UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Blockchain based Intelligent Identity Management

by Suhair Alotaibi

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

under the supervision of Professor. Farookh Khadeer Husain
co-supervision of Professor. Asif Qumer Gill

University of Technology Sydney
Faculty of Engineering and Information Technology

July 2024

CERTIFICATE OF ORIGINAL AUTHORSHIP

I Suhair Alotaibi, declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Computer Science, Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research was supported by an Australian Government Research Training Program (RTP) Scholarship doi.org/10.82133/C42F-K220.

Signature:

Date: July 2024

IN THE NAME OF ALLAH



THE MOST BENEFICIENT
THE MOST MERCIFUL

ABSTRACT

Blockchain-based Intelligent Identity Management

by

Suhair Alotaibi

Digital identity management remains a critical challenge in the digital era, as traditional centralized models are susceptible to data breaches, impersonation, and reliance on single points of authority. To address these limitations, this research proposes a Blockchain─based Intelligent Identity Management (BIIM) framework that integrates blockchain technology with biometric authentication to deliver a secure, transparent, and user-centric paradigm for identity management.

The BIIM framework comprises three core modules: blockchain-enabled biometric identity management, user-driven data ownership, and a federated identity mechanism. Collectively, these modules enable individuals and organizations to securely register, validate, and manage identity records within a decentralized environment. Biometric data serve as a primary authentication factor, while the federated identity feature ensures consistent and verifiable identity utilization across multiple domains, thereby reducing redundancy and enhancing user control.

A prototype implementation of BIIM was developed and empirically evaluated in terms of scalability, security, and operational efficiency in managing user identity. The evaluation results demonstrate that BIIM strengthens defenses against impersonation, enhances transparency in verification processes, and empowers users with full control of their identity data. Nonetheless, limitations persist, particularly regarding transaction costs and latency inherent to blockchain-based systems.

This study contributes to the academic field of decentralized identity management by introducing a biometrics-integrated, blockchain-driven, and federated framework for

secure and autonomous identity governance. The research highlights BIIM's potential to establish a scalable, privacy-preserving, and user-centric identity management system, while underscoring the need for further optimization and regulatory alignment to enable practical deployment and adoption.

Dissertation directed by Professor Farookh Khadeer Hussain
School of Computer Science
Centre for Artificial Intelligence
Faculty of Engineering and Information Technology (FEIT)

Acknowledgements

First and foremost, I offer all honor and glory to God Almighty, without whom none of this would have been possible. I express my profound gratitude for the wisdom and strength granted to me throughout this research journey. With a reflective heart, I acknowledge those who have played pivotal roles in my academic and personal growth.

I extend my deepest thanks to my thesis advisor, Prof. Farookh Hussain, for his mentorship and guidance in laying the foundation for my thesis. His unwavering support throughout my academic journey has been invaluable, and I am proud to have been under his supervision. Additionally, I would like to thank my co-supervisor, Prof. Asif, for his valuable feedback.

I hold a special place in my heart to honor my late parents, whose love and guidance have been my foundation. Though they are no longer with us, their influence remains a constant force in my life. They always had faith in me and supported me, and their belief in my potential, along with their sacrifices to provide me with every opportunity, has been the foundation of my achievements. Every step of this journey has been inspired by their values and dreams for my future. I am forever grateful for the life they gave me and the lessons they taught, which continue to guide me. Their memory was a beacon that sustained me through the challenges of this thesis, and I dedicate this accomplishment to their lasting spirit.

I owe tremendous gratitude to my beloved husband, Ibrahim, whose unwavering support has been my strength throughout this journey. His patience, understanding, and encouragement have been pillars during the most challenging times of my research. To our children, Eyad, Moaath, and Tamim, your laughter and love have been my greatest support. I appreciate all your sacrifices and am eternally grateful. Thank you for being my constant source of inspiration and for filling our home with love and happiness.

My sincere appreciation goes to the Department of Computer Science at the University

of Technology Sydney for providing the facilities, resources, and an academic environment filled with opportunities. I also thank my research colleagues for their collaboration, which has greatly enhanced my experience within this community.

As I conclude this significant chapter of my academic journey, I take a moment to acknowledge myself and recognize the personal resilience, dedication, and perseverance that were as much a part of this journey as the intellectual endeavour. This thesis is a testament to my commitment to my field of study. It marks a profound personal journey, including countless hours of study, breakthroughs, persistence, and hard work, tirelessly refining. This achievement is a professional milestone and a personal triumph, reflecting the culmination of my efforts and dedication.

Suhair Alotaibi

Sydney, Australia, 2024.

List of Publications

The following is a list of the research papers which were published during this PhD study.

Journal Papers

J-1. Mwaheb S. Almadania, Suhair Alotaibi, Hada Alsobhi, Omar K. Hussain and Farookh Khadeer Hussain. **"Blockchain-based multi-factor authentication: A systematic literature review"**, *Elsevier: Internet of Things* (Q1 ranked).

J-2. Suhair Alotaibi and Farookh Khadeer Hussain. **"Blockchain-Powered Identity Management: Future Direction"**, *Knowledge-Based Systems* (Q1 ranked) [under review].

Conference Papers

C-1. Suhair Alotaibi, Hada Alsobhi, Ming Zhao, Farookh Khadeer Hussain. **"Blockchain for Identity Management: Ensuring Trust and Integrity in the Education Sector"**, accepted for publication at IEEE International Conference on E-Business Engineering (ICEBE) 2023.

C-2. H. Alsubhi, A. Mirdad, S. Alotaibi, M. AlAlyan, I. Alanazy, M. Almadani, W. Alharbi, R. Alhazmi and F. Hussien.**"Innovative Blockchain-Based Application-State of the Art and Future Direction"***(The 35th International Conference on Advanced Information Networking and Applications (AINA-2021)).*

Contents

Certificate ii

Abstract iv

Acknowledgments vi

List of Publications viii

List of Figures xvii

List of Tables xxii

Abbreviation xxiv

1 Introduction 1

1.1 Background 1

1.1.1 The Prevalence of Identity Theft and Data Breaches 2

1.2 Blockchain Technology 4

1.3 Identity Management Using Blockchain 7

1.3.1 The Impacts of Blockchain Technology in Identity Management are as follows 8

1.4 Blockchain and Biometric Technology in Identity Management 9

1.4.1 Advantages of Biometric Technology in Identity Management . . 10

1.5 Federated Identity Management 10

1.5.1 Benefits of Federated Identity Management 10

1.6 Research Problems and Contribution 12

1.6.1 Research objectives 12

1.6.2 Research Contributions 13
1.6.2.1 Scientific Contribution 13
1.6.2.2 Social Contribution 13
1.7 Thesis Structure 13
1.8 Conclusion 15

2 Literature Review 17

2.1 Introduction 17
2.2 Key Requirements for Blockchain in Identity Management 18
2.2.1 Ability to Integrate Identity Management and Blockchain 18
2.2.2 Ability to Store Biometrics for Authentication on Blockchain . . . 19
2.2.3 Ability to Integrate Self-Sovereign Identity and Blockchain 19
2.2.4 Ability to Integrate Federated Identity and Blockchain 20
2.3 Systematic Literature Review (SLR) Method 20
2.3.1 Searching the Literature 21
2.3.2 Inclusion and Exclusion Criteria 23
2.3.3 Study Selection Process 23
2.3.4 Quality Assessment Criteria 25
2.4 Data Extraction and Synthesis: Papers selected for the systematic literature review and their categorization in addressing the requirements 26
2.4.1 Review of Shortlisted Papers 27
2.4.1.1 Blockchain-Based Identity Management 28
2.4.1.2 Self-Sovereign Identity and Decentralization 28
2.4.1.3 Security and Authentication 29
2.4.1.4 Integration and Interoperability 29

2.4.2 Comparative Analysis 31
2.5 Open Challenges: Identify Research Gaps 33
2.5.1 Identity Management Capability 33
2.5.2 Capability to Integrate Biometrics for Authentication or Validation 34
2.5.3 Capacity to Concentrate on Self-Sovereignty 35
2.5.4 Integration with Federated Systems 36
2.6 Comprehensive Analysis of SLR Studies: Authentication Methods, Security Mechanisms, Security Threats and Blockchain Platforms 37
2.6.1 Authentication Methods 38
2.6.2 Security Mechanisms 38
2.6.3 Security Threats 38
2.6.4 Blockchain Platforms 39
2.7 Conclusion 39

3 Problem Definition 41

3.1 Introduction 41
3.2 Glossary of key technical terms and key concepts 41
3.2.1 Blockchain 41
3.2.2 Biometrics 41
3.2.3 Identity Management System 42
3.2.4 A Distributed Ledger 42
3.2.5 Federated Identity Management 42
3.2.6 Proof of Work (PoW) 42
3.2.7 End-User 42
3.2.8 Administrator 43

3.2.9 User . . . 43
3.2.10 Organization . . . 43
3.2.11 Design Science Research Methodology (DSRM) . . . 43
3.2.12 Python Django Framework . . . 43
3.2.13 MySQL Database . . . 44
3.3 Problem Definition . . . 44
3.4 Research Question and Sub-Questions . . . 44
3.4.1 Main Research Question . . . 45
3.4.2 Research Sub-Questions . . . 45
3.5 Research Objectives . . . 45
3.6 Conclusion . . . 48

4 Research Methodology and Solution Overview 49

4.1 Introduction . . . 49
4.2 Research Methodology . . . 50
4.2.1 Methodology . . . 50
4.3 Solution Overview . . . 52
4.3.1 Architecture of the BIIM . . . 52
4.4 Overview of Solution for Objective 2 . . . 55
4.5 Overview of Solution for Objective 3 . . . 55
4.6 Overview of Solution for Objective 4 . . . 56
4.7 Overview of Solution for Objective 5 . . . 56
4.8 Conclusion . . . 57

5 Biometric Blockchain Identity Management (BBIM) 58

5.1 Introduction . . . 58

5.2 BBIM System Architecture 60
5.3 The Working of the BBIM System 62
5.4 Blockchain 80
5.5 Implementation 86
5.5.1 System Requirements 86
5.5.2 Software and Configuration Development Framework 86
5.5.3 Storage Architecture, Implementation Tools, and Technologies of the BBIM System 87
5.5.3.1 On-Chain and Off-Chain Storage Architecture 87
5.5.3.2 Implementation Tools and Technologies 88
5.6 Evaluation of the BBIM System 90
5.6.1 Evaluation Methodology 91
5.6.2 BBIM Performance Evaluation 91
5.6.3 BBIM Comparative Evaluation 93
5.6.4 BBIM Algorithm Complexity Analysis 94
5.6.5 BBIM System Health and Monitoring 96
5.7 Comparative Evaluation of the BIIM Integrated System 96
5.7.1 BIIM System vs Traditional Systems 97
5.7.2 BIIM system vs DID Frameworks 98
5.7.3 Applicability and Domain Evaluation 98
5.8 Scenario-Based Evaluation 99
5.8.1 Registration and Biometric Enrollment 100
5.8.2 Administrative Verification 100
5.8.3 Biometric Authentication 100
5.8.4 Profile Management and Change Logging 101

5.8.5 External Organization Request for Verification 101
5.8.6 User Consent and Selective Data Sharing 101
5.8.7 Federated Identity Access 102
5.8.8 Analytical Evaluation and Reflection 102
5.9 Discussion 103
5.10 Conclusion 105

6 User-Driven and Organization-Driven Pre-emptive Privacy-Aware Notifications System (UDOD) 106

6.1 Introduction 106
6.2 UDOD System Architecture 108
6.3 Taxonomy of Notifications 110
6.4 The Working of the UDOD System 112
6.5 The Working of the UD System 115
6.5.1 UD System 116
6.5.1.1 Registration Notification 116
6.5.1.2 Login Notification 119
6.5.1.3 Profile Editing Notification 121
6.5.1.4 Password Reset Notification 123
6.6 The Working of the OD System 126
6.6.1 OD System 127
6.7 Implementation 136
6.8 Evaluation of the UDOD System 136
6.8.1 Evaluation Methodology 137
6.8.2 UDOD Performance Evaluation 137

6.8.3 UDOD Algorithm Complexity Analysis 139
6.8.4 Functional Validation via Scenario-Based Testing 141
6.9 Discussion 142
6.10 Conclusion 144

7 Federated Identity Management System (FIM) 146

7.1 Introduction 146
7.2 FIM System Architecture 148
7.3 The Working of the FIM System 150
7.4 Algorithmic Working of the FIM System 153
7.4.1 *Read Wallet Data* 154
7.4.2 *Add New Identity* 155
7.4.3 *Delete Current Identity* 156
7.4.4 *Open Current URL* 157
7.5 Implementation 158
7.5.1 Implementation Requirements: 158
7.5.2 Implementation Process 160
7.6 Evaluation of the FIM System 166
7.6.1 FIM Experimental Evaluation 166
7.6.1.1 Gas Cost vs. Number of Records 167
7.6.1.2 Time Consumption vs. Number of Records 168
7.6.2 FIM Algorithm Complexity Analysis 170
7.6.3 Functional Validation via Scenario-Based Testing 171
7.7 Discussion 172
7.8 Conclusion 173

8 Conclusion **175**

8.1 Introduction 175

8.2 Thesis Summary 176

8.3 Problems Addressed in this Thesis 177

8.3.1 Research Problem 1: Comprehensive Framework 177

8.3.2 Research Problem 2: Secure and Scalable Storage of Biometric Data 177

8.3.3 Research Problem 3: Proactive Notification Systems 178

8.3.4 Research Problem 4: Integration of Federated Identities with Blockchain 178

8.3.5 Research Problem 5: Evaluation and Validation of Comprehensive Identity Management Systems 178

8.4 Thesis Achievements 178

8.5 Comprehensive Implications of the Blockchain-Based Identity Management System 179

8.5.1 Implications for Research 179

8.5.2 Implications for Practice 180

8.5.3 Implications for Society 181

8.6 Thesis Limitations 181

8.7 Future Research Directions 182

List of Figures

1.1 Impact of Blockchain in Identity Management 9

1.2 Primary Components of the System 12

1.3 Thesis Structure 15

2.1 Percentage of Studies Retrieved by Database 22

2.2 Filtration of Studies by Database 24

2.3 Application of the Systematic Literature Review Process 24

2.4 SLR Categories for the Existing Literature 27

2.5 Number of Studies by Category 27

4.1 DSRM [73] 50

4.2 MVC-Driven Architecture for the BIIM System 53

5.1 BBIM System Architecture 61

5.2 BIIM Class Diagram 63

5.3 Use Case Diagram of BIIM System 64

5.4 Biometric Blockchain-based Identity Management System 66

5.5 User Registration and Confirmation Workflow with Email and Blockchain Integration 67

5.6 Admin/ User Sign Up Interface 68

5.7 Organization Sign Up Interface 68

5.8 Make an Account: Face Scan 68
5.9 100 Images Captured for Face Scan 69
5.10 Face Registered 69
5.11 Registration Failed 69
5.12 Administrator Verifies and Compares the User ID with the Registered Face to Validate the Identity 70
5.13 Administrator Dashboard of Users and Organizations Waiting for Verification and Approval 70
5.14 Administrator Approves/ Verifies Dashboard 71
5.15 Login Process 71
5.16 Credential login 72
5.17 Face Login 72
5.18 Login Successful 74
5.19 Face Matching Failed 74
5.20 Spoofing Found 75
5.21 Login Failed 75
5.22 Face Scan Unavailable 76
5.23 User/ Organization Home Page 76
5.24 Admin Home Page 76
5.25 User Display and Update Profile 77
5.26 View and Manage Profile 77
5.27 Change and Reset Password Process 78
5.28 Change Password Form 79
5.29 Forgot Password 79
5.30 Reset Password 79

5.31 Password Changed 79
5.32 Admin Utility 80
5.33 Overview of the Blockchain Data Storage Mechanism 81
5.34 List of Chains in BIIM 83
5.35 Blockchain Operations and Chain Management 84
5.36 Create BigchainDB Asset Function 85
5.37 Compare Administrator (Real User) with Dataset 94
5.38 System Performance 96

6.1 UDOD System Architecture 109
6.2 Taxonomy of Notifications 110
6.3 Overview of the UDOD Privacy-Aware Notifications System 113
6.4 UD Notification Classification 115
6.5 Notification of the Registration Process 116
6.6 OTP 117
6.7 Sign up Successful 117
6.8 Organization Account has been Waiting for Admin to View and Approve Documents 118
6.9 Account has been Verified 118
6.10 Verification Rejected 118
6.11 Unable to Verify your Documents 119
6.12 Notification of Login Process 119
6.13 Successful Login Using Credentials 120
6.14 Successful Login Using Face Recognition 121
6.15 Login Declined Until Account is Approved 121

6.16 Notification of Profile Update 122
6.17 Successful Profile Update 122
6.18 Notification of Change and Reset Password 124
6.19 Password Reset 124
6.20 Password Reset Unsuccessful 125
6.21 Overview of the OD System Notifications 126
6.22 Organization Requests Access User Information 128
6.23 Organization Enters Postal Code for New Request 128
6.24 Organization's Request Pending/ Awaiting Admin Action 128
6.25 Admin Receives Organization Request 129
6.26 Admin Views Organization Details and Take Action 129
6.27 Admin Approves Organization Request 130
6.28 Admin Approves Organization Request- action 130
6.29 Notification of User Approved Organization Request 131
6.30 Organization Receives Notification After Admin Approval 131
6.31 User Receives Notification After Admin Approval 131
6.32 Organization Sends a Request to the User 132
6.33 Notification with Organization Request 132
6.34 User Receives Organization Request 133
6.35 User Rejects Access to Information After Checking Organizational Details 133
6.36 User Rejects Organization Request 134
6.37 Organization Receives Alert with User Rejection 134
6.38 Organization Checks the Requests and Stats 134
6.39 User Approves Access to the Information 134
6.40 Organization Receives Alert with User Action 135

6.41 Organization Views User Information 135

7.1 FIM System Architecture 149

7.2 Federated Identity System 151

7.3 Federated Identity Management System Using Blockchain Technology . . 152

7.4 Federated Identity Management Process 153

7.5 Connect to Blockchain 154

7.6 Read Wallet Data 155

7.7 Add Identity 156

7.8 Open Current URL 157

7.9 URL 157

7.10 Deploy Code on Remix 161

7.11 Select Appropriate Compiler Version 161

7.12 Smart Contract Successfully Compiled on Remix 162

7.13 Select MetaMask on Remix for Deployment 162

7.14 Smart Contract Deployment Using MetaMask with Test Account 163

7.15 Smart Contract Successfully Deployed on the Local Ethereum Test Network 163

7.16 Ganache Test Accounts 164

7.17 Acquire Test Account's Private Key 164

7.18 Setup for the Ganache Test Network on MetaMask 165

7.19 Import Test Account to MetaMask 165

7.20 Gas Cost vs. Number of Records 168

7.21 Time Consumption vs. Number of Records 169

List of Tables

2.1 Iteration Process to Identify the Most Relevant Studies 25

2.2 Results of Applying the Quality-Assessment Criteria 26

2.3 Descriptions, Categories and Applications of Existing Studies 30

2.4 Comparative Evaluation of Research Papers based on Criteria RQ1– RQ4 32

2.6 Granular Breakdown of Existing Literature based on the Sub-class of Approach Used 37

5.1 BBIM System Evaluation for Varying User Counts 92

5.3 BBIM Algorithm Complexity Analysis 95

5.4 BIIM System vs. Traditional Systems 97

6.1 Performance Metrics for UDOD Notification Events 138

6.3 UDOD Algorithm Complexity Analysis 140

7.1 Experiment Environment 158

7.2 Evaluation Results 167

7.4 FIM Algorithm Complexity Analysis 170

List of Algorithms

1 Account Creation Procedure 67
2 Register Face 72
3 Process Face Images 73
4 Face Login Process 73
5 Change Password Procedure 78
6 Logout Procedure 79
7 Restart Blockchain 82
8 Validate Blockchain 83
9 Notification of Face Registered Process 117
10 Notification of Login Process 120
11 Notification of Update Profile Process 123
12 Notification of Change Password Process 125
13 Submit Admin Response to Organization Request Procedure 130
14 User Notification with Organization Request Procedure 132
15 Read UID Process 154
16 Add Identity Process 155
17 Delete Identity Process 156
18 Open URL Process 157

Abbreviation

BIIM - Blockchain based Intelligence Identity Management

BBIM - Biometric Blockchain Identity Management

UDOD - User-Driven and Organization-Driven Pre-emptive Privacy-Aware Notifications System. A combination of two systems, the UD system and the OD system

UD - User-Driven and Privacy-Aware Information Access System

OD - Organization-Driven and Privacy-Aware Information Access System

AI - Artificial Intelligence

MVC - Model View Controller

BLOB - Binary Large Object

HTML - HyperText Markup Language

CSS - Cascading Style Sheets

BFT - Byzantine Fault Tolerant

PoW - Prof of Work

SLR - Systematic Literature Review

EVM - Ethereum Virtual Machine

Chapter 1

Introduction

1.1 Background

In the evolving landscape of digital transformation, the protection of personal identity has become a critical component of information security and trust. The increasing reliance on online services, cloud storage, and interconnected platforms has amplified both the value and vulnerability of personal data. As cyber threats grow in sophistication, understanding the dynamics and scale of identity theft is essential for developing effective identity management solutions.

Identity theft represents one of the most persistent and costly challenges in the digital era. According to statistics from Javelin Strategy and Research, $16.8 billion was stolen from U.S. consumers in 2017 due to identity theft. Additionally, the Identity Theft Resource Center, in its 2018 End of Year Data Breach Report, reported 1,244 data breaches involving sensitive information that was potentially compromised [17].

Empirical evidence over the past decade demonstrates the growing magnitude of this problem. Recent data highlights both the persistence and scale of the issue. In 2021, approximately 23.9 million U.S. residents aged 16 or older were victims of identity theft, resulting in an estimated $16.4 billion in financial losses [59]. The Federal Trade Commission (FTC) reported over 1.1 million identity theft cases in 2022, with credit card fraud identified as the most common type [24]. In 2023, total fraud-related losses rose to $10.3 billion, representing a 16% increase from the previous year [77]. Most recently, in 2024, the FTC received over 1.16 million identity theft reports, while the FBI documented cybercrime-related losses amounting to $16.6 billion [27]. These statistics demonstrate the pervasiveness of identity theft and the continued vulnerability of personal information to

data breaches.

1.1.1 The Prevalence of Identity Theft and Data Breaches

In the wake of the 2017 data breaches at organizations such as Equifax and Uber, the U.S. has seen increasingly vocal bills and policy proposals. Notably, U.S. Senators Elizabeth Warren and Mark Warner proposed the Data Breach Prevention and Compensation Act. Had this Act been enacted into law, it would not only have enshrined in federal legislation a strict requirement for industries to maintain 'reasonable' cybersecurity measures but also established a 'Data Protection Agency' to enforce statutory requirements, investigate incidents, and provide compensation to consumers. Such proposals indicate that cybersecurity experts, the U.S. government, and citizens alike are conscious of the severity of the situation and are advocating for effective means to prevent future data breaches and identity theft [78], and [72].

Moreover, the Cambridge Analytica scandal revealed significant weaknesses in data privacy, as personally identifiable data from up to 87 million Facebook users was provided to a third-party application, 'This Is Your Digital Life', without their knowledge or consent. The scandal revealed the pressure placed on data managers to continually provide data to third-party companies, raising serious doubts about the effectiveness of existing data access solutions [42]. In contrast, traditional data storage methods rely on large centralized databases. These databases are managed by a single entity, which has the sole responsibility of managing the data and selectively grants access to trusted third parties.

A key to regaining control over personal data access and handling by third parties lies in the intersection of access management and blockchain technology [96]. Blockchain technology has received wide recognition recently due to its contribution to cryptocurrencies. This technology allows secure record management to be created in a single block and linked using cryptography, creating a stable and secure database that can be managed by multiple parties [36].

Identity management is a critical domain concerned with the administration of indi-

vidual attributes and credentials. Robust ID management systems are essential for both personal and organizational communication, underpinning services across sectors such as health, education, business, transportation, and government. Given the importance of secure and reliable identification, individuals and organizations seek systems that ensure data integrity and privacy. In this context, blockchain technology is a compelling solution for securely storing data.

Many institutions still rely on traditional ID systems, which use centralized databases dependent on third parties. This approach leads to a lack of interoperability and numerous security and privacy issues. Additionally, several privacy acts define the ownership of personally identifiable information (PII) and grant legal rights to certain organizations for its use. In 2019, Malaysia ranked fifth globally for the worst personal data security systems, with reported data breaches increasing significantly from 64 in 2018 to 178 in 2019 [35].

To address these emerging challenges in ID management, blockchain ID management studies have recently gained prominence. Various authentication mechanisms have been applied, including smart cards, passwords, and biometric methods such as fingerprints and facial recognition. For instance, Estonia was among the first countries to adopt a public-permissioned blockchain network, having digitized its national ID system as early as 2007 through the citizen digital ID program. It also introduced digital signatures for secure document signing, combining citizen IDs and PINs, and in December 2014, extended its digital identity system to non-citizens through the e-Residency program, enabling them to engage in commercial activities [89].

A self-sovereign identity allows individuals to have full control over their IDs, eliminating the need to rely on third parties. Blockchain technology provides a robust security framework in ID management, enabling users to authenticate and authorize resource access using digital signatures embedded in their digital IDs. Furthermore, blockchain can resolve data storage issues associated with most ID management systems by offering a secure decentralized network, thereby reducing the risk of ID theft [71]. It is an effective way

to reduce fraud by enhancing transparency and providing a resilient solution for protecting and recovering community IDs in disaster scenarios such as fires and earthquakes. In contrast, federated ID systems provide valuable benefits by enabling users to access various services through a single authentication method, reducing digital ID management costs. Prominent solutions in this domain include SAML, Shibboleth, Liberty Alliance framework, OpenID, and WS [45]. Blockchain-based ID systems not only focus on data storage but also offer economic IDs, which preserve individuals' reputation data by storing transactions between users to build trust relationships.

Blockchain-based approaches for managing user identities have universal applications, enabling users to own and control their IDs while easily integrating and managing them. Data is encrypted and stored securely to enhance transparency, privacy, and security. Research in blockchain-based identity management is in its infancy, offering numerous opportunities and research challenges.

1.2 Blockchain Technology

Blockchain, defined as a series of blocks containing specific information, functions as a ledger, ensuring a secure, chronological and immutable record of all transactions [49]. Each block, upon storing new information, leads to the creation of a new block, maintaining the continuity of the chain. The historical evolution of blockchain began with the pioneering work of researchers Stuart Haber and W. Scott Stornetta in 1991, aiming to create a computational solution for timestamping digital documents using cryptography. Subsequent advancements, such as the incorporation of multiple documents into a single block through Merkle Trees and Hal Finney's introduction of the concept of reusable proof of work in 2004 marked significant milestones in the development of blockchain technology. Satoshi Nakamoto's conceptualization of distributed blockchain in 2008 further solidified the foundation of this technology, eventually leading to the release of the Bitcoin White Paper in 2009. Over the years, blockchain technology continued to evolve, finding applications in various sectors and undergoing major developments, such as the separation of blockchain from currency, leading to the emergence of Blockchain 2.0 in

2014. Subsequently, the launch of the Ethereum Frontier Network in 2015 facilitated the creation of decentralized applications and smart contracts, while the introduction of the Hyperledger project by the Linux Foundation expanded the technology's reach. In 2017, the recognition of Bitcoin as a legal currency in Japan and the advent of the EOS blockchain operating system by Block. One underscored blockchain's increasing prominence. The transition of Ethereum from Proof of Work to a Proof of Stake consensus mechanism in 2022 demonstrated the technology's continued growth and adaptation to changing needs and demands [34].

In 2008, blockchain technology was first introduced to the public, along with the emergence of Bitcoin. Blockchain is considered a technological innovation that has broad implications and applications after Ethereum launched the smart contracts [97]. As technological communities and industrial giants are rapidly moving towards distinct application specifications, blockchain applications have come under comprehensive investigation. These systems allow users to obtain services with more sophisticated features. Many blockchain applications are built on immutable ledgers designed for environments where there is a lack of trust between entities. By enabling secure, transparent, and tamper-resistant record keeping, a trustworthy third party is no longer needed. As centralized storage technologies face growing scrutiny for their limitations, a blockchain-based application can increase transparency, provide immutability, and create trust between organizations. Thus, blockchain technology has attracted the attention of many researchers and practitioners due to its more advanced functionalities and features over traditional technology systems. Blockchain technology has recently been used in several applications as a way to maintain reliable records and information in a distributed and reliable manner [8], and [94].

Researchers define blockchain as a distributed ledger technology (DLT) comprising a sequence of blocks to store valuable data and information which can be shared over the network between parties [97]. Blockchain has the following key characteristics: decentralization, persistency, auditability, and anonymity. Blockchain is a technological solution to solve security issues, such as ensuring that all transactions are secured with

cryptographic hashes and asymmetric key pairs to sign and verify any type of transaction. Therefore, once the data are recorded on a blockchain, they become immutable and resistant to tampering.

Within the blockchain network, all historical transactions between nodes are recorded in the distributed ledgers. Nodes or peers are connected to a P2P network and hold a copy of the shared ledger. To add and verify transactions within the system, the miners or crypto miners need to agree on whether any new blocks are valid or not by applying consensus algorithms. The integrity and reliability of the blockchain stem directly from the consensus process. Since blockchain features work without a leader or a trusted third party, it uses consensus mechanisms to make a decision and guarantee ledgers are compatible in various nodes. There are several consensus models, such as the Proof of Work Consensus Model, Proof of Stake Consensus Model, and Proof of Authority Consensus Model. The Consensus Comparison Matrix in [97] compares the different consensus models. Cryptography and hashing mechanisms are used to construct a chain of data blocks to ensure immutability in the append-only distributed ledgers in the blockchain network. Thus, all data blocks contain a series of transactions appended to the previous blocks using the hash values as part of the stored data.

Smart contracts are a set of codes that are executed by miners. The smart contract was defined in 1994 by Nick Szabo as "a computerized transaction protocol that executes the terms of a contract" [99]. The overall goals of smart contracts are designed to satisfy common contractual conditions, such as payment terms, to minimize both malicious and occasional exceptions and to reduce the need for reliable intermediaries. A smart contract is executed by nodes through the blockchain network; all the executed nodes must derive the same results from the execution, and the results of the execution are recorded on the blockchain. However, not all blockchain platforms support smart contract execution [97].

The blockchain, a decentralized framework, plays a role in establishing trust and security for applications in the absence of a central authority. The blockchain framework enables various processes, including validation, verification, and consensus-building. By

leveraging the power of decentralized networks, applications operating on the blockchain create a robust and transparent environment for users to ensure the integrity and reliability of transactions. Blockchain technology has gained considerable recognition for its characteristics, and blockchain storage can be used as a means to establish trust [21]. It is important to document transactions within a distributed ledger composed of blocks. This involves recording each transaction in a series of blocks, which in turn creates an immutable and tamper-proof record. By implementing a consensus protocol, agreement can be reached on which block should be added to the chain. This ensures the integrity and reliability of the entire transaction process.

The persistence of identity theft and large-scale data breaches reveals fundamental weaknesses in conventional, centralized identity-management systems. These systems rely heavily on third-party authorities and centralized data repositories, which create single points of failure and increase the risk of unauthorized access. Addressing these vulnerabilities requires a paradigm shift toward decentralized, transparent, and user-controlled frameworks. Blockchain technology has emerged as a promising foundation for such frameworks, offering distributed trust, immutability, and enhanced security for digital identity management.

Portions of this chapter have been taken from a paper published in [8].

1.3 Identity Management Using Blockchain

Estonia was one of the first countries to employ a permissioned public network on blockchain. They began digitizing identities in the early 2000s, resulting in the assignment of a unique digital identity to each citizen. The document signing process was initiated through the combination of digital technology and personal identification, which allowed citizens to sign documents electronically. In response to insider data manipulation threats in 2007, Estonia took the lead in developing blockchain applications spanning various sectors. As a result, the KSI blockchain formed the basis for multiple government databases. Furthermore, in December 2014, Estonia introduced a program that allows individuals

without Estonian citizenship to obtain a digital identity, granting them the privilege of becoming e-residents [30].

1.3.1 The Impacts of Blockchain Technology in Identity Management are as follows

- *Security:* Blockchain enhances the protection of identity data through cryptographic mechanisms and consensus algorithms that prevent unauthorized access and tampering, ensuring secure authentication and data integrity in identity management systems [56].

