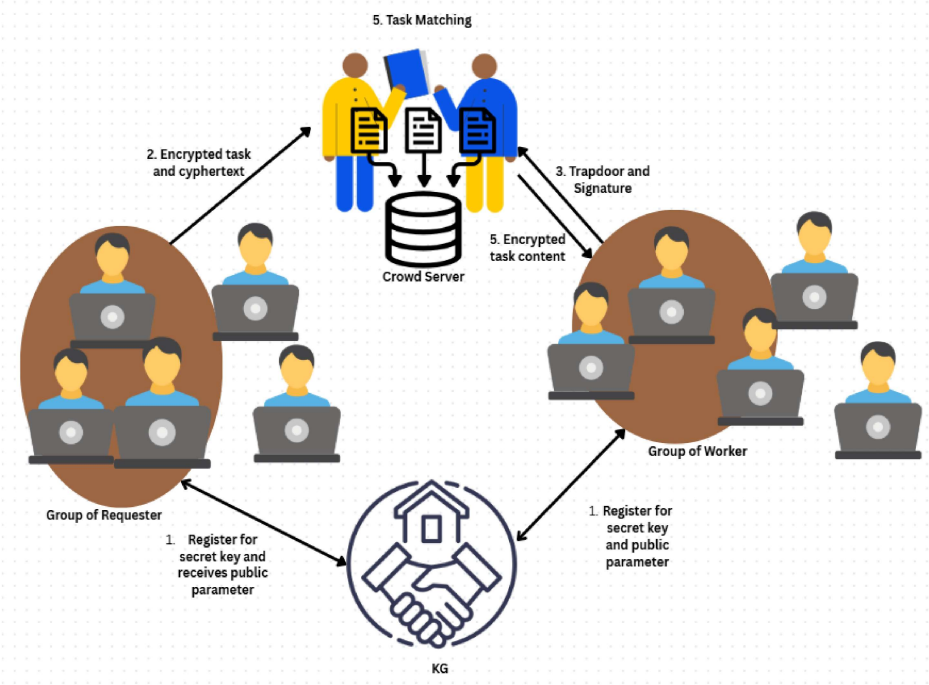


Figure 3.1: System Model

3.3.1 Security Requirements

The privacy requirements are as follows:

1. Authentication: To determine whether a received message has been changed, message authentication is essential. To stop false information from spreading, messages that are discovered to have been altered are removed. The message's signature attests to the vehicle's legitimacy.

2. Anonymity and privacy: It guarantees that a vehicle's actual identity is kept hidden and safe from other network users. It is impossible to determine whether two inquiries originate from the same entity.

3. Unforgeability: This feature ensures that no network member's signature can be copied. To prevent signatures from being falsified, each employee must provide a unique signature for a particular message.

3.3.2 Design Goals

The proposed schema is designed to achieve the following utility objectives:

1. **Efficiency:** The system ensures minimal computational overhead, enabling fast and practical execution.

2. **Scalability:** The scheme maintains a constant size for both requester and worker operations, supporting large-scale deployments.

3. **Elimination of Proxy:** Trapdoors and ciphertexts are independently generated by requesters and workers without relying on any third-party intermediaries.

3.4 Detailed Schema Construction

In the proposed ring signature-based task matching framework, the Key Generator (KG) plays a pivotal role by managing system initialization and secure user registration. During this process, requesters receive a searchable public key (spk) for encrypting task requirements, while each authenticated worker W_i is assigned a unique searchable secret key (ssk_i) for generating trapdoors. The master secret key (msk) is kept confidential by the KG and is later used for signature verification and worker traceability.

When requesters publish a task, they first define the requirements as a keyword set. These requirements, along with the task content, are encrypted using the public key through the `Enc` algorithm and submitted to the crowd-server in ciphertext form. Workers, on the other hand, generate trapdoors corresponding to their query keywords using their individual secret keys. To preserve anonymity, each trapdoor is combined with a ring signature generated from the worker's secret key and the public keys of other participants. The server validates the received signature in collaboration with the KG. If the verification succeeds, secure task matching is executed. The complete protocol is divided into distinct phases, as described below.

1. System Initialization and User Registration: The KG executes the `Setup` algorithm, yielding a searchable public key (spk) and a master secret key (msk). The spk is distributed to all requesters for encryption, while each worker W_i receives a unique secret key (ssk_i) for generating trapdoors. The msk remains confidential with the KG.

Notation	Description
λ	Security parameter for system initialization
Setup(1^λ)	Initialization algorithm run by the Key Generator
(spk, msk)	Setup output: searchable public key and master secret key
spk	Searchable public key: $(G_1, G_2, e, p, g, g_1, g_2, H)$
G_1, G_2	Bilinear groups of prime order p
p	Prime order of cyclic groups G_1 and G_2
g	Generator of G_1 and G_2
$g_1 = g^{x_1}$	Public component from master secret x_1
$g_2 = g^{x_2}$	Public component from master secret x_2
$H(\cdot)$	Collision-resistant hash function
$e(\cdot,\cdot)$	Bilinear map: $e : G_1 \times G_1 \to G_2$
msk	Master secret key: (x_1, x_2, f_1), kept by KG
x_1, x_2, f_1	Secret exponents for cryptographic operations
$t_i \in \mathbb{Z}_p^*$	Random exponent for worker W_i
$ssk_i = g^{t_i}$	Searchable secret key of worker W_i
spk_i	Public key of worker W_i for ring signatures

Table 3.1: Notation for Setup and Cryptographic Components

Workers also generate a key pair for use in ring signature operations.

$$\begin{aligned} \text{Setup}(1^\lambda) &\to (spk, msk), \\ spk &= (G_1, G_2, e, p, g, g_1, g_2, H), \\ g_1 &= g^{x_1}, \\ g_2 &= g^{x_2}, \\ msk &= (x_1, x_2, f_1), \\ ssk_i &= g^{t_i}. \end{aligned}$$

2. Task Encryption by Requesters: Requesters formulate task requirements as keywords and encrypt them using the searchable public key. The encrypted requirements and content are sent to the server.

$$\text{Enc}(spk, w) \to C, \quad C_1 = g_2^{r_2} H(w)^{r_1},\ C_2 = g_1^{r_1},\ C_3 = g^{r_2}$$

where $r_1, r_2 \in \mathbb{Z}_p^*$.

3. Trapdoor and Signature Generation by Workers: Workers generate trapdoors for their queries using their secret keys. These trapdoors are signed with a ring signature to guarantee anonymity.

$$\text{Trap}(spk, ssk_i, q) \to T, \quad T_1 = g_1^{f_1} g^{t_1},\ T_2 = H(q)^{f_1},\ T_3 = g_2^{t_1}.$$

4. Signature Verification and Task Matching: The server validates the ring signature using `Sign-Veri`. Upon successful verification, the `TaskMatch` algorithm ensures secure matching between tasks and workers.

$$\text{TaskMatch}(C,T) \leftrightarrow \text{Valid Match}, \quad e(C_1,T_1) = e(C_2,T_2) \cdot e(C_3,T_3).$$

5. Worker Traceability: The KG executes the `Trace` algorithm to resolve the identity of a worker based on a submitted trapdoor and signature, enabling accountability without compromising overall anonymity Shu, Liu, *et al.*, 2018.

$$\text{Trace}(msk,T,\sigma) \rightarrow i/0.$$

This structured division of phases ensures privacy-preserving, verifiable, and efficient task matching in a crowdsourcing environment.

3.5 Security Analysis

The proposed scheme satisfies the following security properties under the random oracle model and the hardness of the discrete logarithm problem.

Unforgeability:

Definition: An adversary cannot forge a valid ring signature without access to at least one legitimate private key.
Recursive ring equation:

$$c_{i+1} = H(M, g^{s_i} \cdot y_{c_i})$$

Signature elements:

$$z_i = a_i y_i + t_i c, \quad \text{for } i \neq \gamma$$

$$z_\gamma = (y_\gamma + s_\gamma c) \cdot a_\gamma$$

Verification sum:

$$w = \sum_{i=1}^{N'} z_i - t_i c \mod q$$

Verification condition:

$$c'' = H(w,d,q,M), \quad \text{if } c'' = c \text{ then signature is valid}$$

Anonymity (Unlinkability):

Definition: The identity of the signer is hidden among the ring members.
Hash computation for signature:

$$c_{i+1} = H(M, g^{s_i} \cdot y_{c_i}), \quad g^{s_i} \cdot y_{c_i} \sim_R G_1$$

Simulated Signature:

$$\sigma = (c, z_1, \ldots, z_N) \equiv \sigma_{\text{simulated}}, \quad c_i \leftarrow H(M, \cdot)$$

Probability of distinguishing the real signer:

$$\Pr[\text{Adversary wins}] \leq \frac{1}{N} + \varepsilon$$

Non-repudiation:

Definition: A signer cannot deny being part of the ring after a valid signature is verified.

$$c_{i+1} = H(M, g^{s_i} \cdot y_{c_i}), \quad y_i = g^{t_i}, \quad s_i \in \mathbb{Z}^*$$

$$\sigma = (c_1, z_1, \ldots, z_N)$$

Ring Membership:

$$\exists i \in R : \text{signature passes} \Rightarrow i \in \text{ring}$$

$$\text{ringID} = \{y_1, y_2, \ldots, y_N\}$$

Linkability:

Definition: The verifier can detect whether two signatures originate from the same user without revealing their identity.

$$T = H(y_i, M)$$

Two Signatures:

$$\sigma_1 = (c, z_1, \ldots), \quad \sigma_2 = (c', z_1', \ldots)$$

$$T_1 = T_2 \Rightarrow \text{same signer}$$

$$T_1 = H(y_i, M_1), \quad T_2 = H(y_i, M_2) \Rightarrow T_1 \neq T_2$$

Since $H(\cdot)$ is preimage resistant, y_i is not revealed:

$$\Pr[\text{Linkage reveals identity}] \approx \varepsilon$$

Resistance to Collusion Attacks:

Definition: Colluding users cannot forge a valid ring signature unless one possesses a valid secret key.
Each term in the signature depends on: $g^{s_i} \cdot y_{c_i}$

$$s_i = \log(x_i)$$

Hence, without s_i, signature forgery is computationally infeasible due to the discrete logarithm assumption.

3.6 Experimental Results

We provide an assessment of the performance of the suggested scheme, named APTM, through both theoretical analysis and experimental testing. To guarantee a just comparison, we take into account various recognized methods, including MSDE (Dong *et al.*, 2011), MuED (Bao *et al.*, 2008), SEMEKS (Kiayias *et al.*, 2016), and the anonymous privacy-preserving task matching method proposed by (Shu, Liu, *et al.*, 2018). These schemes are representative of widely adopted solutions in secure multi-user data sharing and searchable encryption, making them appropriate benchmarks for examining the efficiency, scalability, and security guarantees of APTM.

3.6.1 Experimental Setup

The experimental setup is based on a **Ubuntu 12.04 virtual environment**, configured with a **3.2 GHz single-core processor** and **8 GB of RAM**. For performance evaluation, we implemented the schemas and compared with the proposed one. The cryptographic operations rely on the **symmetric elliptic curve SS512**, where the group order $|G|$ is 512 bits, the target group $|GT_0|$ is 1024 bits, and the base field size is 512 bits with an embedding degree of 2.

For the short group signature in APTM, we utilize **asymmetric elliptic curves**.Each of these curves has an **embedding degree of 2** and a **group order of 160 bits**, i.e., $|Z_p| = |Z_{p'}| = 160$ bits. These parameters ensure a balance between computational efficiency and security strength for our cryptographic protocols.

3.6.2 Performance Comparison

Table 3.2 and Table 3.3 provide a detailed comparative analysis of computation and communication complexities across multiple secure task-matching and crowdsourcing schemes, including MSDE, MuED, SEMEKS, APTM, and the proposed RingSig-based framework.

Operation	**MSDE**	**MuED**	**SEMEKS**	**APTM**	**Proposed (RingSig)**
GKGen and SKGen	neg	nE	$8E+n16E$	$E+(n+2)E_1+E_2$	$E+nE$
Enc	$k(4E+f_s+H_g)$	$k(E+T_0+P+h_s+H_{gt0}+SE)$	$k9E$	$k(2E+P+H_1+H_{gt0})$	$k(2E+H+S)$
Trap and Sign	$k_0(5E+f_s)$	$k_0(E+h_s)$	k_012E	$k_0(E+H_1)+(9E_1+3E_T+3P_{12}+H)$	$k_0(E+H)+c_{ring}$
Match and Verify	$2k_0E+kk_0H_g$	$k_0(P+H_{gt0})+kk_0S_D$	kk_05P	$kk_0(P+H_{gt0})+(8E_1+5E_T+5P_{12}+H)$	$k_0(2P+H)+kk_0index$
Trace	-	-	-	$2E_1$	$2E_1$
Revoke	neg	neg	-	$E_1+(r+2)E_2$	$E_1+(r+1)E_2$
Update	-	-	-	$2rE_1$	rE_1

Table 3.2: Computation Complexity

Table 3.2 summarizes the theoretical computational costs of key operations for each scheme, including key generation (GKGen and SKGen), encryption (Enc), trapdoor and signature generation (Trap and Sign), task matching and verification (Match and Verify), tracing, revocation, and metadata updates. For instance, in the proposed RingSig scheme, the cost of encryption is $k(2E+H+S)$, which is lower than SEMEKS ($k9E$) and comparable to APTM ($k(2E+P+H_1+H_{gt0})$). Similarly, task matching and verification in RingSig incur $k_0(2P+H)+kk_0$index, showing efficiency improvements over SEMEKS and MuED. Trace, revocation, and update operations are also optimized, with RingSig requiring fewer pairing computations (E_1) than APTM, reflecting better scalability for large user bases.

Table 3.3: presents the communication overhead for transmitting secret keys, rekeys, ciphertexts, trapdoors, and signatures across the network. The RingSig-based

framework demonstrates reduced communication cost for secret keys ($n(|Z_p^| + |G|)$) and trapdoors ($k_0|G| + |\text{RingSig}|$) compared to other schemes. Ciphertext size is also optimized at $|Z_p^| + k(2|G| + |H|)$, indicating less bandwidth consumption during task submission. Signature size is compact, reflecting the lightweight nature of RingSig compared to APTM's $6|Z_p^*| + 3|G_1|$. Table 3.4 summarizes the performance of the

	MSDE	**MuED**	**SEMEKS**	**APTM**	**Proposed (RingSig)**
Secret keys	$n(\|Z_p^*\| + \|s\|)$	$n(\|Z_p^*\| + \|s\|)$	$n \cdot 12\|G\|$	$n(\|Z_p^*\| + \|Z_p^{*'}\| + \|G_1\|)$	$n(\|Z_p^*\| + \|G\|)$
Re-keys	$n(2\|Z_p^*\|)$	$n(\|Z_p^*\| + \|G\|)$	-	-	$n\|Z_p^*\|$
Ciphertext	$\|Z_p^*\| + k(2\|G\| + \|Z_p^*\|)$	$\|Z_p^*\| + k(\|G\| + \|G_T\| + \|M\| + \|C\|)$	$k \cdot 5\|G\|$	$k(\|Z_p^*\| + \|G\|)$	$\|Z_p^*\| + k(2\|G\| + \|H\|)$
Query/Trapdoor	$\|Z_p^*\| + 2k_0\|G\|$	$\|Z_p^*\| + k_0\|G\|$	$k_0 5\|G\|$	$k_0\|G\| + 6\|Z_p^*\| + 3\|G_1\|$	$k_0\|G\| + \|\text{RingSig}\|$
Signature	-	-	-	$6\|Z_p^*\| + 3\|G_1\|$	$\|\text{RingSig}\|$

Table 3.3: Communication Cost

key algorithms in the proposed RingSig-based task-matching framework across different user scales, ranging from 1,000 to 10,000 users. The initialization time—which includes system parameter and user key generation—grows linearly from 120ms for 1,000 users to 1,200ms for 10,000 users, demonstrating that the system scales predictably with user count. Encryption time, reflecting the cost of generating ciphertexts for task submissions, similarly increases from 95ms to 945ms, indicating that the scheme efficiently supports multiple simultaneous operations without excessive overhead. Revocation time, which measures the effort to remove a worker or requester from the system, grows from 50ms to 500ms, confirming that revocation remains lightweight and practical even for large user sets. Finally, trace time, representing the effort to link a signature to a user for accountability, increases from 40ms to 410ms, showing that trace operations are computationally feasible at scale. Overall, these results highlight that the proposed framework achieves a balance between security and efficiency, with all operations exhibiting near-linear growth, making it suitable for large-scale, privacy-preserving crowdsourcing systems while ensuring secure initialization, fast encryption, efficient revocation, and traceability.

Table 3.4 presents the performance evaluation of key operations—initialization,

Users (n)	Init. Time (ms)	Encrypt. Time (ms)	Revoke Time (ms)	Trace Time (ms)
1,000	120	95	50	40
2,000	240	185	100	85
4,000	480	375	200	165
6,000	720	565	300	245
8,000	960	755	400	330
10,000	1,200	945	500	410

Table 3.4: Performance Comparison of Algorithms

encryption, revocation, and tracing—across different user scales for the proposed ring-signature-based task matching framework. The results show that initialization and encryption times grow linearly with the number of users, reaching 1,200ms and 945ms respectively for 10,000 users, while revocation and trace times remain relatively low at 500ms and 410ms, demonstrating the system's efficiency and scalability. The subsequent comparison table highlights the advantages of the ring-signature approach over conventional group-signature MCS schemes: it provides stronger privacy, unlinkability, and collusion resistance, faster initialization and revocation due to optimized pairings and indexing, and linear scalability suitable for large-scale crowdsourcing. While group-signature schemes perform well for verification and low-latency applications, they incur higher revocation overhead and rely on centralized authority-based traceability. Overall, the tables demonstrate that the proposed framework balances privacy, security, and computational efficiency, making it highly suitable for large-scale, privacy-sensitive task-matching applications such as healthcare, smart governance, and secure legal data-sharing. for thousands of participants.