- *Privacy:* Decentralized identity systems leverage blockchain and privacy-preserving technologies—such as zero-knowledge proofs and selective disclosure—to allow users to control their personal data while maintaining confidentiality [3].

- *Efficiency:* By removing intermediaries and enabling direct peer-to-peer credential verification, the blockchain improves the efficiency of identity verification processes, reducing latency and operational costs [82].

- *Decentralization:* Blockchain-based identity systems eliminate centralized authorities using distributed ledgers and self-sovereign identity (SSI) principles, which enhance the resilience of the system and the autonomy of the user [87].

- *Trust:* Blockchain's immutability and verifiable transaction history establish transparency and trust between stakeholders in digital ecosystems, fostering reliable credential verification and reducing fraud [22].

- *Integrity:* The distributed nature of blockchain ensures that identity records remain accurate, consistent, and tamper-proof, enhancing data reliability and authenticity across identity ecosystems [91].

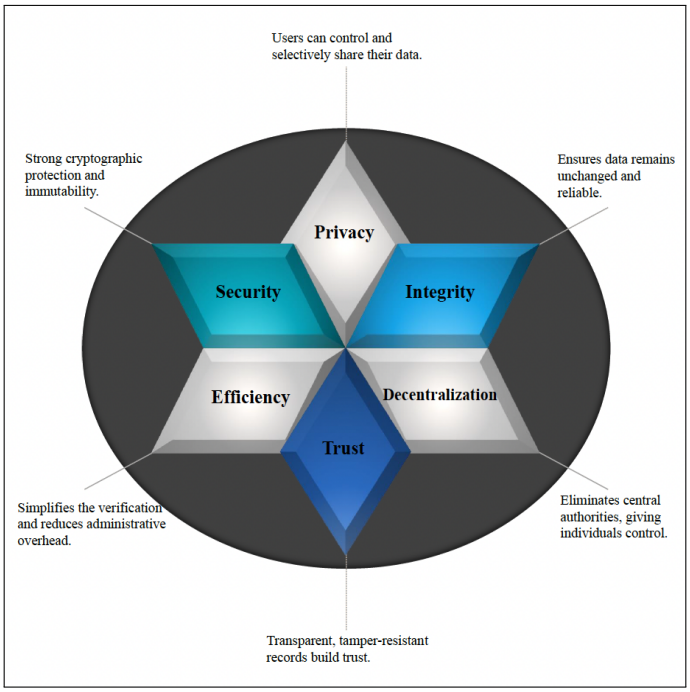


Figure 1.1 : Impact of Blockchain in Identity Management

These principles, as demonstrated in Figure 1.1, are fundamental for a strong and reliable framework in identity management. By upholding these pillars, users, systems, and organizations can establish resilient infrastructures that protect sensitive information, optimize operations, foster collaboration, and uphold data integrity. In addition, blockchain technology provides a decentralized and immutable system that enhances trust and transparency in identity management processes.

1.4 Blockchain and Biometric Technology in Identity Management

Australia has developed a decentralized blockchain ecosystem that includes facial authentication for identity verification in collaboration with IDEMIA (the global leader in Augmented Identity), BAXE (an Australian FinTech) and Haventec (an Australian software company). This collaboration facilitates compliance with Know Your Customer (KYC) requirements and commitment to data privacy regulations. It also enables safe retention of digital identities and allows users to regain access to accounts, recover passwords, and authenticate transactions through facial recognition [12].

The use of fingernail analysis incorporated into blockchain management is recommended to safeguard personal identity and enable secure authorization [53]. In terms of identity management, fingernail images are used as an identification mechanism. Picture processing using a microscope sensor helps to capture the image clearly in which the characteristic value is captured using histograms of directed gradients and local binary patterns. Attributes from an individual fingernail analysis can be stored in the blockchain platform, which has complex cryptography and only shares the identity block upon the user's authorization.

1.4.1 Advantages of Biometric Technology in Identity Management

1. Enhanced Security: Biometric authentication is more secure than passwords or PINs, which can be forgotten, stolen, or hacked.

2. User Convenience: Biometric identification, such as facial recognition, eliminates the need to recall several passwords, making it faster and more comfortable.

3. Non-repudiation: Biometrics can prove a user's identity, reducing fraud and theft.

1.5 Federated Identity Management

Federated identity management has quickly become a de-facto standard for sharing user credentials among related service providers in a trustworthy manner [86]. Facebook Connect and Google Sign-In are good examples of such systems. The maintenance of a federated system typically depends on a set of Identity Providers (IdPs), which can lead to certain points of failure and single points of authority, which makes users subject to the privacy-related policies deployed by the IdPs [75]. Federated identity management based on blockchain technology is proposed in several recent studies. In contrast to traditional federations, such systems have no centralized authority and are not governed by a specific identity provider [13].

1.5.1 Benefits of Federated Identity Management

- One-stop user authentication: One of the key and compelling advantages of federated identity management is that by using only one defined authentication mechanism,

the individual users of multiple but affiliated domains can access their data and information from any available site and service domains [43].

- Enhanced customer experience: With federated identity management, the customer or end-users do not have to keep in mind various user names/IDs, security tokens or passwords specific to different websites and service suppliers. It enables them to log into multiple authorized sites with existing user and security credentials [4].

- Single sign-on (SSO) feature: Federated identity management provides SSO features that eliminate the need to apply and enter similar sign-in and authentication credentials across different applications and services [60].

- Fulfill all security requirements: Federated identity management meets all protection and mechanisms required for an available identity management system and establishes identity & access governance, distinguishing and verifying accessor identities, and then setting identities based on guaranteed identifications [23].

A federated identity management system is integrated with a single sign-on (SSO) concept. The platform grants access to several related yet distinct domains, instead of only one domain being controlled. It allows other organizations' users (business partners, customers, etc.) to manage but also use organizations' resources as well as data, enabling users to use a single set of login data to gain access to the resources from many domains. Linking user identities is a crucial step in the process of finding and resolving multiple unique identities for a single person. After this step, users are able to log in and access IT server resources in the management system. If a user has two or more unique identities, it must be identified and linked before logging into the resources. It is also necessary to ensure data integrity and confidentiality while preserving access to the resource. Identification and authentication are the two key aspects of a security system [83].

1.6 Research Problems and Contribution

Our solution is characterized by the combination of biometric and blockchain technologies to address niche problems in identity management.

1.6.1 Research objectives

This research aims to develop an identity management system by integrating biometrics with blockchain technology. This integration aims to provide a reliable and decentralized system for managing identities, enhancing privacy and security, while empowering individuals to retain control over their personal data. The system offers a user-centered, efficient and resilient architecture for identity management. Figure 1.2 illustrates the primary components of the system, arranged in a chain to emphasize the strength and interconnectedness of blockchain integration. Furthermore, it also explains the relationship between BBIM, UDOD and FIM systems.

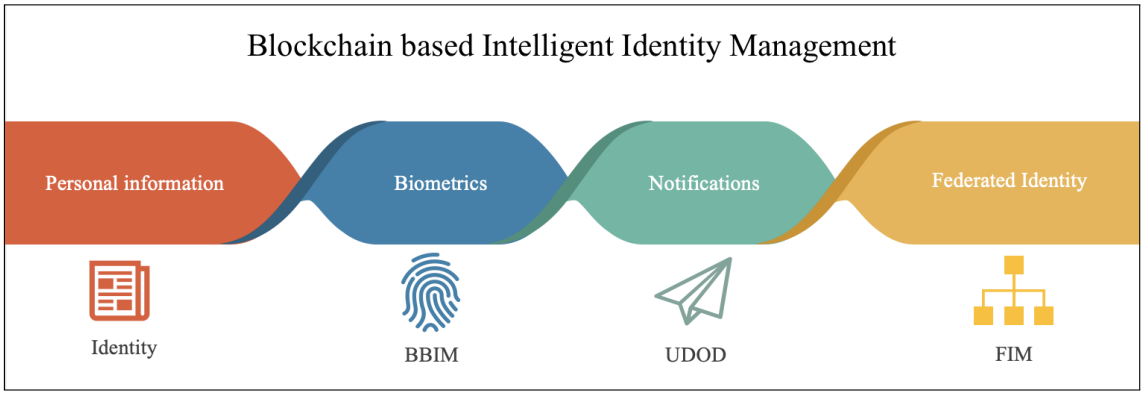


Figure 1.2 : Primary Components of the System

The following sub-objectives will be addressed to achieve our primary objective:

I. To develop a framework (BIIM) that allows the reliable and intelligent storage and management of user identities on the blockchain layer.

II. To develop an innovative measure to store biometric information on top of the blockchain layer.

III. To develop an intelligent privacy-aware measure to inform the owner of the information when personal information is accessed

IV. To develop an innovative measure to integrate federated identities into the developed biometrics-driven blockchain-based identity management system

V. To develop a prototype system to evaluate and validate the approaches (as a software prototype).

1.6.2 Research Contributions

This research provides both scientific and social contributions through the development of the BIIM framework, which advances the theoretical foundations and practical applications of secure, decentralized identity management.

1.6.2.1 Scientific Contribution

This research contributes a holistic approach to user identity management by integrating:

1. biometrics and blockchain to reliably manage user identity.
2. a user-driven approach for identity management.
3. the integration of federated identity as a part of identity management.

1.6.2.2 Social Contribution

– This research is a step towards making the Identity Management System usable from the end user's perspective. By 'usable from the end user's perspective', we mean that it is the first work of its type to develop user-centred and policy-driven approaches to send an alert when someone is requesting access to a user's information.

1.7 Thesis Structure

This dissertation focuses on the application of sophisticated identity management systems driven by blockchain technology and biometrics. It explores innovative methods that

enable people to control their identity securely and autonomously. The thesis maintains a systematic structure consisting of nine comprehensive chapters, each dedicated to examining different aspects of the research, methodology, and findings related to blockchain technologies and identity management. The structure of the thesis is as follows and an overview is provided in Figure 1.3:

Chapter 2: This chapter examines the related literature. The main objective of this chapter is to situate the present research within a suitable framework and identify research gaps that are yet to be explored. To accomplish this objective, we employ the diligent and methodical approach of a systematic literature review (SLR), which enables us to systematically identify and outline these areas of research.

Chapter 3: This chapter explains the significant terms and concepts utilized throughout the thesis. This chapter formally defines the research problem and identifies the relevant sub-questions.

Chapter 4: This chapter presents an overview of the solution for the research question. Furthermore, the sub-components of the solution overview are outlined and discussed.

Chapter 5: This chapter elaborates on the details of the blockchain-based intelligence identity management (BIIM) system and the sub-system biometric blockchain identity management (BBIM) system, their configuration, and functions. In addition, it discusses the implementation processes of these systems and provides a comprehensive evaluation of system performance and outcomes.

Chapter 6: This chapter discusses the details of the user-driven and organization-driven pre-emptive privacy-aware notifications (UDOD) system, expounding on its design, characteristics, and integration with the BIIM framework. Additionally, the chapter assesses the system's operational efficacy and the advantages it presents to its users.

Chapter 7: This chapter investigates the compatibility and expandability of the federated identity management (FIM) system in the framework of identity management based on

blockchain technology. It provides a comprehensive analysis of the implementation, results and evaluation measures of the federated identity system within the context of blockchain-based identity management.

Chapter 8: This chapter delivers an exhaustive encapsulation of the dissertation, shedding light on the paramount discoveries and the outcomes. It also maps out an array of prospective research trajectories.

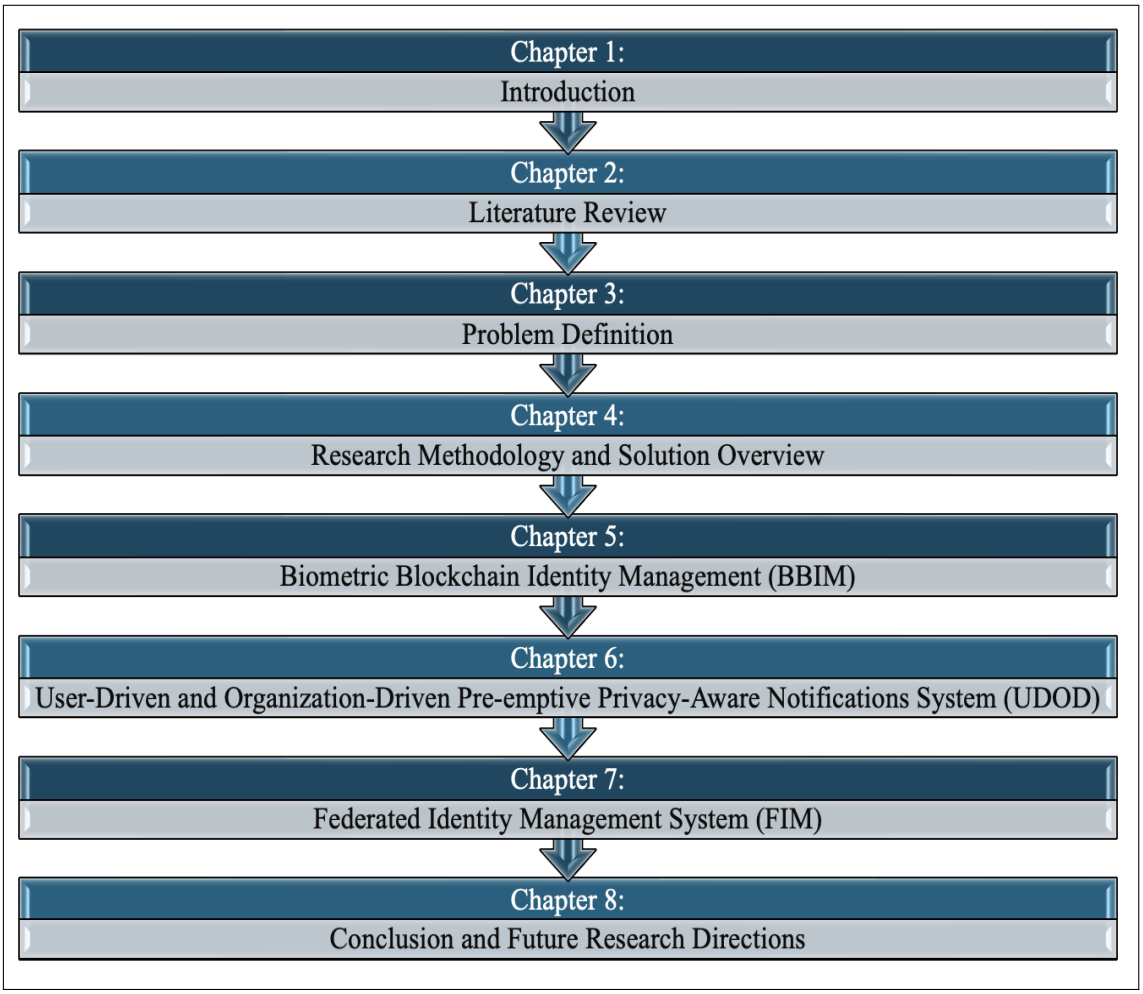


Figure 1.3 : Thesis Structure

1.8 Conclusion

This chapter outlined the significant issues relating to identity theft and data breaches, emphasizing the potential of blockchain technology to address these threats. It discussed

the integration of blockchain with biometric technology for identity management and explored the benefits of federated identity management. The chapter also identified the research problems, objectives, and contributions of this research.

The following chapter presents a systematic review of the applicable literature. This review provides a comprehensive analysis of the current solutions and identifies the gaps in the existing research. The literature review will guide the development of new insights and contribute to the field of identity management.

Chapter 2

Literature Review

2.1 Introduction

An identity management system empowers organizations to assign unique digital identities to users while overseeing authorization, authentication, and secure data sharing both within the organization and across internet-based platforms. The emergence of blockchain technology has garnered significant attention in the field of identity management [54]. Blockchain is a distributed system in which transactions are carried out and validated by all nodes. Identity management involves controlling the identity of users or entities within a system so that resources can be reserved only for authenticated and verified users. Many blockchain platforms have utilized decentralized facilities to enhance the security of digital identities. Given the widespread adoption and growing interest in blockchain, this study investigates the state-of-the-art in this area. Our research investigates the various underlying technologies that support blockchain applications in the domain of identity management. The results of this study will help individuals, governments, and private organizations understand key security issues, implementation considerations, and potential solutions related to identity management on the blockchain [14]. Furthermore, integrating blockchain and federated identity with biometric systems offers significant advantages in enhancing security and improving identity management. The collaborative implementation of these advanced technologies is poised to transform the landscape of identity and access management. In this research, we propose and develop a system for the storage of biometric information on the blockchain, coupled with an AI-based methodology for the comparison of biometric data and notifications. This innovative approach promises to revolutionize the field of identity management and security.

The structure of this chapter is as follows: Section 2.2 outlines the essential require-

ments for our system. Section 2.3 overviews the SLR process. Section 2.4 presents the literature review and categorizes the findings based on the requirements. Section 2.5 discusses the open challenges, and Section 2.6 provides a comprehensive analysis of the SLR studies. Section 2.7 concludes the chapter.

2.2 Key Requirements for Blockchain in Identity Management

This section explores the potential of blockchain technology to enhance identity management systems to improve security, privacy, and user control. Realizing these benefits involves addressing several considerations. The following subsections discuss these requirements, focusing on the integration of identity management with blockchain infrastructure, secure storage of biometric data, support for self-sovereign identity principles, and the enhancement of federated identity management through blockchain-based solutions.

2.2.1 Ability to Integrate Identity Management and Blockchain

Identity management controls access to various business systems and web-based resources, enabling organizations to define user responsibilities in accessing those resources. Identity management encompasses the entire lifecycle of digital identities, including user registration, identity authentication, identity maintenance, and identity abandonment [75]. In traditional identity management systems, such as those relying on the use of usernames and passwords, the company is entrusted with the responsibility of storing credentials such as passwords for every user, effectively acting as a third party in charge of this sensitive information [65]. This conventional setup presents challenges in terms of interoperability, security, and privacy due to the privileged position of the entity controlling the identity information. The blockchain-based approach to identity management emerges as a compelling solution to these problems, given its public accessibility over the network. This design eliminates the burden placed on a single institution for storing and maintaining every record. Moreover, blockchain employs encryption mechanisms based on private and public keys, thereby ensuring robust security [54]. This shift toward blockchain-based identity management offers effective solutions to address issues related to identity management,

access control, and privacy risks [7].

2.2.2 Ability to Store Biometrics for Authentication on Blockchain

Biometric-based authentication systems are frequently utilized in information technology because of their enhanced security and dependability [26]. These systems offer improved authentication, robust monitoring capabilities, non-repudiation, and proof of possession. They can be utilized in numerous domains, including banking, finance, mobile commerce, border movement control, e-health monitoring, and secure access to personal devices like smartphones and laptops. However, these systems typically use centralized enrollment, recognition, and identification databases. In recent years, centralized databases have become a target of choice for cyber-attacks in the form of data breaches, identity fraud, tampering, and privacy violations. As a result, there is a clear need for a decentralized, secure, and reliable authentication system that can safeguard authentication data and mitigate the impact of data privacy breaches [13].

2.2.3 Ability to Integrate Self-Sovereign Identity and Blockchain

Digital transformation has significantly impacted identity management, giving rise to the concept of self-sovereign identity, a new identity model based on the principles of user control over personal identity data [54]. Blockchain has been recognized as a key enabler of self-sovereign identity, providing the technical means to achieve its underlying principles, such as user control, enhanced security, unlinkability of transactions, and robust privacy protections. Verifiable credentials (VCs) and decentralized identifiers (DIDs) are the key standards for implementing self-sovereign identity and leveraging blockchain's immutable ledger for identity management. Once a transaction is recorded on the blockchain, it cannot be modified or deleted from any copy on the blockchain network [80]. This capability can be leveraged to create a single source of truth for identity data across multiple parties, enabling each party to trust that the identity data has not been tampered with at any stage of the lifecycle, thereby empowering organizations with the confidence they need to serve customers based on verified data.

2.2.4 Ability to Integrate Federated Identity and Blockchain

Securing and managing user identities requires the implementation of a federated identity management system [15]. Using federated identity management, users can access all resources across multiple affiliated organizations as if they were part of a single primary organization, thereby eliminating the need for repetitive authentication [13]. However, federated identity management, which allows single sign-on (SSO), is vulnerable to various attacks and suffers from issues arising due to the single point of failure in the form of the centralized identity provider (IdP) architecture. Appropriate integration of federated identity management with blockchain technology has the potential to solve a wide range of challenges [47]. A decentralized trust system can be established upon federated identity management, enhancing trust stability, privacy, and usability. Furthermore, such a system improves data sharing within a federated consortium of organizations [75] and prevents any single entity from controlling or monetizing shared data.

2.3 Systematic Literature Review (SLR) Method

This section details the systematic literature review process and highlights its significance in advancing research on blockchain-based identity management. A SLR is essential for conducting a comprehensive research study. It enables researchers to identify and evaluate relevant studies, identify existing research gaps, clarify research objectives, and assess the relevance and significance of prior work. By following a structured review process, based on the guidelines proposed by [48], the SLR ensures that relevant articles are not overlooked. The steps of the SLR process are as follows:

Step 1) Searching the literature:

This step involves conducting a comprehensive search of the relevant literature using various academic databases. The use of carefully selected search terms and filters is essential for identifying studies that directly address the research question.

Step 2) Developing inclusion and exclusion criteria:

This step involves establishing clear criteria for including and excluding studies from our findings.

Step 3) Study selection process:

This step involves systematically screening the retrieved studies based on the predetermined inclusion and exclusion criteria.

Step 4) Quality assessment criteria:

This step involves evaluating the methodological quality of the selected studies.

Step 5) Data extraction and synthesis:

This step involves extracting relevant data from the included studies using a structured approach. It requires summarizing key findings, including study characteristics, outcomes, and conclusions. Additionally, it involves identifying patterns, trends, and gaps in the data, and drawing meaningful conclusions that address the research question and objectives.

2.3.1 Searching the Literature

The following electronic scientific databases were chosen to collect the literature relevant to our search:

- IEEE (https://open.ieee.org)
- Springer (https://www.springer.com)
- ProQuest (https://www.proquest.com)
- Scopus (https://www.scopus.com)
- Web of Science (https://www.webofscience.com)

These databases were chosen as they are widely used digital platforms to ensure broad access to scholarly literature and the coverage of relevant, high-quality articles. The

search was conducted in the digital libraries of Scopus, IEEE, ProQuest, Springer and Web of Science. The search concentrated on examining records spanning from 2016 to 2024. An initial search was conducted in the databases to identify related works and close studies. The search terms were applied across the selected databases, and 207 studies were retrieved from these sources, as shown in Figure 2.1. We searched different combinations of items using the Boolean operator "OR" to retrieve the maximum number of results, and the "AND" operator to retrieve relevant studies. The search string was structured around two core components: "blockchain" as the primary focus and "identity management" as the secondary theme. These components were combined using Boolean operators and a pilot search was conducted. The search strategy employed a structured string incorporating synonym lists to maximize the retrieval of relevant studies. The selected search string included the following combinations: [("identity management" AND "blockchain" OR "distributed identity"), ("identity management" AND "self-sovereign identity" AND "distributed ledger" OR "blockchain"), ("blockchain-based identity management")]. Articles on blockchain and identity management domains were selected, and keywords in the titles, abstracts, keywords, and content were used to identify relevant articles.

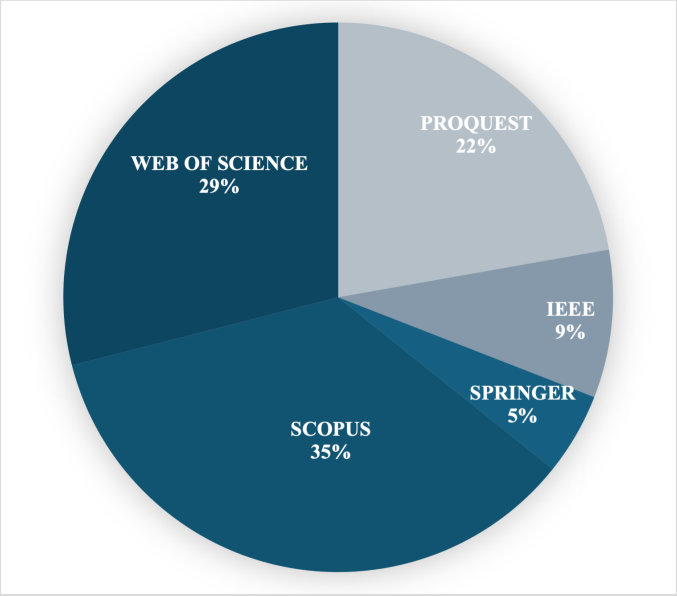


Figure 2.1 : Percentage of Studies Retrieved by Database

2.3.2 Inclusion and Exclusion Criteria

This step involves reviewing the related studies and applying inclusion and exclusion criteria to guide the selection of articles for the SLR. To be considered eligible, a study had to meet the following criteria:

Inclusion Criteria:

- The article is published between 2016 and 2024.
- The article appears in a peer-reviewed journal.
- The full text is available.
- The article focuses on blockchain-based identity.

Exclusion Criteria: The following exclusion criteria were applied:

- Duplicated studies
- Papers not written in English
- Websites, reviews, newspapers, magazines, blogs and podcasts

These inclusion and exclusion criteria ensure that only high-quality studies are included in the SLR.

2.3.3 Study Selection Process

Figures 2.2 and 2.3 display the SLR filtration process, which is a structured method for collecting and critically analyzing multiple research studies or papers. The process starts with a broad search yielding a large number of studies (207). A significant reduction in the number of studies is observed after applying inclusion/exclusion criteria and removing reviews and books. Our inclusion criteria were applied strictly, resulting in 78 studies being selected for further examination. Further filtration was undertaken by analyzing titles, abstracts, and data, leading to a final set of 15 studies being selected. The search alerts were set, and newly published research papers were continuously screened as they appeared during the final review stage.

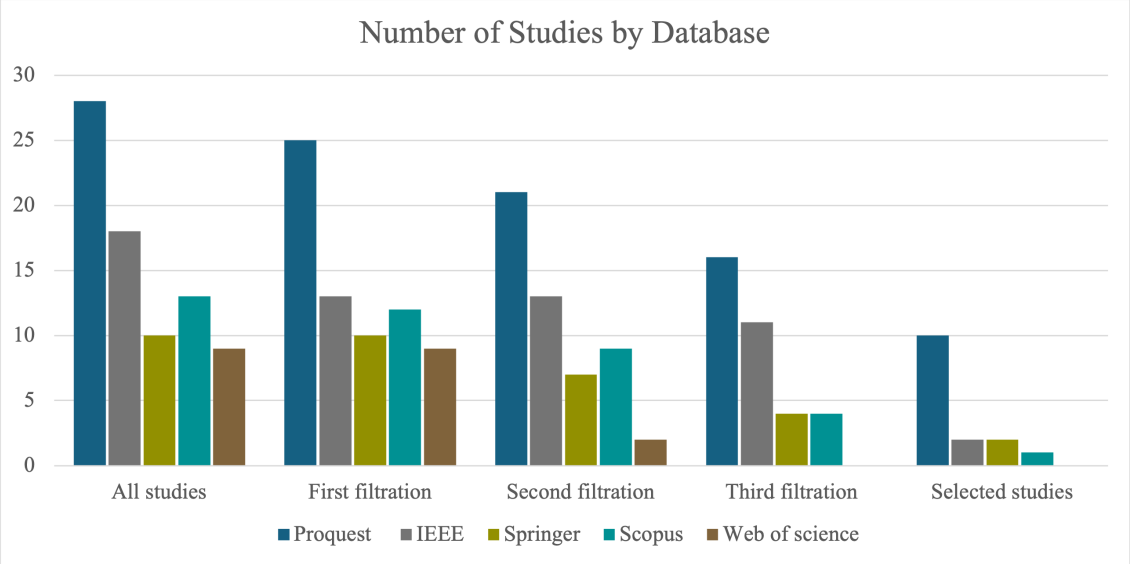


Figure 2.2 : Filtration of Studies by Database

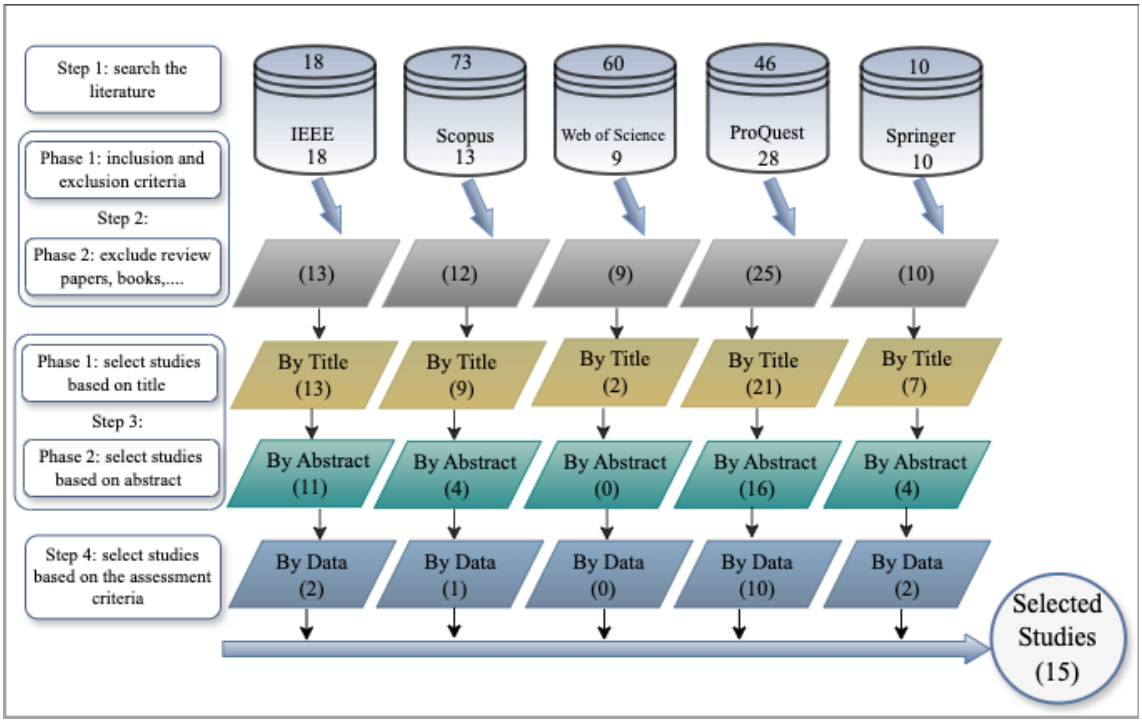


Figure 2.3 : Application of the Systematic Literature Review Process

In this step, our objective is to identify all the relevant studies that match the search string. During the filtration process detailed in Table 2.1, the number of studies decreased to 69 and then these articles were screened, resulting in the elimination of 9 studies by

rating the studies according to their compliance with the research framework. After we carefully reviewed the titles and keywords of the articles, the number of studies reduced to 52. Subsequently, the number of studies was further reduced to 35 based on their abstracts, resulting in a final selection of 15 studies. These selected studies specifically focus on identity as an abstract concept; others focus on how data management should take place when identity data is persistent, and others present functionality that spans the self-sovereignty of identity.

Database	All Studies	1^{st} filtration	2^{nd} filtration	3^{rd} filtration	Selected studies
Proquest	28	25	21	16	10
IEEE	18	13	13	11	2
Springer	10	10	7	4	2
Scopus	13	12	9	4	1
Web of science	9	9	2	0	0
Total	**78**	**69**	**52**	**35**	**15**

Table 2.1 : Iteration Process to Identify the Most Relevant Studies

2.3.4 Quality Assessment Criteria

Applying quality assessment criteria is an important step in the systematic analysis of the selected literature. During this phase, each paper is evaluated against a set of predefined quality assessment questions (QA1, QA2, QA3). To be considered methodologically sound, a paper must satisfy at least two of the three following criteria:

- QA1: Does the paper review relevant research and explore the topic of the study?
- QA2: Does the paper sufficiently explain the methods used in the research?
- QA3: Does the paper offer a detailed description and critical assessment of the results?

Table 2.2 details the results of the studies against the three quality assessment questions (QA1- QA3). To be included in the SLR, each study must meet at least two of these criteria.

Citation	Title	QA1	QA2	QA3
[2]	Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT	✓	✓	✓
[25]	Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain	✓	✗	✓
[40]	ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider	✓	✓	✗
[81]	A Framework for Online Document Verification Using Self-Sovereign Identity Technology	✓	✓	✓
[95]	A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems	✓	✓	✗
[18]	A Lightweight Blockchain-Based IoT Identity Management Approach	✓	✗	✓
[41]	Identity Management and Authentication of a UAV Swarm Based on a Blockchain	✓	✓	✓
[1]	A Blockchain Self-Sovereign Identity for Open Banking Secured by the Customer's Banking Cards	✓	✓	✓
[79]	A Blockchain Based Secure IoT System Using Device Identity Management	✓	✗	✓
[31]	INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain	✓	✓	✓
[57]	NSSIA: A New Self-Sovereign Identity Scheme with Accountability	✓	✓	✓
[64]	Decentralized Factoring for Self-Sovereign Identities	✓	✓	✗
[33]	Exploring the use of self-sovereign identity for event ticketing systems	✓	✓	✗
[46]	DNS-IdM: a blockchain identity management system to secure personal data sharing in a network	✓	✓	✓
[100]	Self-Sovereign Identity Empowered Non-Fungible Patient Tokenization for Patient-Centric Health Information Exchange Using Blockchain Technology	✓	✓	✓

Table 2.2 : Results of Applying the Quality-Assessment Criteria

2.4 Data Extraction and Synthesis: Papers selected for the systematic literature review and their categorization in addressing the requirements

The review and classification of the selected studies are detailed in Section 2.4.1. It begins by examining research on blockchain-based identity management solutions. This

is followed by a thorough investigation into self-sovereign identity and decentralization studies. In subsequent sections, the focus shifts to articles that address security and authentication. Then, the review discusses integration and interoperability. Section 2.4.2 provides a comparative analysis of the selected studies.

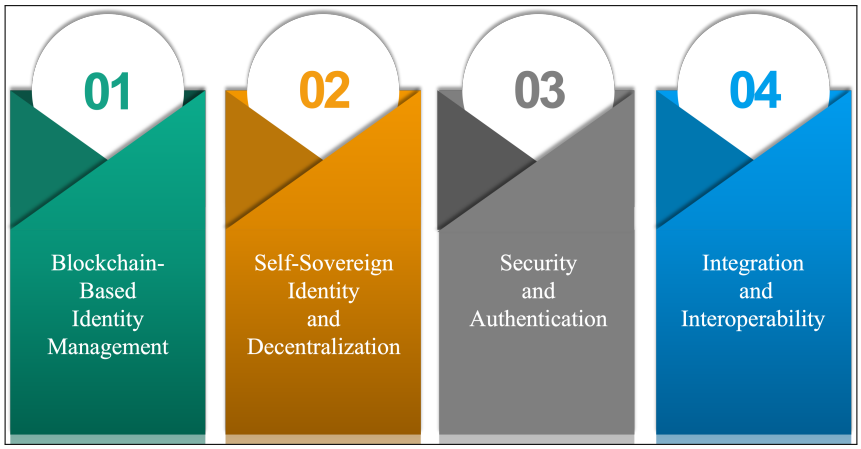


Figure 2.4 : SLR Categories for the Existing Literature

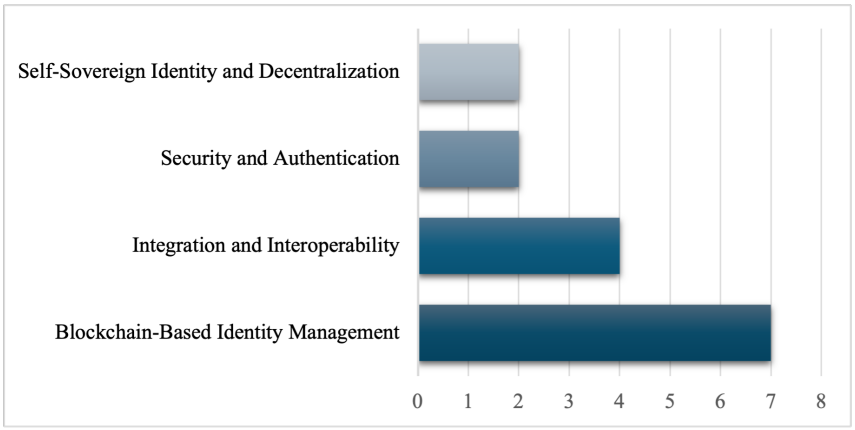


Figure 2.5 : Number of Studies by Category

2.4.1 Review of Shortlisted Papers

This section provides a brief overview of the shortlisted papers, highlighting key findings and contributions.

2.4.1.1 Blockchain-Based Identity Management

In recent years, the intersection of blockchain technology and identity management has generated significant interest across different sectors, including supply chains, healthcare, finance, and IoT. Several studies have explored the potential of blockchain to revolutionize identity management systems by utilizing its decentralized architecture, cryptographic features, and immutable ledger. Research has focused on healthcare applications, highlighting the importance of cybersecurity risk management and permissioned blockchain identity management in protecting sensitive health data [2] and [95]. Similarly, blockchain identity management has been investigated for secure IoT systems, emphasizing the need for enhanced security and trustworthiness in IoT devices and data [79]. In the finance sector, blockchain self-sovereign identity solutions have been proposed for open banking environments, aiming to empower customers with greater control over their financial identities and transactions [1]. Furthermore, INCHAIN, a cyber insurance architecture, integrates self-sovereign identity principles to enhance transparency and efficiency in insurance processes [31]. Additionally, the use of blockchain technology for non-fungible patient tokenization, driven by self-sovereign identity, has been explored to facilitate patient-centric health information exchange [100]. These studies collectively underscore the potential of blockchain to address cybersecurity risks, enhance data privacy, and foster trust in identity management systems across several domains.

2.4.1.2 Self-Sovereign Identity and Decentralization

A common theme among the reviewed articles is the concept of self-sovereign identity, where individuals have control over their own identity without reliance on centralized authorities. For instance, ATIB facilitates efficient integration with existing systems while preserving user autonomy and trust [40]. Similarly, NSSIA enhances privacy and security in digital identity management [57]. These studies highlight the importance of decentralization and user empowerment in addressing privacy concerns and reducing dependency on centralized identity providers.

2.4.1.3 Security and Authentication

A fast and smooth lightweight blockchain-based identity management solution has been advanced for integrating identity solutions into IoT networks without performance bottlenecks [18]. Similarly, online document verification using self-sovereign identity has been explored, focusing on enhancing security and reliability [81]. Further investigations into identity management for UAV swarms with blockchain emphasize secure and decentralized authentication [41]. These studies underscore the role of blockchain in ensuring secure, tamper-proof identity verification processes and authentication mechanisms across various applications.

2.4.1.4 Integration and Interoperability

Integration and interoperability are key considerations in developing blockchain-based identity management systems, particularly in domains such as food supply chains, personal data sharing, and event ticketing. A study of blockchain and self-sovereign identity for food chain quality aims to improve traceability and transparency through decentralized management [25]. Furthermore, the DNS-IdM system provides a blockchain-based approach for sharing personal data, focusing on interoperability and secure data exchange across networks [46]. Research into decentralized factoring for self-sovereign identities addresses interoperability challenges in identity management systems [64]. Additionally, the implementation of self-sovereign identity in event ticketing systems has been investigated to enhance user experiences [33]. These studies highlight the importance of integration and interoperability in realizing the full potential of blockchain-based identity management solutions.

Study	Year	Description	Category	Application
[2]	2022	Developed a framework for managing cybersecurity risks in blockchain, focusing on vulnerabilities in smart contracts, consensus mechanisms, and network infrastructure. Proposed systematic risk assessment and mitigation strategies.	BIM	Health IoT
[25]	2021	Discussed using blockchain and self-sovereign identity to enhance trust, privacy, and security in support services. Highlighted decentralized identity solutions for various contexts like customer service.	II	Food Supply Chain
[40]	2021	Proposed an architecture for brokered self-sovereign identity integration, enabling service providers to aggregate trust-enhancing attributes from multiple identity providers to improve user privacy and data control.	SSI	Service Providers
[81]	2022	Developed a blockchain framework for online document verification, using tamper-proof hashing and smart contract-based verification processes to enhance security and trust in digital documents.	SA	Document Verification
[95]	2020	Implemented an identity management system using permissioned blockchain, storing identity attributes on-chain with smart contract-enforced access controls, balancing decentralization and privacy for enterprises.	BIM	E-Health Systems
[18]	2021	Designed a lightweight blockchain-based identity management system for IoT devices, utilizing lightweight consensus mechanisms and optimized data structures to minimize resource requirements while ensuring security.	BIM	IoT
[41]	2022	Developed authentication mechanisms for UAV systems, ensuring secure interactions with ground control and other UAVs. Addressed challenges in securing UAV communications and identity assertions.	SA	UAV Systems
[1]	2023	Developed a self-sovereign identity solution for open banking, enhancing user control over personal data through decentralized identity management systems on blockchain, ensuring secure and verifiable interactions.	BIM	Open Banking
[79]	2022	Enhanced IoT device security using blockchain technology, focusing on device identity management to protect against data breaches and unauthorized access.	BIM	IoT
[31]	2024	Designed a cyber insurance architecture with smart contracts and self-sovereign identity on blockchain, improving transparency and efficiency. Proposed a decentralized insurance marketplace with automated claims settlement.	BIM	Cyber Insurance
[57]	2022	Introduced a novel self-sovereign identity scheme integrating cryptographic primitives, decentralized identifiers, and verifiable credentials to enhance user privacy, data ownership, and interoperability.	SSI	General
[64]	2021	Discussed decentralized factoring for self-sovereign identities, emphasizing secure and efficient identity management through blockchain technology.	II	Decentralized Factoring
[33]	2022	Explored self-sovereign identity in e-commerce, enhancing user control over personal data and reducing reliance on centralized identity providers. Addressed identity-related challenges and user consent management.	II	Event Ticketing
[46]	2019	Designed a blockchain-based identity management system for secure personal data sharing, integrating privacy-enhancing technologies like zero-knowledge proofs and data encryption to protect user data.	II	Personal Data Sharing
[100]	2023	Applied self-sovereign identity and blockchain for secure health information exchange. Proposed a tokenization framework for patient health records, enhancing data integrity and patient privacy through controlled access.	BIM	Health Information Exchange

Blockchain-Based Identity Management (BIM), Self-Sovereign Identity and Decentralization (SSI), Security and Authentication (SA), and Integration and Interoperability (II).

Table 2.3 : Descriptions, Categories and Applications of Existing Studies

2.4.2 Comparative Analysis

We gathered data from the selected studies and arranged them in a table against each research question. We analyzed and classified the studies into several categories. The first category comprises research works where identity management can be used efficiently to ensure privacy. The second category relates to the biometric authentication of users' identities. The third category focuses on self-sovereign identity. The fourth category concentrates on federated identity management.

Based on the review of the existing literature discussed previously, we conducted a critical comparative analysis across four key dimensions, as follows:

a) Does the paper address identity management?

b) Is biometrics employed in the authentication or validation?

c) Does the paper focus on self-sovereignty?

d) Is there any discussion of federated systems?

Table 2.4 compares and analyses the 15 articles with respect to the key requirements RQ1- RQ4. We faced challenges during this step, mostly related to defining the classification categories. Iterating the process led to clearer themes and more consistent classification categories. It also highlighted the need to exclude a category or theme due to an insufficient number of papers classified under those domains.

Study	Title	RQ1	RQ2	RQ3	RQ4
[2]	Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT	✓	✓	✗	✗
[25]	Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain	✓	✗	✓	✗
[40]	ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider	✓	✗	✓	✗
[81]	A Framework for Online Document Verification Using Self-Sovereign Identity Technology	✓	✗	✓	✗
[95]	A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems	✓	✓	✗	✗
[18]	A Lightweight Blockchain-Based IoT Identity Management Approach	✓	✗	✗	✗
[41]	Identity Management and Authentication of a UAV Swarm Based on a Blockchain	✓	✗	✗	✗
[1]	A Blockchain Self-Sovereign Identity for Open Banking Secured by the Customer's Banking Cards	✗	✓	✓	✗
[79]	A Blockchain Based Secure IoT System Using Device Identity Management	✓	✗	✗	✗
[31]	INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain	✗	✗	✓	✗
[57]	NSSIA: A New Self-Sovereign Identity Scheme with Accountability	✗	✗	✓	✗
[64]	Decentralized Factoring for Self-Sovereign Identities	✗	✗	✓	✗
[33]	Exploring the use of self-sovereign identity for event ticketing systems	✗	✗	✓	✗
[46]	DNS-IdM: a blockchain identity management system to secure personal data sharing in a network	✓	✗	✗	✗
[100]	Self-Sovereign Identity Empowered Non-Fungible Patient Tokenization for Patient-Centric Health Information Exchange Using Blockchain Technology	✗	✓	✓	✗

Table 2.4 : Comparative Evaluation of Research Papers based on Criteria RQ1– RQ4

Based on the comparative analysis, we identify the following research gaps in the literature on blockchain-based identity management:]

a) The existing blockchain-based identity management systems do not take into account biometrics.

b) The existing literature lacks blockchain and AI-driven approaches to intelligently and reliably manage self-sovereign identities

c) The existing literature does not use blockchain and AI-driven approaches to manage federated identities

Our review indicates that while many studies have explored the use of blockchain in identity management, none have addressed the aforementioned shortcomings. Additionally, our analysis highlights a significant research gap: there is no existing work on using blockchain to intelligently provision, manage, and decommission self-sovereign and federated identities.

In the future, carrying physical copies of documents such as driver's licenses, birth certificates, passports, and visas may become unnecessary. We can simplify our lives by storing all identity information in an easily manageable location. Blockchain collaborates at various levels in identity management to enhance security and reduce costs, particularly when managing sensitive personal data [57].

2.5 Open Challenges: Identify Research Gaps

2.5.1 Identity Management Capability

Most studies address identity management, with many utilizing blockchain technology. For instance, a framework for identity management and user authentication within e-health systems employs the fundamental security features of a permissioned blockchain to ensure data confidentiality and integrity [95]. Another study explores blockchain-based authentication for UAV swarms, alongside the implementation of identity systems tailored to the custom requirements of enhanced e-health environments [41]. Furthermore, a proposed blockchain-based system designed for secure personal data sharing within networks highlights the technology's versatile role in identity management [46]. Other research similarly emphasizes the use of blockchain for robust identity management across diverse sectors [25] and [18].

Considerable research focuses on IoT identity management, particularly within the healthcare sector [2], [79], and [18]. A proposed framework for managing cybersecurity risks in blockchain-based identity systems for Health IoT (HIoT) highlights how a de-centralized, immutable ledger enhances secure identity management [2]. This research reviews potential security risks in HIoT systems utilizing blockchain-based identity man-

agement (IdM), noting that while the technology improves security and privacy, inherent risks remain. Consequently, a new framework was developed to assist organizations in managing these cybersecurity risks for HIoT systems. Similarly, investigations into IoT identity management provide insightful perceptions regarding blockchain applications for enhancing operational efficiencies [79] and [18]. However, further work is required to advance these technologies, particularly by developing robust solutions for the complex challenge of identifying individuals in medical settings during healthcare delivery.

While scholars have extensively examined various aspects of identity management, there remains a notable gap in the development of solutions capable of addressing multiple identity-related problems simultaneously. Many papers discuss identity management systems exclusively for a particular industry, such as healthcare, finance, or IoT. The narrow focus on specific industries undermines the broader requirements of the identity management domain. Nevertheless, our system aspires to exceed inter-sector or application demarcations by means of a systematic identity management technique that is also replicable across different sectors and areas. The application of blockchain technology allows users to secure the management of all their identities and control their privacy across different platforms and services. This approach, therefore, fosters a flexible and interoperable framework that may be employed across different industries and applications that require verifiable identities.

2.5.2 Capability to Integrate Biometrics for Authentication or Validation

Biometrics are employed in several of the reviewed papers, often in conjunction with blockchain-based identity frameworks [2] and [95]. However, as evidenced by the current state of the literature, scant research has been conducted in this field. Surprisingly, the issue of biometric integration is not addressed adequately by some of the most prominent references in the domain of self-sovereign identification. Some approaches incorporate biometric techniques into authentication mechanisms, utilizing blockchain to securely store and manage biometric data [2] and [95]. In other applications, such as blockchain self-sovereign identity systems for open banking, biometrics are integrated using customer

banking cards secured with biometric data [1]. These instances highlight the selective and significant use of biometrics in authentication processes.

Another study [100] on blockchain-based secure data sharing for healthcare provides a new method for applying patient tokenization in blockchain-based systems, which suggests the possibility of adding biometric data to future solutions. Their concept of self-sovereign identity and their use case for non-fungible patient tokenization for patient-centric health information exchange using blockchain technology provides a valuable framework on which future research can build. However, the integration and utilization of biometrics in blockchain-based IDM frameworks is a research direction that holds significant potential for improving security measures, as well as the authentication and user identification processes. Although some of the existing research is focused on the need to use biometric data for identity verification, further study and experiments need to be conducted that will advance the identity authentication process based on biometric data.

2.5.3 Capacity to Concentrate on Self-Sovereignty

Several studies focus on self-sovereign identity, with blockchain being a key enabling technology. The work in [25], [1], [31] and [100] provides information on the importance of individuals having sovereignty over their identity, particularly regarding control of access rights to their identity data. These studies also highlight the need for more research and practical application of self-sovereign identity concepts. While the concept of self-sovereignty is expanding, there are still significant gaps that need to be addressed to fully realize its benefits.

The use of blockchain and self-sovereign identity has been explored to enhance quality within the food supply chain, granting individuals control over their personal data while ensuring its authenticity [25]. Furthermore, various frameworks and architectures for self-sovereign identity utilize blockchain to facilitate decentralized identity management and enhance trust through transparent, tamper-proof records [40] and [81]. Detailed explanations of how self-sovereign identity principles operate on the blockchain demonstrate how these notions can be practically implemented and scaled in real-world scenarios [40].

While current research suggests the need for improved strategies and innovative tools, existing theories provide a solid foundation for enhancing self-sovereign capabilities. Notably, the potential of self-sovereign identity frameworks, including user-friendly standards such as Verifiable Credentials and Decentralized Identifiers (DIDs), has been significantly advanced in recent models [81] and [64].

Research emphasizes that several issues beyond vision must be addressed to establish a Self-Sovereign Identity. This includes the necessity for user support regarding individual data mobilization notices, which may be more critical than current protocols and standards [57]. Furthermore, steps must be taken to ensure individuals maintain full control over their identifying data, necessitating the real-world implementation of decentralized identity solutions that empower individual autonomy [81]. Such gaps create significant opportunities for future research to develop decentralized identity management systems while reinforcing the privacy rights of citizens in the digital environment [1] and [31]. Collectively, these studies highlight blockchain's crucial role in realizing self-sovereign identity.

Research into identity management through blockchain incorporates privacy-preserving elements for personal data use within network identity provider-based systems [100]. However, studies focusing specifically on self-sovereign identity and blockchain-based management remain limited. Therefore, a deeper analysis of emerging innovations and challenges in identity management across various fields is essential to address these gaps.

2.5.4 Integration with Federated Systems

Federated systems are not prominently discussed in the reviewed literature, as there is a clear preference for decentralized or self-sovereign identity systems facilitated by blockchain technology. This gap indicates an area for future research to explore the potential application of blockchain in enhancing federated identity management across various organizations and domains. For instance, the healthcare sector could greatly benefit from such advancements, particularly in securely and efficiently sharing patient details. Similarly, in banking, fintech, and other established sectors, there is a critical need for

robust and reliable identity management systems. Blockchain can promote cross-system integration and trust within federated environments, significantly improving the prospects of these solutions. Implementing blockchain would substantially enhance the overall utility and security of the identity management framework.

2.6 Comprehensive Analysis of SLR Studies: Authentication Methods, Security Mechanisms, Security Threats and Blockchain Platforms

Table 2.6 provides a comprehensive summary of various studies that explore different classifications of blockchain-based systems, focusing on authentication methods, security mechanisms, primary security threats, and blockchain platforms. The sub-class represents the primary approach used for identity management. Each study presents its contributions and addresses specific challenges within the identity context.

Classification	Sub-class	Study
Authentication Methods	Attribute	[25], [40], [81], [18], [79], [41], [31], [2], [64], [33], [46]
	Biometrics	[57], [95], [1], [100]
Security Mechanisms	Encryption	[25], [40], [64], [81], [95], [41]
	Tokenization	[100]
	Smart Contracts	[1], [18], [79], [31], [2], [46]
	Accountability	[57], [33]
Security Threats	Data Breaches	[2], [25], [40], [95], [18], [1], [41], [57], [46], [100]
	Unauthorized Access	[40], [95], [18], [1], [46], [81], [64], [79], [100]
	Fraud Prevention	[18], [81], [57], [33], [31]
	Identity Theft	[57], [2], [100]
Blockchain Platforms	Hyper-ledger Fabric	[41], [18]
	Ethereum	[46], [31], [25], [40], [57], [64], [1], [79]
	Hyper-ledger Indy	[81]
	Quorum	[100]
	Other	[2], [33], [95]

Table 2.6 : Granular Breakdown of Existing Literature based on the Sub-class of Approach Used

2.6.1 Authentication Methods

We have further divided the literature on authentication methods into two sub-classes, namely attribute and biometrics. Authentication methods are essential in ensuring the identity of users in various systems. Several studies [25], [40], [81], [18], [41] , [79], [41], [31], [2], [64] and [46] focus on credentials, digital certificates, and attribute-based authentication, highlighting the use of specific attributes or characteristics to verify identity. Biometrics, which includes unique physical characteristics like fingerprints or facial recognition, is explored in several studies [57], [95], [1] and [100].

2.6.2 Security Mechanisms

Security mechanisms involve various methods and technologies designed to protect data and ensure secure operations. In the literature, these mechanisms are categorized into several sub-classes, including encryption, tokenization, smart contracts, and accountability mechanisms. Encryption, which secures data by transforming it into unreadable formats that cannot be decrypted without the correct decryption key, is discussed in several studies [25], [40] [64], [81], [95] and [41]. Tokenization, discussed in [100], is a process where sensitive data is replaced with unique identification symbols. Several studies [1], [18], [79], [2], [31] and [46] explore smart contracts, which are self-executing agreements with terms directly encoded into software. These contracts ensure security and transparency in transactions. Accountability mechanisms, which ensure that actions can be traced back to responsible parties, are discussed in [57] and [33].

2.6.3 Security Threats

Security threats encompass various risks and vulnerabilities, forming a primary classification within the literature. These are further subdivided into several sub-classes, including data breaches, unauthorized access, fraud prevention, and identity theft. Data breaches, involving the compromise of sensitive information, are a major focus of extensive research citeAlamri, [25], [40], [95], [18], [1], [41], [57], [46] and [100]. Similarly, unauthorized access, where attackers gain unsanctioned entry to systems, is explored in multiple studies

[40], [95] [18], [1], [46], [81], [64], [79] and [100]. Fraud prevention, aimed at detecting and mitigating fraudulent activities, is also widely discussed [18], [81], [57], [31] and [33], while identity theft and the misappropriation of personal information are specifically covered in [2], [57] and [100]. This emphasis on data breaches and unauthorized access reflects their critical impact on system security. Notably, while some frameworks address general security, certain studies do not explicitly detail specific sub-classifications related to these threats [2].

2.6.4 Blockchain Platforms

The literature in this classification is systematically divided into five sub-classes, where various blockchain platforms ensure the secure functioning of systems and protocols. For instance, Hyperledger Fabric has been analyzed as a foundational blockchain framework [41], [18], while Ethereum, a decentralized platform for executing smart contracts, is extensively discussed across multiple studies [46], [25], [40], [57], [31], [64], [1] and [79]. Additionally, Hyperledger Indy, which provides dedicated tools for identity management, is a primary focus for decentralized solutions [81], and Quorum is explored as a permissioned blockchain service [100]. This variety in blockchain platforms demonstrates the diverse strategies employed to enhance security within identity management systems.

2.7 Conclusion

This chapter explored the intersection of blockchain technology and identity management to understand the current landscape and future potential of this integration. It reported on a systematic literature review conducted to identify and analyze existing research within the domain. This comprehensive review identified significant research gaps and highlighted areas requiring further investigation. These findings provide a solid foundation for guiding the research direction to address the most pertinent and unexplored issues in the field. By uncovering these gaps, this work aims to contribute to the development of more secure, efficient, and user-centric identity management systems leveraging blockchain technology. Ultimately, this review sets the stage for innovative solutions that can transform digital

identity management practices.

The next chapter identifies the primary terms used in this research, ensuring clarity and a shared understanding of key concepts. Additionally, it presents the research questions and objectives, establishing the framework for a detailed exploration of the research aims and methodology in the subsequent chapters.

Chapter 3

Problem Definition

3.1 Introduction

This chapter presents the main research question and objectives, following a comprehensive review of the relevant literature in Chapter 2. The literature review and the evaluation enabled us to examine the related research and identify the key gaps that serve as the basis for the research objectives outlined in this chapter. Section 3.2 defines the key technical terms and concepts. Section 3.3 introduces the problem, and Section 3.4 discusses the research questions and subquestions. Section 3.5 details the research objectives, and the chapter concludes in Section 3.6.

3.2 Glossary of key technical terms and key concepts

Blockchain identity management involves a distinct set of terminologies, although different projects may adopt varying terminology. It is important to understand the meaning of the following terminologies:

3.2.1 Blockchain

A blockchain is a distributed ledger technology (DLT) that enables a secure, immutable, and transparent record of transactions and assets. It operates as a decentralized database; each "block" contains transaction data and is cryptographically linked to the previous block, forming a chain. This structure provides a reliable and tamper-proof record [49].

3.2.2 Biometrics

Biometrics is the science of defining or verifying the identity of a person based on behavioral and physiological characteristics [76].

3.2.3 Identity Management System

An identity management system stores the attributes associated with users and employs these attributes to facilitate authorization [16].

3.2.4 A Distributed Ledger

A distributed ledger is a database that is accessible from different locations, nations, or even different organizations [19].

3.2.5 Federated Identity Management

Federated identity management (FIM) is a set of distributed trust domains and trust-building mechanisms. The most popular and widely deployed FIM system is the one developed by Liberty Alliance. FIM is a single sign-on (SSO) that allows users, either individuals or organizations, to authenticate at a single domain and use the same identification data to obtain access to multiple systems [11]. In the SSO, a service provider (SP) trusts authentication statements from an external identity provider (IdP) that is responsible for authenticating multiple diverse constituencies [86].

3.2.6 Proof of Work (PoW)

Proof of Work (PoW) serves as one of the underlying consensus mechanisms used in blockchain systems. It plays a critical role in validating and securing blocks before they are appended to the blockchain. This mechanism ensures that transactions are verified and safely incorporated into the distributed ledger through cryptographic verification and computational effort [44].

3.2.7 End-User

The end-user is the individual or organization that ultimately interacts with the BIIM system, actively employing its features and functionalities.

3.2.8 Administrator

The administrator is responsible for the verification of documents. The terms admin and administrator are used interchangeably. In BIIM, the role of the administrator is as follows:

- The administrator is not responsible for managing any user identities.
- The administrator verifies all accounts when uploading a new ID.
- The administrator facilitates communication between users and organizations.
- The administrator ensures that the user and the organization are verified accounts, which adds a layer of security and oversight.

3.2.9 User

A user is an individual who uses BIIM to manage and control their identity.

3.2.10 Organization

An organization is any third party, such as an institution, that uses BIIM to authenticate their accounts and access user information securely.

3.2.11 Design Science Research Methodology (DSRM)

This is a process for conducting design science research, which is a research approach aimed at developing and evaluating innovative artifacts, such as methods, models, and systems, to solve practical problems [73].

3.2.12 Python Django Framework

Django is a high-level, free and open-source Python web framework constructed by experienced developers. It is designed to facilitate expedited development and support a structured and practical design. The Python Django framework facilitates rapid development and supports a structured and practical design. It effectively allows developers to focus on application logic rather than dealing with redundant tasks [29].

3.2.13 MySQL Database

The MySQL database management system is an open-source relational database solution that organizes data into separate tables instead of a centralized storage system and is known for its speed, reliability and scalability. It is utilized in web applications for data storage and retrieval. In addition, it is compatible with various programming languages and platforms[69].

The next section defines the problem.

3.3 Problem Definition

Based on the extensive systematic literature review and the discussion in Chapter 2, the following research gaps have been identified:

a) The existing blockchain-based identity management solutions have not been integrated with artificial intelligence. AI can be used on top of blockchain-based solutions to help both providers and consumers, as well as in carrying out identity management such as biometrics-based authentication.

b) Lack of blockchain and AI-driven approaches to intelligently and reliably manage self-sovereign identities.

c) Lack of blockchain and AI-driven approaches to manage federated identities.

To address the identified research gaps, the next section defines the research question and sub-questions.

3.4 Research Question and Sub-Questions

A systematic review of the literature was detailed in Chapter 2. In light of this, we identified the following main research questions and sub-questions to guide our research objectives:

3.4.1 Main Research Question

How can biometrics-based approaches *integrated* with the use of blockchain be used to provide reliable and scalable identity management?
To address this research question, we break it down into the following sub-questions:

3.4.2 Research Sub-Questions

Research Question 1: How can we develop a scalable framework to collect and store personal data required to establish user identities?

Research Question 2: How can biometric information collected from individuals be stored in a reliable and scalable manner in the blockchain layer?

Research Question 3: How can intelligent approaches be used to alert the owner of the information prior to anyone accessing or changing the user's identity details?

Research Question 4: How can existing federated identities be integrated into the developed biometrics-driven blockchain-based identity management system?

Research Question 5: How can the proposed framework be evaluated and validated?

3.5 Research Objectives

The primary objective of this thesis is to integrate biometrics and blockchain for identity management. This integration aims to create a distributed, reliable identity management system that enhances privacy and security while allowing users to maintain a self-sovereign identity. The approach offers a highly secure, efficient, and user-centric model of identity management, utilizing the immutability of blockchain to protect biometric data and maintain data integrity. This objective will be accomplished by achieving the following sub-objectives 1 to 5:

Objective (1): To develop a framework (BIIM) that enables the reliable and intelligent storage and management of user identities on the blockchain layer.

This objective will be achieved by implementing the BIIM platform, which facilitates

the secure storage and management of user identities using the blockchain. It involves the user registering with a unique email address and their comprehensive data and biometric information being securely stored on the blockchain layer, preventing duplicate identities and ensuring data integrity.

The system also ensures privacy by allowing users to manage their identities independently and decide whether to share or withhold data from any third party, with the recognition that governments can access data when required. This user-centric approach empowers individuals to effectively govern their identities. In addition, in the organizational context, the system ensures the trustworthy handling of registered individual identities. The organization is mandated to share a specific code to request access to the identity or data of any user associated with that code. This process establishes a secure and controlled means of obtaining the necessary information from the system when the user is allowed access. Furthermore, BIIM maintains transparency by storing identity information and modifications on the blockchain, ensuring a tamper-proof record and reinforcing user confidence in the security of their data. The detailed solution to this objective can be found in Chapter 5.

Our proposed system (BIIM) comprises the following subsystems: *BBIM system*, *UDOD system* and *FIM system*.

Objective (2): To develop innovative measures to store biometric information on top of the blockchain layer.

This objective will be achieved by implementing the BBIM system in the BIIM platform using a face recognition algorithm. BBIM focuses on the biometric aspect, whereas the BIIM is the overall system. The aim is to store biometric information securely on the blockchain, enhancing the security and reliability of user identity verification. The system stores the user's information on a block, and then their biometric data including detection of non-real or duplicate identities. This ensures maximum security and minimizes the risk of breach or falsification. The detailed solution to this objective can be found in Chapter 5.

Objective (3): To develop an intelligent privacy-aware measure to inform the owner of the information if their information has been accessed

This objective will be achieved by implementing the UDOD system in BIIM, which sets notifications based on interaction within BIIM and communication between BIIM entities. The approach will include control over personal data to ensure that the BIIM system remains aligned with the self-sovereignty of user identity. The detailed solution to this objective can be found in Chapter 6.

Objective (4): To develop an innovative measure to integrate federated identities into the developed biometrics-driven blockchain-based identity management system

This objective will be achieved by implementing the FIM system using Ethereum. The aim is to enable the integration of various identity sources and platforms to store and manage identities securely. The approach involves generating a token for each identity and storing it in a wallet, allowing users to access multiple services or applications. A detailed solution for this objective can be found in Chapter 7.