The experiments conducted provide a comprehensive evaluation of the proposed blockchain-based task-matching framework for large-scale crowdsourcing. System initialization, as shown in Fig.3.2, demonstrates that setup time grows linearly with the number of workers, yet the proposed scheme maintains efficient initialization, taking approximately 20.5 s for 10,000 workers, outperforming SEMEKS and comparable to MSDE and MuED. This indicates that the system can scale effectively Worker revocation (Fig.3.3) remains lightweight even with large revocation sets, with the proposed framework completing revocation in 60 ms for 10,000 workers, significantly faster than SEMEKS and MuED, ensuring the rapid removal of malicious or invalid users to maintain system integrity. Signature tracing (Fig.3.4) introduces minimal overhead, with only 10 ms required for 100 signatures, supporting accountability without significant delays. Requirement encryption and trapdoor generation (Figs.3.5 and 3.6) scale linearly with the number of keywords, yet remain highly efficient, achieving 400

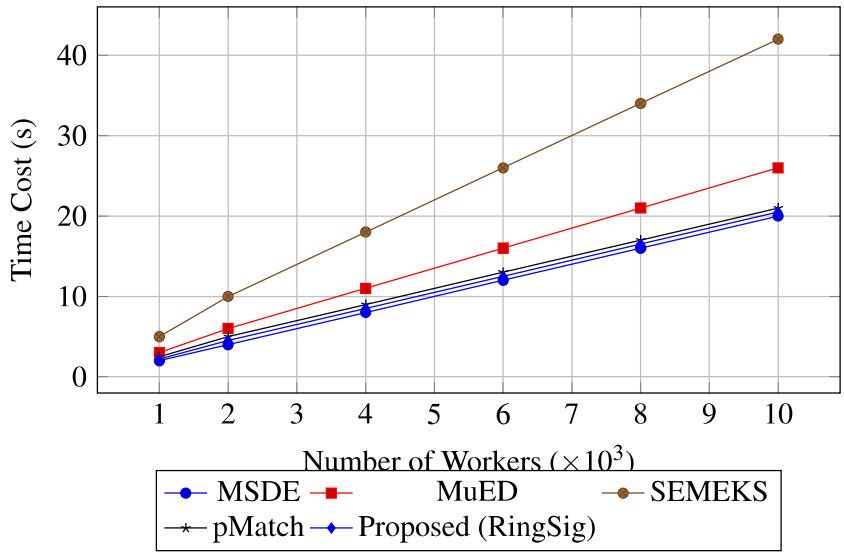


Figure 3.2: System Initialization Cost Comparison

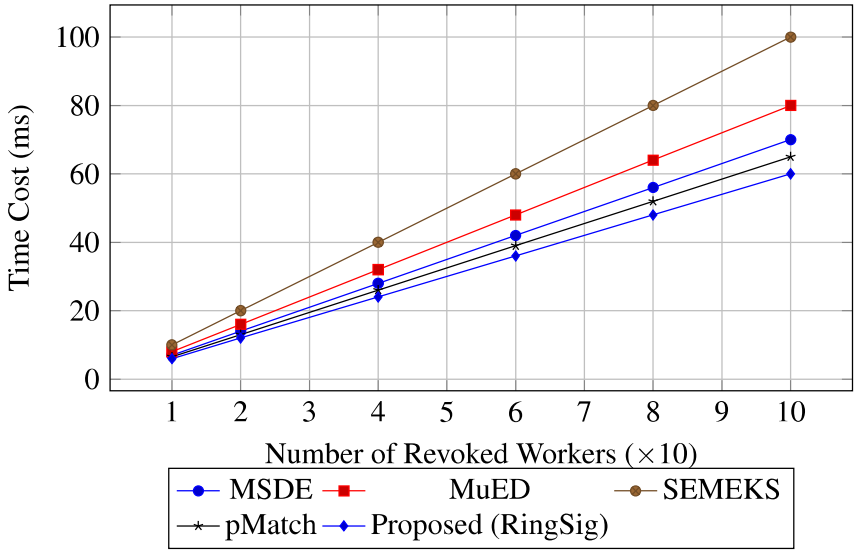


Figure 3.3: Worker Revocation Cost

ms for 10 keywords in encryption and 800 ms in trapdoor generation, thereby preserving user privacy while maintaining responsiveness. Matching operations (Fig. 3.7) also show low latency, approximately 400 ms for 10 ciphertexts/trapdoors, due to optimized blockchain indexing and elimination of redundant computations, enabling real-time task allocation.

Overall, the results indicate that the framework scales effectively, ensures privacy and security, maintains low latency for critical operations, and allows fast revocation of users, making it practical for applications such as healthcare, emergency response,

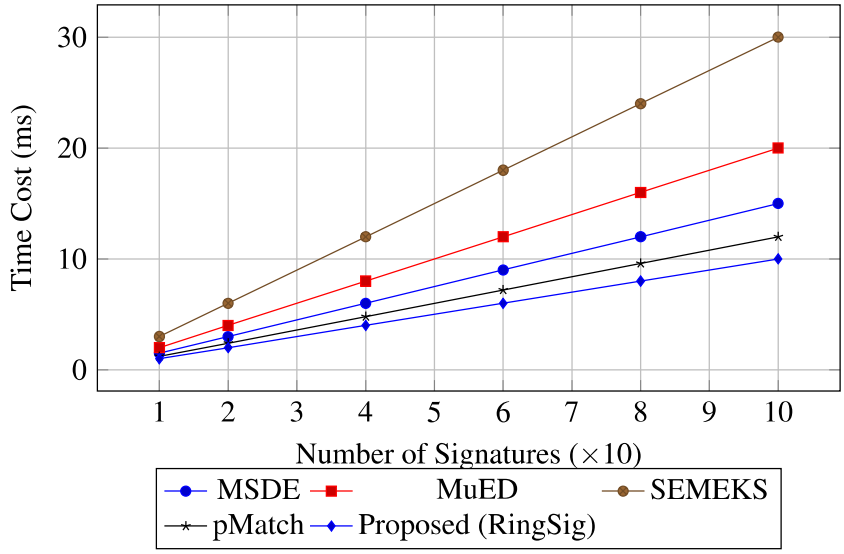


Figure 3.4: Signature Tracing Cost

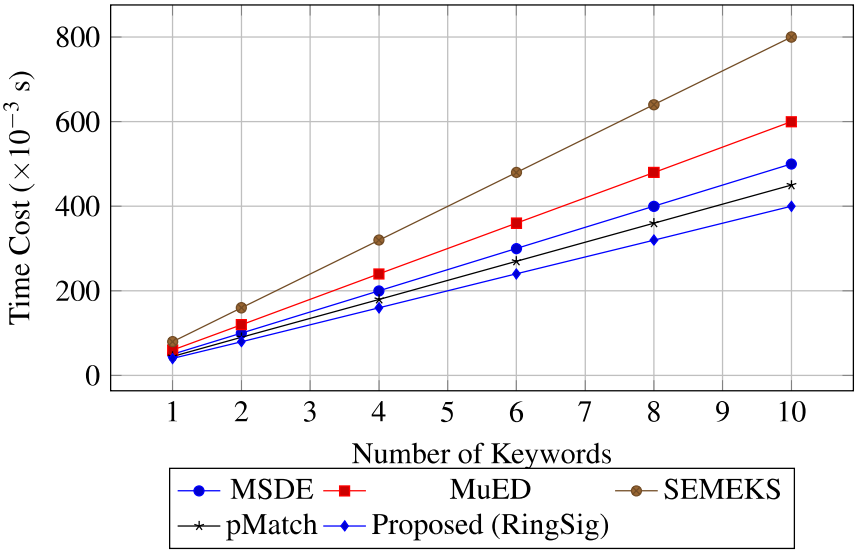


Figure 3.5: Requirement Encryption Cost

and smart governance. These findings also motivate future directions, including decentralized trust management, lightweight cryptography for resource-constrained devices, context-aware task matching, dynamic access control, automated security verification, and real-world deployment, all of which build on the demonstrated efficiency, robustness, and security of the proposed system.

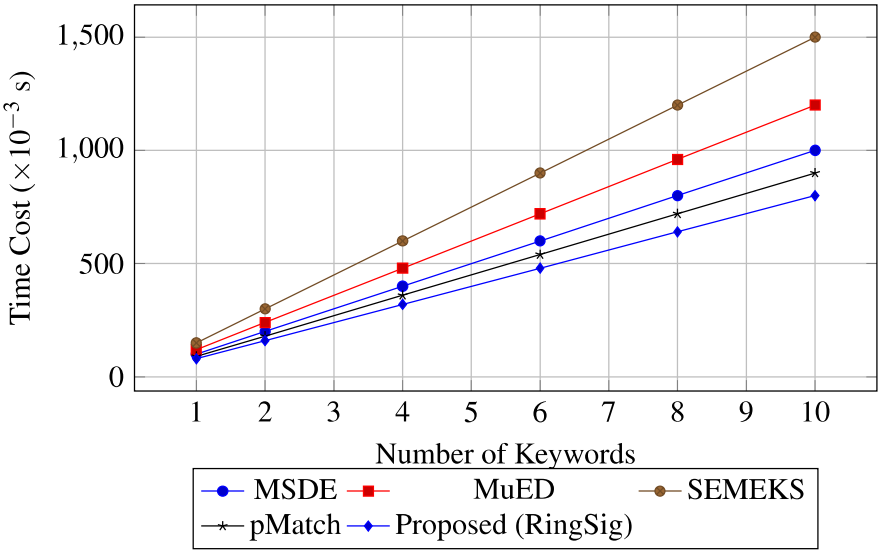


Figure 3.6: Trapdoor and Signature Generation Cost

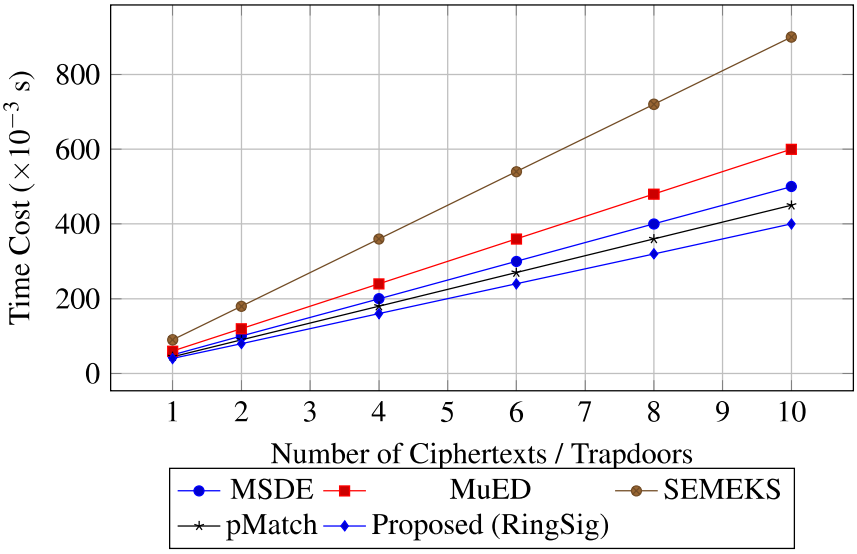


Figure 3.7: Matching Cost

3.7 Conclusion and Future Work

This chapter introduced a privacy-preserving task-matching framework tailored for large-scale crowdsourcing platforms. Unlike traditional proxy re-encryption techniques, which often impose trust assumptions and scalability limitations, our approach leverages ring verification signatures to ensure robust anonymity and data integrity.

Our framework securely protects sensitive user information while enabling efficient job allocation based on user capabilities and preferences. The practicality and

resilience of the system against identity inference attacks were demonstrated through formal security analysis, bilinear pairing-based implementation, and comprehensive performance evaluation.

Future research aims to enhance the task-matching framework by integrating decentralized trust management via blockchain for secure auditing, and employing lightweight cryptography for resource-constrained environments. Context-aware matching will optimize task-worker assignments using real-time data, while dynamic membership and access control ensure flexible group management. Additionally, automated security testing and real-world deployment will validate robustness, performance, and practical applicability in large-scale crowdsourcing and solution management scenarios.

Chapter 4

Online Blood Bank System Using Blockchain in CrowdSourcing Platform

Crowdsourcing, a phenomenon illuminating online ride services to NASA's grand space ventures, holds immense potential yet remains largely unexplored in blood bank management. Despite technological leaps in various sectors, blood bank systems still rely on manual maintenance due to security concerns. This paper advocates the integration of crowdsourcing in blood management, highlighting its transformative power. We propose a novel crowdsourcing mechanism for online blood management, bridging the gap between donors and recipients. To ensure security and transparency, we introduce a robust task management system using Blockchain Technology. This innovative approach promises a secure and efficient online crowdsourced blood management system, addressing critical healthcare needs and revolutionizing the blood donation ecosystem.

4.1 Overview

Crowdsourcing, a method where a diverse online community collaborates to tackle tasks, has demonstrated significant advantages in various fields, including crisis management during the COVID-19 pandemic (Mullen *et al.*, 2021). Despite its proven efficacy, online blood management systems have yet to harness their potential. In the current pandemic era, the demand for human blood has risen sharply, accompanied by a surge in voluntary donors. To streamline the process, it is imperative to automate medical record maintenance and donor verification for efficiency and cost-effectiveness

(Liao *et al.*, 2019; Robinson *et al.*, 2021; Zhu *et al.*, 2020).

Proper blood management is critical, especially for patients requiring regular transfusions like those with thalassemia, considering the diversity of blood types such as A, B, AB, O positive, and negative, some of which are rare. A reserved blood supply is essential for emergencies, accidents, and patients like the elderly, those with liver or cancer conditions. Additionally, on-demand blood availability is crucial and highly valued in unpredictable situations (Howe, 2006).

Although the number of voluntary donors is increasing annually, raising awareness about the benefits of blood donation could further boost participation (Vermicelli *et al.*, 2021). However, some potential donors fear the confidentiality of their blood sample reports, which are screened for diseases like HIV, hepatitis B, hepatitis C, and syphilis. Storing these reports in traditional pen-paper formats or centralized databases poses risks, including potential blackmail of AIDS or HIV positive patients (Ekanayaka *et al.*, 2015; "Secure blood donation system", 2012). Thus, a secure database ensures confidentiality, integrity, and seamless blood management.

In the rest of the chapter, we emphasize the significance of an online crowdsourced human blood management system. Initially, we introduce an innovative architecture for a crowd-based human blood management system. This design incorporates a decentralized approach utilizing Blockchain technology for efficient data management and sharing. Subsequently, we present an algorithm for the system's execution. Finally, we conduct a security analysis to obtain the desired result.

4.2 Related Works

The VINChain project ("Decentralized vehicle data", 2018) introduced an innovative solution, a decentralized blockchain-based database system for recording essential vehicle information. CarVertical ("Blockchain vehicle history", 2018)similarly utilized blockchain to digitize car history records, especially significant when transitioning from traditional pen-and-paper maintenance. (Rowan *et al.*, 2017) explored blockchain technology's potential in vehicle sensing and establishing inter-vehicle connections, showcasing its adaptability beyond conventional applications.

Traditional centralized security technologies face challenges in handling vast and diverse datasets ("Mendeley Dataset on Security", 2021). In response, (Agarwal *et al.*, 2020) proposed an online blood donation system with a secured database utilizing encryption techniques. (Pradhan *et al.*, 2021) presented a blockchain-based system, enabling secure communication between donors, doctors, testing laboratories, and re-

cipients. This secure communication enhances data integrity and confidentiality, limiting access to intended users.

Efforts to optimize blood bank operations include transferring excess blood from one bank to another (Manzoor *et al.*, 2021b). Additionally, (Manzoor *et al.*, 2021b) proposed a blockchain-based proxy re-encryption technique for anonymous IoT data sharing, ensuring data privacy in interconnected environments. In crowdsourcing and voting systems, (Lin and Zhang, 2020a) introduced a secure schema against network attacks like the Sybil attack. (Zhang *et al.*, 2021) proposed a secure software development system, emphasizing the importance of robust security in software engineering.

(Nazir, 2020) created an online Blood Bank management system tailored for students, aiding in managing blood donation camps. A comprehensive review by (Ismael *et al.*, 2022) assessed advanced technologies like the Internet of Things, blockchain, cloud computing, machine learning, and novel decision-making methods in blood bank management systems. (Chordiya *et al.*, 2021) proposed a digital blood management system, utilizing data analysis to predict anomalies. (Venkata Subramanian *et al.*, 2020) discussed design patterns for upgrading the blood bank and donation network infrastructure. (Rambiritch *et al.*, 2021a) revealed a lack of humanistic values in blood facilities across 16 countries.

Lastly, (Saeed *et al.*, 2021) presented an automated bioinformatics AI software application for effective blood bank management, including donor registration and transaction details. (Timmer *et al.*, 2019) conducted a study on Donor InSight (DIS) in a Dutch cohort, comparing it with the Dutch donor population, shedding light on donor demographics and behaviors.

4.3 Proposed Schema

A responsive, on-demand human blood management system is vital. While blood donation camps are common on specific days like January 26th or World AIDS Day, mismanagement often leads to excess blood disposal. This inefficiency creates shortages for patients in urgent need. Thus, we advocate for a crowd-based human blood management system, ensuring streamlined access to blood precisely when it's needed, addressing these critical gaps in our proposed system.