Objective (5): To develop a prototype system to evaluate and validate the approaches (as a software prototype).

This objective will be achieved by evaluating the BIIM system, which involves the utilization of methodologies such as usability testing to assess the functionality and requirements of the system. This requires testing the system's security and overall performance to identify areas for improvement. The objectives must follow a structured, step-by-step process to ensure systematic validation. The detailed solution to this objective can be found in Chapters 5, 6 and 7.

Each objective plays a critical role in achieving the primary goal of developing a reliable and distributed identity management system. By addressing these objectives, a comprehensive approach will be developed to secure a user-centric identity management system that leverages the strengths of blockchain and biometric technologies.

3.6 Conclusion

This chapter elaborates on the fundamental terms used in this research and presents the research questions and objectives that are explored in the subsequent chapters. By clarifying these terms, we set the stage for a deeper understanding of the study's context and significance.

The next chapter thoroughly discusses the research methodology and justifies our approaches. This includes a solution overview detailing how they align with our research objectives. This comprehensive discussion provides a clear framework for the implementation and evaluation of our solutions.

Chapter 4

Research Methodology and Solution Overview

4.1 Introduction

The scientific contribution of the BBIM subsystem is reflected in the design and implementation of algorithms that embed biometric identifiers within the BIIM framework. The subsystem captures biometric data such as facial images and generates a profile, which is cross-validated against government-issued identity documents. Following verification, the biometric template and associated identity attributes are immutably recorded on the blockchain, ensuring integrity, non-repudiation, and resistance to tampering. Systematic evaluation of the BBIM has demonstrated its scalability, data integrity, and detection accuracy, with results confirming reliability, efficiency, and applicability in real-world contexts. The social contribution of the BBIM subsystem lies in the provision of tamper-resistant authentication that enhances confidence between users and service providers. Through the protection of sensitive biometric identifiers and the empowerment of individuals to control their identity data, BBIM enhances trust, transparency, and accountability within digital identity ecosystems. Within the BIIM architecture, the novelty of the BBIM subsystem is located not only in the immutable recording of biometric identifiers but also in its coherent integration with the FIM and UDOD subsystems. By ensuring secure, duplication-resistant, and verifiable enrollment, BBIM provides the foundation on which FIM and UDOD operate. Collectively, these subsystems advance a comprehensive, user-centric framework of digital identity management.

In the previous chapter, we discussed the problem statement, the research statement, the research subquestions, and the objectives. Building on this, we present an overview of the solutions proposed to address these problems. This chapter is systematically structured as follows: Section 4.2 presents the research methodology, detailing the approaches and

techniques adopted to achieve the study objectives. Section 4.3 provides a comprehensive overview of the BIIM framework's architecture. Sections 4.4- 4.7 describe the proposed solutions addressing each research objective. Finally, Section 4.8 summarizes the key findings and insights derived from the chapter.

4.2 Research Methodology

This section outlines the research methodology adopted to design and validate the BIIM framework. A structured and iterative approach was essential to ensure the system's accuracy, adaptability, and alignment with the research objectives. Therefore, the design science research methodology (DSRM) [73] was selected to guide the development, evaluation, and refinement of the BIIM system.

4.2.1 Methodology

We consciously adopted the design science research approach to address our objectives and develop an effective identity management system. This approach provides an iterative and systematic framework to guide the process. The iterative nature of this approach allows us to refine and reshape the BIIM until it aligns perfectly with the research objectives. DSRM can be broken down into stages, and we follow these steps in our research. The outcome will be a prototype that meets the objectives we have determined. An overview of the design research methodology is shown in Figure 4.1.

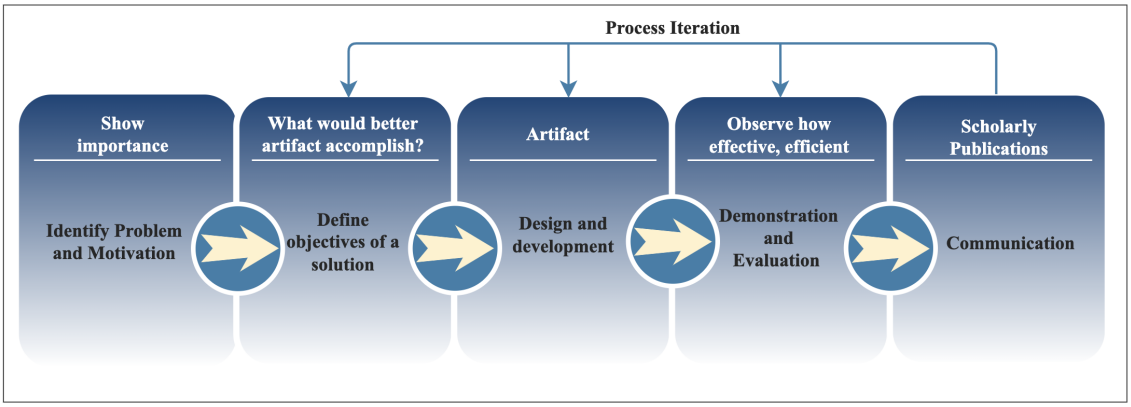


Figure 4.1 : DSRM [73]

The primary aim of this research is to design and empirically evaluate a novel framework under controlled, laboratory conditions. We adopt the DSRM to ensure problem relevance and methodological validity. DSRM structures the investigation as an iterative build-evaluate cycle encompassing problem identification, artifact design and instantiation, and empirical assessment within a research-driven context.

Identify the Problem and Literature Review Phase:

The DSRM process starts with the identification and motivation of the problem. In this initial phase, we summarized and discussed the problem by reading relevant studies. A systematic literature review was conducted, and existing systems were examined. As a result, we found there was a lack of blockchain and AI-driven approaches to managing self-sovereign identities and federated identities in the existing literature. Through this analysis, we critically determined the gaps and identified the problem. The SLR process is documented in Chapter 2. Based on the outcome of the SLR process, the research problem is identified in Chapter 3.

Identify Objective and Define Solution Phase:

In this stage, we identified the potential solutions that aligned with our objectives and initiated the design of a prototype with additional functionalities designed to achieve our goals. The main focus of our research is the integration of blockchain and biometric technologies for the development of a robust identity management system. Furthermore, this design strategically incorporates artificial intelligence elements to enhance the overall utility for both end-users and the blockchain platform. The documentation process can be found in Chapters 3 and 4.

Design and Development Phase:

In this phase, we designed and developed the working of our system by proposing the method and architecture. The design and development phases can be found in Chapters 5, 6, and 7.

Demonstration and Evaluation Phase:

In this phase, we demonstrated the system and then used relevant metrics to evaluate it. This phase focuses on testing the working of the system along multiple dimensions. The evaluation phase is found in Chapters 5, 6, and 7.

Communication Phase:

In this phase, we focused on disseminating the findings of our work through conferences and journals. The output of this phase can be found in the list of publications section.

4.3 Solution Overview

This section presents an overview of the BIIM system, which is designed using the Model–View–Controller (MVC) architectural framework. The MVC paradigm enforces a clear separation of concerns among the model, view, and control layers, thereby improving system modularity, maintainability, and scalability.

4.3.1 Architecture of the BIIM

The architecture of the BIIM system is structured into three distinct layers, as illustrated in Figure 4.2, each fulfilling a specialized role in ensuring secure, robust, and privacy-preserving identity management. This design ensures the integrity and confidentiality of sensitive user data. These components collectively define the operational foundation of the proposed solution, with primary research contributions concentrated in the control layer.

Within the BIIM framework, different subsystems employ distinct blockchain infrastructures according to their functional requirements. The BBIM and UDOD subsystems are implemented using BigchainDB, where a Byzantine Fault Tolerant (BFT) consensus protocol is responsible for transaction validation and ordering, while Proof of Work (PoW) is applied as a transaction admission control mechanism to regulate and filter incoming transactions. In contrast, the FIM subsystem is deployed on the Ethereum blockchain, where PoW functions as the primary network-level consensus mechanism for smart contract execution and decentralized token management.

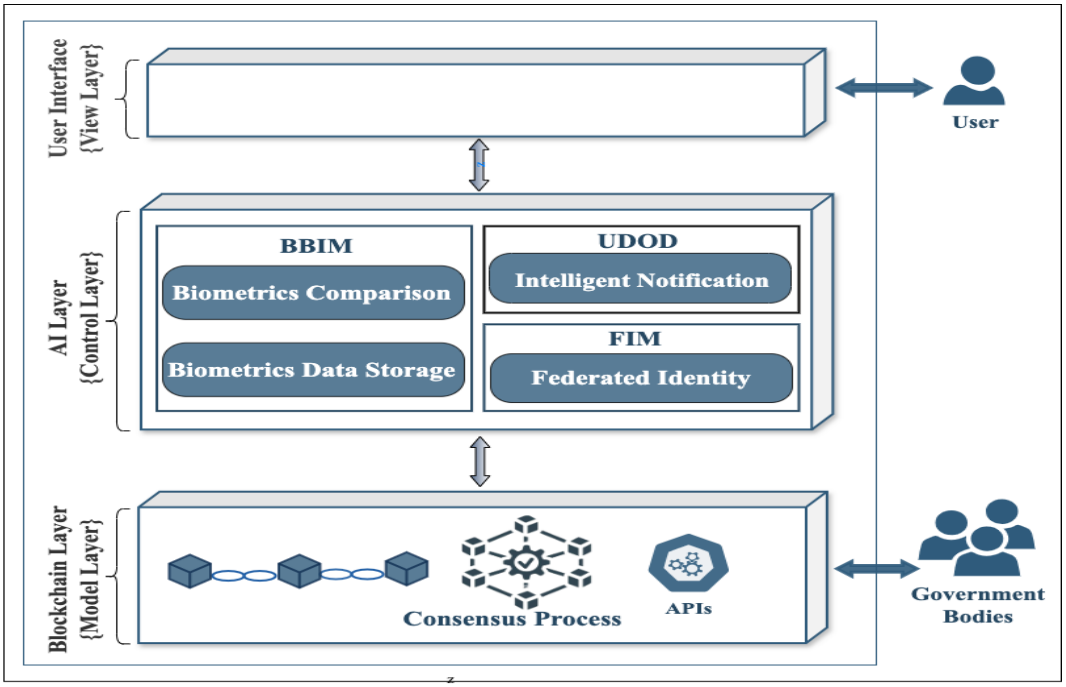


Figure 4.2 : MVC-Driven Architecture for the BIIM System

The following is a refined and elaborated description of the system:

1. View Layer: This layer, also known as the user interface layer, serves as the primary interface for users interacting with the BIIM system, providing a user-friendly interface that enables users to explore the functionality of the system. The design and functioning of this layer are crucial for delivering an integrated user experience and enabling simple access to the system's functionalities.

2. Control Layer: This layer, also known as the AI layer, constitutes the fundamental section of the system responsible for carrying out the essential functions necessary for its operation. These functions include:

- The BIIM system combines biometric data storage with biometric comparison, as follows:
  - *Biometric Comparison:* This process involves the analysis and comparison of biometric data to verify identity authenticity.
  - *Biometric Data Storage:* A mechanism for securely storing biometric data

within the system.

- *Intelligent Notification:* An advanced feature that alerts users of relevant activities when interacting with BIIM or between entities within BIIM.
- *Federated Identity Management:* A sophisticated approach to managing and synchronizing identity information across different systems and platforms.

3. Model Layer: This layer, also known as the storage layer, provides a secure and immutable repository for all identity information. Accessibility to these data is not universally open as it only allows authorized government bodies direct access.

- *Decentralized Storage:* By leveraging blockchain technology, the system ensures that identity data is stored in a decentralized manner, enhancing security and reducing the risk of centralized data breaches. Within the BIIM framework, blockchain interaction takes place during the transaction phase. This process includes the submission of new user identities for validation, as well as the updating of existing records. Each operation is validated and immutably recorded on the distributed ledger, ensuring consistency, traceability, and integrity across the decentralized environment.
- *Direct Access for Government Bodies:* Authorized parties can directly access this layer, facilitating efficient and secure data retrieval and management. Access to user information by government bodies occurs only when authorized agencies retrieve user data as part of regulatory, legal, or security-related procedures. In such instances, the system ensures that this access cannot be denied. However, to maintain transparency and user awareness, the system automatically generates notifications to inform the affected user that their information has been accessed.
- *Consensus Process:* The blockchain layer employs a BFT consensus protocol within BigchainDB to validate and commit transactions for the BBIM and UDOD subsystems. PoW is utilized solely as a transaction admission control mechanism to regulate access and prevent abuse, rather than serving as the primary consensus

protocol. In contrast, the FIM subsystem leverages the Ethereum blockchain, where PoW is used as the network's primary consensus mechanism during experimental deployment. Further details are discussed in Chapters 5, 6, and 7.

- *API Integration:* Application Programming Interfaces (APIs) allow external government bodies to interact directly with the BIIM system, enabling them to retrieve identity information.

Figure 4.2 presents the architecture of the overall system. The BIIM system is a framework composed of three structured layers that are designed to securely manage and protect identity information. Each layer is critical to ensuring the system's functionality, security, accessibility, and user management. The architectures of the three subsystems are subsequently discussed in detail in Chapters 5, 6, and 7, providing a comprehensive understanding of the overall functionality of the BIIM system.

4.4 Overview of Solution for Objective 2

In order to achieve objective 2, our proposed solution, known as the BBIM system, stores biometric data securely. The process starts with registration with the BIIM system, and then personal information is stored, and valid IDs are uploaded. Our method is to collect images while scanning the face to store the biometric data. The system creates a biometric profile and compares it with the uploaded IDs to verify and authenticate the identity. The essential process is to store the biometric data and compare it with a valid ID to be eligible for an account and use other system features. Our solution is comprehensively detailed in Chapter 5.

4.5 Overview of Solution for Objective 3

In order to achieve objective 3, our proposed solution, known as the UDOD system, prioritizes user-driven control and ensures privacy-conscious data access. Our method guarantees that users receive instant updates while maintaining privacy regulations. The

system enables users to control access permissions and receive immediate notifications of any activities or access to their identity.

In the alert system, notifications maintain transparency and user awareness. The registration notification informs users of account creation, pending subsequent admin verification. In contrast, the login notification process employs advanced authentication methods, triggering email alerts upon successful logins and providing relevant error messages. Modification notifications cover processes such as password resets and profile edits, ensuring a precise validation process.

Our system extends its services to any organization that seeks to communicate and access user information in BIIM. In this scenario, the organization notifies the administrator with a postal code to obtain an efficient user list. Subsequently, the organization requests access to user information, granting access only with explicit user permission. Meanwhile, the system notifies both the organization and the user of all requests and actions. A detailed discussion of our solution can be found in Chapter 6.

4.6 Overview of Solution for Objective 4

In order to achieve objective 4, our proposed solution, known as the FIM system, connects to the blockchain, enabling users to store different identities securely in a digital wallet. Our method allows users to add a new identity; the system verifies the credentials and generates a unique token. This token and associated credentials are added to the user's digital wallet, ensuring consistent and secure identity verification across various platforms. The system stores transaction records on the blockchain for auditability. A detailed discussion of our solution is provided in Chapter 7.

4.7 Overview of Solution for Objective 5

Evaluation in our research is divided into two parts: experimental evaluation and system-driven evaluation. Experimental evaluation requires testing the BIIM system and each objective in controlled environments based on performance indicators. However, system-

driven evaluation concentrates on the performance of a system under actual conditions. This process implies testing the system in its own environment and measuring its quality against established criteria.

4.8 Conclusion

This chapter provides a comprehensive analysis of the fundamental research methodology, including an exploration of the BIIM architecture. The chapter also overviews the solutions to our objectives.

The next chapter focuses on the BIIM system as a fundamental framework and the BBIM as an essential subsystem. Furthermore, the workings of the blockchain within the BIIM system are explained in detail.

Chapter 5

Biometric Blockchain Identity Management (BBIM)

5.1 Introduction

In recent years, biometric technologies have become central to advancing secure and reliable digital identity management systems. As digital interactions continue to grow across various sectors, there is a rising demand for authentication mechanisms that ensure both accuracy and privacy [85]. Traditional identity management systems, which rely on centralized authorities, are often exposed to risks such as data breaches, identity theft, and unauthorized data modification [6]. To address these challenges, blockchain-based biometric identity management (BBIM) has emerged as a promising approach that combines the uniqueness of biometric identifiers with the immutability and transparency of distributed ledger technologies [50].

The BBIM subsystem forms a key component of the BIIM framework. BBIM is designed to capture biometric information, such as facial images, and securely link it with verified identity documents. Once validated, cryptographic representations of the biometric template and its associated identity attributes are permanently recorded on the blockchain, ensuring data integrity, authenticity, and resistance to tampering. This immutable storage structure provides strong guarantees of traceability and supports non-repudiation of identity records.

The scientific contribution of the BBIM system lies in the conceptual design and implementation of algorithms that integrate biometric identifiers within the BIIM framework. These algorithms 1, 2, 3, 4, 5, 6, 7, and 8 support biometric data acquisition, validation against government-issued credentials, and blockchain-based registration. Systematic evaluations of the BBIM system have demonstrated scalability, data integrity, and high

detection accuracy, confirming its robustness and applicability in real-world contexts.

The social contribution of BBIM is demonstrated through its ability to provide tamper-proof authentication mechanisms and integrate user-controlled biometric data within a transparent and accountable digital ecosystem. By enabling individuals to retain control over their biometric information, the subsystem promotes privacy, trust, and user empowerment. Furthermore, its integration with the FIM and UDOD subsystems strengthens interoperability and coherence within the overall BIIM architecture. Collectively, these subsystems establish a holistic and user-centric framework for secure digital identity management.

The previous chapter presented an overview of the BIIM framework, outlining its objectives, architecture, and foundational components. Building on this foundation, this chapter focuses on the design, implementation, and evaluation of the BBIM subsystem. Section 5.2 presents the BBIM system architecture, including the view, control, and model layers, as well as the BIIM and BBIM workflow. Section 5.3 describes the operational principles of BBIM and its role within the BIIM framework. Section 5.4 introduces the blockchain integration component of the system. Section 5.5 details the technical implementation, outlining the software environment, configuration, and on-chain/off-chain storage mechanisms. Sections 5.6 and 5.7 provide a comprehensive evaluation of the system, including performance analysis, algorithmic complexity, comparative assessment, and applicability across domains. Section 5.8 illustrates the system's functionality through a scenario-based analysis demonstrating interoperability with the UDOD and FIM subsystems. Section 5.9 discusses the results, theoretical implications, and system integration within the BIIM framework. Finally, Section 5.10 summarizes the key findings and highlights the BBIM subsystem's contribution to user-controlled, privacy-preserving, and decentralized identity management.

5.2 BBIM System Architecture

Figure 5.1 illustrates the architecture of the BBIM system, designed to combine biometric authentication with blockchain mechanisms for secure and verifiable identity management. The architecture is organized into three fundamental layers: the view layer, the control layer, and the model layer, which together provide a modular, scalable, and privacy-preserving framework for managing digital identities.

The view layer functions as the primary point of interaction between users and the BBIM system, enabling core biometric operations such as facial registration, authentication, and logout. It provides an intuitive and secure front end that abstracts the underlying biometric and blockchain complexity. This design enhances usability and accessibility while maintaining responsiveness and safeguarding user privacy, thereby supporting the system's objective of delivering secure and user-centric identity services.

The control layer operates as the central processing and coordination unit responsible for managing biometric workflows. It manages components such as the *Register Face*, *Process Face Images*, *Face Login Process*, and *Logout Procedure*, as illustrated in Figure 5.1. Serving as an intermediary between the view and model layers, it supervises facial data acquisition, preprocessing, feature extraction, and verification processes. This layer also maintains secure communication channels across components, validates input data, and enforces compliance with authentication policies. Although it introduces computational overhead due to real-time biometric processing, it significantly enhances reliability, accuracy, and overall system integrity.

The model layer, also referred to as the storage layer, establishes the blockchain-enabled data management foundation of the BBIM subsystem. It integrates secure off-chain databases with a blockchain ledger to balance operational performance and trust assurance. Raw biometric data are maintained in protected off-chain repositories, while the blockchain immutably records cryptographic representations and verification outcomes. Consensus mechanisms based on a BFT protocol ensure that blockchain records of biometric transactions remain immutable, auditable, and verifiable across the distributed network.

PoW is employed solely as a transaction admission control mechanism rather than as the primary consensus protocol, providing additional resistance to abuse and spam without altering the core consensus layer. This architecture preserves the tamper resistance and transparency of biometric verification processes while supporting the confidentiality and integrity of user data through cryptographic protections and off-chain storage. As a result, the system reduces the risk of tampering and unauthorized access.

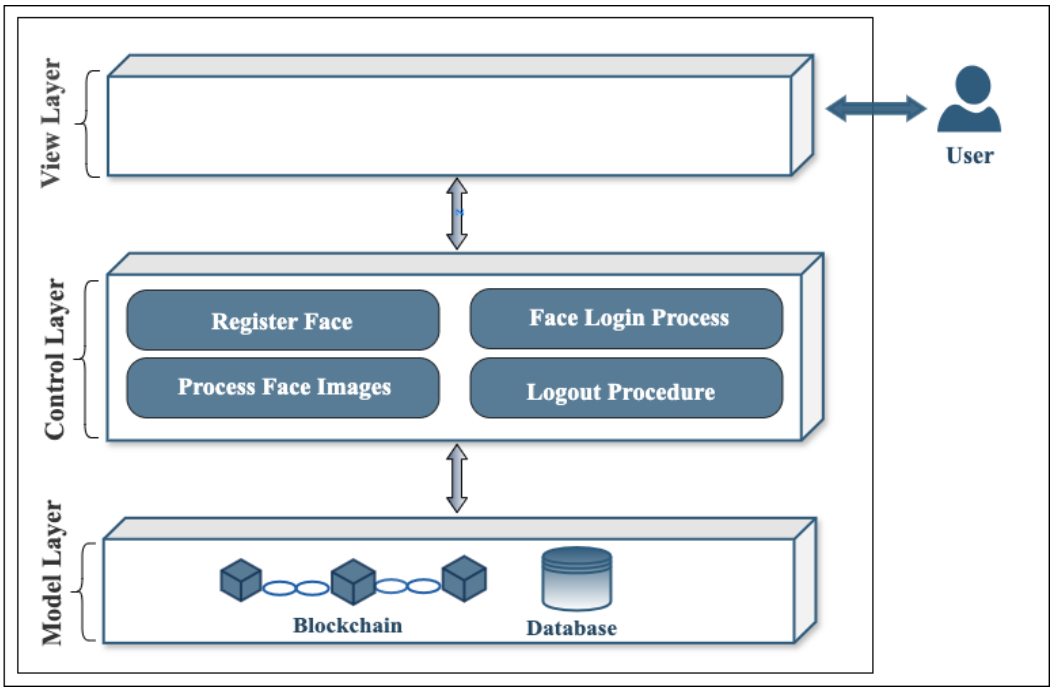


Figure 5.1 : BBIM System Architecture

The BBIM architecture provides a robust framework for blockchain-integrated biometric identity management. Through the integration of decentralized trust mechanisms and cryptographic verification within a modular architecture, the system eliminates single points of failure while improving transparency, resilience, and data protection. As a foundational component of the broader BIIM framework, the BBIM subsystem supports secure and privacy-preserving authentication processes that complement the FIM and UDOD subsystems in delivering a cohesive identity management system.

5.3 The Working of the BBIM System

The working of the BBIM system can be understood by first reviewing the workflow of the BIIM framework, as BBIM is developed as a core component within it. The BIIM system serves as the foundational structure that defines how identity registration, verification, and data integrity are achieved in a decentralized environment.

As outlined in Chapter 3, the BBIM system constitutes an essential component of the BIIM architecture. In this thesis, the terms *BBIM system* and *BBIM subsystem* are used interchangeably to describe the blockchain-based biometric identity management functionality responsible for the secure authentication, verification, and integrity of biometric data within BIIM.

BBIM extends the BIIM framework by incorporating biometric mechanisms to enhance authentication and ensure that identity data are securely validated and stored on the blockchain. Accordingly, the following subsections explain the workflow of the BIIM system, followed by the detailed workflow of the BBIM system, to demonstrate their functional integration within the overall identity management framework.

BIIM is designed to allow users to have control over their personal information, preserve privacy, and ensure data security. BIIM allows users to manage their identity proactively and offers them the authority to accept or decline organizational requests. However, organizations registered in BIIM can retrieve user information based on a provided postal code, addressing the specific needs of organizations seeking access to relevant user data. A postal code was used as a simple method to search for a user and retrieve user details. In future implementations, other identifiers associated with users, such as state or country, can be used to perform user searches.

The class diagram in Figure 5.2 represents the procedural interactions between the components of the system. BIIM introduces innovative methods for authenticating and managing digital identities, presenting a comprehensive framework for implementing blockchain technology in identity management.

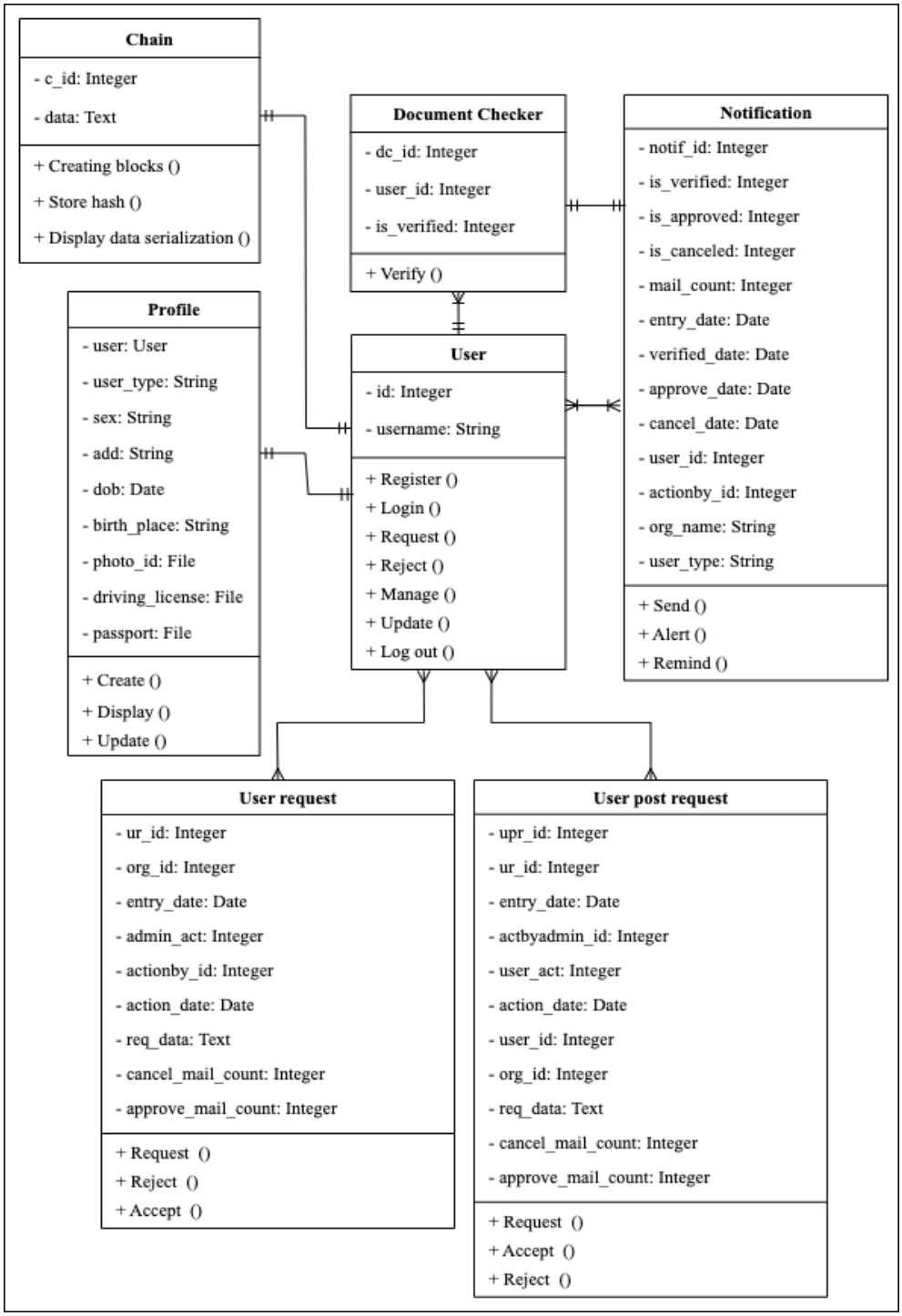


Figure 5.2 : BIIM Class Diagram

BIIM has three types of end-users: administrator, organization, and user. Each end-user must complete a registration process to have an account in BIIM. The diagram of the BIIM system, as demonstrated in Figure 5.3, provides a structured representation of the

system's functionalities and how different users interact with these processes. The use-case diagram conveys how administrators, users, and organizations interact with BIIM through common functionalities: signing up, logging in, changing passwords, managing profiles, logging out, and notifications. The administrator has additional responsibilities such as verifying user identity, approving organisation documents, and accessing the admin utility function, which is described later. On the other hand, organizations have a unique use case that requests user information and focuses on interacting with the system to access user information in a secure manner.

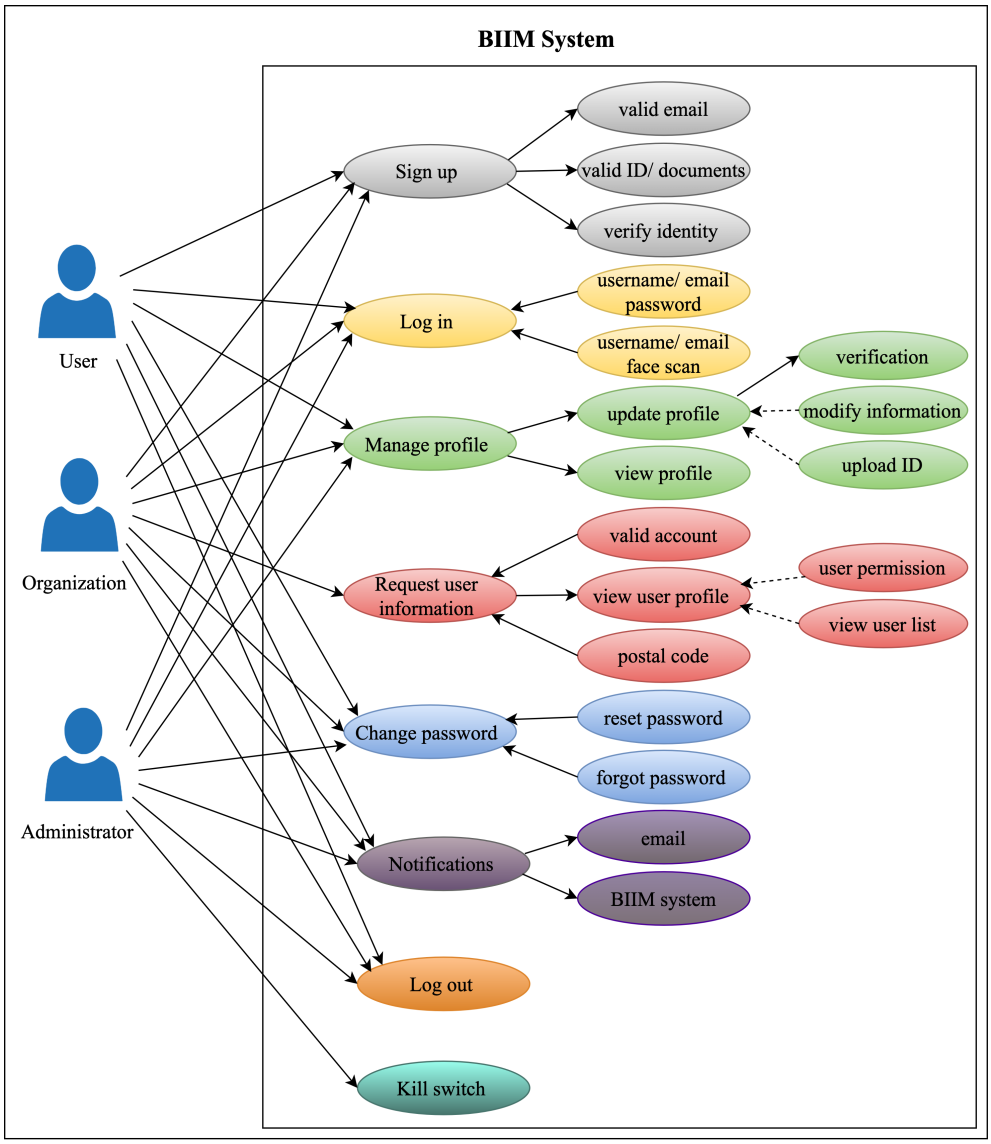


Figure 5.3 : Use Case Diagram of BIIM System

The key functionalities of the BIIM system are as follows:

Sign-up: The sequence diagram in Figure 5.5 explains the user registration and confirmation process within BIIM. The registration process comprises two phases, which must be run consecutively in order to create an account safely, as well as to secure the stored personal and biometric data. The registration process for all users is as follows:

Phase 1. Storing personal information through BIIM:

As outlined in Algorithm 1, the user starts by creating an account and must start by entering a unique username and email address. Each account must have a unique email address to receive an email verification code. Subsequently, users complete the registration process by entering their first name, last name, gender, date of birth, address, etc.