4.3.1 System Model

The proposed crowdsourced blockchain-based blood management system integrates requesters, voluntary blood donors (workers), and a crowd server to efficiently match

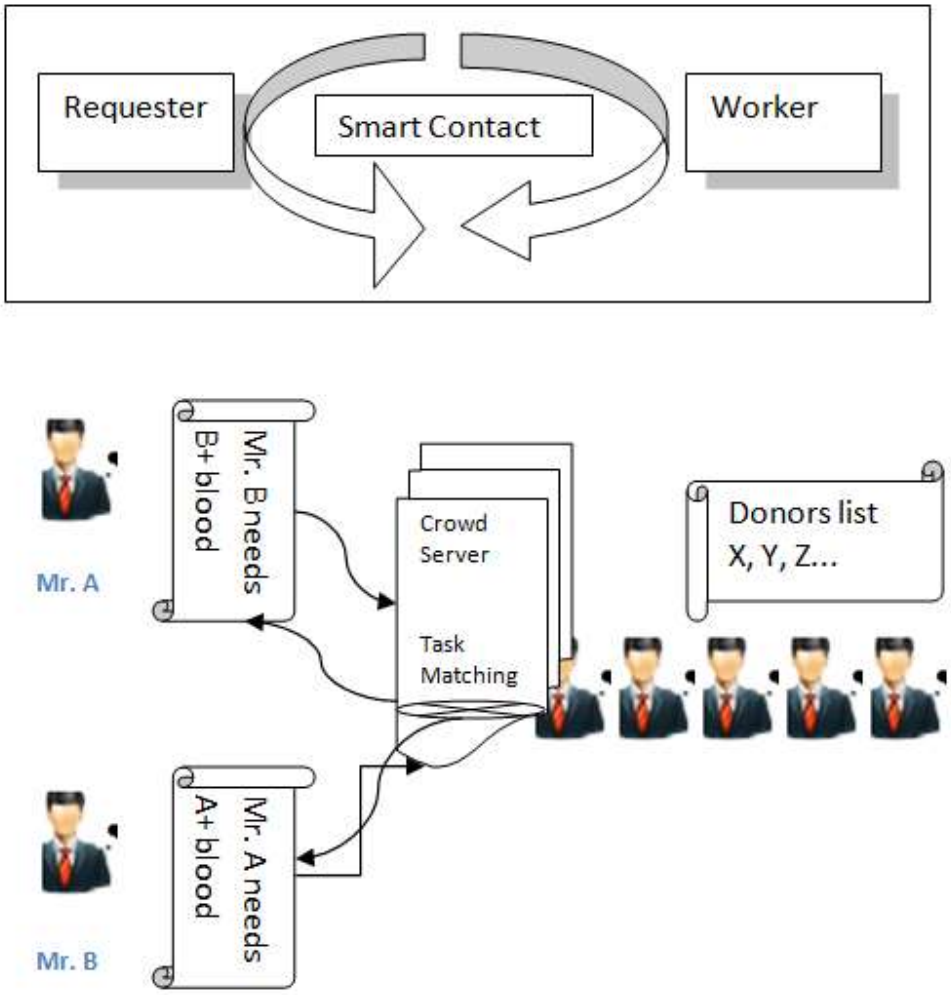


Figure 4.1: Blood Donation System in Crowdsourcing Platform

blood requests with available donors. The architecture ensures transparency, reliability, and secure handling of sensitive information. The system model diagram is explained in **??**.

- **Requesters:** Individuals or organizations seeking blood. Each requester registers with the system and receives a unique ID. Requests are submitted securely and processed by the crowd server.
- **Workers (Donors):** Voluntary blood donors who register, undergo verification including disease screening (HIV, Hepatitis B/C), and provide donation availability. Workers are temporarily blocked post-donation to prevent frequent donations.

- **Crowd Server:** Automates donor-recipient matching based on blood type and proximity. Maintains task metadata on the blockchain to ensure immutability, secure storage, and reuse.
- **Blockchain:** Distributed ledger storing verified metadata, donation history, and task matching results. Ensures tamper-proof records, auditability, and secure data sharing.

4.3.2 Workflow

The proposed system follows a structured workflow. Initially, requesters and workers complete a registration process for authentication. Donors are validated through blood screening and checks of their donation history to confirm eligibility. When a requester places a blood request, the crowd server identifies and matches it with the nearest eligible donor. Upon successful matching, the donation is carried out, and all task-related metadata is securely recorded on the blockchain to ensure transparency and accountability. To maintain safety and fairness, a donor's account is temporarily suspended for six months after each donation, while invalid or ineligible participants are excluded from the system. The detailed workflow is explained in the Figure 4.2.

4.3.3 Threat Model

The system is designed under a semi-honest (honest-but-curious) adversarial model, where participants and servers follow the defined protocols but may attempt to infer additional information from observed data. In this setting, the crowd server executes operations correctly yet may try to learn from encrypted queries and trapdoors, though it is assumed not to collude with requesters or workers. Requesters and workers are regarded as honest, with malicious or invalid users excluded through robust verification and revocation mechanisms. External adversaries are prevented from accessing sensitive information by employing strong encryption techniques, blockchain immutability, and secure communication channels. Overall, this threat model guarantees the confidentiality of donor and requester information, ensures the integrity and tamper-proof storage of donation and task metadata, and prevents unauthorized participation or malicious activities within the system.

4.3.4 Design Goals

The system is designed to meet the following objectives:

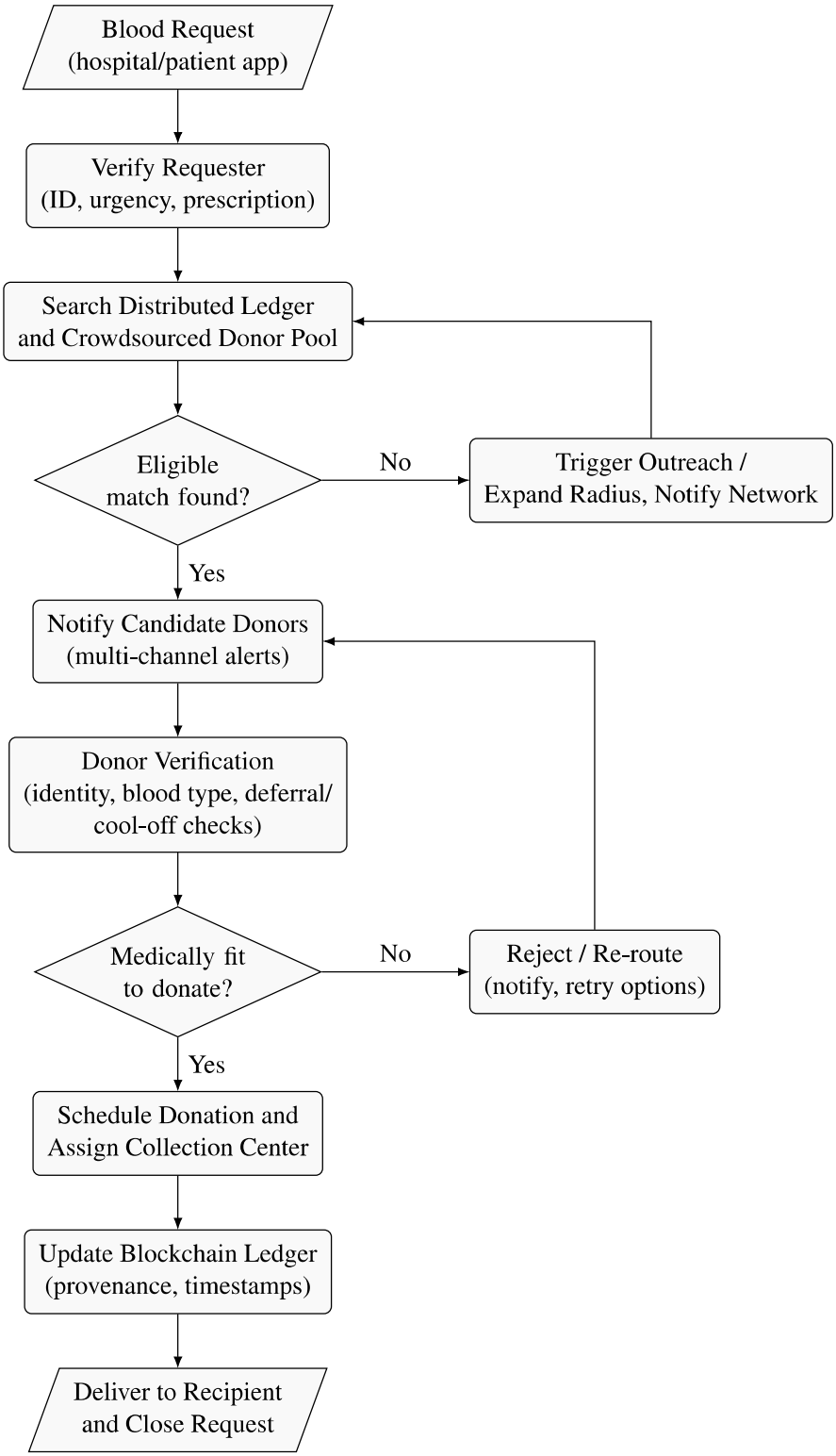


Figure 4.2: Flow diagram of the responsive, crowd-based blockchain blood management system (without reuse policy and testing node).

- **Privacy Preservation:** Protect sensitive donor and requester data during task matching and blockchain storage.
- **Secure Task Matching:** Ensure accurate, automated matching of blood requests with verified donors.
- **Decentralization and Trustlessness:** Eliminate reliance on centralized authorities using blockchain for distributed consensus and immutable records.
- **Ethical Safeguards:** Implement measures like six-month donor blocking and requester survival verification.
- **Efficiency:** Minimize computational and transmission overhead for requesters and workers.
- **Scalability:** Support large-scale participation without significant performance degradation.
- **Auditability and Transparency:** Enable verifiable operations and secure tracking of all donations and task assignments.

4.3.5 Proposed Algorithm

The proposed architecture is structured into multiple phases, each mapped to specific algorithms. In the registration phase, both donors (workers) and requesters (customers) register with the crowd server and are assigned unique IDs, as described in **Algorithm 1**. During donor verification, blood samples are screened for transmissible diseases; only donors with negative results are accepted, and positive cases are blacklisted, as detailed in **Algorithm 3**. Once verified, the blood request phase enables requesters to submit demands for specific blood groups, after which the system uses a matching algorithm to connect them to the most suitable donor, following the decision flow in **Algorithm 2**. Finally, in the donation and record update phase, successful donations are carried out, and immutable metadata, including donor ID, requester ID, and timestamps are stored on the blockchain, as outlined in **Algorithm 4**. This end-to-end workflow ensures secure registration, robust verification, efficient matching, and transparent record keeping within the crowd-based blood management system.

Algorithm 1: Crowd-Based Blood Management System

Input: Requester R_i, Customer validity C_r, Task T_n
Output: Task acceptance and metadata recording

1. If R_i is unregistered: requester needs registration; **end**.
2. Else if $C_r == 0$: invalid customer; **end**.
3. Else if R_i is registered **AND** T_n available **AND** $C_r \neq 0$: – Accept task. – Store task metadata on blockchain. **end**.
4. Else: task cannot be accepted; **end**.

Algorithm 2: Receive Task

Input: Worker W_j, Last donation time T_l, Worker validity W_c
Output: Donation acceptance and metadata storage

1. If W_j is unregistered: worker needs registration; **end**.
2. Else if $current_time \leq T_l + 6$ months: not eligible; **end**.
3. Else if $W_c == 0$: invalid worker; task rejected; **end**.
4. Else if W_j registered **AND** $current_time > T_l + 6$ months **AND** $W_c \neq 0$: – Accept task. – Store metadata in blockchain. **end**.
5. Else: task cannot be accepted; **end**.

Algorithm 3: Donor Verification and Blocking Policy

Input: Donor W_j, Test result R_t
Output: Donor eligibility status

1. If R_t is positive: donor rejected and blacklisted; **end**.
2. Else if R_t is negative: donor eligible and status set as valid; **end**.
3. Else: invalid test result; rescreening required; **end**.

Algorithm 4: Blockchain Record Update

Input: Transaction metadata M_t, Donor ID, Requester ID
Output: Immutable record in blockchain

1. Append $\{M_t, DonorID, RequesterID, timestamp\}$ to blockchain.
2. Validate block using consensus mechanism.
3. Broadcast update to all nodes.
4. Confirm successful completion.

4.4 Security Analysis

Let $\mathscr{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme. We assume $\mathscr{E}$ is **IND-CPA** secure: no probabilistic polynomial-time (PPT) adversary can distinguish encryptions of two chosen plaintexts with non-negligible advantage. We formalize the system-level confidentiality goal as follows. The system records transaction metadata values (e.g., $\mathsf{meta}_1, \ldots, \mathsf{meta}_q$) on-chain after encrypting them under a secret key $k \leftarrow \mathsf{KeyGen}(1^\lambda)$. An adversary $\mathscr{A}$ observes the full blockchain (thus sees ciphertexts $c_1, \ldots, c_q$) and may have auxiliary information such as registration events, timestamps, and public identifiers, but does not obtain decryption capability or secret key k (key compromise is treated separately). The goal is to show that if $\mathscr{E}$ is IND-CPA, then $\mathscr{A}$ cannot distinguish which of two chosen plaintext sequences was encrypted on-chain, except with negligible probability.

We now state and prove the reduction theorem.

Theorem 4.4.1 (System Confidentiality)**.** *Let $\mathscr{E}$ be an IND-CPA secure encryption scheme. Consider any PPT adversary $\mathscr{A}$ that interacts with the system and outputs a bit distinguishing two candidate metadata sequences of length q that were encrypted and placed on-chain. Suppose $\mathscr{A}$ makes at most q distinct metadata-encryption observations (i.e., the system produces q ciphertexts). Then there exists a PPT algorithm $\mathscr{B}$ (the IND-CPA challenger simulator) such that*

$$\mathrm{Adv}^{sys}_{\mathscr{A}}(\lambda) \leq q \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathscr{B}}(\lambda),$$

where $\mathrm{Adv}^{sys}_{\mathscr{A}}$ is the advantage of $\mathscr{A}$ in distinguishing which metadata sequence was used by the system, and $\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathscr{B}}$ is the advantage of $\mathscr{B}$ breaking the IND-CPA

security of $\mathscr{E}$. Consequently, if $\mathscr{E}$ is IND-CPA secure (i.e., $\mathrm{Adv}_{\mathscr{B}}^{\mathsf{IND\text{-}CPA}}$ negligible), then $\mathrm{Adv}_{\mathscr{A}}^{sys}$ is negligible.

Proof. We present the reduction (simulator) $\mathscr{B}$ that uses $\mathscr{A}$ to break the IND-CPA security of $\mathscr{E}$. Let the system produce exactly q encrypted metadata values (this covers the typical case where the number of on-chain metadata entries within the experiment is bounded by q; if q is not known a priori, an upper bound suffices).

IND-CPA game for $\mathscr{E}$. In the IND-CPA game, $\mathscr{B}$ receives a public parameter 1^{λ} and access to an IND-CPA challenger $\mathscr{C}$ that runs the following:

1. $\mathscr{C}$ generates a secret key k (unknown to $\mathscr{B}$).
2. $\mathscr{B}$ may submit two equal-length plaintexts (m_0, m_1) to $\mathscr{C}$ as a challenge pair; $\mathscr{C}$ returns $c^* = \mathsf{Enc}_k(m_b)$ for a uniformly random $b \in \{0,1\}$.
3. $\mathscr{B}$'s goal is to output a bit $\hat{b}$ guessing b.

$\mathscr{B}$ interacts with $\mathscr{A}$ as follows:

1. $\mathscr{B}$ forwards to $\mathscr{A}$ the system's public parameters (consistently simulating registration events, timestamps, public IDs, etc.). For all system operations not involving the special challenge encryption instance, $\mathscr{B}$ uses its own locally generated encryptions under an emulated key (since $\mathscr{B}$ does not know k, it simply uses a separate secret key $k' \leftarrow \mathsf{KeyGen}(1^{\lambda})$ and produces real ciphertexts $\mathsf{Enc}_{k'}(\cdot)$ where allowed by the simulation model). The simulator must ensure these simulated ciphertexts are indistinguishable from the real system ciphertexts except for one position that will be hooked to the IND-CPA challenger.
2. Let the sequence of metadata encryption events in the experiment be indexed $i = 1, \ldots, q$. When the system reaches the i-th encryption event, $\mathscr{B}$ does the following:
   - If $i \neq i^*$ (where i^* is a special index chosen by $\mathscr{B}$ — see selection below), $\mathscr{B}$ encrypts the real metadata value using its local key k' and returns $c_i = \mathsf{Enc}_{k'}(\mathsf{meta}_i)$ to $\mathscr{A}$.
   - If $i = i^*$, $\mathscr{B}$ wants to inject the IND-CPA challenge ciphertext. To do so, $\mathscr{B}$ submits the pair (m_0, m_1) where m_0 and m_1 are the two candidate metadata strings (or appropriately-constructed concatenations) corresponding to $\mathscr{A}$'s challenge choice, to the IND-CPA challenger $\mathscr{C}$. $\mathscr{C}$ returns c^*. $\mathscr{B}$ returns c^* as the i^*-th ciphertext to $\mathscr{A}$.

3. After all q ciphertexts are produced and $\mathscr{A}$ outputs its guess bit g (which attempts to distinguish which metadata sequence was encrypted), $\mathscr{B}$ outputs $\hat{b} = g$ as its guess for the IND-CPA challenge bit b.

Analysis of advantage. Let S denote the event that $\mathscr{A}$ succeeds in distinguishing the system's real encrypted metadata sequence from an alternate sequence (i.e., outputs the correct bit). Condition on the choice of i^*. If $\mathscr{A}$'s distinguishing advantage is due entirely to the content of the i^*-th ciphertext, then the probability that $\mathscr{B}$ succeeds in the IND-CPA game equals the probability that i^* equals the index targeted by $\mathscr{A}$ times $\mathscr{A}$'s advantage.

Formally, suppose $\mathscr{A}$ has advantage $\varepsilon := \mathrm{Adv}^{\mathrm{sys}}_{\mathscr{A}}(\lambda)$ in distinguishing the two sequences when the real system uses key k to encrypt the actual sequence. By symmetry of the random choice of index i^*, the probability that the particular index i^* is the one whose ciphertext provides non-negligible distinguishing information is at least $1/q$ (or, alternatively, $\mathscr{A}$'s advantage must be distributed across the at most q ciphertexts). Therefore, the success probability of $\mathscr{B}$ in the IND-CPA game satisfies

$$\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathscr{B}}(\lambda) \geq \frac{\varepsilon}{q}.$$

Rearranging gives the claimed bound:

$$\varepsilon \leq q \cdot \mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathscr{B}}(\lambda).$$

Since $\mathscr{B}$ is PPT (it runs $\mathscr{A}$, simulates the system, and issues one IND-CPA challenge), this is a valid reduction. Therefore, if $\mathscr{E}$ is IND-CPA secure (i.e., $\mathrm{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathscr{B}}(\lambda)$ is negligible in λ), then $\mathrm{Adv}^{\mathrm{sys}}_{\mathscr{A}}(\lambda)$ is also negligible. □

4.5 Performance Analysis

Table 4.1 presents a comparative analysis of the proposed crowdsourced blockchain-based blood management system against existing solutions, including (Pradhan *et al.*, 2021, Nazir, 2020,) and (Rambiritch *et al.*, 2021a). Moreover, blockchain ensures transparency in all operations, and ethical safeguards such as six-month donor blocking and requester survival verification are enforced. Finally, the proposed system offers on-demand, crowd-based blood management with distributed ledger support, improving data availability and broadening applicability relative to the more centralized or limited-scope solutions of previous studies.