Phase 2. Storing biometric information through the BBIM within the BIIM:

Figure 5.4 shows an identification storage and verification flowchart. The user must upload identification documents, including a valid ID, driver's license, and passport documents. Then, the system collects biometric data by scanning the user's face. The system captures 100 images during the scan, and these photos generate a biometric profile from different perspectives and expressions. Following the scanning process, the system performs a verification procedure that compares the biometric data with the submitted documents to confirm consistency. Once the system's algorithms confirm the accuracy of the information and establish that no additional data is required, the identity is validated and the account is successfully created. However, if the system fails to authenticate the identification, the account remains unverified and will request additional information for further processing. Once the identification has been verified, the system sends the information to the biometrics layer for additional processing or storage. After the identity is verified and the biometric profile is stored in the database, a transaction record of this entire process is recorded on the blockchain to ensure traceability and integrity of the identity verification process.

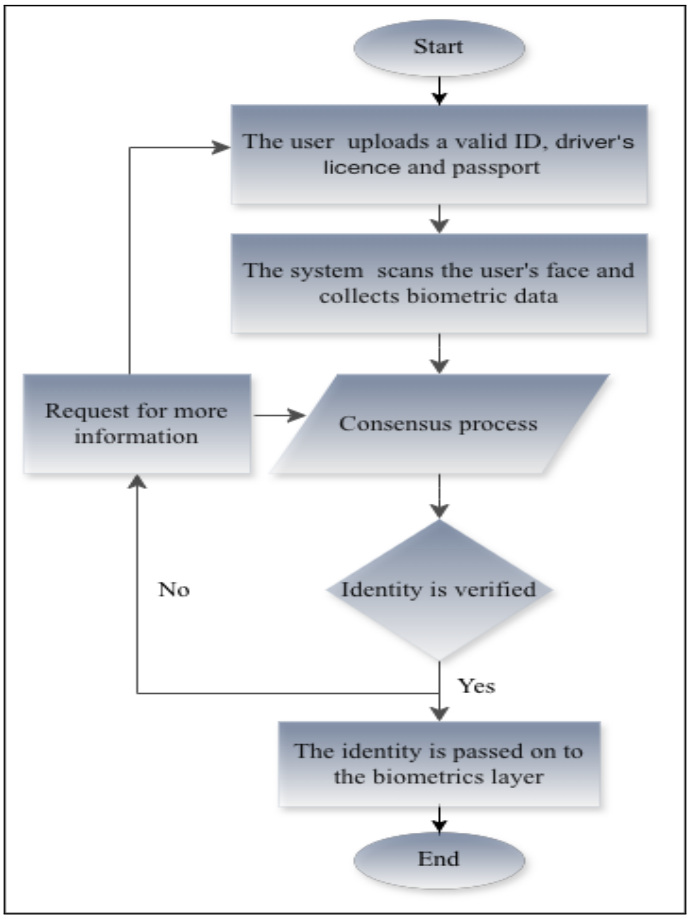


Figure 5.4 : Biometric Blockchain-based Identity Management System

Conceptually, the BBIM system is designed to operate using a decentralized validation model supported by BigchainDB's BFT-style consensus and a PoW-based admission mechanism. However, for implementation simplicity, the prototype replaces the decentralized validation process with an administrative verification component.

The process of the BBIM system within the BIIM system:

The user must upload a valid ID, as illustrated in Figure 5.6, while the organization must upload a document, as illustrated in Figure 5.7. Once the form is submitted, a subsequent 'make an account' page will be displayed, as illustrated in Figure 5.8, requiring the administrator or user to complete the registration process using the face detection mechanism.

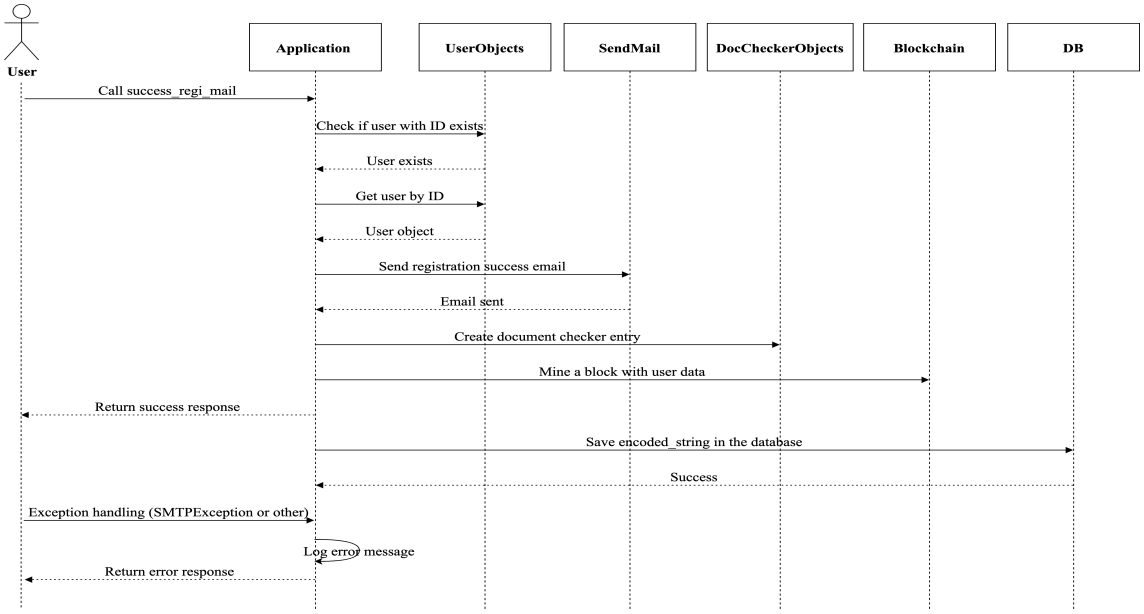


Figure 5.5 : User Registration and Confirmation Workflow with Email and Blockchain Integration

Algorithm 1 Account Creation Procedure

```
1:  function SIGNUP(request)
2:      if request.user.is_authenticated then
3:          return REDIRECT("home")
4:      end if
5:      if request.method is "POST" then
6:          data ← extract_post_data(request)
7:          documents ← handle_document_uploads(request)
8:          errors ← validate_form(data, documents)
9:          if not errors then
10:             user, profile ← save_user_profile(data, documents)
11:             if int(data['user_type']) == 3 then
12:                 return RENDER(request, 'signup.html',{'successUserIdAfterSaveForOrg': user.id})
13:             else
14:                 return RENDER(request, 'signup.html', {'userIdAfterSave': user.id})
15:             end if
16:         end if
17:     end if
18: end function
```

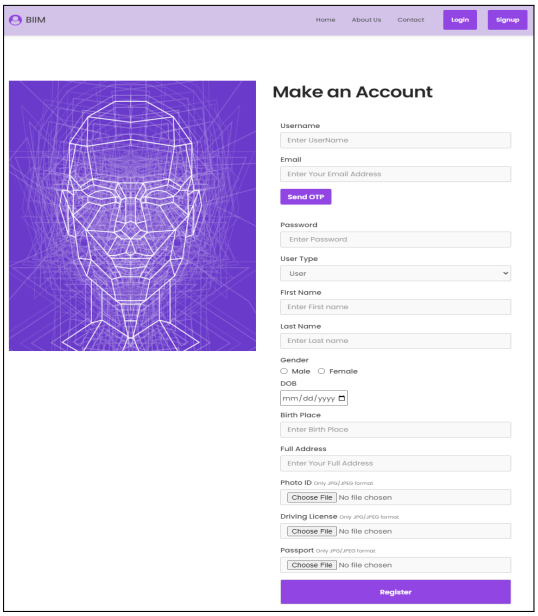


Figure 5.6 : Admin/ User Sign Up Interface

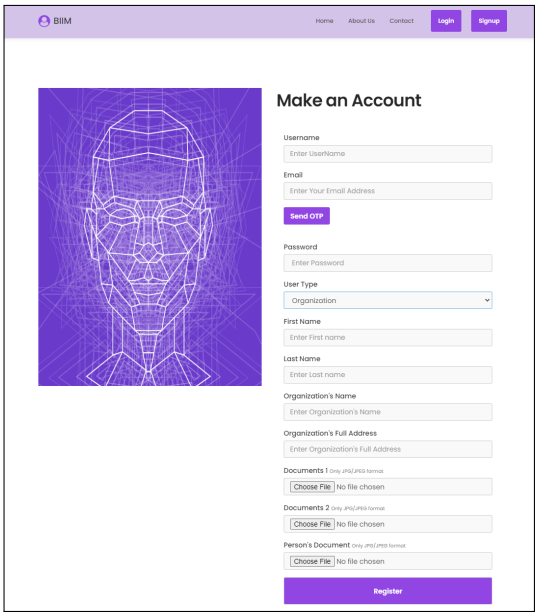


Figure 5.7 : Organization Sign Up Interface

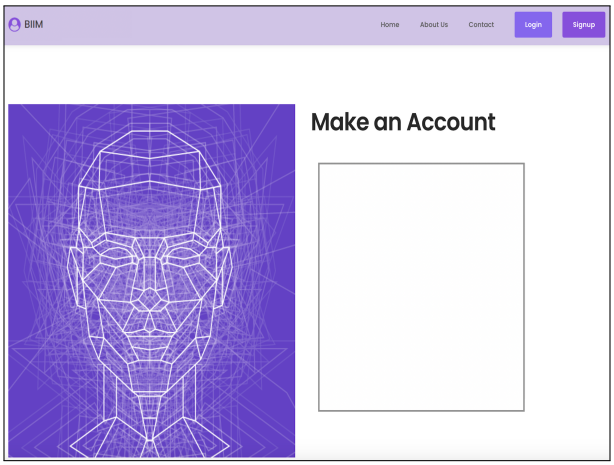


Figure 5.8 : Make an Account: Face Scan

During biometric registration, the system will detect spoofing and previously registered faces, as illustrated in Figure 5.11. The face is successfully registered, as shown in Figure 5.10 after BBIM captures 100 face images to create a data set, as illustrated in Figure 5.9. However, for organizations, the process does not include a face detection mechanism; instead, they need to provide different details for registration. BIIM prioritizes individual management, privacy, and data integrity.



Figure 5.9 : 100 Images Captured for Face Scan

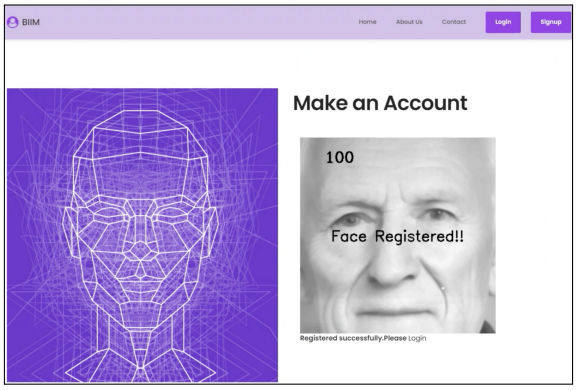


Figure 5.10 : Face Registered

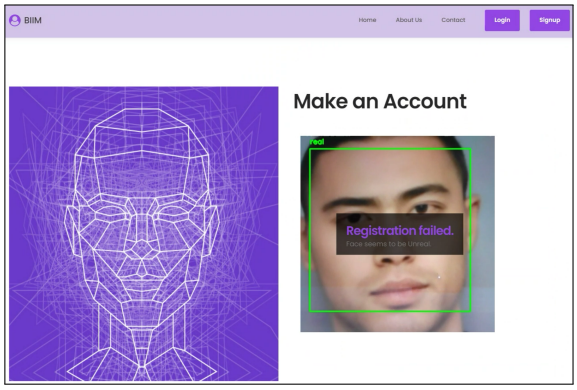


Figure 5.11 : Registration Failed

However, to improve security, an important verification step is integrated into the registration process to ensure a robust identity management system that allows the administrator to verify and compare the user ID with the registered facial images to validate the identity, as illustrated in Figures 5.12.



Figure 5.12 : Administrator Verifies and Compares the User ID with the Registered Face to Validate the Identity

In addition, the administrator reviews and approves the documents provided by the organization. Users and organizations are listed for verification and approval in the administrator dashboard, as shown in Figures 5.13 and 5.14.

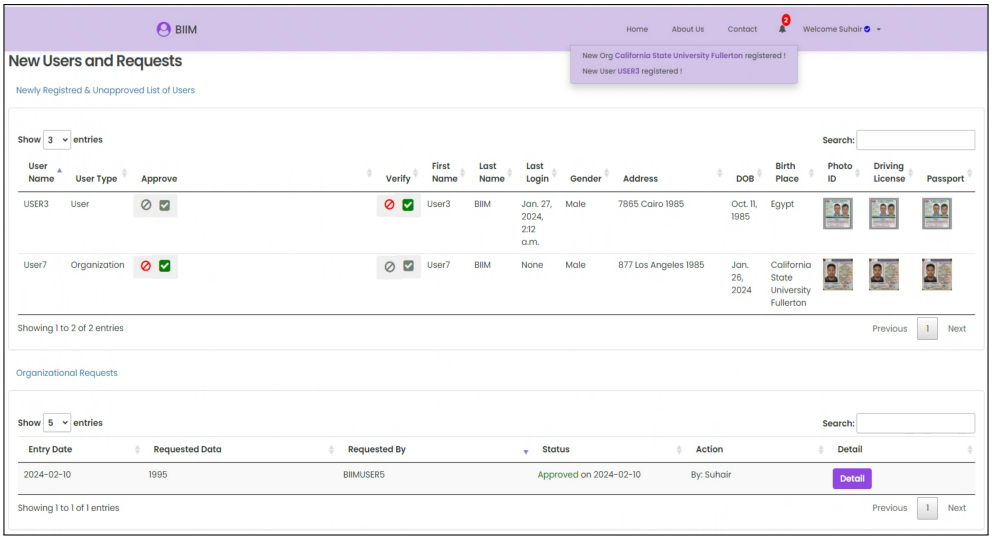


Figure 5.13 : Administrator Dashboard of Users and Organizations Waiting for Verification and Approval

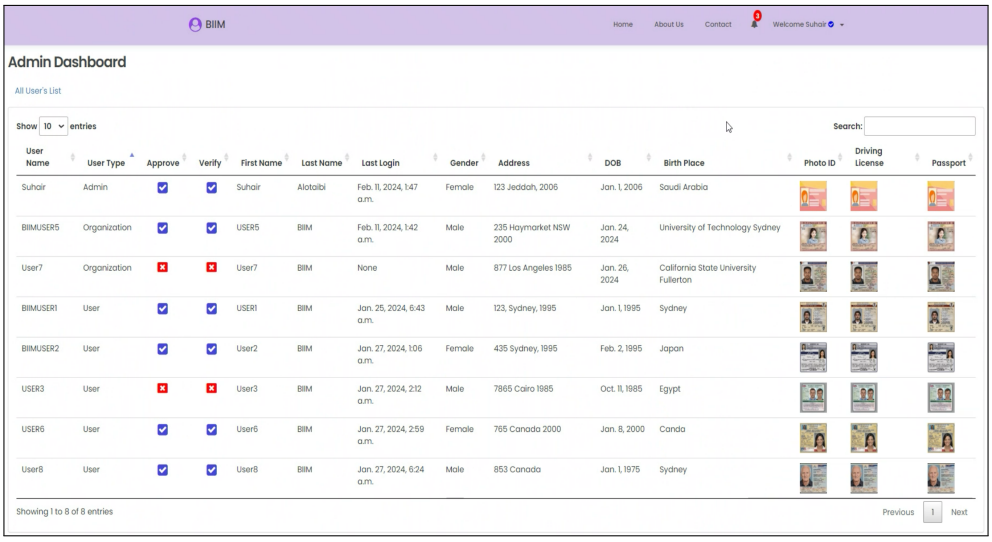


Figure 5.14 : Administrator Approves/ Verifies Dashboard

Login: A detailed explanation of the user login process in BIIM is illustrated in Figure 5.15. The BBIM system integrates advanced authentication and secure login methods, offering both face recognition and credential-based login mechanisms for administrators and users, as illustrated in Figures 5.16 and 5.17.

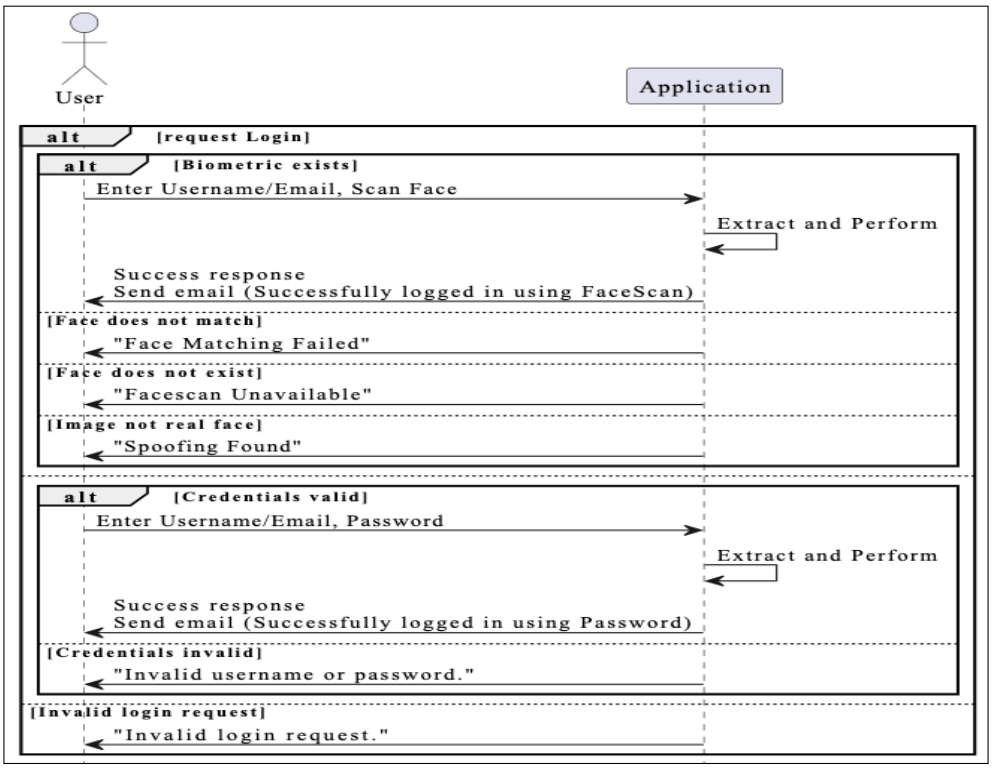


Figure 5.15 : Login Process

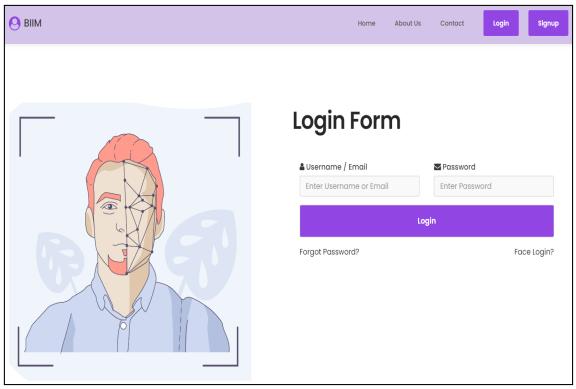


Figure 5.16 : Credential login

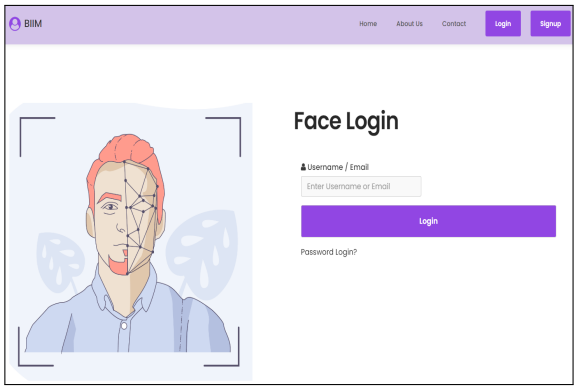


Figure 5.17 : Face Login

The face recognition feature employs biometric algorithms to compare a user's facial features against pre-stored images in the database, offering robust security and access control flexibility. The detailed steps for capturing and registering facial data are outlined in Algorithm 2, which handles image preprocessing, validation, and dataset creation. The subsequent facial image refinement and grayscale transformation process is described in Algorithm 3.

Algorithm 2 Register Face

```
function GRAYSCALENEW(data, uid)
    global face_classifierGlobal, ds_factor
    img ← from_b64(data)
    folderCreation(uid)
    countFace ← checkLatestFile(uid)
    if face_extractor(img) ≠ None and countFace < 101 then
        face ← processFace(img, uid, countFace)
        LOGGER.INFO("Face Found: ", countFace)
        return to_b64(face)
    else
        return handleNonFace(countFace, img, uid)
    end if
end function
```

Algorithm 3 Process Face Images

```
function PROCESSFACE(img, uid, countFace)
    extractedFace ← FACE_EXTRACTOR(img)
    resizedFace ← CV2.RESIZE(extractedFace, (400, 400))
    grayFace ← CV2.CVTCOLOR(resizedFace, cv2.COLOR_BGR2GRAY)
    filePath ← BUILDFILEPATH(uid, countFace)
    CV2.IMWRITE(filePath, grayFace)
    ANNOTATEIMAGE(grayFace, countFace, (50, 50))
    jpegFace ← CV2.IMENCODE('.jpg', grayFace)
    return jpegFace
end function
```

The complete login workflow, including user authentication and response handling, is implemented in Algorithm 4.

Algorithm 4 Face Login Process

```
Input username/email; display error if invalid.
Capture face scan
if user data are verified then
    Grant access and redirect to home page
else
    if user not found then
        Display "Wrong Username or Email"
    else
        Check profile type
        if organization user then
            Display "Facescan unavailable"
        else
            Prompt user to retry authentication
        end if
    end if
end if
```

This process results in one of three outcomes:

1. Successful Login: If the scanned facial features align accurately with the stored images, the user is redirected to their home page, indicating a successful login, as demonstrated in Figure 5.18.

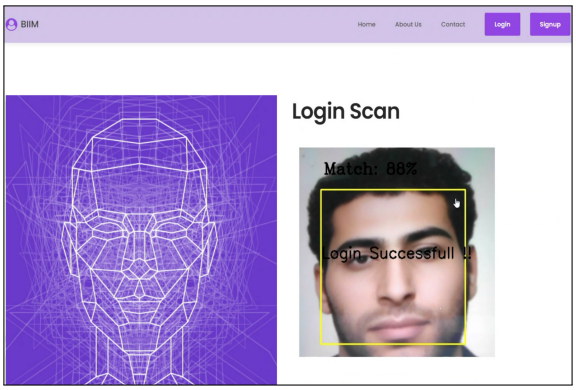


Figure 5.18 : Login Successful

2. Face Matching Error: In instances where the facial scan does not correspond with the stored images or if other conditions, such as insufficient lighting, affect the scan, the system displays a ”face matching failed” error. This serves as a prompt for the user to retry or switch to an alternative login method, as illustrated in Figure 5.19.

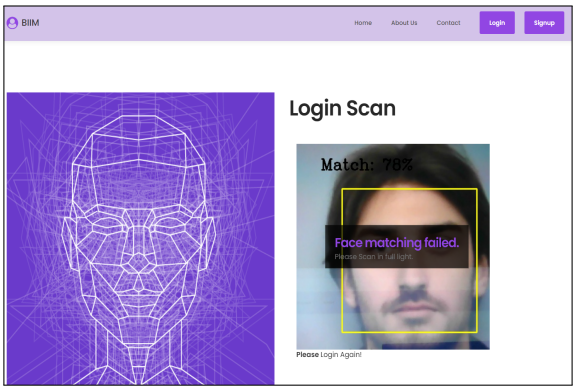


Figure 5.19 : Face Matching Failed

3. Spoofing Detection: The BBIM system is also equipped to identify spoofing attempts, such as when a photograph is used instead of an actual face. The system detects

spoofing attempts, as illustrated in Figure 5.20.

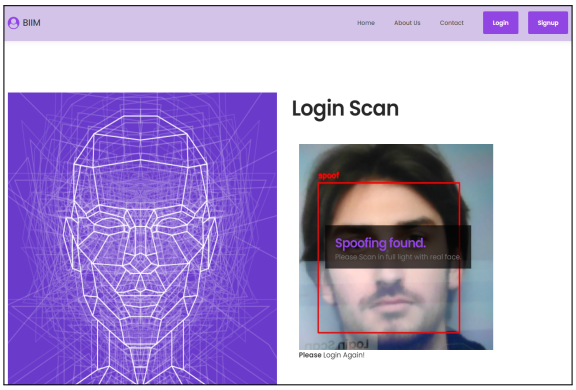


Figure 5.20 : Spoofing Found

Logging in with an unverified yet approved registered account will trigger a message, as shown in Figure 5.21.

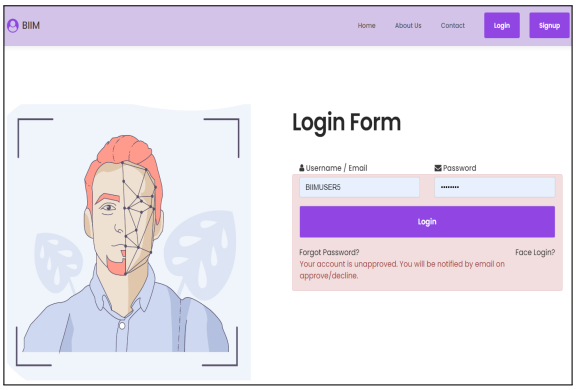


Figure 5.21 : Login Failed

For organizations, the system requires the use of a credential-based login, using a username/email and password, as shown in Figure 5.16. If the credentials are incorrect or the organization logs in using the biometric approach, the system displays the error message, as illustrated in Figure 5.22. In contrast, for administrators and individual users who prefer traditional authentication methods, BIIM also provides the option of a credential-based login as a secondary method, along with the advanced face recognition feature.

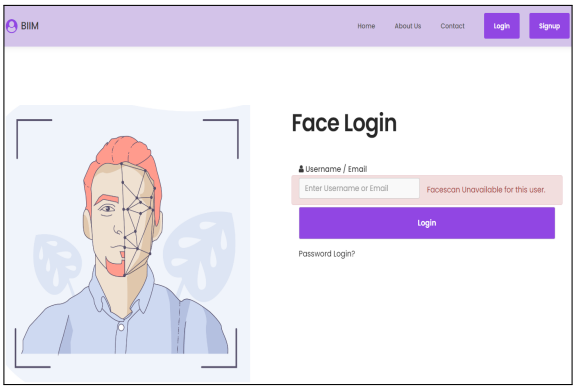


Figure 5.22 : Face Scan Unavailable

Successful authentication redirects users to the user home page. The system's functionality is visually detailed in the user manual, with Figures 5.23 and 5.24 showing the home page after login.

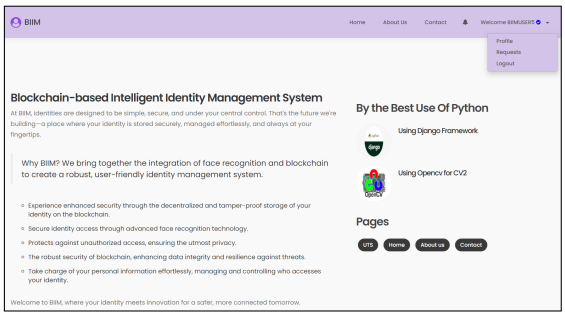


Figure 5.23 : User/ Organization Home Page

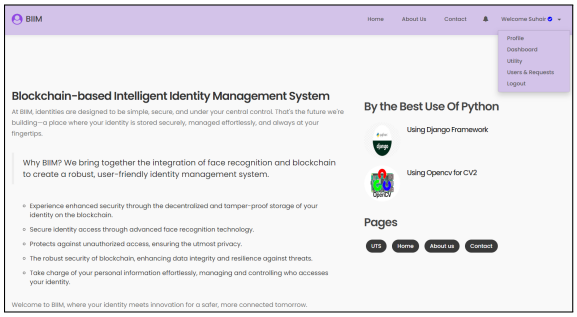


Figure 5.24 : Admin Home Page

User Profile: The procedure for viewing and updating a profile is detailed in the sequence diagram shown in Figure 5.25. As illustrated in Figure 5.26, BIIM allows users to manage their profiles, excluding sensitive fields such as registered facial recognition data, username, email, and date of birth. Any modifications trigger an automatic email notification to ensure transparency. Furthermore, to enhance security, uploading new identification documents results in a temporary account suspension until administrative verification is complete.

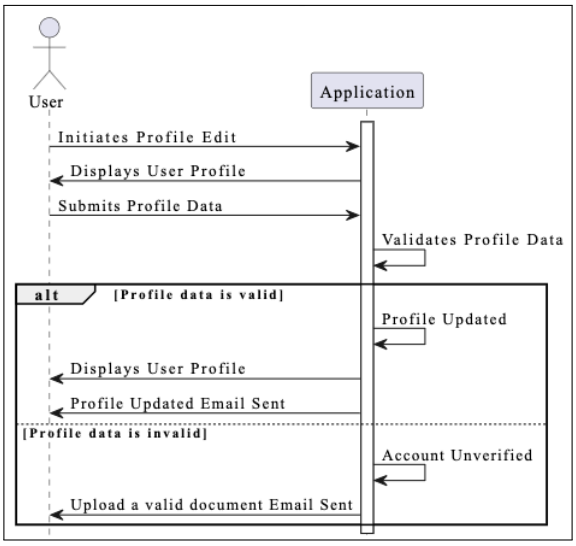


Figure 5.25 : User Display and Update Profile

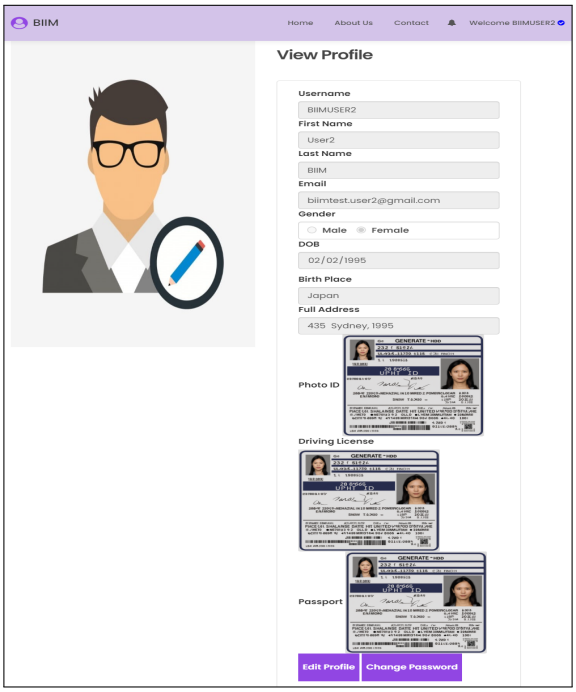


Figure 5.26 : View and Manage Profile

Change Password: Figure 5.27 illustrates the sequential procedure for changing and resetting a password in BIIM. This is a standard security feature that maintains account security by allowing users to alter their passwords. The logical flow of this procedure is detailed in Algorithm 5, which handles the validation and secure update of user passwords.