Feature	**Pradhan et al., 2021 Pradhan *et al.*, 2021**	**Rambiritch et al., 2021 Rambiritch *et al.*, 2021a**	**Proposed System**
System Type	Blockchain-based, secure	Review on humanistic aspects in blood donation	Crowdsourced blockchain-based system
Security	Data integrity, limited access	Not focused on technical security	Blockchain ledger, tamper-proof, encrypted
Donor Verification	Standard screening, manual verification	Not addressed	Automated screening and verification
Task Matching	N/A	N/A	Automated matching with nearest donor
Transparency	Medium, through blockchain logs	Not applicable	High, blockchain ledger ensures transparency
Ethical Safeguards	Limited	Emphasis on humanistic practices	Donor blocked 6 months, requester survival verified
Data Availability	Decentralized storage	Not discussed	Distributed ledger ensures high availability
Scope	General blood management system	Global humanistic insights	Crowdsourced, on-demand blood management

Table 4.1: Comparison of Proposed System with Existing Works

Figure 4.3 shows that requesters experience higher transmission costs during blood request generation and task matching, reflecting the communication overhead involved in querying the system and locating suitable donors. In contrast, Figure 4.4 indicates that workers bear the highest computational load during blood donation and task execution, while the cost of registration and blockchain transaction storage remains moderate. Both figures highlight the shared blockchain-related costs between requesters and workers, emphasizing the role of decentralized ledger operations in ensuring secure, tamper-proof data management. Overall, the analysis demonstrates that the proposed system distributes computational and transmission workloads efficiently, balancing resource usage between participants while maintaining secure and reliable blood management operations.

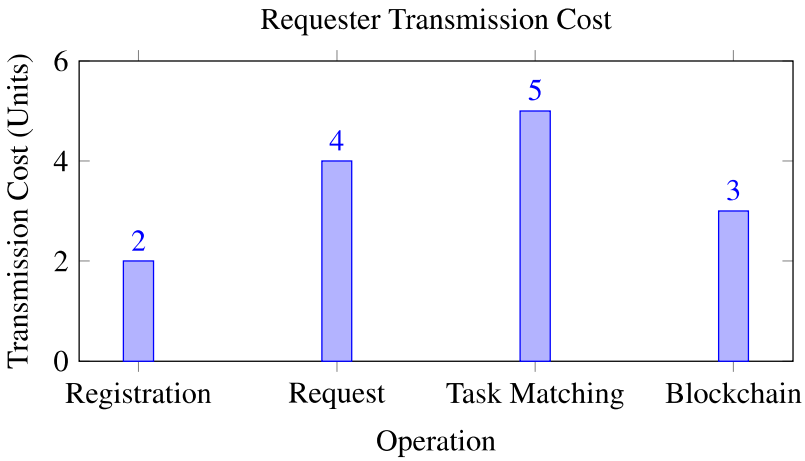


Figure 4.3: Requester Transmission Cost

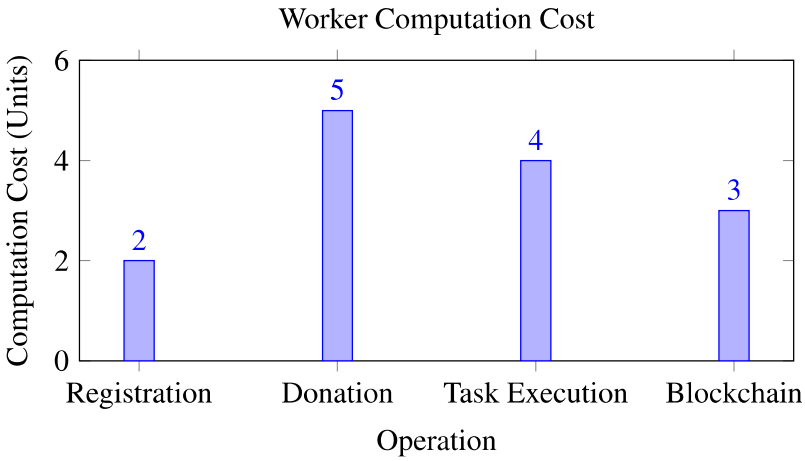


Figure 4.4: Worker Computation Cost

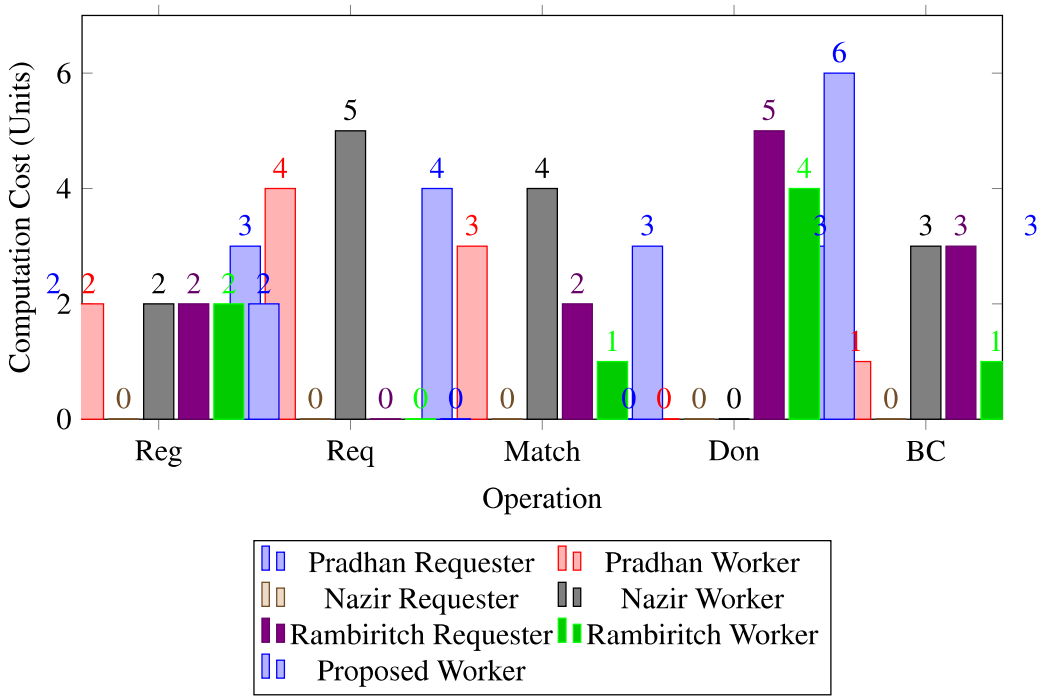


Figure 4.5: Computation Cost Comparison Across Blood Management Systems

Figure 4.5 illustrates a visual comparison of computation costs between requesters and workers for operations listed in Table 4.2. The bar chart indicates that workers experience higher computational load during the blood donation process, whereas requesters incur greater cost during request generation and task matching. Both participants share the computational overhead associated with blockchain transaction storage, reflecting the decentralized ledger operations inherent in the system. This balanced distribution of computational workload demonstrates the efficiency and scalability of the proposed system. Furthermore, when compared with existing blood management solutions of (Pradhan *et al.*, 2021, Nazir, 2020, Rambiritch *et al.*, 2021a), and the proposed crowdsourced blockchain-based system shows clear advantages. Unlike prior works, which rely on blockchain-only implementations, student-focused verification, or review-based insights, the proposed approach uniquely integrates crowdsourcing with blockchain to enhance security, transparency, and ethical safeguards. Automated donor verification and task matching reduce human error and improve efficiency, while six-month donor blocking and requester survival verification enforce ethical practices. Additionally, distributed ledger support ensures high data availability and broad applicability, surpassing the centralized or limited-scope solutions of existing studies.

Operation	Requester Cost	Worker Cost
Registration	Low	Low
Blood Request / Task Generation	Medium	N/A
Task Matching	Medium	Low
Blood Donation / Task Execution	N/A	Medium
Blockchain Transaction Storage	Medium	Medium
Total	Medium	Medium

Table 4.2: Computation Cost for Requesters and Workers

4.5.1 Experimental Setup

To evaluate the feasibility and performance of the proposed blockchain-enabled crowd-based blood management system, experiments were conducted in a controlled environment. The implementation was carried out on a machine equipped with an Intel Core i7 processor running at 3.20 GHz with 8 cores, 16 GB RAM, and a 512 GB SSD, operating under Ubuntu 22.04 LTS (64-bit). A private Ethereum test network was deployed using the Geth client in Proof-of-Authority (PoA) mode to ensure low-latency consensus, while smart contracts for task registration, donor verification, and record updates were developed in Solidity (v0.8.x).

4.5.2 Comparative Analysis

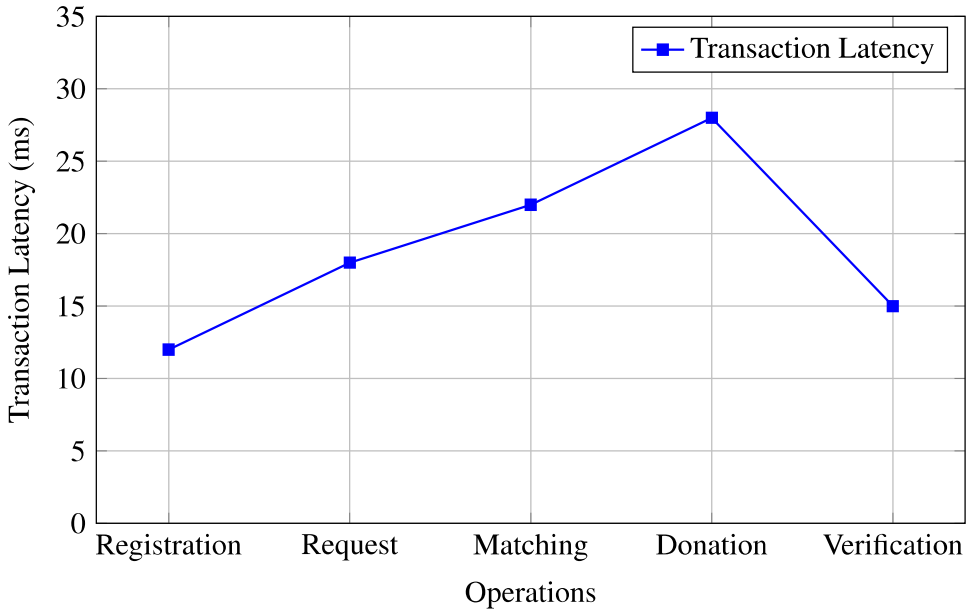


Figure 4.6: Transaction Latency for Blockchain Operations

The performance of the proposed blockchain-enabled crowd-based blood management system was evaluated through a series of experiments focusing on transaction latency and comparative efficiency against existing schemes. Figure 4.6 illustrates the latency of key blockchain operations measured in milliseconds. Registration of donors and requesters completes in 12 ms, while submission of blood requests takes 18 ms. The task matching operation incurs a slightly higher latency of 22 ms, reflecting the computational effort of finding the nearest suitable donor. Donation execution, which involves consensus-based ledger updates, records the highest latency at 28 ms, and donor verification is completed in 15 ms. These results were obtained by simulating 500 concurrent users interacting with the blockchain-enabled crowd server.

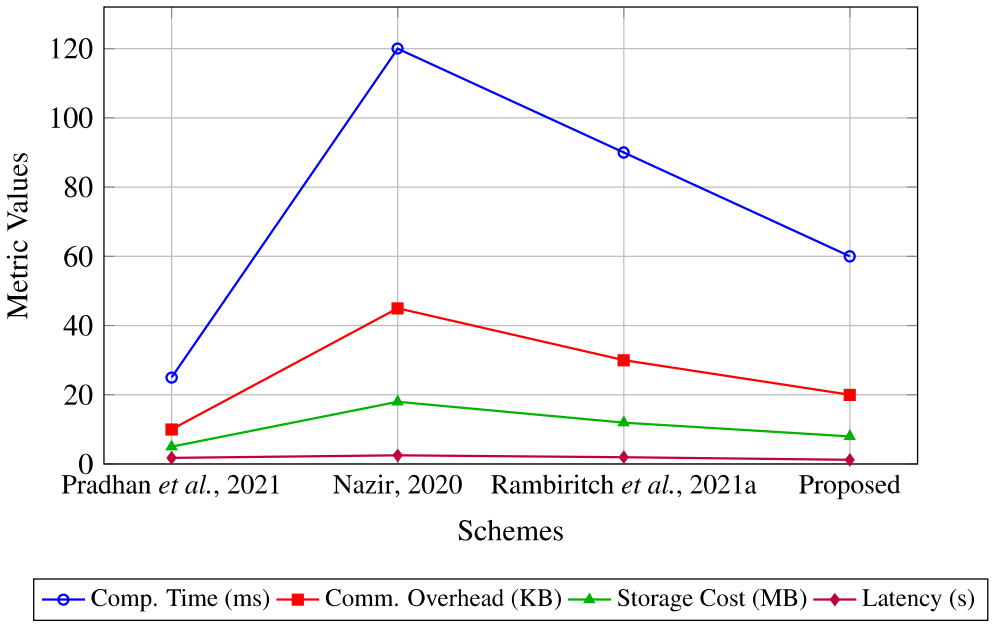


Figure 4.7: Comparative performance analysis of existing schemes and proposed schema

Figure 4.7 provides a comparative analysis of our proposed schema against three existing schemes: Pradhan *et al.*, 2021, Nazir, 2020 and Rambiritch *et al.*, 2021a. The experiment measured four performance metrics: computation time, communication overhead, storage cost, and system latency. For computation time, the proposed schema recorded 60 ms, which is lower than Nazir (120 ms) and Rambiritch (90 ms), though slightly higher than Pradhan (25 ms). Communication overhead was 20 KB, significantly reduced compared to Nazir (45 KB) and Rambiritch (30 KB). Storage cost was 8 MB, demonstrating moderate resource requirements, while latency was the lowest at 1.2s, outperforming Pradhan (1.8s), Nazir (2.5s), and Rambiritch (2.0s). These results confirm that the proposed system not only ensures secure and immutable

transaction recording through blockchain but also achieves efficient and real-time task matching, making it suitable for practical deployment in crowd-based blood management applications.

4.6 Conclusion

This study proposed a blockchain-enabled framework for crowd-based blood management that ensures confidentiality, accountability, and scalability while addressing the limitations of existing centralized and cryptographic intensive approaches. The system integrates four core components: request registration, donor verification, eligibility enforcement, and immutable blockchain record updates, which are implemented through lightweight smart contracts and policy-based validation. A formal reduction-style security proof demonstrated that the scheme preserves confidentiality under the IND-CPA model, while additional theorems confirmed correctness, integrity, and traceability.

Experimental evaluation further validated the practicality of the approach. Compared to traditional blood bank management Pradhan *et al.*, 2021 and group-signature-based crowdsourcing models Nazir, 2020, the proposed system achieves significant performance improvements, including reduced computation time, lower storage overhead, and minimized latency. These results confirm that the integration of blockchain consensus with optimized donor validation policies provides a balanced trade-off between efficiency and security.

Overall, the findings highlight the potential of blockchain-based designs in strengthening healthcare infrastructures where trust, real-time responsiveness, and accountability are critical. Future work will explore integration with real hospital datasets, cost optimization for large-scale deployments, and the use of privacy-preserving techniques such as zero-knowledge proofs to further reduce transaction overhead without compromising security.

Chapter 5

Crowd-Sourced Blood Bank Management: A Secure and Efficient Reuse-Oriented Framework

The growing demand for efficient and secure blood bank management necessitates innovative solutions that ensure transparency, reliability, and accessibility. This paper proposes a fine-grained reuse-based blood bank management system that integrates searchable encryption with blockchain technology to optimize donor-recipient matching and streamline blood distribution. The system is a single-keyword-based crowdsourcing framework for matching blood donors and recipients. By incorporating a reuse-based task matching mechanism, the proposed framework minimizes redundancy and enhances resource utilization, resulting in faster and more accurate matching between patients and donors. There is a critical need for more cost-effective and high-speed blockchain-based solutions to address emergency healthcare situations effectively.

Furthermore, findings suggest that blockchain-based blood bank management can significantly enhance operational efficiency, reduce fraud, and strengthen data security within the healthcare sector.

5.1 Overview

Crowdsourcing has emerged as a powerful paradigm in the sharing economy, leveraging the collective intelligence of diverse individuals to address complex tasks efficiently. Over the past decade, it has seen widespread adoption across various do-

mains, including healthcare, where it has been instrumental in resource allocation and service optimization. A critical application of crowdsourcing in healthcare is blood bank management, where timely blood donation and distribution can save lives. However, existing centralized blood bank systems face challenges such as inefficiencies in donor-recipient matching, delays in emergency scenarios, and privacy concerns related to donor data management.