BIIM allows users to change their password through a user interface, which is illustrated in Figure 5.28. The form requires the following fields to be completed: old password, new password, new password confirmation, and then submit. On the other hand, with a reset password, which is the 'Forgot password' feature, an email notification is sent to the user to complete the process. BIIM allows users to change their passwords or use the 'Forgot Password' feature, as shown in Figures 5.29 and 5.30. At the initiation of the password reset procedure, the system automatically sends an email notification to the user. A successful password change is confirmed, as illustrated in Figure 5.31.

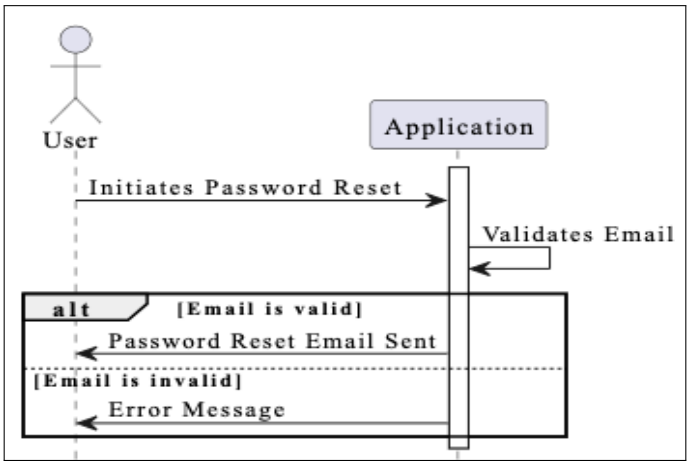


Figure 5.27 : Change and Reset Password Process

Algorithm 5 Change Password Procedure

```
1:  function CHANGEPASSWORD(request)
2:      LOGGER.DEBUG("Inside ChangePassword")
3:      if request.method is 'POST' then
4:          LOGGER.DEBUG("Handling POST request in ChangePassword")
5:          form ← PASSWORDCHANGEFORM(user=request.user, data=request.POST)
6:          HANDLEPASSWORDCHANGEPOST(request, form)
7:      else
8:          LOGGER.DEBUG("Handling GET request in ChangePassword")
9:          form ← PASSWORDCHANGEFORM(user=request.user)
10:     end if
11:     return RENDER(request, 'registration/change-password.html', {'form': form})
12: end function
```

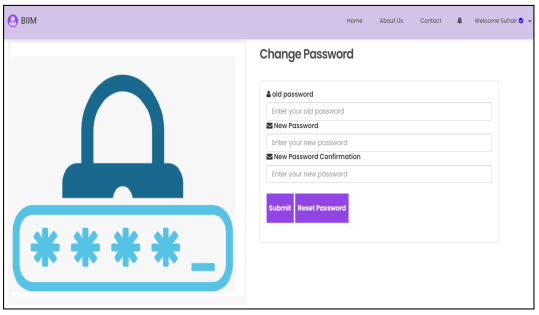


Figure 5.28 : Change Password Form

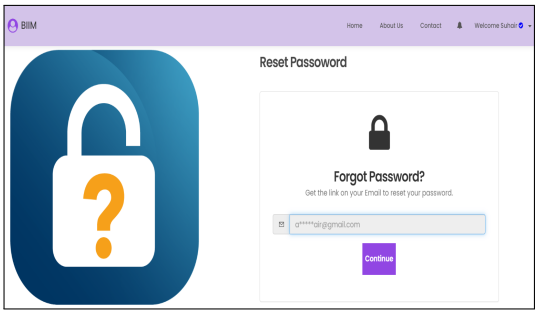


Figure 5.29 : Forgot Password

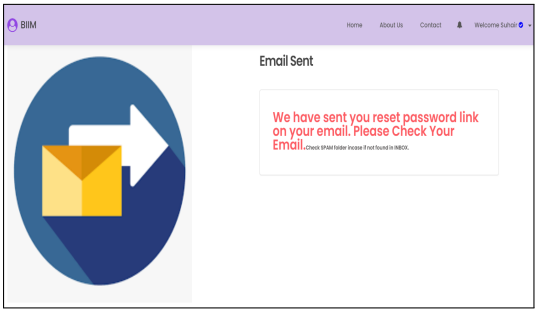


Figure 5.30 : Reset Password

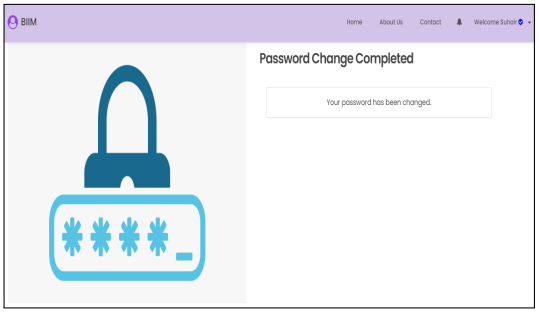


Figure 5.31 : Password Changed

Logout: The user will be able to log out of the system through the designated logout routine, which terminates the current user session and redirects the user to the home interface, as described in Algorithm 6. This procedure ensures that all session data are cleared securely, preventing unauthorized reaccess or residual authentication artifacts.

Algorithm 6 Logout Procedure

```
1: procedure LOGOUT
2:     logger.debug('Accessing Logout Page from View')
3:     LOGOUT(request)
4:     logger.debug('Logged Out and redirecting to Home')
5: end procedure
```

Alert and Notification: The BIIM framework provides real-time alerts via email or notifications on the BIIM portal, which enhances the overall security and reliability of the

system. We refer to the alert and notification system as the UDOD system. In Chapter 6, we discuss the workings of the UDOD system in detail.

Admin Utility: A kill switch feature, as illustrated in Figure 5.32, is developed for testing purposes and allows the administrator to remove and erase the entire database, the registered images, and the trained data set from BIIM. The erased data will not be retrievable.

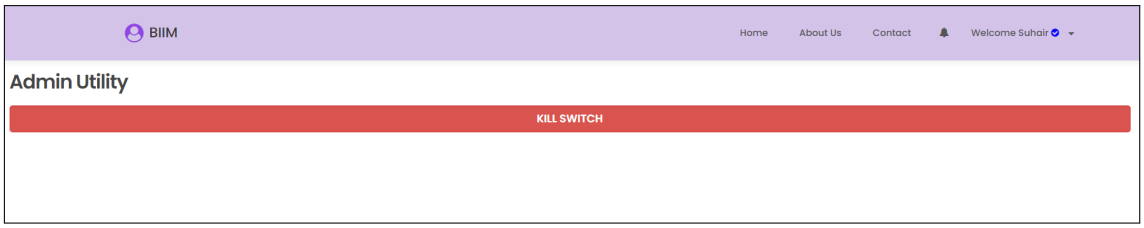


Figure 5.32 : Admin Utility

All modifications made will correspond to the updates in the blockchain.

5.4 Blockchain

In our system, the blockchain serves as a method for storing digital data. This process involves the organization of data into interconnected blocks, facilitated by cryptographic hashes, thus forming the “blockchain”. Each block is secured and interconnected through a hashing mechanism, ensuring resilience against unauthorized manipulation.

Data storage within the BIIM system employs the widely adopted JSON format, selected for its lightweight structure and ease of interoperability across system components. Data are structured and recorded within blockchain blocks, each capable of containing multiple entries associated with identity or authentication events. Once appended to the blockchain, these blocks become immutable, meaning new records can be added only as subsequent blocks, thereby preserving the integrity of all previously stored data. Each update or state change is systematically recorded on the blockchain, ensuring that user-specific data remain securely stored, traceable, and uniquely identifiable within the

standardized structure of shared blocks, thereby maintaining transparency, accountability, and overall data integrity [90].

The security infrastructure is maintained through the utilization of hashing, employing the SHA256 hashing algorithm. Each block retains its unique cryptographic code and also stores the code of the preceding block, thereby ensuring the integrity of the sequential arrangement. This chaining mechanism ensures a continuous and secure sequence, with each block precisely linked to its predecessors and successors through its hash, as demonstrated in Figure 5.33.

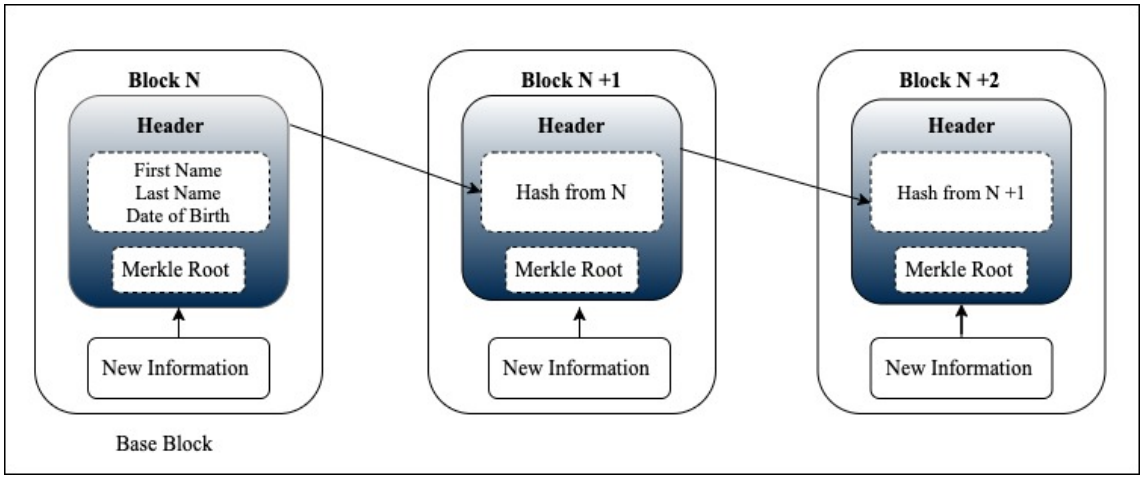


Figure 5.33 : Overview of the Blockchain Data Storage Mechanism

The blockchain initialization process is managed through a restart routine, which reconstructs the chain from stored data and reestablishes the blockchain state as described in Algorithm 7. This ensures that the system can recover the existing chain from the database and correctly rebuild the block sequence during startup or after a system interruption.

Algorithm 7 Restart Blockchain

```
1: function RESTART_CHAIN
2:     Retrieve the first Chain object from the database as dbObj
3:     Log "called db obj"
4:     if dbObj exists then
5:         Log "found db obj"
6:         Evaluate dbObj.data to get chain
7:         for each chain_data in chain do
8:             if chain_data["index"] is 1 then
9:                 Log "inside index = 1"
10:                Initialize global blockchain with chain_data
11:            else if chain_data["index"] > 1 then
12:                Log "inside index > 1"
13:                Add block to blockchain with chain_data
14:            end if
15:        end for
16:    end if
17: end function
```

In the PoW process, transaction data are subjected to examination and hashing using the SHA-256 algorithm with hexadecimal digest encoding. When a user decides to modify information, a new hash operation is invoked through the deployment of the SHA-256 algorithm to satisfy the predefined PoW requirements. Consequently, a new transaction is generated and submitted to the blockchain, containing the updated information, including user details, email address, timestamp, proof documents, and the previous record's hash. Each update is then verified through the blockchain validation mechanism as outlined in Algorithm 8, which ensures that the chain remains consistent and that no unauthorized alterations have occurred. This process maintains the immutability and trustworthiness of the ledger, as illustrated in Figure 5.34, where all user records are stored sequentially to preserve the integrity of digital data.

Algorithm 8 Validate Blockchain

```
1: procedure VALIDATEBLOCKCHAIN
2:     valid ← CHAINVALID(blockchain.chain)
3:     if valid then
4:         response ← {'message': 'The Blockchain is valid.'}
5:     else
6:         response ← {'message': 'The Blockchain is not valid.'}
7:     end if
8: end procedure
```

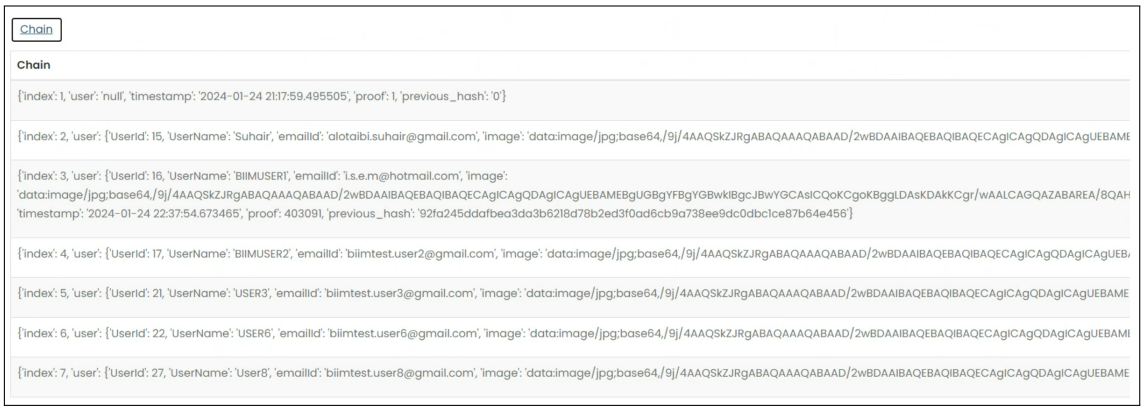


Figure 5.34 : List of Chains in BIIM

Figure 5.35 illustrates the interaction framework between the "BIIM" system and the "blockchain" network. In this configuration, the BIIM subsystem functions as a mediating layer that conceals the operational complexity of blockchain processes while facilitating the execution of higher-level identity management functions such as registration, data retrieval, and transaction authorization. The blockchain operates autonomously to perform its fundamental tasks, such as block creation, consensus validation, hash computation, and chain maintenance, ensuring consistency, integrity, and reliability across the distributed ledger. As shown in Figure 5.35, the integration of BIIM-initiated operations with blockchain processes exemplifies how the proposed framework achieves secure, transparent, and efficient interaction while maintaining architectural coherence and operational robustness.

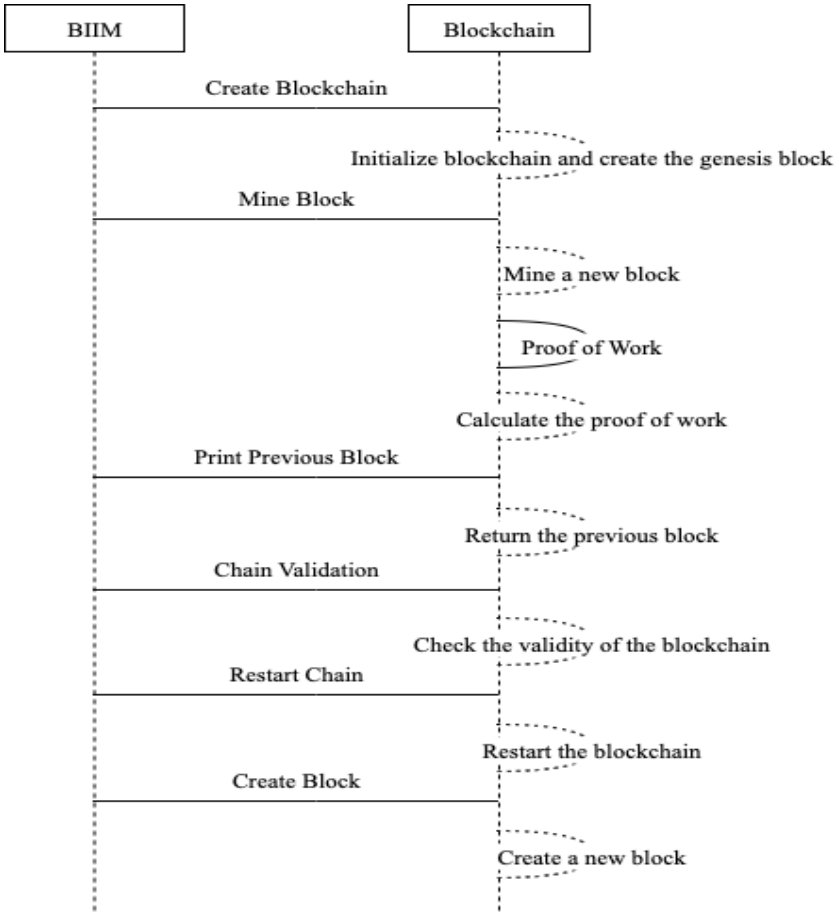


Figure 5.35 : Blockchain Operations and Chain Management

Blockchain technology enables the secure storage and sharing of identity-related metadata, including cryptographic hashes and references to personal identification documents, biometric templates, and authentication records. Its decentralized structure provides an additional layer of trust and security, as no single entity holds complete control over the data. This makes it suitable for managing sensitive identity information while preserving its integrity. Relational, NoSQL and document databases are efficient for various data management tasks but may lack the transparency and immutability necessary for secure identity management.

BigchainDB is a type of blockchain database that combines the key features of a distributed database with the capabilities of blockchain technology. It is a high-performance and scalable blockchain database that is well suited for our system. BigchainDB supports horizontal scalability by allowing each node in the network to contribute storage and

computational resources. For example, cloud-based instances such as AWS d2.8xlarge can provide up to approximately 48 TB of storage per node, enabling aggregate storage capacities exceeding one petabyte in multi-node deployments, depending on replication and fault-tolerance configurations [63].

Figure 5.36 illustrates the interactions between the application, the BigchainDB module, and the generate_keypair function. The generate_keypair participant represents the function responsible for generating the key pairs necessary for the transaction. The diagram also illustrates the communication flow, allowing for a clear understanding of the different stages involved in the asset creation process, including the preparation, fulfillment and retrieval of relevant data from the BigchainDB. The interactions between the components are displayed in the sequence diagram through a series of messages and function calls, providing a visual representation of the flow of control and data during the execution of the **creatBigDBAsset function**.

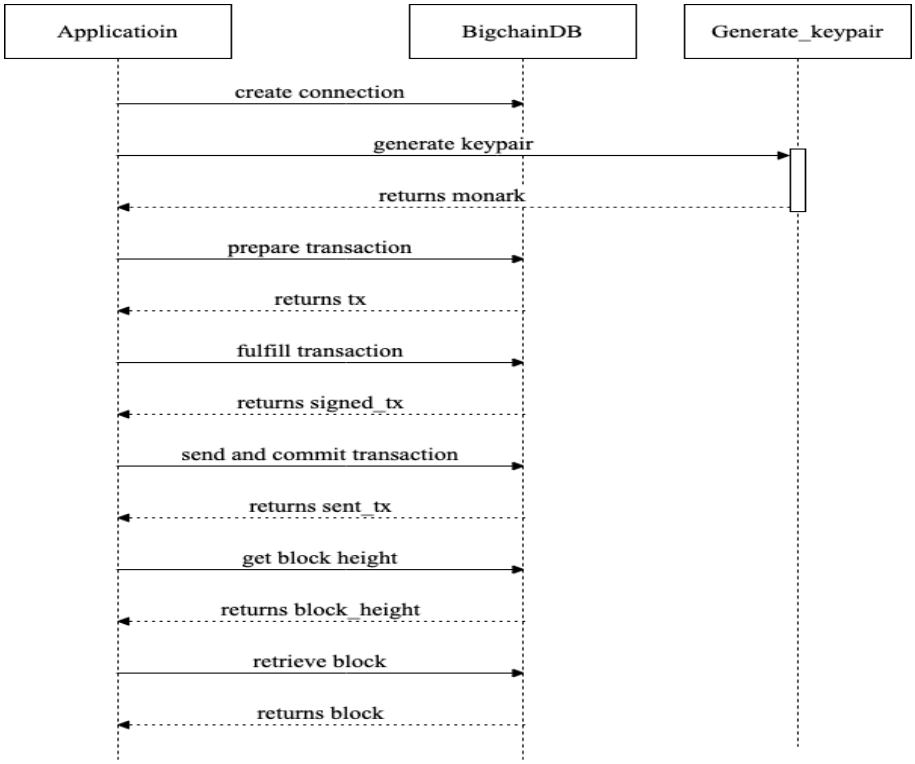


Figure 5.36 : Create BigchainDB Asset Function

5.5 Implementation

This section provides a comprehensive description of the technical implementation of the BBIM system. It outlines the software environment, system requirements, framework configuration, and core storage architecture. This section also explains the integration of blockchain, database, and machine learning technologies that together enable secure and scalable biometric identity management.

5.5.1 System Requirements

The BIIM system is designed for the Windows operating system, preferably Windows 11 or later. The recommended hardware configuration comprises 32 GB of RAM and an 8 GB graphics card (GPU). The use of TensorFlow for facial recognition introduces a GPU dependency, although the software can operate without it. In such cases, the system issues a warning message during server startup to notify the user that the GPU is unavailable.

5.5.2 Software and Configuration Development Framework

The foundational architecture of BIIM is built on the Django framework [1] and Python, with a significant emphasis on installation [2]. Version 4.2 [3] is utilized to develop our system, with Python serving as the primary programming language. The `requirements.txt` file includes comprehensive lists of the necessary packages, the installation of which is imperative for the operation of the application. Developers are instructed to download and install these packages using the `pip install` command in the command prompt. After successful installation, the server is initiated to launch the application.

A MySQL database [4] was established to facilitate efficient data management and storage. The face detection algorithms used in BBIM were sourced from existing imple-

[1] https://www.djangoproject.com/

[2] https://docs.djangoproject.com/en/4.2/intro/install/

[3] https://docs.djangoproject.com/en/4.2/intro/install/

[4] https://dev.mysql.com/doc/refman/8.0/en/windows-installation.html

mentations, including the Face Cascade [5], HAAR Cascade [6], smiling face cascade [7] , and eye cascade [8] algorithms, which enable facial expression and blink detection during user registration and login processes.

The complete code for the implementation of the BBIM system is hosted on GitHub. This repository provides access to the source code and dependencies, allowing for replication and further development by other researchers and practitioners. For detailed access, the project files can be found in our GitHub repository at Blockchain-based Intelligent Identity Management Repository, where all files are systematically organized and actively maintained.

5.5.3 Storage Architecture, Implementation Tools, and Technologies of the BBIM System

5.5.3.1 On-Chain and Off-Chain Storage Architecture

In the BBIM system, on-chain and off-chain storage mechanisms are employed to manage biometric user identity data, including document hashes, biometric information, and authentication records. Although it is technically possible to store entire documents directly on-chain, this approach is often impractical due to blockchain storage constraints, increased latency, higher costs, and reduced system efficiency [32]. To address these limitations, the BBIM architecture integrates the on-chain and off-chain approach: the cryptographic hash of each document is recorded on the blockchain, while the document itself is securely stored off-chain. This ensures data integrity and tamper-proof verification, as any modification to the off-chain document results in a hash mismatch.

Within this framework, the Binary Large Object (BLOB) data type is utilized to handle large unstructured binary data, such as biometric images and facial scans. BLOBs enable efficient interaction between the BBIM layers and the underlying database by

[5]https://medium.com/@ynaveenv/face-detection-using-open-cv-a2e6c406fa64

[6]https://www.bogotobogo.com/python/OpenCV_Pythonṗhp

[7]https://github.com/ysnvatsal/OpenCV/blob/master/haarcascade_frontalface_default.xml

[8]https://github.com/ysnvatsal/OpenCV/blob/master/haarcascade_eye.xml

allowing SQL scripts and other programmatic mechanisms to securely retrieve, process, and manage biometric data [52]. Moreover, BLOBs support version control mechanisms that align with blockchain principles, ensuring the immutability, integrity, and traceability of biometric records. Each update to biometric data is securely logged and verifiable within a decentralized ledger, maintaining a tamper-proof, consistent, and auditable record throughout its lifecycle [90].

By reducing on-chain data load and leveraging off-chain efficiency, this approach enhances system scalability, performance, and security [32]. While traditional databases offer robust data management capabilities, they lack the transparency, immutability, and decentralized trust that are inherent to blockchain technology. Therefore, BBIM's design achieves an optimal balance between operational efficiency and the distinct security advantages provided by blockchain-based identity management.

5.5.3.2 Implementation Tools and Technologies

The BBIM system implements the on-chain and off-chain storage approach using a combination of blockchain, databases, and machine learning technologies. Each component plays a distinct role in ensuring the scalability, integrity, and performance of the overall system:

1. **Python and Django Framework:** The BIIM system, along with BBIM and UDOD is implemented using Python and the Django framework, which provides a robust and modular foundation for connecting system components. Django ensures the secure handling of data transactions between the database and the user interface, supporting the seamless integration with blockchain technology.

2. **BigchainDB:** BigchainDB serves as the blockchain-enabled component responsible for maintaining immutable metadata, such as hashes of biometric data and identity documents. This ensures the authenticity, integrity, and non-repudiation of sensitive information without incurring the storage and latency costs associated with storing large data directly on-chain [63].

3. **MySQL Database:** MySQL functions as the primary relational database for managing structured data, including user profiles, access credentials, and system logs. It provides transactional reliability and performance for data operations that do not require blockchain-level immutability. MySQL also stores metadata that links to biometric files stored in BLOB fields, thereby integrating structured and unstructured data management within the same database environment.

4. **A BFT-based consensus protocol:** BFT is employed as the primary mechanism for validating and ordering transactions within the BigchainDB layer. This protocol ensures fault tolerance and consistency across distributed nodes, enabling the system to maintain reliable operation even in the presence of faulty or malicious participants [51].

5. **InnoDB Storage Engine:** InnoDB is used as the underlying storage engine for MySQL, chosen for its transactional integrity, crash recovery capabilities, and support for foreign key constraints. These features ensure referential integrity and data consistency across multiple related tables in the BBIM system.

6. **BLOB Storage:** The BLOB data type is used within MySQL to manage large unstructured binary data, such as encrypted biometric images and facial scans [52].

7. **TensorFlow:** TensorFlow is integrated into the BBIM system to perform facial recognition and biometric matching through deep learning. This enhances identity verification accuracy, security, and reliability.

By integrating these components, BBIM effectively achieves a balance between operational efficiency and blockchain-driven security. The combined use of on-chain and off-chain mechanisms enables the system to ensure immutability, integrity, and scalability, while maintaining responsiveness for real-time biometric verification tasks [90].

5.6 Evaluation of the BBIM System

This section evaluates the BBIM subsystem as a key element of the BIIM framework. Although the main focus is on BBIM's biometric storage and verification functions, several evaluation aspects also represent the overall BIIM system. These results indicate BBIM's contribution to BIIM's overall performance and its integrated operation with the UDOD and FIM subsystems.

In the BBIM system, one of the key challenges encountered during this research was the lack of access to authentic biometric data due to privacy and legal restrictions. To address this limitation, AI-generated biometric data were used as a substitute. As a result, all registered users, except for the administrator, are synthetic identities generated by artificial intelligence using the *Playground* platform (https://playground.com). This platform provides AI-generated facial photographs specifically created for biometric testing and validation in this study.

BBIM is designed to register authentic facial images. However, during the testing phase, the system's matching criteria were modified to accept synthetic (AI-generated) identities and images. Despite these adjustments, the system maintained its capability to identify and reject other images that lacked authenticity. This configuration allowed for the secure storage of biometric identifiers and the verification of identities in a controlled environment suitable for testing and development.

Once the synthetic data were generated, they were recorded onto the blockchain. During experimentation, a system administrator played a crucial role in verifying that the proposed BBIM system correctly recognized individual identities, particularly given its use of synthetic biometric data instead of real facial inputs. The administrator's involvement was limited to the testing phase and served multiple purposes: (i) managing and safeguarding synthetic data to ensure its integrity, (ii) overseeing identity verification procedures, and (iii) acting as a benchmark for evaluating the system's facial recognition accuracy. This comparative approach enabled consistent validation of system behavior while acknowledging the limitations of synthetic data in replicating the complexity of

real-world biometric patterns. The administrator thus provided a controlled reference point to maintain testing accuracy and reliability. In future deployments involving real biometric data, the BBIM system is designed to operate without manual oversight by transitioning to a fully automated verification process.

5.6.1 Evaluation Methodology

The evaluation of the BBIM system employs a combination of system-driven, experimental, and scenario-based assessments. Given the architecture and operational objectives of the system, the evaluation is primarily system-driven, focusing on the internal performance of core components such as database transactions, cryptographic hashing, and blockchain operations. The system consistently performs as designed, demonstrating stability and reliability across varying load conditions. These evaluation approaches provide a comprehensive foundation for analyzing BBIM's capabilities in terms of performance, scalability, data integrity, and readiness for real-world deployment.

5.6.2 BBIM Performance Evaluation

The system was evaluated by registering biometric identities for seven separate batches of users: 10, 50, 100, 500, 1,000, 5,000, and 10,000 users. Each user was assigned 100 biometric images captured during the identity registration process. These images were grouped into a single file to represent the user's biometric profile, which was hashed using the SHA-256 algorithm. The original images were stored off-chain, while the hashes were recorded on-chain to ensure data integrity without compromising storage efficiency. Each transaction was validated and committed to the distributed ledger using a BFT-based consensus protocol, while PoW was employed as an auxiliary admission control mechanism. The biometric file itself was stored off-chain, whereas metadata such as file path, cryptographic hash, user ID, and transaction ID were stored in a MySQL database using the InnoDB storage engine, selected for its transactional integrity and indexing performance.

The system was evaluated based on the following metrics:

- SQL Time: Time required to insert image metadata into MySQL (per user).
- Blockchain Time: Time required to perform the PoW computation and for the transaction to be validated and committed to the blockchain (per user).
- Total Time: Combined SQL and blockchain processing time (per user).
- Total Duration: Total time required to process all users.

The total duration was calculated using the following equation:

$$\text{Total Duration} = \text{Average Total Time per User} \times \text{Number of Users}$$

This evaluation simulates real-world registration performance and helps predict scalability for larger deployments. The results of the evaluation are summarized in Table 5.1.

User Count	**Avg SQL Time (s)**	**Avg Blockchain Time (s)**	**Avg Total Time (s)**	**Total Duration**
10	0.0140	1.201	1.215	12.15 seconds
50	0.0139	1.204	1.218	61.20 seconds
100	0.0137	1.199	1.213	121.30 seconds
500	0.0135	1.203	1.217	∼10 minutes
1,000	0.0132	1.206	1.219	∼20 minutes
5,000	0.0130	1.198	1.211	∼100 minutes
10,000	0.0128	1.196	1.209	∼200 minutes

Table 5.1 : BBIM System Evaluation for Varying User Counts

The evaluation confirms that the BBIM system is capable of scaling efficiently and maintaining consistent performance under varying loads, ranging from 10 to 10,000 users. A key aspect of the BBIM architecture is its use of a single SHA-256 hash per user, computed from a file containing 100 biometric images. This design choice significantly reduces the storage footprint of the ledger and improves transaction validation efficiency, as only cryptographic hashes and essential user metadata are stored on-chain. This structure offers a practical balance between data verifiability and system performance. Any change in the biometric image file, whether malicious or accidental, results in a completely different

hash, thereby ensuring tamper detection at the record level. Although this design sacrifices image-level granularity in tamper detection, it supports high scalability and performance, making it well-suited for production environments where block size and processing speed are critical factors.

With blockchain block creation times consistently averaging around 1.20 seconds and SQL metadata insertion times below 0.014 seconds per user, the system maintained an average total processing time of approximately 1.21 seconds per user across all scales. This predictability and linearity confirm the BBIM system's readiness for real-world deployment in environments requiring secure and scalable biometric identity registration.

5.6.3 BBIM Comparative Evaluation

Figure 5.37 showcases the efficacy of the biometric system by comparing time efficiency across real and AI-generated users. It illustrates the duration, measured in seconds, required for each individual to complete face registration and subsequent login using facial recognition. As mentioned previously, Playground.com was used to generate biometric identities for users within the system. In this experiment, synthetic biometric data were generated via Playground.com for users 1, 2, 3, 4, and 5. In contrast, the administrator's real biometric identity was used to evaluate system performance under authentic conditions. From the graph, it can be observed that the time required for face registration varies more significantly among users than the time for face login, which remains relatively consistent. The results show that the administrator exhibits the shortest duration for both registration and login processes, underscoring the system's capability to provide swift and efficient authentication for genuine users. This analysis highlights the system's differential response between synthetic and real biometric data, indicating potential avenues for further optimization and performance enhancement.

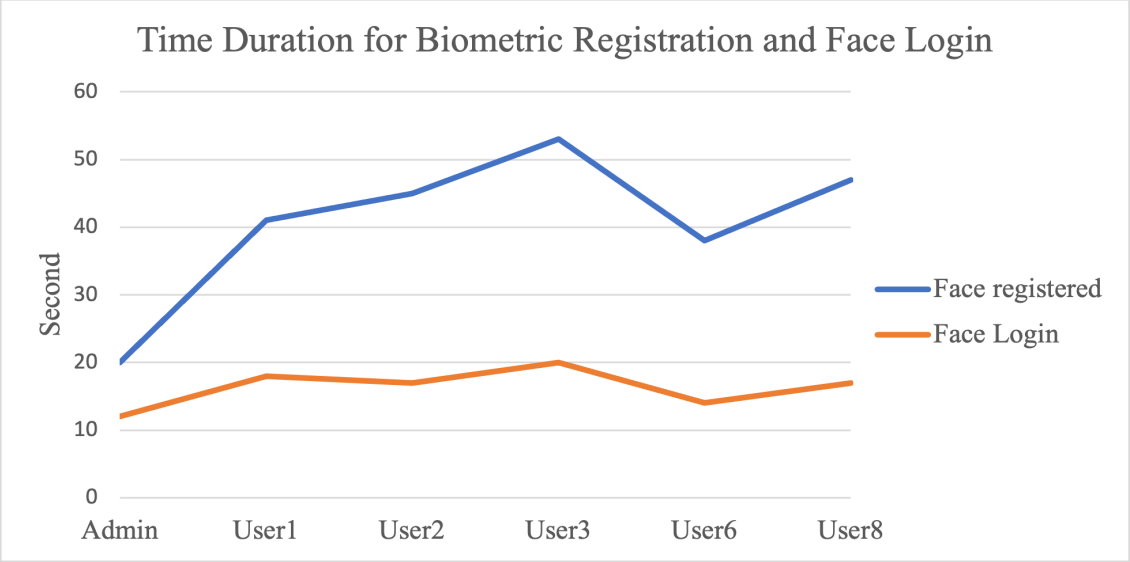


Figure 5.37 : Compare Administrator (Real User) with Dataset

5.6.4 BBIM Algorithm Complexity Analysis

Table 5.3 presents a computational analysis of the primary authentication and blockchain-related Algorithms 1- 8, implemented within the BBIM subsystem. This analysis evaluates the computational efficiency of key processes such as user registration, biometric processing, and blockchain validation. Each algorithm is categorized according to its asymptotic time complexity, expressed using Big O notation [92], which provides insight into how computational cost scales as the input size (n) increases. In this analysis, n represents the input size specific to each process, such as the number of users, facial images, or blockchain blocks, depending on the operation being evaluated. The results illustrate the scalability and operational characteristics of the BBIM subsystem under varying loads.

Algorithm	Complexity	Discussion
Account Creation Procedure	$\mathcal{O}(n)$	Involves storing user and biometric data, scaling linearly with user count. Each additional user adds proportional storage and verification time, resulting in predictable linear growth.
Register Face	$\mathcal{O}(1)$	Handles biometric registration by storing metadata and hash values. Execution time remains constant for each registration, ensuring scalability.
Process Face Images	$\mathcal{O}(n^2)$	Performs preprocessing tasks such as resizing, filtering, and feature extraction. Complexity grows quadratically with the number of images, affecting throughput.
Face Login Process	$\mathcal{O}(n^2)$	Conducts real-time facial matching by comparing input images with all stored templates. The quadratic cost can be optimized through indexing, hashing, or parallel matching.
Change Password Procedure	$\mathcal{O}(1)$	Executes a direct password update in the database. Independent of data size, the operation runs in constant time, ensuring immediate response.
Logout Procedure	$\mathcal{O}(1)$	Terminates a user session by clearing session variables. The operation's cost remains constant regardless of user or system size.
Validate Blockchain	$\mathcal{O}(n)$	Sequentially verifies each block's integrity and consistency. Validation time increases linearly as the blockchain expands, ensuring reliability.

Table 5.3 : BBIM Algorithm Complexity Analysis

Table 5.3 indicates that most BBIM operations exhibit either linear or quadratic growth relative to system scale. Quadratic time processes, particularly those involving facial image processing, represent the primary computational overhead due to the intensive nature of feature extraction and matching. These operations can be optimized through techniques such as indexing, feature dimensionality reduction, or parallel computation [28], [98] and [55]. In contrast, linear time operations, including account creation and blockchain validation, maintain scalability and system stability as the number of users and stored blocks increases. These characteristics ensure that the BBIM system remains efficient, predictable, and capable of sustaining performance under increasing workload conditions.

5.6.5 BBIM System Health and Monitoring

The BBIM performance metrics provide insights into the health and efficiency of various underlying services, such as MySQL, InnoDB, etc. Regularly reviewing the system metrics enables proactive planning for scalability, system optimization, and fault tolerance before potential issues affect overall performance. As illustrated in Figure 5.38, the BBIM performance dashboard continuously monitors several key infrastructure parameters, such as MySQL efficiency (99%) and InnoDB buffer pool usage (17%), etc.

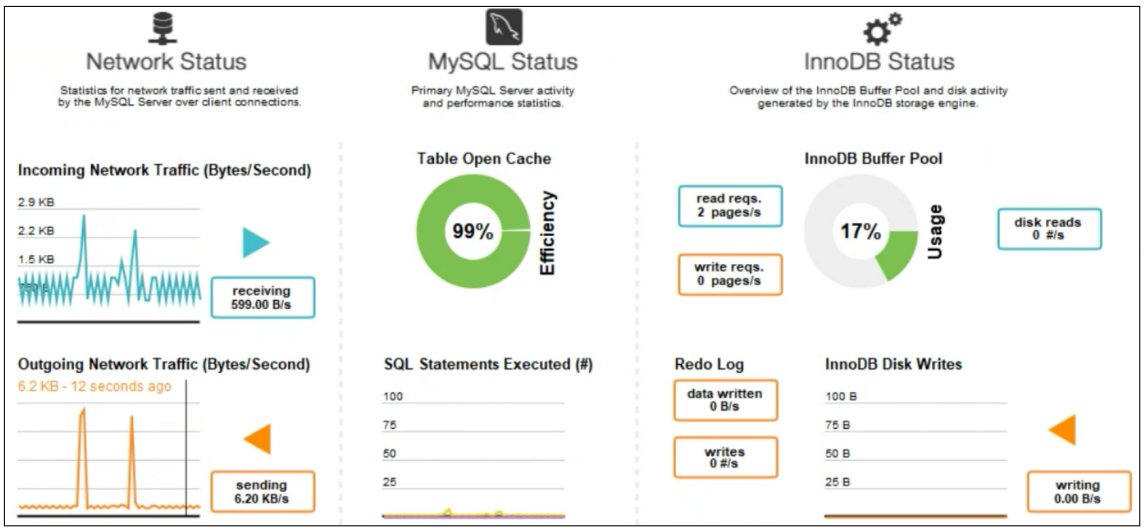


Figure 5.38 : System Performance

Monitoring these metrics provides essential visibility into BBIM's operational performance. It allows researchers and administrators to identify performance bottlenecks, manage resource allocation efficiently, and plan for scalability under varying system loads. Maintaining continuous oversight of these indicators ensures optimal performance, data integrity, and reliability across the BIIM framework, supporting the long-term sustainability and robustness of biometric identity management operations.

5.7 Comparative Evaluation of the BIIM Integrated System

This section compares the BIIM framework with traditional identity systems and decentralized identifier (DID) solutions to evaluate its performance, scalability, and security

capabilities.

5.7.1 BIIM System vs Traditional Systems

To further demonstrate the advantages of the proposed BIIM framework, this subsection presents a comparative analysis between BIIM and traditional identity management systems. The comparison focuses on key operational and security parameters, highlighting BIIM's enhancements in data integrity, transparency, scalability, and regulatory compliance, as summarized in Table 5.4.

Feature	**Traditional Systems**	**BIIM System**
Data Integrity	Data can be modified by privileged system administrators	Tamper-resistant through cryptographic hashing
Auditability	Centralized, mutable audit logs	Immutable and verifiable audit trails via blockchain ledger
Tamper Detection	No native tamper detection mechanism	Data modifications detectable through cryptographic hash validation
Scalability	Dependent on centralized infrastructure capacity	Demonstrated scalability under experimental workloads
Storage Model	Centralized database storage	Off-chain data storage with on-chain cryptographic hash references
Security Model	Relies on firewalls and access control mechanisms	Security reinforced through cryptographic chaining and decentralized consensus
Performance (Write Time)	Generally low latency	Moderate latency due to blockchain consensus processing
Compliance Support	Limited cryptographic support for non-repudiation	Cryptographic mechanisms supporting verifiable compliance
System Architecture	Centralized identity management architecture	Blockchain-based modular architecture integrating BBIM, UDOD, and FIM

Table 5.4 : BIIM System vs. Traditional Systems

Table 5.4 presents a comparative overview of the proposed BIIM system and traditional identity management frameworks. The findings demonstrate that BIIM substantially enhances data integrity, auditability, and tamper detection through the integration of blockchain technology and cryptographic hashing. In contrast to conventional centralized systems—where administrative manipulation, data breaches, or unauthorized access remain possible—BIIM ensures immutability and transparency by recording all identity transactions on a distributed ledger. Moreover, despite the computational overhead introduced by cryptographic operations and PoW-based transaction admission mechanisms,

BIIM maintains consistent scalability and performance. These attributes position BIIM as a secure, verifiable, and compliance-ready digital identity management framework, well-suited for real-world implementation.

5.7.2 BIIM system vs DID Frameworks

The contributions of this research extend beyond the conventional scope of Decentralized Identifier (DID) frameworks by addressing their inherent limitations in architectural design and system integration. DIDs, as standardized by the W3C [93], establish a self-sovereign identity model that emphasizes portability, interoperability, and the use of verifiable credentials. However, their functionality remains largely confined to the generation and verification of identifiers, offering only a foundational mechanism for decentralized identity representation without comprehensive support for trust management, biometric validation, or federated access.

In contrast, the BIIM framework introduces an expanded architectural model that unifies biometric authentication, AI-assisted verification, federated identity management, and privacy-aware notification mechanisms within a single cohesive system. Through this integration, the framework advances existing decentralized identity paradigms by offering a holistic, scalable, and user-centric architecture that delivers enhanced guarantees of security, privacy, and trust that extend beyond those achievable through DID-based approaches.

5.7.3 Applicability and Domain Evaluation

The applicability of the BIIM system extends across multiple domains, highlighting its versatility and potential for real-world deployment. In the healthcare sector, the system can ensure secure and efficient management of patient records, minimizing the risk of identity theft and fraud while enabling authorized professionals to access medical histories seamlessly. Within the financial industry, it can enhance the security of transactions and user verification processes, providing a robust defense against fraudulent activities and unauthorized access.

For government and public service applications, the BIIM system can optimize processes such as passport issuance, voting, and social benefit distribution, ensuring that only eligible individuals gain access to services. In the corporate sector, it can manage employee identities and access permissions, safeguarding sensitive data while improving operational efficiency. By effectively addressing the challenges associated with securely managing biometric information, the BIIM system demonstrates distinct advantages over conventional blockchain-based identity solutions that lack such comprehensive, privacy-preserving, and user-centric capabilities. These features collectively validate its applicability and potential to advance identity management across diverse sectors.

5.8 Scenario-Based Evaluation

This section presents a comprehensive, scenario-based evaluation of the BIIM system through a realistic, user-centered journey. The scenario illustrates how BIIM's integrated subsystems (BBIM, UDOD, and FIM) collaborate to manage, authenticate, and federate digital identities in a decentralized and privacy-preserving environment. By simulating genuine user interactions and potential adversarial conditions (e.g., spoofing), the evaluation assesses BIIM's functional robustness, security resilience, and usability. It demonstrates how biometric data are registered and hashed on the blockchain, how user consent governs data access, and how federated login is achieved through verifiable identity tokens. The case study thereby establishes BIIM's operational validity under practical conditions and provides the foundation for the subsequent evaluation chapters.

System Usage Scenario: Bob's Journey Through BIIM

The following scenario illustrates a complete user journey within the BIIM framework. It follows **Bob**, an end user, from registration through federated access, demonstrating the interaction among the BBIM, UDOD, and FIM subsystems. **Alice**, the system administrator, oversees verification and access control processes. The scenario highlights BIIM's end-to-end interoperability, transparency, and trust mechanisms.

5.8.1 Registration and Biometric Enrollment

Bob begins registration through the BIIM web portal as detailed in Algorithm 1. After submitting his basic credentials, including name, email, and password, the system sends a one-time password (OTP) via the UDOD notification module, as illustrated in Figures 6.5-6.7. Once the OTP is verified, Bob provides additional personal details such as date of birth and address and uploads a government-issued ID, as depicted in Figure 5.6. Next, the BBIM subsystem initiates biometric enrollment. The facial recognition module captures 100 facial images, as shown in Figure 5.9 using the enrollment logic defined in Algorithm 2. These images are processed to generate a biometric template using Algorithm 3. The resulting biometric template is hashed using the SHA-256 algorithm and immutably stored on BIIM's permissioned blockchain, as presented in Figures 5.33 and 5.34. Bob receives a registration success notification through the UDOD subsystem, as described in Algorithm 9 and further illustrated in Figure 6.7. This step demonstrates BIIM's decentralized approach to secure identity creation and the integrity of its biometric hashing mechanism.

5.8.2 Administrative Verification

Alice receives a verification alert via the BIIM Admin Dashboard, as visualized in Figure 5.13. She validates Bob's submitted identity and biometric data through the comparison interface shown in Figure 5.12. Once the biometric hash is confirmed to match the stored template, she approves Bob's account, as depicted in Figure 5.14. Upon approval, UDOD automatically issues a verification success notification using the administrative response workflow defined in Algorithm 13 and illustrated in Figures 6.8- 6.11, ensuring auditability and operational transparency. This phase validates the reliability of the human-in-the-loop verification process while preserving decentralized record integrity.

5.8.3 Biometric Authentication

Following approval, Bob logs in using the facial recognition feature, as shown in Figure 5.17. The system captures a live image and compares it with the blockchain-stored hash using the face login procedure described in Algorithm 4. A successful match grants

system access, as shown in Figure 5.18. In the event of a mismatch, the system triggers a failure notification or detects spoofing, as illustrated in Figures 5.19 and 5.20. During this process, the UDOD subsystem generates real-time login alerts via Algorithm 10, as visualized in Figures 6.12- 6.15. BBIM's liveness detection prevents replay and photo-based attacks by validating both facial movement and depth cues.

5.8.4 Profile Management and Change Logging

Within the user dashboard Figure 5.23, Bob updates personal details and resets his password using the profile management interface, as illustrated in Figures 5.27- 5.31 and the change-password procedure outlined in Algorithm 5. Each modification is securely logged on the blockchain, and corresponding notifications are issued by UDOD using Algorithm 11 for profile updates and Algorithm 12 for password changes, as shown in Figures 6.16- 6.20. This mechanism enforces transparency and provides a verifiable audit trail to maintain sovereignty over Bob's identity data.

5.8.5 External Organization Request for Verification

A registered organization (such as a university) submits a request to verify Bob's identity, as depicted in Figure 5.32 and Figures 6.22- 6.24. This request is routed through the UDOD subsystem to ensure consent-driven processing. Alice reviews the legitimacy of the request using the administrative interfaces presented in Figures 6.25 and 6.26, guided by the administrative response logic detailed in Algorithm 13. Bob receives a comprehensive notification describing the requester's identity, the scope of the request, and the intended data usage, as defined by Algorithm 14 and visualized in Figures 6.29- 6.34. This dual-layer approval process exemplifies BIIM's privacy-by-design framework.

5.8.6 User Consent and Selective Data Sharing

When the access request is received, Bob reviews its details and either approves or rejects the request using the consent management interfaces illustrated in Figures 6.35- 6.41. The decision is processed entirely by the UDOD subsystem, which enforces user-driven

control over identity data sharing. If Bob approves the request, the system securely records the consent decision and notifies the requesting organization, granting access only to the explicitly authorized attributes. If the request is rejected, the organization is notified without any data exposure. This selective disclosure mechanism demonstrates BIIM's adherence to data minimization and transparency.

5.8.7 Federated Identity Access

Bob later accesses the university's online portal using the "Log in with BIIM" option. The FIM subsystem validates his biometric identity through a brief liveness check and resolves his decentralized identity via Algorithm 15. The federated identity workflow is outlined in Figures 7.3 and 7.4, while secure service redirection is executed through Algorithm 18, and further shown in Figures 7.8 and 7.9. The university's system authenticates the blockchain-backed token, enabling seamless access without requiring redundant credentials.

5.8.8 Analytical Evaluation and Reflection

This scenario collectively demonstrates BIIM's effectiveness as an intelligent, decentralized identity management ecosystem. Each subsystem contributes distinct but interdependent roles: BBIM ensures biometric immutability via Algorithms 1– 8, UDOD upholds user consent and transparency through Algorithms 9- 14, and FIM enables privacy-preserving federated access as defined in Algorithms 15– 18. The coordinated operation validates BIIM's architectural objectives, namely trust decentralization, security, and interoperability.

From a research perspective, this scenario highlights BIIM's capacity to maintain operational reliability and security, even under simulated attacks and cross-domain use cases. The evaluation confirms that integrating blockchain with biometric verification and consent-driven governance achieves a verifiable, user-centric identity management framework. Ultimately, this analytical validation establishes a robust foundation for the quantitative performance assessments presented in the subsequent chapters.

5.9 Discussion

The evaluation results confirm that the BBIM subsystem effectively addresses the theoretical and practical limitations identified in Chapter 2, particularly the challenge of developing a secure identity management system that remains under user control. Earlier approaches concentrated on protecting biometric templates in centralized systems but failed to achieve user sovereignty or to integrate biometrics into a broader privacy-preserving ecosystem. The BBIM framework responds to this gap by combining biometric registration and verification within a decentralized blockchain structure, ensuring immutability, verifiability, and resistance to tampering while maintaining individual authority over identity data.

From a theoretical perspective, BBIM demonstrates that blockchain can operate as a distributed trust layer for biometric identity management. By shifting trust from centralized institutional control to cryptographically verifiable and consensus-backed transaction records, the architecture enhances system integrity and resilience. Each enrollment and verification event is permanently recorded on-chain, ensuring transparency and auditability of identity operations. The separation of on-chain and off-chain storage further enhances privacy and efficiency: hashed biometric references are maintained on-chain to support integrity verification, whereas encrypted biometric templates are stored off-chain to minimize data exposure and preserve user control over sensitive information.

Experimental evaluation verified the computational performance and scalability of the framework. As shown in Table 5.1, system performance remained stable under increasing user load, and Table 5.3 outlines the algorithmic complexity of the core processes. Registration, encryption, and blockchain insertion demonstrated linear time complexity $\mathcal{O}(n)$, where n represents the number of processed identities, confirming predictable scalability as the user base grows. In contrast, facial image preprocessing and matching operations exhibit quadratic behavior $\mathcal{O}(n^2)$ due to the intensive nature of feature extraction and template comparison. Despite this higher cost at the algorithmic level, the empirical results show that end-to-end registration and verification times remain within acceptable

bounds under the evaluated loads, indicating that biometric identity management can scale efficiently in decentralized environments.

Comparative results in Table 5.4 show that BBIM outperformed traditional identity systems in reliability, transparency, and fault tolerance while maintaining acceptable computational overhead. These outcomes confirm that biometric identity management can scale efficiently in decentralized environments

Security and privacy findings substantiated the theoretical foundation of the framework. The integration of biometric data into blockchain transactions enhanced non-repudiation and reduced credential misuse by substituting static identifiers with cryptographically verifiable proofs. The immutability of the ledger prevented duplication or manipulation of identity records, while consensus validation ensured that false or duplicate identities were detected in real-time. The storage approach preserved user sovereignty by granting individuals exclusive control over access and verification. Scenario-based evaluations verified that users could authorize or deny access to their biometric-linked identity data, demonstrating the feasibility of user-controlled authentication within a decentralized network.

Within the BIIM architecture, the BBIM subsystem establishes the secure and verifiable enrollment foundation required for the UDOD and FIM subsystems. These components address the central challenge of enabling a biometric-based system that remains fully under user control while supporting interoperability and accountability across multiple domains. BBIM authenticates and anchors trusted digital identities; UDOD extends this capability by allowing users to manage access of identity data transparently; and FIM ensures that these verified identities can operate securely across federated environments. Through this layered integration, the BIIM architecture achieves a coherent, user-centric model of digital identity governance.

Research on the integration of blockchain with biometric data is relatively limited. However, the innovative approach of the BIIM system in this area is remarkable for its ability to securely store personal information and biometric data while ensuring high

levels of privacy protection. The core strength of the BIIM system lies in its robust user management and secure identity features. The BBIM subsystem significantly reduces the risks associated with biometric data breaches by maintaining an immutable and tamper-proof record on the blockchain. This approach not only enhances the overall trustworthiness of the system but also sets a new standard in identity management.

The BBIM system represents a significant technical and conceptual contribution to biometric identity management. The evaluation and complexity analysis demonstrated that blockchain can sustain secure, scalable, and transparent biometric verification while preserving user authority. By combining biometric authentication with decentralized storage and integrating it with the UDOD and FIM subsystems, BBIM achieves its objective of creating a user-controlled, privacy-aware, and interoperable digital identity framework. These findings position BBIM as a key enabler for trustworthy, next-generation identity ecosystems built on the principles of decentralization and user sovereignty.

5.10 Conclusion

This chapter provided a comprehensive analysis of the fundamental components of BIIM, including an exploration of the blockchain-based data storage mechanism, blockchain operations, and chain management. The detailed implementation of the BBIM system constitutes a crucial step toward achieving the next research objective of this thesis.

The following chapter focuses on user-driven identity access control, emphasizing privacy awareness. This stage will offer valuable insights into BIIM within the identity and access management domain, thereby enhancing our understanding of data security and user-centric privacy measures.

Chapter 6

User-Driven and Organization-Driven Pre-emptive Privacy-Aware Notifications System (UDOD)

6.1 Introduction

Over the past few years, the rapid growth of digital decentralized technologies has transformed the landscape of data management, sharing, and security. While blockchain-based identity frameworks such as BIIM and BBIM have strengthened data integrity, authentication, and accountability, significant challenges remain regarding privacy protection and user awareness of data access activities [67]. Traditional identity management systems generally operate with limited transparency, failing to inform users about who accesses their data, under what conditions, and for what purpose. This lack of visibility undermines users' trust and limits their control over personal information in digital environments.

To overcome these limitations, the User-Driven and Organization-Driven Pre-emptive Privacy-Aware Notifications System (UDOD) notification subsystem is introduced as an enhancement to the BIIM framework. UDOD is a privacy-aware, intelligent notification mechanism designed to ensure real-time visibility and control over identity-related data access. It integrates two complementary components: the *User-Driven (UD)* notification mechanism and the *Organization-Driven (OD)* notification mechanism. These components deliver proactive, context-aware alerts that enable users to make informed decisions about their data sharing activities while ensuring transparency and accountability.

Integrating blockchain technology into the UDOD subsystem provides a secure, tamper-evident, and verifiable notification mechanism. Transaction validation logic at the application layer encodes the rules that determine when and how notifications are triggered, validated, and recorded. For example, a notification is automatically generated when

access to user data is requested or when an identity verification event is completed. This blockchain-enabled approach enhances auditability and accountability while preserving data privacy and integrity across all recorded transactions.

The scientific contribution of the UDOD subsystem lies in the design and implementation of Algorithms 9, 10, 11, 12, 13, and 14. These algorithms integrate blockchain and database technologies to detect access events, analyze contextual parameters, and generate verifiable notifications that allow users to respond dynamically to data requests. Experimental evaluation confirms the system's scalability, computational efficiency, and real-time responsiveness within decentralized identity environments. From a social perspective, the UDOD subsystem represents a major step toward user empowerment and data transparency. It provides individuals with fine-grained control and visibility over their identity data usage, enhancing trust between users and organizations. Within the BIIM architecture, the UDOD subsystem complements the roles of BBIM and FIM by adding a real-time awareness and accountability layer, thereby strengthening BIIM's holistic, user-centric approach to decentralized identity management.

In the previous chapter, we explored the implementation and operation of the BIIM and BBIM systems and discussed the integration of blockchain within the BIIM framework. This chapter focuses on the UDOD subsystem, emphasizing its design, architecture, and operational mechanisms for privacy-aware notifications. The structure of this chapter is as follows: Section 6.2 presents the overall architecture of the UDOD subsystem, establishing the technical foundation for its operation. Section 6.3 introduces the taxonomy of notifications within the BIIM framework. Section 6.4 explains the operational workflow of the UDOD system. Sections 6.5 and 6.6 describe the User-Driven and Organization-Driven components, respectively. Section 6.7 presents the implementation details, followed by Section 6.8, which evaluates the system's performance in terms of scalability, responsiveness, and computational efficiency. Section 6.9 provides a critical discussion of the experimental findings and their implications for decentralized identity management. Finally, Section 6.10 summarizes the key insights and concludes the chapter.

6.2 UDOD System Architecture

Figure 6.1 illustrates the architecture of the UDOD subsystem, which facilitates decentralized notification management and access governance within the BIIM framework. The architecture adopts a three-layer design comprising the *view*, *control*, and *model* layers. Each layer operates collaboratively to ensure real-time awareness, policy enforcement, and transparency across user–organization interactions.

The view layer functions as the primary point of interaction between end users or organizational entities and the UDOD system. Through this interface, users can perform operations such as registration, login, profile modification, and identity access requests. The view layer abstracts the complexity of the underlying blockchain and notification mechanisms, offering an intuitive and responsive interface that enhances accessibility and user experience while maintaining high standards of privacy and security.

The control layer serves as the operational core of the UDOD subsystem, responsible for generating, processing, and managing intelligent notifications. It encompasses processes such as *Registration Process Notification*, *Face Registered Process Notification*, *Change and Reset Password Notification*, *Login Process Notification*, *Profile Update Notification*, and *Organization Request Notification*, as illustrated in Figure 6.1. These notifications are automatically triggered in response to predefined user or organizational activities, providing immediate alerts before sensitive operations are executed. By facilitating timely awareness and enabling user validation, the control layer reinforces accountability and ensures that access privileges and identity actions remain transparent, auditable, and user-authorized.

The model layer, also referred to as the storage layer, provides the blockchain-enabled data management foundation of the UDOD subsystem. It integrates both on-chain and off-chain components to balance efficiency and trust assurance. Notification data and monitoring records are processed and preserved in secure off-chain databases, while the blockchain immutably records proofs of alerts and user-related events. The UDOD system employs a BFT consensus mechanism to validate identity notifications, such as identity modification and request events across participating nodes, while PoW is integrated as an

auxiliary admission control mechanism to regulate event submission. This ensures that all user- and organization-driven actions are transparent, verifiable, and tamper-resistant, enhancing accountability and maintaining an auditable trail of access and updates within the decentralized environment. This configuration combines the scalability of off-chain storage with the verifiability of distributed ledger technology, delivering a secure and auditable foundation for decentralized notification management.

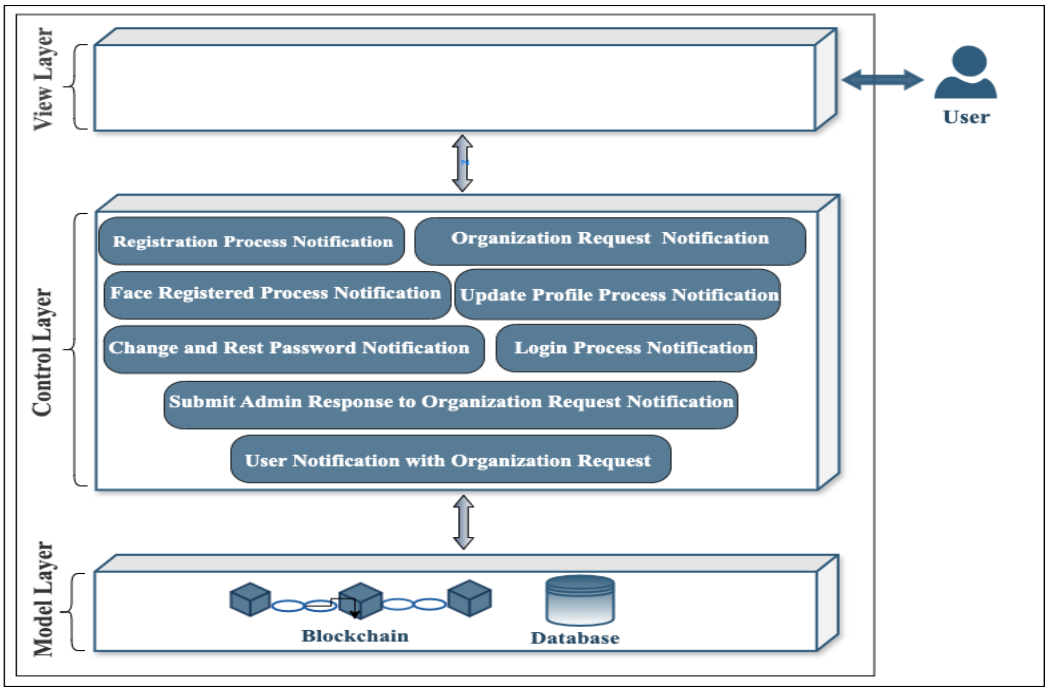


Figure 6.1 : UDOD System Architecture

The UDOD architecture establishes a privacy-preserving and transparent notification framework that empowers users with granular control over identity-related activities. Through the integration of blockchain-based verification into real-time notification processes, the UDOD subsystem enhances accountability, strengthens user awareness, and complements the BBIM and FIM components in achieving a secure, decentralized, and user-governed identity management system.

6.3 Taxonomy of Notifications

The taxonomy of all the notifications and the relationship between them is presented in Figure 6.2. It outlines a structured classification of notifications within the BIIM system and helps to understand how the system communicates with its users, ensuring transparency and security. The taxonomy provides a clear description for the UDOD system to categorize the different types of notifications that users receive within the combined UD and OD systems. In Figure 6.2, notifications are represented using a solid arrow, and dotted arrows represent a process or a part of the process.