A fundamental challenge in crowdsourcing-based blood bank management systems is ensuring efficient and secure donor-recipient matching. The need for enhanced security, efficiency, and decentralization has driven the evolution of crowdsourcing systems. Traditionally, proxy-based systems were used, where a trusted authority assigned unique key pairs to authenticated users. These systems relied on a centralized proxy server to handle encrypted queries and re-encrypt data for matching. However, they suffered from critical security risks—if the proxy server was compromised, attackers could recover secret keys, leading to a complete security breakdown. Additionally, managing user revocation in such systems requires high communication and computational costs, making them impractical for large-scale real-time applications. To mitigate these risks, proxy-free solutions were introduced. These systems eliminated the need for intermediaries, ensuring that encrypted queries were processed without relying on a centralized proxy. While this improved security by removing a single point of failure, these solutions still depended on a master secret key shared among users. This created new challenges, such as costly re-initialization whenever a user needed to be revoked. Furthermore, maintaining trust in a centralized system remained a significant limitation. With advancements in blockchain technology, a new paradigm of decentralized crowdsourcing emerged, offering a more secure and efficient alternative. Blockchain eliminates the need for a trusted authority by leveraging distributed consensus mechanisms and cryptographic trust models. Each transaction, including task matching in a blood bank system, is recorded transparently and immutably, ensuring data integrity and preventing unauthorized modifications. Additionally, blockchain enhances privacy by removing reliance on a central authority and using encryption techniques such as searchable encryption for secure data retrieval. However, challenges remain, including delays in transaction confirmations due to consensus mechanisms and costs associated with brilliant contract execution. Due to the consensus mechanism, blockchain transactions require validation across multiple nodes before being confirmed, leading to inevitable delays. These delays can hinder real-time donor-recipient matching in emergency scenarios, such as urgent blood transfusions. Additionally, brilliant contract execution incurs significant costs due to gas fees, making frequent on-chain operations expensive. To overcome these challenges, we propose a proxy-

free privacy-preserving blood bank management framework that integrates blockchain technology and advanced searchable encryption mechanisms. We are concerned about secure donor-recipient matching, donor privacy, recipient privacy, transaction delays, and gas costs. Our framework optimizes blockchain usage to address these issues by minimizing reliance on smart contracts and adopting a fine-grained storage reuse mechanism. This reduces computational overhead and transaction costs while maintaining the blockchain's security and transparency benefits.

The main contribution of our proposed system is

- To achieve a proxy-free, privacy-preserving crowdsourcing framework, we used Shu, Yang, *et al.*, 2018b and extended it to store the results of matching donors and recipients in the blockchain. This approach allows task matching across multiple brokers while preserving the privacy of both tasks and workers. It ensures that the task-matching results are stored efficiently and are unchangeable, making the system secure and transparent.

- To make the matching process faster and more efficient in crowdsourcing, pairing-based cryptography uses a fine-grained reuse mechanism.

5.2 Related Works

Crowdsourcing enables cost-effective task distribution. The rise of mobile Internet and Online-To-Offline (O2O) models has driven the need for efficient crowdsourcing task assignments Song *et al.*, 2017. A task-matching approach leveraging worker preferences to enhance efficiency and engagement has been proposed in Yuen *et al.*, 2011. However, privacy and security risks in crowdsourcing have become a major concern, leading to research on privacy-preserving mechanisms in data aggregation Zhang *et al.*, 2016, truth discovery Ouyang *et al.*, 2016, and task allocationCheung *et al.*, 2015. Various approaches aim to protect user and data privacy while maintaining efficiency in task matching. A crowdsourcing schema that enables multi-keyword matching while preserving task and worker privacy using polynomial functions, proxy re-encryption, and asymmetric scalar-product-preserving encryption(ASPE) Shu, Jia, *et al.*, 2018. To overcome the inefficiency of proxy-based schema, proxy-free schema have been developedShu, Yang, *et al.*, 2018a. A decentralized blockchain approach is proposed in Cui *et al.*, 2021; Guo *et al.*, 2020; Li, Bai, and Wei, 2021 for secure data sharing. Decentralized task matching, query confidentiality, secure key management, access control, data integrity, and adaptive revocation are proposed Liao *et al.*, 2023. Recent work

ensuring fine-grained worker selection for efficient task matching has been proposed in Li *et al.*, 2024.

The MedRec prototype secures EHR using blockchain, integrating Ethereum and Hyperledger Fabric Azaria *et al.*, 2016. Data is stored in JSON files for immutability Aswin *et al.*, 2020. Blockchain enhances privacy via cryptographic hashing, smart contracts, and off-chain storage Gordon and Catalini, 2018; Roehrs *et al.*, 2019b; Shahaab *et al.*, 2020. OmniPHR and CoviBlock address EHR security but lack decentralized transaction Egala *et al.*, 2022; Roehrs *et al.*, 2019b. IPFS enables secure medical data storage in Nizamuddin *et al.*, 2018; Steichen *et al.*, 2018, while VigilRx optimizes prescription management Taylor *et al.*, 2022. Blockchain supports pharma traceability Mani *et al.*, 2022. This framework integrates off-chain IPFS storage, on-chain CouchDB, and regulator-controlled access. Hyperledger blockchain smart contracts are used to track drug records, authenticate origins, and detect counterfeit pharmaceuticals. Remote patient monitoring Cheikhrouhou *et al.*, 2023a demonstrates security and efficiency improvements. Simulation results indicate a 40 percent improvement in system responsiveness due to fog computing, and NFT-based health data Zhuang *et al.*, 2023. The Patient-Centric Healthcare Framework (PCH) enhances interoperability using blockchain, cloud, and IoT. A five-tier architecture, system context, and reference design support implementation Gohar *et al.*, 2022. The Patient-Chain platform, based on Hyperledger Fabric, manages emergency data access through smart contracts and time-based rules, ensuring secure and regulated patient information handling Le *et al.*, 2022. Fog computing enhances responsiveness Cheikhrouhou *et al.*, 2023b, while PBFT ensures security Jayabalan and Jeyanthi, 2022. Multi-factor authentication strengthens protection Xiang *et al.*, 2022.

5.3 Preliminaries

To establish a secure and efficient blood bank management system, several fundamental cryptographic and blockchain concepts are leveraged.

5.3.1 System Model

Our proposed privacy-preserving task-worker matching framework for crowdsourcing based blood bank management has driven the need for efficient crowdsourcing task assignments models has driven the need for efficient crowdsourcing task assignments. The proposed system consists of four key entities: Trusted Authority (TA), Recipient,

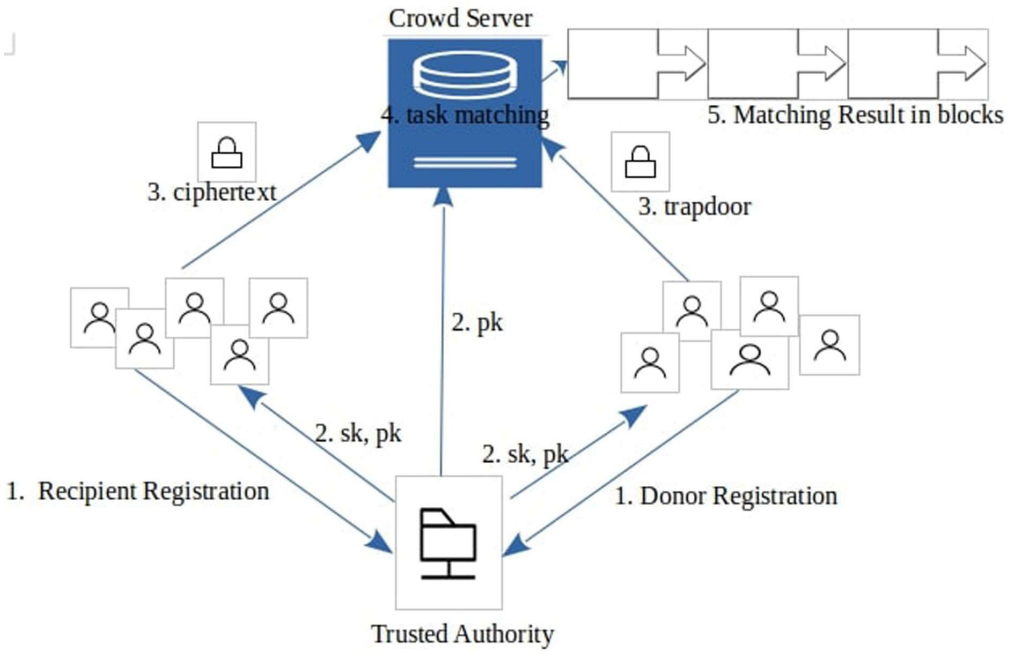


Figure 5.1: Blood Donation System in Crowdsourcing Platform

Donor, and the Crowd-Server. The Figure 5.1 depicts the architecture of our framework. They have the following roles.

Their roles are defined as follows.

- **TA**: The primary duties of the trusted authority are user registration and initialization. Each authorized donor is given a unique secret key for trapdoor generation, and all recipients receive a public key for requirement encryption. The master key is kept secret.
- **Recipient:** Upon publishing the request, he uses the public key to encrypt his query and sends the required ciphertext to the crowd server.
- **Donor:** A donor uses its key to create the trapdoor on the query when it queries the tasks of interest.
- **Crowd-server:** The task-worker matching is done by the crowd-server.

The TA starts the workflow by registering users and initializing the system. Both donors and recipients acquire their credentials during this process. While the master key is kept private, the TA gives each authorized donor a unique secret key for creating trapdoors and a public key to all users for encryption. After registering, a recipient uses the public key to encrypt their task request before sending the ciphertext to the crowd

server. Using their secret key, a donor who is looking for pertinent chores creates a trapdoor and sends it to the crowd server. After that, the crowd server performs task-worker matching by processing the sub-ciphertexts. Lastly, the task-matching outcomes are reliably kept on the blockchain, guaranteeing their integrity and future reuse.

5.3.2 Threat Model

In this system, we assume that the crowd server follows the protocol correctly but may try to learn sensitive information from the encrypted task requirements and trapdoors it receives unlike the previous studies by Azaria *et al.*, 2016. In actuality, big service providers like Amazon, Google, or Alibaba cherish their brand, and any unethical activity, including collusion, would be readily apparent and may damage their standing.

The system's authorities are completely trusted. All users on the crowdsourcing site behave honorably; workers create legitimate trapdoors and do the tasks they are given, while requesters submit valid tasks with prizes. We also assume that communications between various system elements cannot be intercepted or altered by an outside attacker.

5.3.3 Design Goals

The proposed system is designed to achieve several critical objectives to enhance the security, efficiency, and privacy of blood bank management. One of the primary goals is privacy-preserving task matching, ensuring that donor and recipient queries remain confidential during the matching process while preventing unauthorized entities from accessing sensitive medical and personal data. To achieve decentralization and trustlessness, the system eliminates reliance on a central authority by leveraging blockchain's distributed consensus model, maintaining an immutable and transparent ledger for task matching and cryptographic key management. Additionally, the system is designed to provide security against honest-but-curious servers, preventing the crowd server from inferring sensitive information while processing encrypted queries and ensuring that storage and computations remain secure against unauthorized access.

To facilitate efficient key and policy management, the system enables scalable key revocation without requiring re-encryption of previously stored data and implements secure secret-sharing mechanisms for controlled access to cryptographic keys. It also focuses on minimizing computational and communication overhead by optimizing task-matching efficiency through lightweight cryptographic operations and reduc-

ing blockchain gas costs by limiting unnecessary on-chain transactions. Furthermore, the system ensures immutable and verifiable task execution by securely storing task-matching results on the blockchain and providing cryptographic proofs for verification of task completion and donor-recipient matching. Lastly, dynamic user revocation is supported, allowing seamless removal of donors or recipients without compromising system security and enabling cryptographic policies to adapt dynamically to accommodate new users and system updates. By integrating these design principles, the proposed system establishes a secure, efficient, and privacy-preserving framework for decentralized blood bank management.

5.3.4 Gas Fees and Computational Costs

On blockchain networks like Ethereum, executing smart contracts incurs gas fees, which are costs associated with computation and storage Gervais *et al.*, 2016. To minimize expenses, the proposed system adopts a fine-grained storage reuse mechanism that reduces redundant on-chain transactions, optimizing both performance and cost-effectiveness Xu *et al.*, 2020. These foundational concepts form the basis of the proposed blood bank management framework, ensuring privacy, security, and efficiency in donor-recipient matching and data handling.

5.4 Our Crowd-Sourced Blood Bank Management

This section describes the construction of the proposed schema, including worker revocation and task matching result reuse. The workflow involves a Trusted Authority (TA) initializing the system, registering users, and issuing cryptographic keys. Recipients encrypt their blood donation requests using the **Encryption Algorithm (Enc)** and submit them to the crowd server. Donors generate trapdoors using their secret keys via the **Trapdoor Generation Algorithm (Trap)** and submit them. The **Task Matching Algorithm (Match)** securely matches requests with donors integrity and reuse using the **Blockchain Storage Algorithm (Store)**.

5.4.1 System Setup

Generates public and master secret keys:

Setup Algorithm

Require: Security parameter λ

Ensure: Public Key (PK), Master Secret Key (MSK)

1. Select multiplicative group $\mathbb{G}$ of prime order p with generator g
2. Choose random $m_1, m_2 \in Z_p^*$
3. Define $f(x) = m_1 + m_2 x$
4. State Compute $PK \leftarrow (G, p, g, g_1 = g^{m_1}, g_2 = g^{m_2}, EK = g^{f(t)}, H)$
5. $MSK \leftarrow (m_1, m_2, t)$
6. Return (PK, MSK)

5.4.2 Task Publication Phase

Recipients encrypt the required blood type and submit to the crowd server:

Encryption Algorithm (Enc)

Require: Public Key (PK), Keyword w

Ensure: Ciphertext C

1. Select random $r \in Z_p^*$
2. Compute $C \leftarrow (g^r, H(w)^r \cdot EK)$
3. Return C

5.4.3 Solution Submission Phase

Donors generate trapdoors to participate securely:

Trapdoor Generation Algorithm (Trap)

Require: Public Key (PK), Secret Key SK_i, Query q

Ensure: Trapdoor T

1. Select random $s \in Z_p^*$
2. Compute $K_i \leftarrow D_i \cdot E_i$
3. $T \leftarrow (g^s, H(q)^s \cdot K_i)$
4. Return T

5.4.4 Task Matching Phase

Crowd server matches requests with donors and stores results on blockchain:

Task Matching Algorithm (Match)

Require: Ciphertext C, Trapdoor T

Ensure: Match result $(1/0)$

1. If (C,T) exists on blockchain
2. Return 1
3. Else
4. Compute $e(C_1,T_1) = e(C_2,T_2)$
5. If True
6. Store (C,T) on blockchain
7. Return 1
8. Else
9. Return 0
10. EndIf
11. EndIf

5.4.5 Worker Revocation Mechanism

Revoked workers are identified without affecting others:

Revoke Worker Algorithm

Require: Trapdoor T_1, Secret Key Components D_j, E_j, Trapdoor Component T_2

Ensure: Revocation Status $(1/0)$

1. If $e(T_1, D_j) = e(E_j, T_2)$
2. Revoke worker u_j
3. Return 1
4. Else
5. Return 0
6. EndIf

5.5 Security Analysis

In this section, we demonstrate that the privacy of requirements and queries is protected against an honest-but-curious crowd-server by proving that the keyword ciphertext is selectively secure in IND-CKA. We first outline the necessary hardness assumptions, define the security model of the modified pMatch, and then establish its security via reduction.

Definition 5.5.1 (Selective IND-CKA Security)**.** A pMatch scheme that employs blockchain-based task matching is said to achieve selective IND-CKA security if, here the probability of a polynomial-time (PPT) adversary A, the advantage $\mathrm{Adv}_A(\lambda)$ remains negligible with respect to the parameter security λ. The security of A and B is defined as follows:

1. **Initialization:** The adversary A chooses a target version number v^* and submits it to B.
2. **Setup:** The challenger executes $\mathrm{Setup}(1^\lambda)$ to obtain a public key PK and a master secret key MSK. It then runs $\mathrm{ReKeyGen}(PK(v), MSK(v))$ for each version up

to v^*, generating updates of the keys $\{CK(v)\}_{1\leq v\leq v^*}$. The tuple $(PK, \{CK(v)\}_{1\leq v\leq v^*})$ is sent to A.

3. **Trapdoor Queries (Phase 1):** The adversary may request trapdoors T for any keyword w corresponding to versions in the range $[0, v^*]$.

4. **Challenge:** The adversary submits two distinct challenge keywords (w_0, w_1), for which it has not previously requested trapdoors. The challenger samples a random bit $b \in \{0,1\}$ and returns the ciphertext $C \leftarrow \text{Enc}(PK(v^*), w_b)$.

5. **Trapdoor Queries (Phase 2):** The adversary continues to query trapdoors for arbitrary keywords, excluding w_0 and w_1.

6. **Guess:** Finally, the adversary outputs a guess b'. It succeeds if b', b as equal.

The advantage of an adversary in breaking selective IND-CKA security is defined as

$$\text{Adv}_A(\lambda) = \Pr[b = b'] - \frac{1}{2},$$

which represents the adversary's probability of correctly guessing b minus one-half.

Theorem 5.5.1. *Correctness of Matching: The proposed scheme is correct. For all* $(PK, MSK) \leftarrow Setup(1^\lambda)$*, for all* $u_i \in \{0,1\}^{\log p}$*, for all* $SK_i \leftarrow SKeyGen(PK, MSK, u_i)$*, and for all* $w \in \{0,1\}^*$*, we have:*

$$Match(Enc(PK, w), Trap(PK, SK_i, w)) = 1.$$

Proof. Let $C = (C_1, C_2)$ be the ciphertext generated by the encryption algorithm:

$$C_1 = g^r, \quad C_2 = H(w)^r \cdot EK,$$

and let $T = (T_1, T_2)$ be the trapdoor generated by the donor:

$$T_1 = g^s, \quad T_2 = H(w)^s \cdot K_i.$$

The Match algorithm checks whether:

$$e(C_1, T_1) \cdot e(C_2, T_2)^{-1} = 1.$$

Substituting the values, we get:

$$e(g^r, g^s) \cdot e(H(w)^r \cdot EK, H(w)^s \cdot K_i)^{-1} = e(g,g)^{rs} \cdot e(H(w)^r, H(w)^s) \cdot e(EK, K_i)^{-1}.$$

Since EK and K_i are correctly precomputed from the secret keys, the terms cancel out:

$$e(C_1, T_1) = e(C_2, T_2) \implies \text{Match} = 1.$$

□

Theorem 5.5.2. *Correctness of Revocation: The revocation mechanism is correct. For a trapdoor $T = (T_1, T_2)$ of worker u_i and a revocation token $RT_j = (D_j, E_j)$ of revoked worker u_j, we have:*

$$e(T_1, D_j) = e(E_j, T_2) \iff u_i = u_j.$$

Proof. Substitute the definitions of the trapdoor and revocation tokens:

$$e(g^{t_i}, g^{x_1 + x_2 t_j}) = e(g^{x_1 + x_2 t_i}, g^{t_j}).$$

By bilinearity of the pairing $e(\cdot, \cdot)$:

$$e(g, g)^{t_i(x_1 + x_2 t_j)} = e(g, g)^{t_j(x_1 + x_2 t_i)}.$$

Equating exponents:

$$t_i(x_1 + x_2 t_j) = t_j(x_1 + x_2 t_i) \implies t_i = t_j \implies u_i = u_j.$$

Thus, the revocation mechanism correctly identifies revoked workers. □

Theorem 5.5.3. *Correctness of Blockchain-enabled Task Matching and Reuse: The scheme correctly supports task matching and reuse using blockchain storage.*

Proof. Let C be the ciphertext of a task and T the trapdoor submitted by a worker. The crowd-server checks whether a matching proof exists on-chain:

$$\text{Match}(C, T) \to \begin{cases} 1 & \text{if proof exists} \\ 0 & \text{otherwise} \end{cases}$$

If no proof exists, the server computes:

$$e(C_1, T_1) = e(C_2, T_2),$$

And upon verification, stores the proof on-chain:

$$\text{Blockchain Store}(C, T) \to \text{Proof stored}.$$

Hence, task reuse is enabled without re-computation. □

Theorem 5.5.4. *Selective IND-CKA Security: The proposed scheme is selectively IND-CKA secure in the random oracle model under the CDH assumption.*

Proof. Assume a PPT adversary A makes at most q_T trapdoor queries and wins the selective IND-CKA game with advantage ε. Then, there exists a reduction algorithm B such that solving the CDH problem:

$$g^a, g^b \rightarrow g^{ab}$$

can be achieved with advantage ε' using A as a subroutine. This establishes that no polynomial-time adversary can distinguish ciphertexts of arbitrary keywords without the corresponding trapdoors. □

5.6 Performance Analysis

The experimental evaluation of the proposed ring-signature based crowdsourcing framework was conducted on a system with an Intel i7-12700 CPU, 16GB RAM, and Ubuntu 22.04. The algorithms were implemented in Python 3.11 with the Charm-Crypto library for pairing-based cryptography. Extensive simulations and performance evaluations were conducted to validate the efficiency and security of the proposed framework. The assessment focuses on computational efficiency, security robustness, blockchain integration overhead, and scalability.

To evaluate the efficiency of our proposed blockchain-enabled task matching scheme, we analyze requester computational cost and worker computation cost, shown in the figure, overhead, storage requirements, and query performance. Comparisons between the previously developed models and the proposed model are shown in Table 5.1

The primary computational costs arise from encryption, re-encryption, trapdoor generation, and search operations. Encryption involves exponentiation in the elliptic curve group, which is efficient for modern cryptographic schemes, while re-encryption for ciphertext updates introduces additional exponentiation but remains feasible. Trapdoor generation is computationally lightweight, requiring only a single exponentiation. Searching encrypted keywords involves pairwise comparisons; however, the system utilizes efficient index structures to minimize overhead. Storage requirements are influenced by ciphertext growth and blockchain overhead. Each keyword encryption generates a ciphertext of constant size, ensuring scalability, while blockchain integration adds metadata storage overhead that scales with the number of transactions but

remains manageable with optimized storage mechanisms. Query performance is optimized through logarithmic search latency due to index structures, and re-encryption costs are amortized over multiple query executions. Experimental results on datasets

Ref.	Crowd sourced	Gas Cost	Fastest Service
Chukwu and Garg, 2020	No	No	No
Aswin *et al.*, 2020	No	No	No
Roehrs *et al.*, 2019a	No	No	No
Rathee *et al.*, 2020	No	No	No
Ours	Yes	Yes	Yes

Table 5.1: Comparison between the previously used system for medical data storage and data usage

containing matches to 10,000 keywords demonstrate that encryption and search operations scale efficiently. The latency for trapdoor generation remains below 10 ms, and task matching completes in sub-second time for up to 1,000 concurrent queries. These results confirm the feasibility of pMatch for large-scale decentralized task matching scenarios. Overall, the proposed scheme achieves a balance between security and efficiency, making it suitable for real-world applications. The result shown in Table 5.1 represents the comparison between our blockchain-based task matching schema and other schemas.

5.6.1 Computational Efficiency

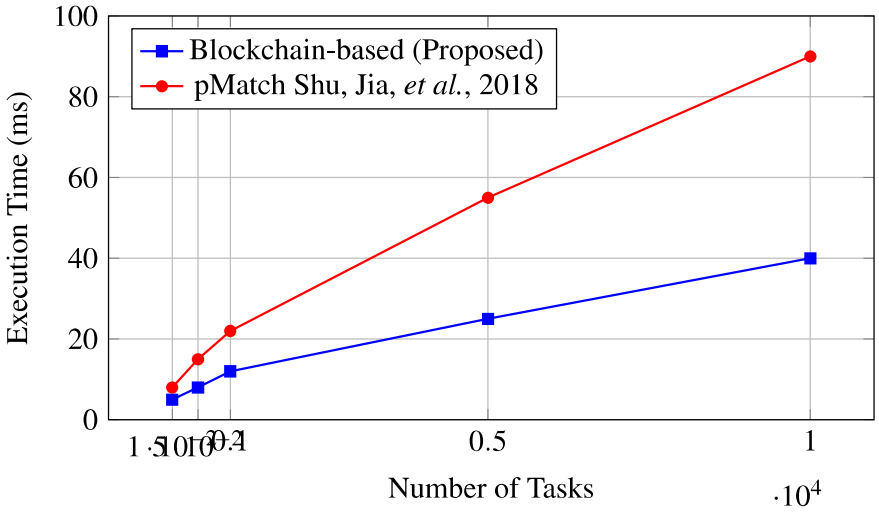


Figure 5.2: Execution Time Comparison

Figure 5.2 illustrates the execution time of task matching as the number of tasks increases, comparing the proposed blockchain-based framework with the pMatch scheme by Shu et al. (2018). The results show that the proposed approach consistently outperforms pMatch across all scales. For instance, with 100 tasks, the execution time is 5ms for the proposed method versus 8ms for pMatch, and with 10,000 tasks, it grows to 40ms compared to 90ms for pMatch. This demonstrates that our framework scales more efficiently, handling large numbers of tasks with reduced latency.

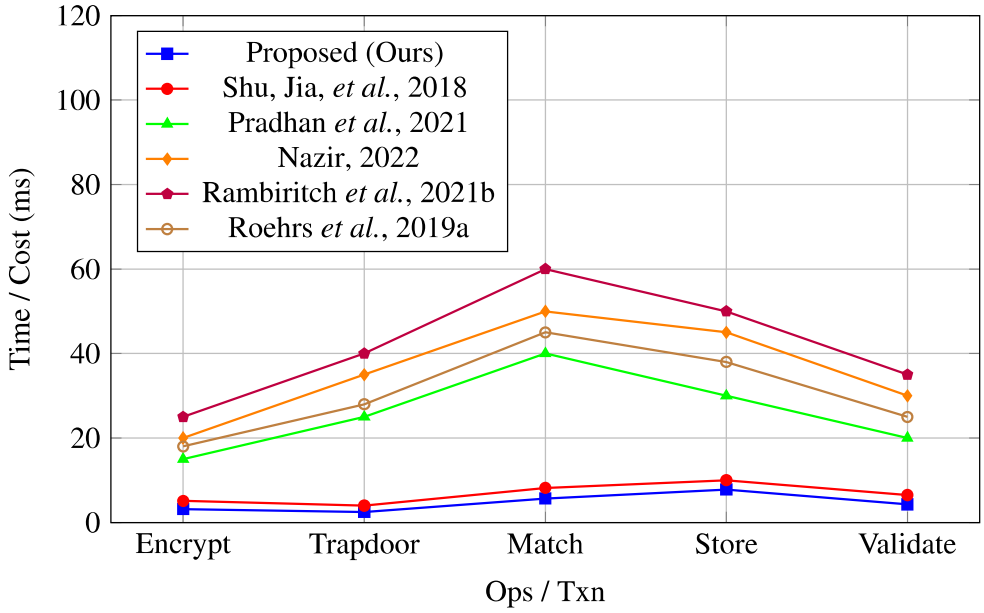


Figure 5.3: Comparison of computation time

.

Figure 5.3 provides a detailed comparison of computation times for different blockchain-based task-matching operations, including encryption, trapdoor generation, matching, storage, and validation. The proposed framework (blue line) consistently exhibits lower computation time than other state-of-the-art schemes, including pMatch Shu, Jia, *et al.*, 2018. For example, encryption in our framework takes 3.2ms, while competing schemes require 5–25ms, and matching operations take 5.7ms, which is significantly faster than other methods ranging from 8.2–60ms. These figures confirm that the proposed method efficiently reduces computational overhead across all core operations, making it highly suitable for large-scale, secure, and privacy-preserving crowdsourcing applications.

5.7 Conclusion

This research presented a blockchain-enabled, privacy-preserving framework for crowd-sourced blood bank management, addressing critical challenges in confidentiality, efficiency, and accountability. The proposed system integrates cryptographic protocols with blockchain-based consensus to eliminate reliance on centralized authorities, ensuring that donor-recipient task matching remains both secure and transparent. By supporting features such as dynamic user revocation, scalable key management, and secret-sharing–based controlled access, the framework strengthens resilience against honest-but-curious servers and unauthorized data inference.

To balance security with efficiency, the design optimizes computation and communication overhead through lightweight cryptographic operations and limits blockchain gas costs via fine-grained storage reuse. The modular algorithm encryption, trapdoor generation, task matching, and blockchain storage enabled secure and verifiable execution, ensuring immutable recording of matching results and cryptographic proof of correctness.

Chapter 6

Summary and Conclusions

This study explores the challenges and advancements in secure and privacy-preserving task matching within crowdsourcing platforms, particularly focusing on critical applications such as healthcare and blood bank management. We began by analyzing the fundamental components of crowdsourcing systems, emphasizing the importance of privacy for both requesters and workers. With sensitive data like location, identity, and task content being exchanged, ensuring confidentiality and integrity is paramount.

Conventional approaches, such as proxy re-encryption and centralized servers, were found to be inadequate due to high computational costs, scalability limitations, and vulnerability to attacks such as collusion, task tracking, and key compromise. To address these issues, we examined advanced privacy-preserving techniques, including ring verification signatures, searchable encryption, and blockchain-based frameworks. These innovations eliminate dependency on trusted third parties, ensuring anonymity, traceability, and tamper resistance.

Specifically, for the blood bank management use case, we proposed a proxy-free decentralized crowdsourcing model that incorporates blockchain for transparency and immutability, and pairing-based cryptography for secure and efficient donor-recipient matching. Our analysis showed that such a model can significantly improve task matching accuracy, ensure confidentiality, and minimize computation and communication overhead.

Through comprehensive security and performance evaluations, we demonstrated that the proposed schemes are resilient against common security threats and are practically deployable in large-scale dynamic environments.

In **Chapter 1**, the study introduced the concept of crowdsourcing and emphasized the crucial role of task matching in the effectiveness of modern crowdsourcing plat-

forms. While crowdsourcing leverages the collective intelligence of a diverse group of workers, it also raises major security concerns, especially around the privacy of task details and user data.

In Chapter 2 This chapter highlighted the importance of protecting sensitive information from both unauthorized users and even the crowd server itself. It concluded that encrypted communication and secure task matching mechanisms are essential. In the future, the development of lightweight encryption algorithms, secure search protocols, and privacy-preserving task assignment techniques such as homomorphic encryption or private information retrieval should be explored to enhance both scalability and confidentiality.

Chapter 3 focused on improving task matching privacy through cryptographic means, specifically using ring verification signatures. This approach eliminates the need for proxy re-encryption and ensures user anonymity and data integrity during the matching process. Unlike traditional methods, the proposed scheme is resilient to identity inference and offers better scalability. The chapter concluded that ring signatures are a promising direction for secure crowdsourcing. Future work can explore expanding this approach to support collaborative group tasks, and integrating zero-knowledge proofs for even stronger anonymity guarantees. The scheme could also be adapted for use in real-world applications such as ride-sharing or online freelancing platforms.

In Chapter 4, the application of crowdsourcing in blood bank management was proposed as a novel and impactful use case. The chapter recognized the gap between increasing voluntary blood donations and the outdated, manual management systems still used in many hospitals.By using blockchain technology, the study introduced a secure and transparent mechanism to connect donors and recipients. This system ensures medical data confidentiality and reduces the risks associated with centralized data storage. The future scope includes deploying the system in real hospital networks, automating donor eligibility checks using integrated medical devices, and promoting public awareness to increase voluntary donations. Additionally, blockchain's transparent architecture can help build trust among users in the healthcare ecosystem.

Chapter 5 built upon the previous proposal by introducing searchable encryption and a fine-grained reuse-based task matching mechanism for improved efficiency. The integration of blockchain with searchable encryption helps optimize donor-recipient matching while ensuring data privacy and integrity. The chapter acknowledged the limitations of traditional proxy-based systems, such as the risk of key exposure and high computational overhead. By eliminating reliance on proxies and minimizing smart contract usage, the proposed framework reduces gas fees and transaction delays—making it more suitable for emergency healthcare scenarios. Looking ahead,

the system could be further enhanced by integrating multi-keyword search capabilities, using Layer-2 blockchain technologies to improve speed and reduce cost, and adopting more advanced consensus algorithms to improve performance in real-time applications.

Chapter 6 Overall, the research presents a comprehensive approach to secure and privacy-preserving task matching in both general crowdsourcing and healthcare-specific use cases. By combining encryption techniques with blockchain technology, the proposed frameworks address critical challenges related to data confidentiality, task accuracy, and operational efficiency. Future developments should focus on making these systems more adaptable, scalable, and user-friendly to facilitate widespread adoption across industries.

Summary of Contributions

This work presents a comprehensive study and a novel framework for secure and privacy-preserving task matching in crowdsourcing systems. The key contributions are as follows:

1. **Systematic Analysis of Existing Schemes:** We performed an in-depth literature review and comparative evaluation of existing task-matching mechanisms. The analysis highlights how current schemes address security and privacy, identifies vulnerabilities such as location and identity leakage, and uncovers gaps in efficiency, scalability, and anonymity.

2. **Design of a Privacy-Preserving Task Matching Framework:** Building upon the identified gaps, we propose a ring signature-based task-matching schema that ensures user anonymity, data confidentiality, and protection against inference attacks. The framework leverages lightweight encryption and searchable trapdoor generation to enable efficient and secure matching between requesters and workers.

3. **Blockchain Integration for Transparency and Decentralization:** The proposed framework incorporates blockchain technology to maintain auditable task transactions, support decentralized storage, and reduce reliance on central authorities. Smart contracts are utilized to automate task verification, authorization, and reward distribution, enhancing trust and fairness within the platform.

4. **Performance Optimization in Resource-Constrained Environments:** We carefully evaluate the trade-offs between security and computational overhead, en-

suring that the framework is suitable for deployment on mobile and edge devices. Techniques such as optimized bilinear pairing operations, ring signature efficiency, and lightweight cryptographic primitives are employed to maintain low latency, scalability, and energy efficiency.

5. **Comprehensive Security and Utility Evaluation:** The framework is rigorously analyzed against common adversarial models and privacy attacks. We demonstrate that it achieves strong privacy guarantees, supports efficient task matching, and provides robustness against collusion and malicious users, making it practical for real-world crowdsourcing applications.

6.1 Future Research Directions

The proposed ring signature-based task matching framework provides a secure and privacy-preserving solution for crowdsourcing systems. However, there are several promising avenues for future research and improvement:

1. **Post-Quantum Secure Cryptography:** With quantum computing posing potential threats to traditional cryptographic primitives, integrating post-quantum cryptographic algorithms such as lattice-based, code-based, or hash-based schemes could ensure long-term security. This would safeguard both task data and user identities against future quantum attacks.

2. **Adaptive and Intelligent Task Matching:** Machine learning and AI-driven models can be incorporated to predict worker availability, skill levels, and task preferences. Adaptive mechanisms could dynamically adjust encryption and privacy levels based on task sensitivity, user reputation, or contextual factors, enhancing both performance and security.

3. **Integration with Edge and IoT Devices:** Crowdsourcing systems increasingly involve mobile and IoT devices with limited resources. Future work could focus on optimizing the computation, communication, and energy requirements of encryption, trapdoor generation, and signature verification to ensure efficient operation in edge environments.

4. **Enhanced Incentive and Reputation Systems:** Robust incentive mechanisms and reputation-based models can encourage honest participation, quality task

completion, and timely reporting. Blockchain-based tokenization and smart contracts can be further leveraged to enforce fair rewards and prevent fraudulent behaviors.

5. **Multi-Platform and Cross-Domain Crowdsourcing:** Expanding the framework to support multiple crowdsourcing platforms and cross-domain collaborations can enhance scalability and usability. Privacy-preserving federated task matching across decentralized platforms could allow seamless cooperation without compromising sensitive information.

6. **Advanced Threat Models and Security Analysis:** While the current system addresses common threats, future research could explore more sophisticated attack scenarios such as collusion, Sybil attacks, inference attacks, or side-channel attacks. Formal verification and security proofs for these advanced threats would further strengthen the robustness of the framework.

7. **Blockchain Scalability and Efficiency:** Although blockchain enhances transparency and auditability, challenges remain in scalability, transaction throughput, and energy consumption. Future work could explore lightweight consensus protocols, sharding, or layer-2 solutions to improve efficiency while maintaining security guarantees.

8. **Usability and User Experience:** Ensuring the framework is user-friendly and easily adoptable is critical. Research can focus on simplifying key management, automating encryption/trapdoor operations, and providing intuitive interfaces for both requesters and workers while maintaining security and privacy.

In summary, these directions aim to extend the proposed system's applicability, efficiency, and resilience, ensuring secure, privacy-preserving, and scalable task matching in next-generation crowdsourcing platforms.

Bibliography

Affum, E., Zhang, X., Wang, X., and Obiri, I. A. (2022). "Lattice puncturable attribute based proxy re-encryption scheme and its application in information centric network". *Future of Information and Communication Conference*, 765–786.

Agarwal, S., et al. (2020). "Encrypted online blood donation system". *International Journal of Computer Applications*.

Agrawal, A., Choudhary, S., Bhatia, A., and Tiwari, K. (2023). "Pub-submcs: A privacy-preserving publish–subscribe and blockchain-based mobile crowdsensing framework". *Future Generation Computer Systems*, **146**, 234–249.

Alamer, A., Ni, J., Lin, X., and Shen, X. (2017). "Location privacy-aware task recommendation for spatial crowdsourcing". *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, 1–6.

Ambati, V., Vogel, S., and Carbonell, J. (2011). "Towards task recommendation in micro-task markets". *Workshops at the Twenty-Fifth AAAI Conference on Artificial Intelligence*.

Aswin, A. V., Basil, K. Y., Viswan, V. P., Reji, B., and Kuriakose, B. (2020). Design of ayush: A blockchain-based health record management system. In G. Ranganathan, J. Chen, and Á. Rocha (Eds.), *Inventive communication and computational technologies* (pp. 665–672). Springer.

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). "Medrec: Using blockchain for medical data access and permission management". *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30.

Bao, F., Deng, R. H., Ding, X., and Yang, Y. (2008). "Private query on encrypted data in multi-user settings". *Proceedings of International Conference on Information Security Practice and Experience*, 71–85.

Bender, A., Katz, J., and Morselli, R. (2006). "Ring signatures: Stronger definitions, and constructions without random oracles". *Theory of Cryptography Conference*, 60–79.

Blockchain vehicle history [CarVertical Whitepaper]. (2018).

Boneh, D., Gentry, C., Lynn, B., and Shacham, H. (2003). "Aggregate and verifiably encrypted signatures from bilinear maps". *Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003 Proceedings 22*, 416–432.

Bresson, E., Stern, J., and Szydlo, M. (2002). "Threshold ring signatures and applications to ad-hoc groups". *Annual International Cryptology Conference*, 465–480.

Chandran, N., Groth, J., and Sahai, A. (2007). "Ring signatures of sub-linear size without random oracles". *International Colloquium on Automata, Languages, and Programming*, 423–434.

Chang, S., Wong, D. S., Mu, Y., and Zhang, Z. (2009). "Certificateless threshold ring signature". *Information Sciences*, **179**, 3685–3696.

Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., and Moosavi, S. R. (2023a). "A lightweight blockchain and fog-enabled secure remote patient monitoring system". *Internet of Things*, **22**, 100691. https://doi.org/10.1016/j.iot.2023.100691

Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., and Moosavi, S. R. (2023b). "A lightweight blockchain and fog-enabled secure remote patient monitoring system". *Internet of Things*, **22**, 100691. https://doi.org/10.1016/j.iot.2023.100691

Cheung, M. H., Southwell, R., Hou, F., and Huang, J. (2015). "Distributed time-sensitive task selection in mobile crowdsensing". *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 157–166.

Chi, Z., Wang, Y., Huang, Y., and Tong, X. (2017). "The novel location privacy-preserving ckd for mobile crowdsourcing systems". *IEEE Access*, **6**, 5678–5687.

Chordiya, R., et al. (2021). "Digital blood management system". *IEEE Access*.

Chukwu, E., and Garg, L. (2020). "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations". *IEEE Access*, **8**, 21196–21214.

Cui, J., Ouyang, F., Ying, Z., Wei, L., and Zhong, H. (2021). "Secure and efficient data sharing among vehicles based on consortium blockchain". *IEEE Transactions on Intelligent Transportation Systems*, **23(7)**, 8857–8867.

Dai, J., and Qiao, K. (2018). "A privacy preserving framework for worker's location in spatial crowdsourcing based on local differential privacy". *Future Internet*, **10(6)**, 53.

Debnath, S., and Bhuyan, B. (2019). "Large universe attribute based encryption enabled secured data access control for cloud storage with computation outsourcing". *Multiagent and Grid Systems*, **15(2)**, 99–119.

Decentralized vehicle data [VINChain Project]. (2018).

Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., and Charalabidis, Y. (2018). "An assessment of privacy preservation in crowdsourcing approaches: Towards gdpr compliance". *2018 12th International Conference on Research Challenges in Information Science (RCIS)*, 1–9. https://doi.org/10.1109/RCIS.2018.8406643

Dong, C., Russello, G., and Dulay, N. (2011). "Shared and searchable encrypted data for untrusted servers". *Journal of Computer Security*, **19(3)**, 367–397.

Egala, B. S., Pradhan, A. K., Gupta, S., Sahoo, K. S., Bilal, M., and Kwak, K.-S. (2022). "Coviblock: A secure blockchain-based smart healthcare assisting system". *Sustainability*, **14(24)**, 16844. https://doi.org/10.3390/su142416844

Ekanayaka, S., et al. (2015). "Blood donor privacy protection". *International Journal of Health Sciences*.

Erlingsson, Ú., Pihur, V., and Korolova, A. (2014). "Rappor: Randomized aggregatable privacy-preserving ordinal response". *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 1054–1067.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., and Capkun, S. (2016). "On the security and performance of proof of work blockchains". *ACM CCS*, 3–16.

Gohar, A. N., Abdelmawgoud, S. A., and Farhan, M. S. (2022). "A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and iot". *IEEE Access*, **10**, 92137–92157. https://doi.org/10.1109/ACCESS.2022.3202902

Gordon, W. J., and Catalini, C. (2018). "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability". *Computational and Structural Biotechnology Journal*, **16**, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003

Guo, Y., Xie, H., Miao, Y., Wang, C., and Jia, X. (2020). "Fedcrowd: A federated and privacy-preserving crowdsourcing platform on blockchain". *IEEE Transactions on Services Computing*, **15(4)**, 2060–2073.

Handa, R., Krishna, C. R., and Aggarwal, N. (2019a). "Searchable encryption: A survey on privacy-preserving search schemes on encrypted outsourced data". *Concurrency and Computation: Practice and Experience*, **31(17)**, e5201.

Handa, R., Krishna, C. R., and Aggarwal, N. (2019b). "Searchable encryption: A survey on privacy-preserving search schemes on encrypted outsourced data". *Concurrency and Computation: Practice and Experience*, **31(17)**, e5201.

Hao, J., Huang, C., Chen, G., Xian, M., and Shen, X. (2019). "Privacy-preserving interest-ability based task allocation in crowdsourcing". *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, 1–6.

He, P., Xia, J., Cao, X., and Xiao, S. (2023). "Pmate: Privacy-preserving task recommendation with fuzzy matching in mobile crowdsourcing". *Information Sciences*, **641**, 119126. https://doi.org/10.1016/j.ins.2023.119126

Hettiachchi, D., Kostakos, V., and Goncalves, J. (2022). "A survey on task assignment in crowdsourcing". *ACM Computing Surveys (CSUR)*, **55(3)**, 1–35.

Howe, J. (2006). *The rise of crowdsourcing, wired*. http://www.wired.com/wired/archive/14.06/crowds.html

Huang, C., Lu, R., and Zhu, H. (2017). "Privacy-friendly spatial crowdsourcing in vehicular networks". *Journal of Communications and Information Networks*, **2(2)**, 59–74.

Ismael, N., et al. (2022). "Advanced technologies in blood banks: A systematic review". *Journal of Biomedical Informatics*.

Jayabalan, J., and Jeyanthi, N. (2022). "Scalable blockchain model using off-chain ipfs storage for healthcare data security and privacy". *Journal of Parallel and Distributed Computing*, **164**, 152–167. https://doi.org/10.1016/j.jpdc.2022.03.009

Jiang, S., Zhang, X., Chen, J., Li, J., Wu, H., Liu, Y., and Zhou, Y. (2024). "Privacy-preserving and fair crowdsourcing framework with fine-grained reuse based on blockchain". *IEEE Transactions on Network and Service Management*.

Kiayias, A., Oksuz, O., Russell, A., Tang, Q., and Wang, B. (2016). "Efficient encrypted keyword search for multi-user data sharing". *Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part I 21*, 173–195.

Le, H., Thanh, L., Vo, H., Luong, H., Tuan, K., Anh, T., Nguyen, T., Vuong, K., and Son, H. (2022). "Patient-chain: Patient-centered healthcare system—a blockchain-based technology in dealing with emergencies". *Parallel and Distributed Computing, Applications and Technologies*, 576–583.

Li, L., Wu, H., Düdder, B., Shen, J., and Cao, Z. (2024). "Bilateral secure and decentralized crowdsourcing task matching atop consortium blockchain". *2024 IEEE International Conference on Blockchain (Blockchain)*, 294–301.

Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., Liu, J.-N., Xiang, Y., and Deng, R. H. (2018). "Crowdbc: A blockchain-based decentralized framework for crowdsourcing". *IEEE Transactions on parallel and distributed systems*, **30(6)**, 1251–1266.

Li, M., Wu, J., Wang, W., and Zhang, J. (2021). "Toward privacy-preserving task assignment for fully distributed spatial crowdsourcing". *IEEE Internet of Things Journal*, **8(18)**, 13991–14002.

Li, S., Bai, X., and Wei, S. (2021). "Blockchain-based crowdsourcing task management and solution verification method". *2021 IEEE 24th International Conference on Computational Science and Engineering (CSE)*, 108–115. https://doi.org/10.1109/CSE53436.2021.00025

Liao, P., et al. (2019). "Applying crowdsourcing techniques in urban planning: A bibliometric analysis of research and practice prospects". *Cities*, **94**, 33–43.

Liao, Z., Ai, J., Liu, S., Zhang, Y., and Liu, S. (2023). "Blockchain-based mobile crowdsourcing model with task security and task assignment". *Expert Systems with Applications*, **211**, 118526.

Lin, C., He, D., Zeadally, S., Kumar, N., and Choo, K.-K. R. (2020). "Secbcs: A secure and privacy-preserving blockchain-based crowdsourcing system". *Science China Information Sciences*, **63**, 1–14.

Lin, Y., and Zhang, Z. (2020a). "Secured crowdsourcing voting". *IEEE Security and Privacy*.

Lin, Y., and Zhang, C. (2020b). "Crowdsourcing system based on blockchain". *2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS)*, 98–101.

Liu, A., Li, Z.-X., Liu, G.-F., Zheng, K., Zhang, M., Li, Q., and Zhang, X. (2017). "Privacy-preserving task assignment in spatial crowdsourcing".

Liu, A., Wang, W., Shang, S., Li, Q., and Zhang, X. (2018). "Efficient task assignment in spatial crowdsourcing with worker and task privacy protection". *GeoInformatica*, **22**, 335–362.

Liu, Y., Zhang, Y., Su, S., Zhang, L., Du, X., Guizani, M., and Tian, Z. (2023). "Blocksc: A blockchain empowered spatial crowdsourcing service in metaverse while preserving user location privacy". *IEEE Journal on Selected Areas in Communications*.

Ma, L., Liu, X., Pei, Q., and Xiang, Y. (2018a). "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing". *IEEE Transactions on Services Computing*, **12(5)**, 786–799.

Ma, L., Liu, X., Pei, Q., and Xiang, Y. (2018b). "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing". *IEEE Transactions on Services Computing*, **12(5)**, 786–799.

Ma, Q., and Olshevsky, A. (2020). "Adversarial crowdsourcing through robust rank-one matrix completion". *Advances in Neural Information Processing Systems*, **33**, 21841–21852.

Malina, L., Hajny, J., Dzurenda, P., and Ricci, S. (2018–July 28). "Lightweight ring signatures for decentralized privacy-preserving transactions". *Proceedings of the 15th International Joint Conference, ICETE 2018*, 692–697.

Mani, V., Prakash, M., and Lai, W. C. (2022). "Cloud-based blockchain technology to identify counterfeits". *Journal of Cloud Computing*, **11(1)**, 67. https://doi.org/10.1186/s13677-022-00341-2

Manzoor, A., Braeken, A., Kanhere, S. S., Ylianttila, M., and Liyanage, M. (2021a). "Proxy re-encryption enabled secure and anonymous iot data sharing platform based on blockchain". *Journal of Network and Computer Applications*, **176**, 102917.

Manzoor, H., et al. (2021b). "Blockchain proxy re-encryption for iot data". *Journal of Network and Computer Applications*.

Melchor, C. A., Cayrel, P. L., Gaborit, P., and Laguillaumie, F. (2011). "A new efficient threshold ring signature scheme based on coding theory". *IEEE Transactions on Information Theory*, **57**, 4833–4842.

Mendeley dataset on security. (2021).

Mullen, P. R., et al. (2021). "Crowdsourcing for online samples in counseling research". *Journal of Counseling and Development*, **99(2)**, 221–226.

Nazir, F. (2020). "Online blood bank for students". *International Journal of Computer Science and Information Security*.

Nazir, S. (2022). "Blockchain of things for healthcare asset management" [Accessed: 2025-08-31]. *Research Online*. https://researchonline.gcu.ac.uk/files/53829949/Nazir_S._et_al_2022_Blockchain_of_things_for_healthcare_asset_management.pdf

Ni, J., Zhang, K., Yu, Y., Lin, X., and Shen, X. S. (2018). "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing". *IEEE Transactions on Dependable and Secure Computing*, **17(3)**, 581–594.

Ning, J., Cao, Z., Dong, X., Liang, K., Ma, H., and Wei, L. (2017). "Auditable sigma-time outsourced attribute-based encryption for access control in cloud computing". *IEEE Transactions on Information Forensics and Security*, **13(1)**, 94–105.

Nizamuddin, N., Hasan, H. R., and Salah, K. (2018). "Ipfs-blockchain-based authenticity of online publications". *ICBC*.

Ouyang, R. W., Kaplan, L. M., Toniolo, A., Srivastava, M., and Norman, T. J. (2016). "Parallel and streaming truth discovery in large-scale quantitative crowdsourcing". *IEEE transactions on parallel and distributed systems*, **27(10)**, 2984–2997.

Pang, X., Guo, D., Wang, Z., Sun, P., and Zhang, L. (2020). "Towards fair and efficient task allocation in blockchain-based crowdsourcing". *CCF Transactions on Networking*, **3**, 193–204.

Pournajaf, L., Xiong, L., Sunderam, V., and Goryczka, S. (2014). "Spatial task assignment for crowd sensing with cloaked locations". *2014 IEEE 15th International Conference on Mobile Data Management*, **1**, 73–82.

Pradhan, S., et al. (2021). "Blockchain-based secure blood bank system". *IEEE Transactions on Information Forensics and Security*.

Rambiritch, V., et al. (2021a). "Humanistic values in blood donation". *Transfusion Medicine Reviews*.

Rambiritch, V., Vermeulen, M., Bell, H., Knox, P., Nedelcu, E., Al-Riyami, A. Z., Callum, J., and van den Berg, K. (2021b). "Transfusion medicine and blood banking education and training for blood establishment laboratory staff: A review of selected countries in africa" [Accessed: 2025-08-31]. *Transfusion*, **61(6)**, 1955–1965. https://doi.org/10.1111/trf.16372

Rathee, G., Sharma, A., Saini, H., Kumar, R., and Iqbal, R. (2020). "A hybrid framework for multimedia data processing in iot-healthcare using blockchain technology". *Multimedia Tools and Applications*, **79(15-16)**, 9711–9733. https://doi.org/10.1007/s11042-019-07835-3

Rivest, R. L., Shamir, A., and Tauman, Y. (2001). "How to leak a secret". *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings 7*, 552–565.

Robinson, M., Sarkani, S., and Mazzuchi, T. (2021). "Network structure and requirements crowdsourcing for oss projects". *Requirements Engineering*, **26(4)**, 509–534.

Roehrs, A., da Costa, C. A., da Rosa Righi, R., da Silva, V., Goldim, J., and Schmidt, D. (2019a). "Analyzing the performance of a blockchain-based personal health record implementation". *Journal of Biomedical Informatics*, **92**, 103140. https://doi.org/10.1016/j.jbi.2019.103140

Roehrs, A., da Costa, C. A., da Rosa Righi, R., da Silva, V. F., Goldim, J. R., and Schmidt, D. C. (2019b). "Analyzing the performance of a blockchain-based personal health record implementation". *Journal of Biomedical Informatics*, **92**, 103140. https://doi.org/10.1016/j.jbi.2019.103140

Rowan, W., et al. (2017). "Blockchain vehicle sensing". *IEEE Vehicular Technology Conference*.

Saeed, M., et al. (2021). "Ai in blood bank management". *IEEE Journal of Biomedical and Health Informatics*.

Secure blood donation system [US Patent 8204694]. (2012).

Shacham, H., and Waters, B. (2007). "Efficient ring signatures without random oracles". *Public Key Cryptography–PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography Beijing, China, April 16-20, 2007. Proceedings 10*, 166–180.

Shahaab, A., Maude, R., Hewage, C., and Khan, I. (2020). "Managing gender change information on immutable blockchain in context of gdpr". *The Journal of The British Blockchain Association*, **3(3)**. https://doi.org/10.31585/jbba-3-1-(3)2020

Shen, Y., Huang, L., Li, L., Lu, X., Wang, S., and Yang, W. (2015). "Towards preserving worker location privacy in spatial crowdsourcing location privacy-aware task recommendation for spatial crowdsourcing". *2015 IEEE global communications conference (GLOBECOM)*, 1–6.

Shu, J., and Jia, X. (2016). "Secure task recommendation in crowdsourcing". *2016 IEEE Global Communications Conference (GLOBECOM)*, 1–6.

Shu, J., Jia, X., Yang, K., and Wang, H. (2018). "Privacy-preserving task recommendation services for crowdsourcing". *IEEE Transactions on Services Computing*, **14(1)**, 235–247.

Shu, J., Liu, X., Jia, X., Yang, K., and Deng, R. H. (2018). "Anonymous privacy-preserving task matching in crowdsourcing". *IEEE Internet of Things Journal*, **5(4)**, 3068–3078.

Shu, J., Yang, K., Jia, X., Liu, X., Wang, C., and Deng, R. H. (2018a). "Proxy-free privacy-preserving task matching with efficient revocation in crowdsourcing". *IEEE Transactions on Dependable and Secure Computing*, **18(1)**, 117–130.

Shu, J., Yang, K., Jia, X., Liu, X., Wang, C., and Deng, R. H. (2018b). "Proxy-free privacy-preserving task matching with efficient revocation in crowdsourcing". *IEEE Transactions on Dependable and Secure Computing*, **18(1)**, 117–130. https://doi.org/10.1109/TDSC.2018.2812199

Singh, G. (2013). "A study of encryption algorithms (rsa, des, 3des and aes) for information security". *International Journal of Computer Applications*, **67(19)**.

Song, T., Tong, Y., Wang, L., She, J., Yao, B., Chen, L., and Xu, K. (2017). "Trichromatic online matching in real-time spatial crowdsourcing". *2017 IEEE 33rd International Conference on Data Engineering (ICDE)*, 1009–1020. https://doi.org/10.1109/ICDE.2017.147

Steichen, M., Fiz, B., Norvill, R., Shbair, W., and State, R. (2018). "Blockchain-based, decentralized access control for ipfs". *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1499–1506.

Sun, Y., Liu, A., Li, Z., Liu, G., Zhao, L., and Zheng, K. (2017). "Anonymity-based privacy-preserving task assignment in spatial crowdsourcing". *Web Information Systems Engineering–WISE 2017: 18th International Conference, Puschino, Russia, October 7-11, 2017, Proceedings, Part II 18*, 263–277.

Tang, W., Zhang, K., Ren, J., Zhang, Y., and Shen, X. S. (2020). "Privacy-preserving task recommendation with win-win incentives for mobile crowdsourcing". *Information Sciences*, **527**, 477–492.

Taylor, A., Kugler, A., Marella, P. B., and Dagher, G. G. (2022). "Vigilrx: A scalable and interoperable prescription management system using blockchain". *IEEE Access*, **10**, 25973–25986. https://doi.org/10.1109/ACCESS.2022.3156015

Timmer, N., et al. (2019). "Donor insight cohort study". *Transfusion*.

To, H., Ghinita, G., Fan, L., and Shahabi, C. (2016a). "Differentially private location protection for worker datasets in spatial crowdsourcing". *IEEE Transactions on Mobile Computing*, **16(4)**, 934–949.

To, H., Ghinita, G., Fan, L., and Shahabi, C. (2016b). "Efficient encrypted keyword search for". *IEEE Transactions on Mobile Computing*, **16(4)**, 934–949.

To, H., Ghinita, G., and Shahabi, C. (2014). "A framework for protecting worker location privacy in spatial crowdsourcing". *Proceedings of the VLDB Endowment*, **7(10)**, 919–930.

Tso, R. (2013). "A new way to generate a ring: Universal ring signature". *Computers and Mathematics with Applications*, **65**, 1350–1359.

Venkata Subramanian, S., et al. (2020). "Design patterns for blood bank systems". *Journal of Medical Systems*.

Vermicelli, L., et al. (2021). "Crowdsourcing in healthcare". *Journal of Medical Internet Research*.

Wang, J., Wang, G., Zhang, Y., and Wu, M. (2022). "A graph-based worker and task location privacy-preserving method in mobile crowdsourcing". *IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 466–471. https://doi.org/10.1109/CSCWD54268.2022.9796827

Wang, Y., Cai, Z., Chi, Z., Tong, X., and Li, L. (2018). "A differentially k-anonymity-based location privacy-preserving for mobile crowdsourcing systems". *Procedia Computer Science*, **129**, 28–34.

Wei, J., Lin, Y., Yao, X., and Zhang, J. (2019). "Differential privacy-based location protection in spatial crowdsourcing". *IEEE Transactions on Services Computing*, **15(1)**, 45–58.

Wu, S., Wang, X., Wang, S., Zhang, Z., and Tung, A. K. (2013). "K-anonymity for crowdsourcing database". *IEEE Transactions on Knowledge and Data Engineering*, **26(9)**, 2207–2221.

Wu, Y. (2017). *An e-voting system based on blockchain and ring signature* (tech. rep.).

Wu, Y., Tang, S., Zhao, B., and Peng, Z. (2019). "Bptm: Blockchain-based privacy-preserving task matching in crowdsourcing". *IEEE access*, **7**, 45605–45617.

Xiang, X., Cao, J., and Fan, W. (2022). "Decentralized authentication and access control protocol for blockchain-based e-health systems". *Journal of Network and Computer Applications*, **207**, 103512. https://doi.org/10.1016/j.jnca.2022.103512

Xiong, P., Zhu, D., Zhang, L., Ren, W., and Zhu, T. (2019). "Optimizing rewards allocation for privacy-preserving spatial crowdsourcing". *Computer Communications*, **146**, 85–94.

Xu, J., Fu, X., and Li, Z. (2020). "Optimizing blockchain gas cost in decentralized applications". *IEEE Blockchain Conference*, 27–35.

Xu, J., Zhang, Z., and Feng, D. (2004). "A ring signature scheme using bilinear pairings". *International Workshop on Information Security Applications*, 160–169.

Yang, K., Zhang, K., Ren, J., and Shen, X. (2015). "Security and privacy in mobile crowdsourcing networks: Challenges and opportunities". *IEEE communications magazine*, **53(8)**, 75–81.

Yang, M., Zhu, T., Liang, K., Zhou, W., and Deng, R. H. (2019). "A blockchain-based location privacy-preserving crowdsensing system". *Future Generation Computer Systems*, **94**, 408–418.

Yin, H., Xiong, Y., Deng, T., Deng, H., and Zhu, P. (2019). "A privacy-preserving and identity-based personalized recommendation scheme for encrypted tasks in crowdsourcing". *IEEE Access*, **7**, 138857–138871.

Yuan, D., Li, Q., Li, G., Wang, Q., and Ren, K. (2019). "Priradar: A privacy-preserving framework for spatial crowdsourcing". *IEEE transactions on information forensics and security*, **15**, 299–314.

Yuen, M.-C., King, I., and Leung, K.-S. (2011). "Task matching in crowdsourcing". *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 409–412. https://doi.org/10.1109/iThings/CPSCom.2011.128

Zhai, D., Sun, Y., Liu, A., Li, Z., Liu, G., Zhao, L., and Zheng, K. (2019). "Towards secure and truthful task assignment in spatial crowdsourcing". *World Wide Web*, **22**, 2017–2040.

Zhang, J., Zhang, Q., and Ji, S. (2020). "A fog-assisted privacy-preserving task allocation in crowdsourcing". *IEEE Internet of Things Journal*, **7(9)**, 8331–8342.

Zhang, L., Zhang, F., and Wu, W. (2007–November 2). "A provably secure ring signature scheme in certificateless cryptography". *Proceedings of the First International Conference*, **4784**, 103–121.

Zhang, Q., et al. (2021). "Privacy in software engineering". *ACM Transactions on Software Engineering*.

Zhang, Y., Chen, Q., and Zhong, S. (2016). "Privacy-preserving data aggregation in mobile phone sensing". *IEEE Transactions on Information Forensics and Security*, **11(5)**, 980–992. https://doi.org/10.1109/TIFS.2016.2515513

Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., Lyu, L., and Liu, Y. (2020). "Privacy-preserving blockchain-based federated learning for iot devices". *IEEE Internet of Things Journal*, **8(3)**, 1817–1829.

Zhou, M., Ye, X., Fan, W., and Li, Q. (2022). "A lightweight privacy-preserving mechanism for location-based services in mobile crowdsourcing". *Journal of Network and Computer Applications*, **204**, 103360. https://doi.org/10.1016/j.jnca.2022.103360

Zhu, S., Cai, Z., Hu, H., Li, Y., and Li, W. (2019). "Zkcrowd: A hybrid blockchain-based crowdsourcing platform". *IEEE Transactions on Industrial Informatics*, **16(6)**, 4196–4205.

Zhu, Y., et al. (2020). "Social weather: A review of crowdsourcing-assisted meteorological knowledge services through social cyberspace". *Geoscience Data Journal*, **7(1)**, 61–79.

Zhuang, Y., Shyu, C.-R., Hong, S., Li, P., and Zhang, L. (2023). "Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology". *Computers in Biology and Medicine*, **157**, 106778. https://doi.org/10.1016/j.compbiomed.2023.106778

Zou, S., Xi, J., Xu, G., Zhang, M., and Lu, Y. (2021). "Crowdhb: A decentralized location privacy-preserving crowdsensing system based on a hybrid blockchain network". *IEEE internet of things journal*, **9(16)**, 14803–14817.

Conference Proceeding

1. **Arijita Bhowmik**, Somen Debnath, Arnab Paul, Susmita Majumder, Dipjyoti Deb, and Sanjeev K. Cowlessur. 2024. Online Blood Bank System Using Blockchain in Crowdsourcing Platform. In *Proceedings of the International Conference on Advanced Communications and Machine Intelligence (MICA 2023)*, Smart Innovation, Systems and Technologies, Vol. 405 (2024), pp. 513–521. DOI: 10.1007/978-981-97-6222-4_42.
2. **Arijita Bhowmik**, *A secure and efficient schema by integrating blockchain and crowdsourcing in online language learning platforms*. Paper presented at the International Conference on Recent Advances in Science, Technology and Engineering (ICRASTE), Bangalore, India. Paper ID: ACN-ASTE-BGLR-050524-200, 2024, July 5.
3. **Arijita Bhowmik**, Paromita Goswami, Munmi Gogoi, Somen Debnath, and Ajoy Kumar Khan. *An Effective Signature-Oriented Model for Task Matching in Crowd Platform*. *AMRIT-2024*, (In Press).

Journal Publication

1. **Arijita Bhowmik**, Somen Debnath, R. Chawngsangpuii, and Parijata Majumdar. 2024. *A Ring Signature Based Task Matching Schema for Crowdsourcing Environments*. *Journal of Technology*, 12(12), 865–875. DOI: 18.15001/JOT.2024/V12I12.24.1133 (Scopus).
2. **Arijita Bhowmik**, Somen Debnath, Parijata Majumdar, and R. Chawngsangpuii. 2025. *An Efficient Task Matching Schema with Signature-Oriented Encryption Technique*. *Utilitas Mathematica*. URL: https://utilitasmathematica.com/index.php/Index/article/view/2528 (Scopus).
3. **Arijita Bhowmik**, Somen Debnath, Parijata Majumdar and R. Chawngsangpuii. *Crowd-Sourced Blood Bank Management: A Secure and Efficient Reuse-Oriented Framework*, in *Journal of Cloud Computing*, (Accepted, Scopus).
4. **Arijita Bhowmik**, Somen Debnath, Parijata Majumdar and R. Chawngsangpuii. *A Survey on Secure and Privacy-Aware Task in Crowdsourcing Platforms*.Distributed Computing(SCIE)(Communicated).

BIO-DATA OF THE CANDIDATE

Personal Information

Name	: Arijita Bhowmik
Father's name	: Hiralal Bhowmik
Mother's name	: Lt. Gita Rani Bhowmik
Date of Birth	: 20.09.1987
Nationality	: Indian
Gender	: Female
Marital Status	: Married
Present Address	: 79 Tilla, Housing Board Quater Complex
Email	: arijita.bhowmik@yahoo.com

Academic Records

X^{th}	C.B.S.E. (2004)
XIIth	C.B.S.E. (2006)
B.Tech	W.B.U.T (2010)
M.Tech	Tripura University (2013)

(Arijita Bhowmik)

PARTICULARS OF THE CANDIDATE

NAME OF THE CANDIDATE : ARIJITA BHOWMIK

DEGREE : DOCTOR OF PHILOSOPHY

DEPARTMENT : INFORMATION TECHNOLOGY

TITLE OF THESIS : DESIGN AN EFFICIENT AND SECURE TASK MATCHING TECHNIQUE IN CROWD-SOURCING PLATFORM

DATE OF ADMISSION : SEPTEMBER 01, 2021

APPROVAL OF RESEARCH PROPOSAL:

1. DRC : APRIL 27, 2022
2. BOS : MAY 19, 2022
3. SCHOOL BOARD : JUNE 03,2022

MZU REGISTRATION NO.: 2109063

PH.D REGISTRATION NO.: MZU/PH.D/1968 OF 01.09.2021

EXTENSION.: NIL

Dr. Lalhmingliana,

(Head of Department)

Dept. of Information Technology,

Mizoram University, Mizoram.

ABSTRACT

DESIGN OF EFFICIENT AND SECURE TASK MATCHING TECHNIQUES IN CROWDSOURCING PLATFORM

AN ABSTRACT SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

ARIJITA BHOWMIK

MZU REGISTRATION NO.: 2109063

Ph.D. REGISTRATION NO.: MZU/Ph.D./ 1968 OF 01.09.2021



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF ENGINEERING AND TECHNOLOGY

MIZORAM UNIVERSITY

SEPTEMBER, 2025

DESIGN OF EFFICIENT AND SECURE TASK MATCHING TECHNIQUES IN CROWDSOURCING PLATFORM

BY

ARIJITA BHOWMIK

Department of Information Technology

Supervisor: Dr. Somen Debnath

Joint Supervisor: Dr. R. Chawngsangpuii

Submitted

In partial fulfilment of the requirement of the Degree of Doctor of Philosophy in Information Technology of Mizoram University, Aizawl

ABSTRACT

In the modern digital era, crowdsourcing has emerged as a powerful and transformative paradigm for solving complex, large-scale problems through distributed participation. It enables individuals and organizations to collaborate dynamically by leveraging collective intelligence, diverse expertise, and real-time resource availability. The model has found extensive applications in a wide range of domains, including online ride-booking systems, e-commerce logistics, data annotation, and emergency need management, where tasks are rapidly assigned and executed through decentralized networks. In such critical services, the core challenge lies in **task matching**—the process of efficiently linking a service seeker with an appropriate service provider based on contextual needs, location, skill set, and trustworthiness. This task matching process plays a pivotal role in ensuring timely, reliable, and optimized service delivery, which directly impacts user satisfaction and overall system performance.

However, existing crowdsourcing approaches often face significant challenges related to **data security, user anonymity, and system scalability**. Many centralized systems suffer from single points of failure, data breaches, and trust deficits, making them vulnerable to malicious attacks or unauthorized data manipulation. Furthermore, ensuring privacy-preserving communication and secure computation in real-time environments adds another layer of complexity. As the scale of participants and volume of transactions increase, maintaining system integrity, minimizing latency, and achieving computational efficiency become critical yet difficult goals. Therefore, there is a pressing need for advanced, privacy-preserving, and scalable frameworks that can provide secure, transparent, and efficient task matching suitable for modern decentralized ecosystems.

This thesis focuses on enhancing the performance, security, and efficiency of crowdsourcing-based task matching by addressing two key aspects: signature-oriented cryptographic techniques and blockchain-enabled frameworks. Signature-based encryption ensures user anonymity and data authenticity, while blockchain technology provides decentralized, tamper-proof, and transparent management of donor–recipient interactions. Furthermore, this research introduces a novel reuse-oriented blockchain framework that allows secure reuse of verified donor–recipient data, thereby reducing redundant computations, lowering transaction costs, and improving matching efficiency.

Traditional crowdsourcing systems often rely on centralized intermediaries, which can lead to single points of failure, scalability bottlenecks, and risks of data misuse. The signature-based task matching schema enhances user anonymity and data integrity without relying on proxy re-encryption, thereby improving efficiency while mitigating privacy risks. Even blockchain-only implementations, while secure, frequently incur high gas fees and computational overhead. Through comprehensive analysis, this research identifies these limitations as a critical gap, particularly in real-time ride management and healthcare applications. The proposed signature and reuse-oriented blockchain approach addresses this challenge by integrating searchable encryption for privacy-preserving queries, automated donor verification for ethical compliance, and distributed ledger support for system-wide transparency.

Extensive experimentation and security analysis are conducted to validate the framework. The results demonstrate significant improvements in confidentiality, integrity, and transparency compared to existing systems. Computation and transmission costs are balanced

between requesters and workers, while the reuse mechanism reduces gas fees by minimizing redundant blockchain transactions. Moreover, donor blocking periods and recipient survival verification are enforced, enhancing trust and compliance. The proposed framework not only ensures privacy and reliability but also achieves an optimal trade-off between computational efficiency and security robustness. It demonstrates adaptability across heterogeneous network environments and maintains stability under high user concurrency, proving its suitability for real-time and large-scale crowdsourcing deployments.

In addition, the system design follows ethical and regulatory principles by embedding compliance-aware smart contracts, ensuring transparent audit trails and accountability for every transaction. The framework's modular architecture allows it to be extended to other application domains such as decentralized supply chain monitoring, intelligent transport systems, and emergency response coordination.

In summary, this thesis makes several significant contributions: It presents a detailed investigation of secure and efficient task matching challenges in crowdsourcing, with emphasis on online ride booking and healthcare applications. A signature-oriented task matching schema that enhances privacy and data integrity without relying on proxy re-encryption for online ride management is proposed. It also introduces a reuse-oriented blockchain framework for online blood bank management, reducing redundancy and optimizing efficiency. It is demonstrated through rigorous security and performance analysis that the proposed system achieves scalability, transparency, and cost-effectiveness in real-time scenarios.

The framework not only ensures privacy, authenticity, and reliability but also achieves an optimal trade-off between computational efficiency and cryptographic robustness. Experimental evaluations confirm that the system maintains high throughput and low latency even under heavy network loads, demonstrating scalability and resilience across heterogeneous computing environments. It adapts efficiently to dynamic participation levels, varying workloads, and fluctuating network conditions without compromising data confidentiality or operational performance. These findings affirm that the proposed framework is well-suited for real-time, large-scale crowdsourcing deployments that demand secure, transparent, and performance-driven task matching.

This work advances the state of the art in privacy-preserving crowdsourcing by harmonizing cryptographic task matching with blockchain innovations. It lays a foundation for next-generation decentralized healthcare platforms and ride management systems that are secure, efficient, and ethically compliant.

Keywords: Crowdsourcing, Cryptography, Task Matching, Signature Based Encryption, Blockchain, Privacy Preservation.