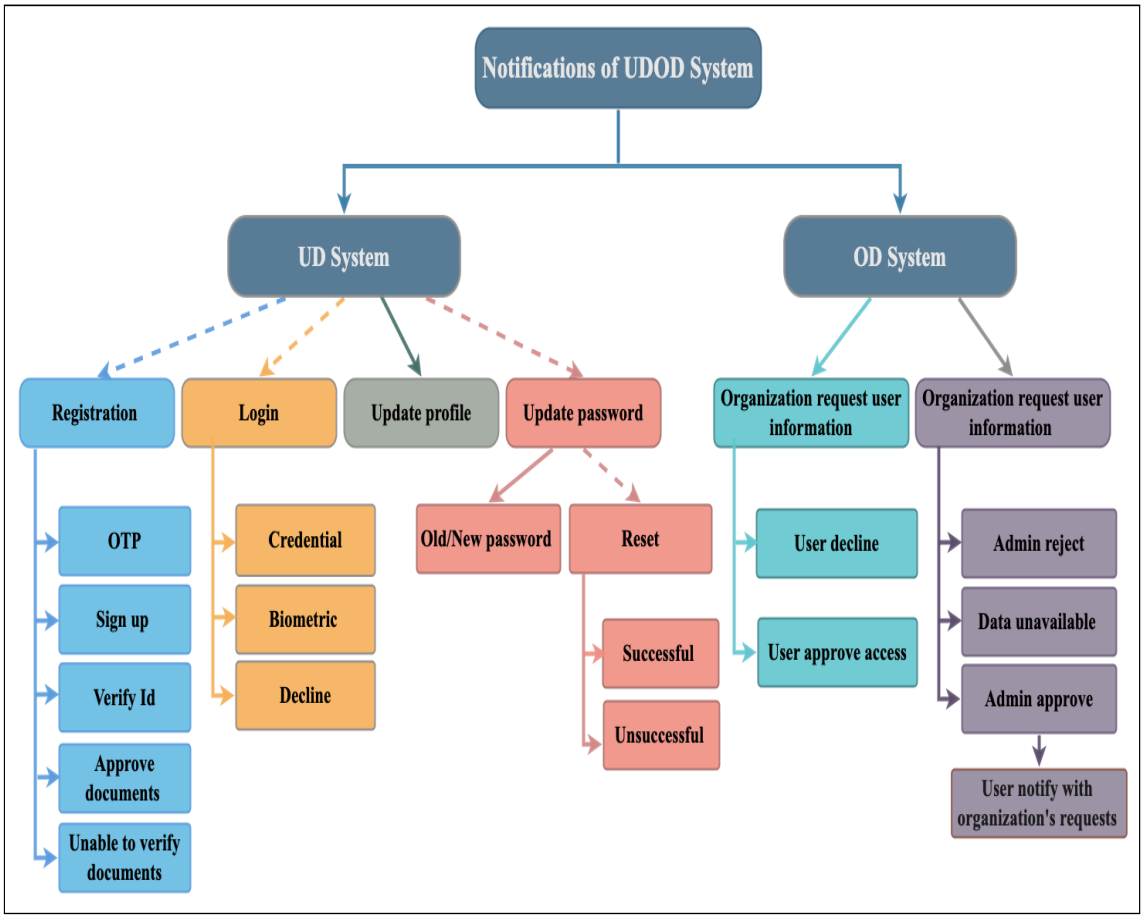


Figure 6.2 : Taxonomy of Notifications

Notifications can be categorized into the following:

- **UD System, which interacts with BIIM notifications:**

  These are automated messages generated by BIIM to inform users about their activities and address security concerns about their identity. They include registration, log-in, profile updates, and password changes. Notifications related to the verification process of a user's identity, such as requests for additional documentation, verification status updates, or verification completion confirmations, are also included. These notifications are directly related to the interactions of users with the BIIM. The following are the notifications for the UD system, as explained in detail in Section 6.5:

  1. *OTP*
  2. *Unable to verify documents*
  3. *Sign up successfully*
  4. *Approve documents*
  5. *Verify ID*
  6. *Reset the password using old and new password*
  7. *Successfully reset password*
  8. *Unsuccessfully reset password*
  9. *Login successfully using credential*
  10. *Login successfully using biometric*
  11. *Login Decline*
  12. *Update profile*

- **OD System, which interacts between entities within the BIIM notifications:**

  These notifications concern transactions involving the organization's attempts to access the user's digital identity. They include confirmations of successful access

and alerts about pending transactions that require user action. These notifications are directly related to the interactions between entities within the BIIM. The following are the notifications for the UD system, which are explained in detail in Section 6.6:

1. *Administrator receives the organization request*
2. *Administrator approves the organization request*
3. *Administrator rejects the organization request*
4. *Administrator notifies organization with unavoidable data*
5. *User notifies when an organization requests access*
6. *Organization requests user information*
7. *User approves access to organization request*
8. *User declines organization request*

6.4 The Working of the UDOD System

As outlined in Chapter 3, the UDOD system is a core component of the BIIM architecture. In this thesis, the terms *UDOD system* and *UDOD subsystem* are used interchangeably to denote the user-driven and organization-driven notification framework that enables real-time, privacy-aware monitoring of data access activities within BIIM.

Figure 6.3, highlights the importance of user-driven and organization-driven access control, empowering individuals to determine the specific entities allowed to access their information and those which are restricted.

The UDOD system is part of the BIIM framework. As such, it extensively leverages blockchain infrastructure alongside complementary storage systems such as MySQL, which is used to manage and store identity documents. The system's operation is governed by a policy-driven architecture in which the blockchain records and verifies default data access rules, while the AI-based control layer dynamically manages and adapts these policies based on contextual factors and system usage. The working of the UDOD system is therefore guided by the following key principles and elements:

- All modifications to a user's identity are processed through the blockchain's BFT-based consensus mechanism (explained in detail in Chapter 5). Records of all changes and updates are stored sequentially on the blockchain.
- Whenever a modification to a user's identity occurs, the user receives an email notification informing them of the change.
- All notifications are dispatched in real-time, ensuring that users are promptly aware of any updates.

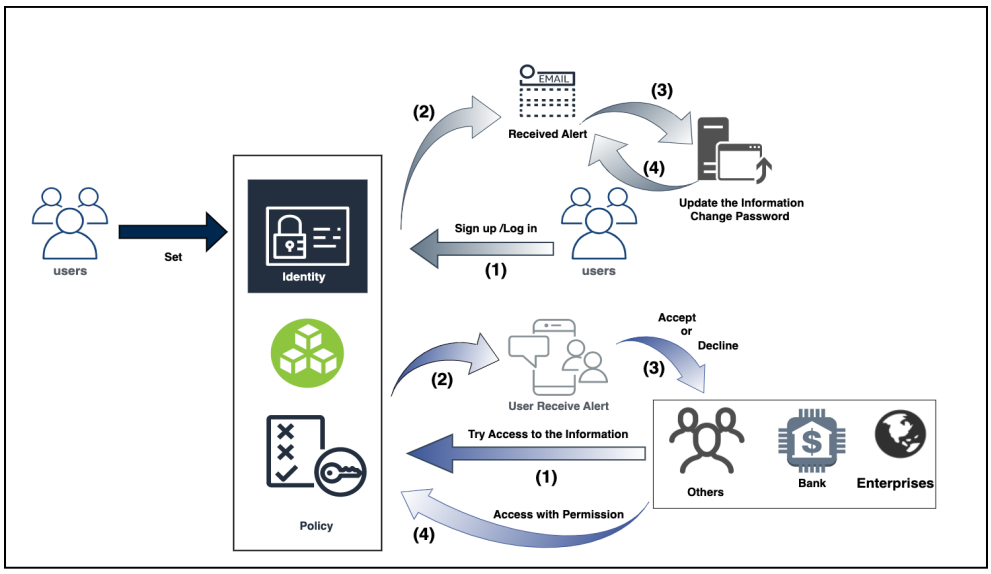


Figure 6.3 : Overview of the UDOD Privacy-Aware Notifications System

In the context of BIIM, the blockchain policy ensures that users retain full control over the visibility and use of their data. These policies define the conditions under which notifications are activated, validated, and processed. Notifications are securely triggered only under specific, predefined circumstances, such as when a request is made to access user data or when an identity-verification procedure is completed. This blockchain-enabled approach provides a transparent and tamper-resistant notification framework, thereby strengthening user trust in the integrity of system interactions. It is also important to acknowledge that governmental authorities may access user information when legally

required [70], and users are notified accordingly. All other forms of data access, including those requested by banks, retail enterprises, credit institutions, and financial organizations, require explicit permission from the data owner. These access-control and notification mechanisms, supported by blockchain policies, are further examined in the subsequent sections.

The UD system enables users to receive instant alerts for any interactions within BIIM. Users are notified promptly of activities such as registering, logging in, updating profiles, and changing passwords. A real-time alert gives users the ability to monitor their accounts in real-time and promptly respond to any changes or actions taken, enhancing the platform's overall security.

The OD system serves as a layer of defense against potential security threats or unauthorized access. It allows users to receive alerts for any attempted access to their information, ensuring that they are immediately informed of such activities. Authorized government bodies can proceed with data access, while external entities, such as enterprises and organizations, are required to obtain explicit permission, triggering notifications that require a response and acknowledgment.

The UDOD subsystem operates as an intelligent notification mechanism rather than a conventional alerting process. Its intelligence is rooted in context-aware, rule-based decision logic embedded within the control layer, which dynamically determines how and when notifications are generated. Unlike static alert systems, UDOD differentiates between user-initiated and organization-initiated actions, applying adaptive rules defined through blockchain-enforced policies. These rules evaluate contextual parameters such as data sensitivity, authorization level, and request frequency to autonomously adjust notification priority and delivery. The control layer thus functions as an inference mechanism, interpreting contextual conditions and executing the appropriate notification workflow without requiring manual intervention. Through asynchronous, event-driven execution, the system maintains real-time responsiveness under varying transaction loads. All notification events are recorded on the blockchain in a tamper-evident manner, ensuring verifiable audit

trails that strengthen transparency and accountability. This combination of adaptive logic, autonomous control, and immutable verification substantiates the UDOD subsystem's role as an intelligent, privacy-aware notification framework within the BIIM environment.

6.5 The Working of the UD System

Figure 6.4 illustrates the alert and notification architecture within the BIIM framework. The system preserves user account integrity through both email and in-system notifications, some of which require user action. This mechanism enhances error handling and ensures effective, real-time communication across the identity management process.

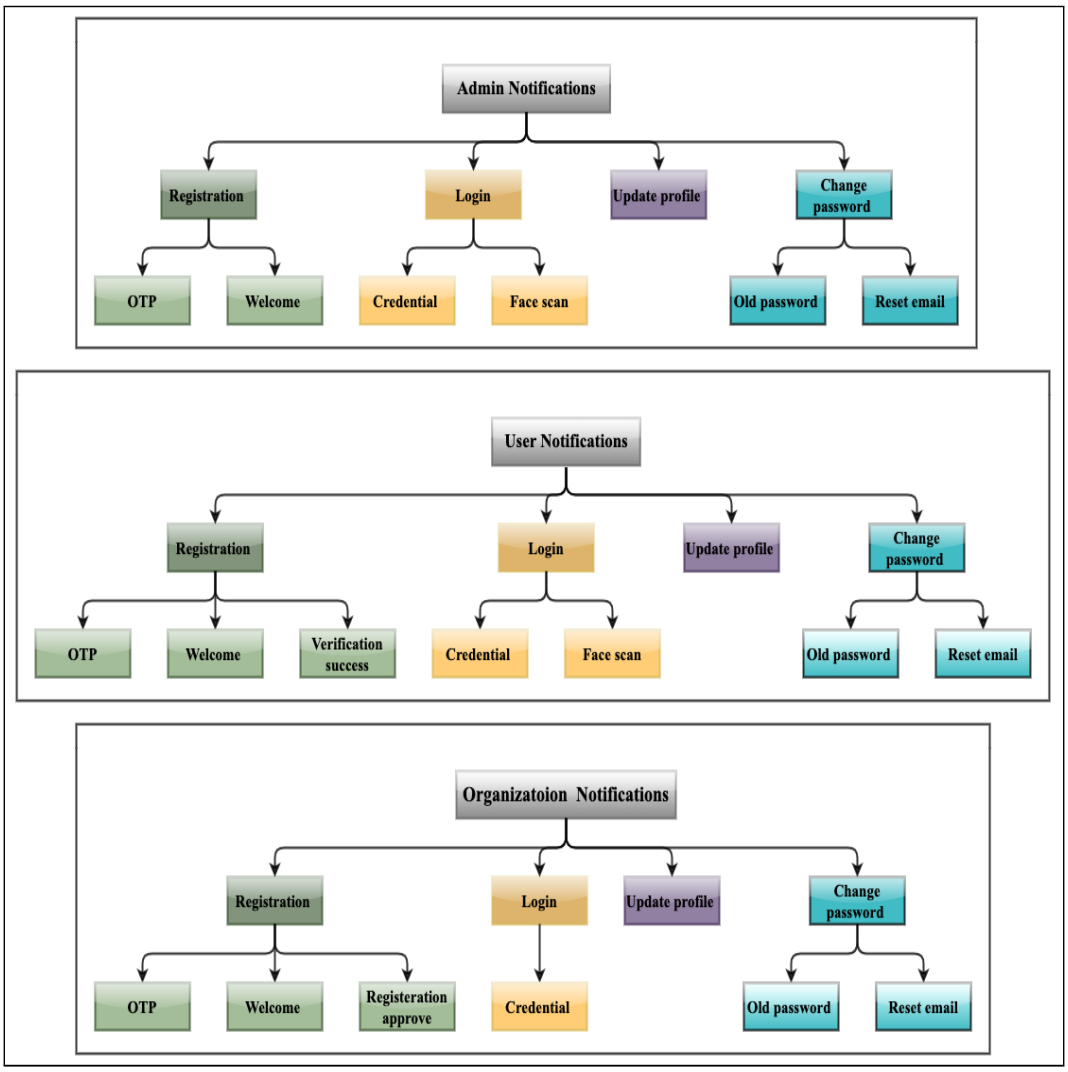


Figure 6.4 : UD Notification Classification

6.5.1 UD System

As part of the UD system, users are informed of their registration status and all interaction activities within BIIM. This enables users to closely monitor their accounts.

6.5.1.1 Registration Notification

Figure 6.5 shows the operation of the registration process in the UD system within BIIM. The fundamental logic is articulated through Algorithm 9, which manages the authentication workflow and the generation of corresponding user notifications. It validates login attempts, either biometric or credential-based, and triggers automated alerts that inform users of successful or failed login activities within the BIIM environment. Users receive an OTP code based on the initial registration process in our system, as shown in Figure 6.6. After the registration process, an email notification is sent containing the unique ID, as shown in Figure 6.7.

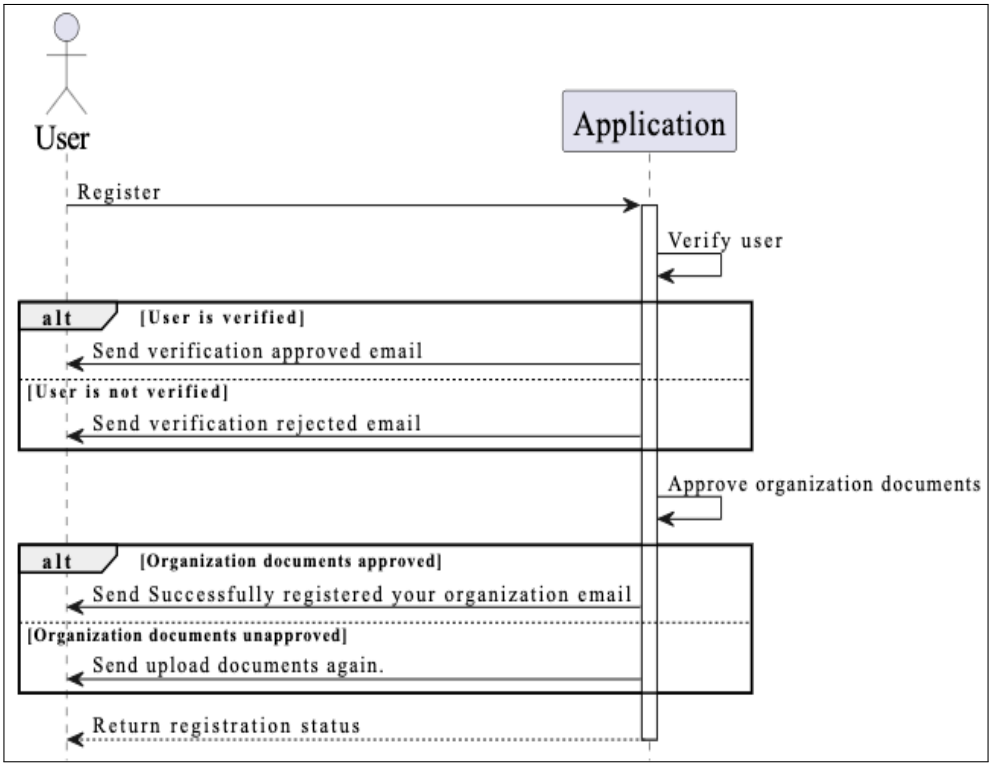


Figure 6.5 : Notification of the Registration Process

Algorithm 9 Notification of Face Registered Process

```
function HANDLEFACECAPTURE(countFace, img, uid)
    if countFace > 100 then
        Log "Recognition stopped due to high face count."
        Convert img to grayscale.
        Set notification message to "Face Registered!!".
        Annotate img with the notification message.
    else
        Log "Face not found."
    end if
    return the processed image.
end function
```

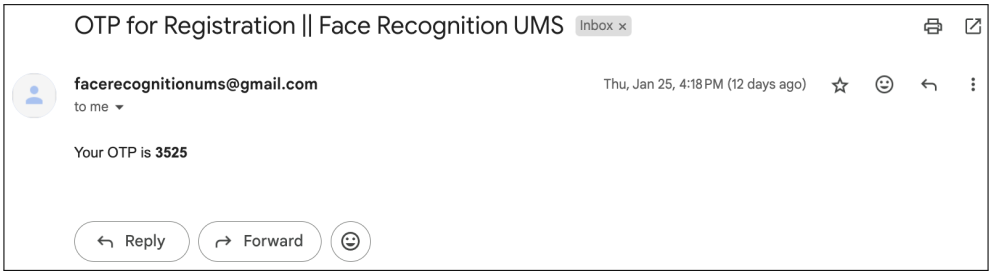


Figure 6.6 : OTP

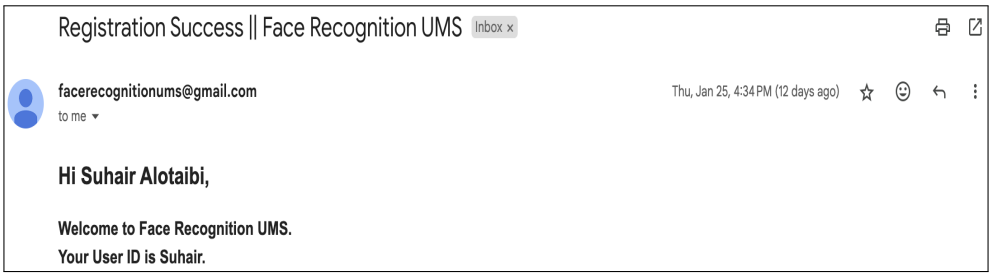


Figure 6.7 : Sign up Successful

In contrast, organizational accounts receive an email notification that ensures their registration and requests to wait for the administrator to approve their documents, as shown in Figure 6.8. Following this, the administrator must verify the user account and approve

organizational documents, after which end users receive an email that allows them to begin using their account, as illustrated in Figure 6.9. However, if the data submitted does not match, the administrator will reject the verification and send an email to the user, as illustrated in Figure 6.10. In the event that the user uploads invalid documents, the system considers the account unverified. The user is then notified to upload a valid document to complete the verification process, as shown in Figure 6.11.

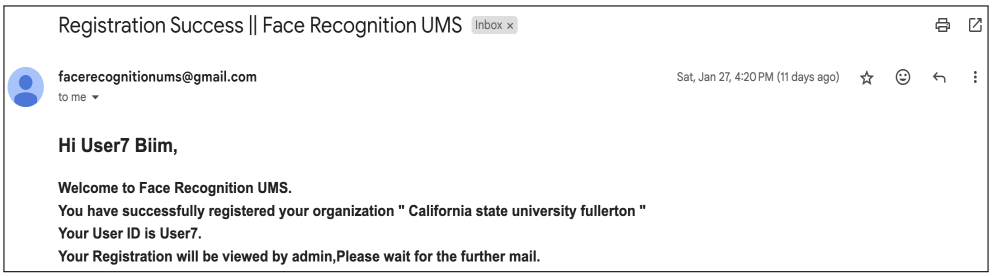


Figure 6.8 : Organization Account has been Waiting for Admin to View and Approve Documents

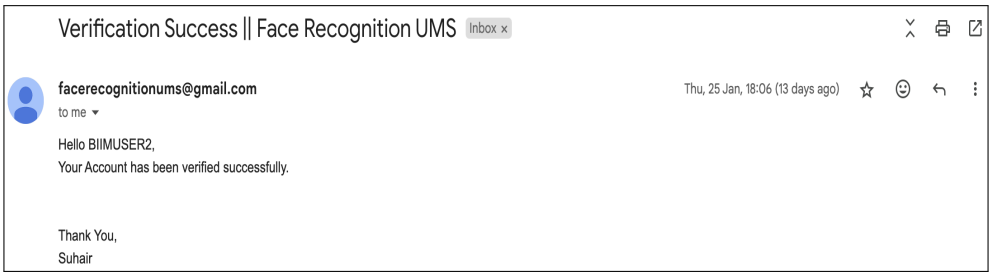


Figure 6.9 : Account has been Verified

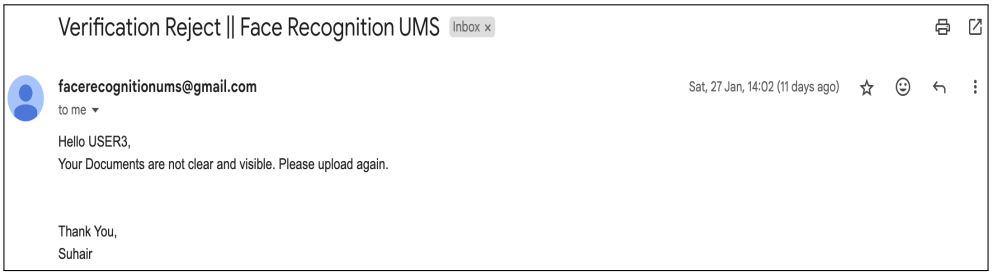


Figure 6.10 : Verification Rejected

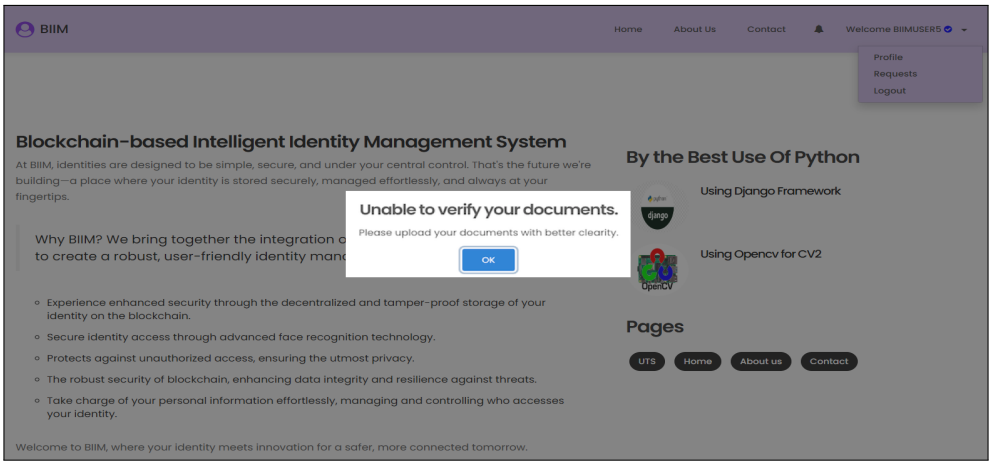


Figure 6.11 : Unable to Verify your Documents

6.5.1.2 Login Notification

Figure 6.12 illustrates the operation of the UD system in the login process within BIIM. The user initiates the login sequence by entering a username and password or a user ID and biometric. The system verifies the user's credentials against the stored database, as outlined in the Algorithm 10. In a scenario where the user exists and the credentials provided are accurate, the system guides the user to the home page while simultaneously sending a success email to the user, notifying them of the successful login, as shown in Figure 6.13 and Figure 6.14. Conversely, an error message is displayed when the administrator does not verify the account, if the user does not exist in the database or if there is an inconsistency in the biometric information, as shown in Figure 6.15.

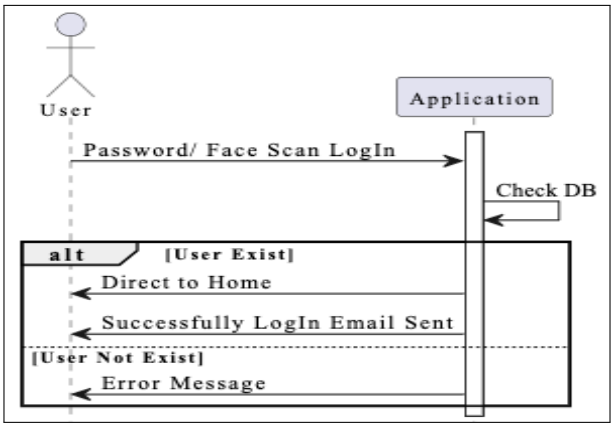


Figure 6.12 : Notification of Login Process

Algorithm 10 Notification of Login Process

```
1:  function LoginProcess(request)
2:      if request.method = "POST" then
3:          if request includes face scan then
4:              username ← extract from
5:              uid ← extract face ID from request
6:              if User exists with username, uid then
7:                  perform face login using uid
8:                  return "You have successfully logged-in using FaceScan"
9:              else
10:                 return "Failed facelogin !!"
11:             end if
12:         else if request includes username and password then
13:             username ← extract from request.POST['username']
14:             password ← extract from request.POST['password']
15:             if Credentials valid for username, password then
16:                 perform username/password login for username, password
17:                 return "You have successfully logged-in using Password"
18:             else
19:                 return 'Invalid username or password.'
20:             end if
21:         else
22:             return 'Invalid login request.'
23:         end if
24:     else
25:         return redirect to login page
26:     end if
27: end function
```

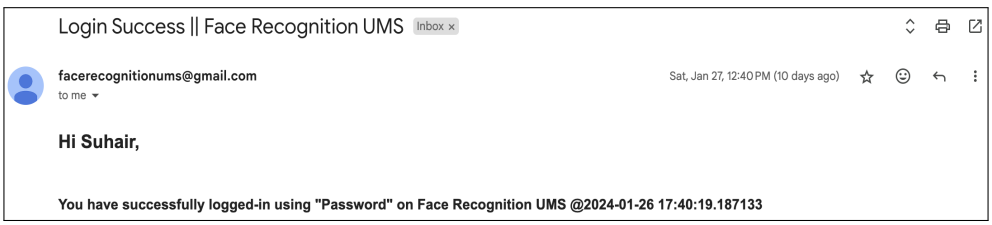


Figure 6.13 : Successful Login Using Credentials

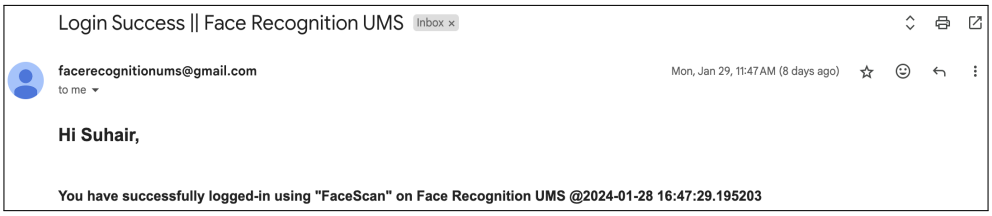


Figure 6.14 : Successful Login Using Face Recognition

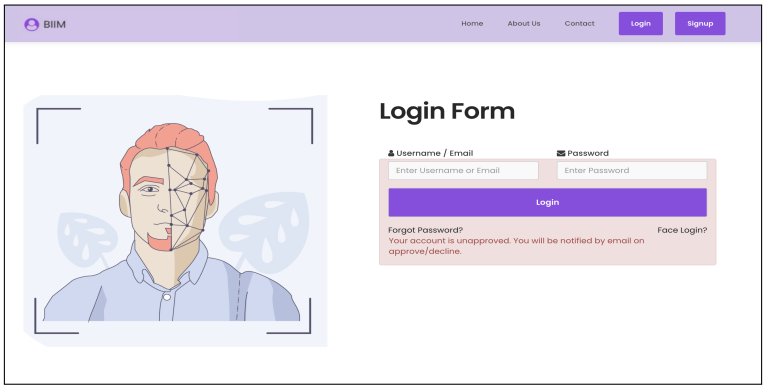


Figure 6.15 : Login Declined Until Account is Approved

6.5.1.3 Profile Editing Notification

The sequence diagram in Figure 6.16 outlines the procedural flow between a user and a BIIM during the profile editing process. The user visits the profile page and edits the profile data. The application then validates the submitted information, leading to two possible outcomes. When the profile data is valid, the system updates the user profile, displays the revised information, and sends an email notification confirming the successful update, as illustrated in Figure 6.17. The notification logic governing this process is formalized in Algorithm 11, which coordinates data validation, profile updates, and the generation of real-time user notifications. The algorithm ensures that every modification to a user's profile triggers an appropriate alert, maintaining transparency and accountability within the UD system.

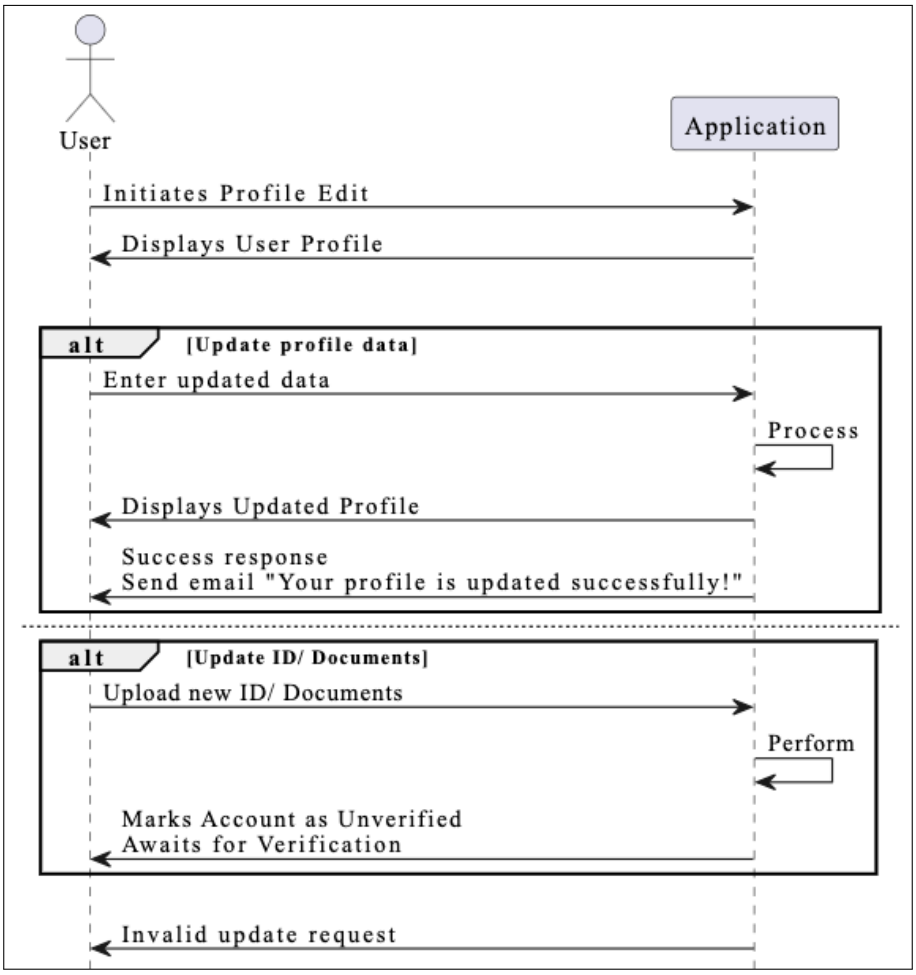


Figure 6.16 : Notification of Profile Update

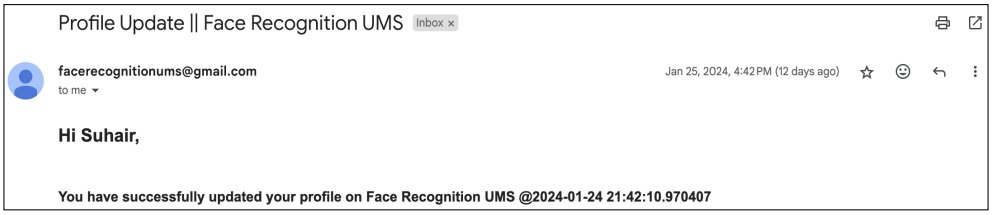


Figure 6.17 : Successful Profile Update

Algorithm 11 Notification of Update Profile Process

```
1: function HANDLEPASSWORDCHANGEPOST(request, form)
2:     if request method is POST then
3:         user_form ← EditProfileForm
4:         for each field in request do
5:             Validate field
6:             if validation fails then
7:                 Update error message for field
8:             end if
9:         end for
10:        if all validations pass then
11:            user ← FORM.SAVE
12:            UPDATE_SESSION_AUTH_HASH(request, user)
13:            MESSAGES.SUCCESS(request,'Your profile is updated successfully!')
14:            return REDIRECT('view_profile')
15:        else
16:            LOGGER.DEBUG("Validation error in profile update form")
17:            Profile will not be saved due to errors
18:        end if
19:    else
20:        Load and show the profile edit form with current user information
21:    end if
22: end function
```

6.5.1.4 Password Reset Notification

The sequence diagram in Figure 6.18 illustrates the procedural flow between a user and a BIIM during the password reset process. To reset a password, the user prompts the application to validate the provided email. Subsequently, if the email proves to be valid, the application immediately sends a password reset email to the user, as illustrated in Figure 6.19, otherwise, it displays an error message, as shown in Figure 6.20. The notification logic that governs this process is formalized in Algorithm 12, which handles both password change and reset operations. The algorithm validates user inputs, updates credentials, and ensures that each action triggers a corresponding real-time notification

to inform users of successful or unsuccessful password operations, thereby reinforcing transparency and security within the UD system.

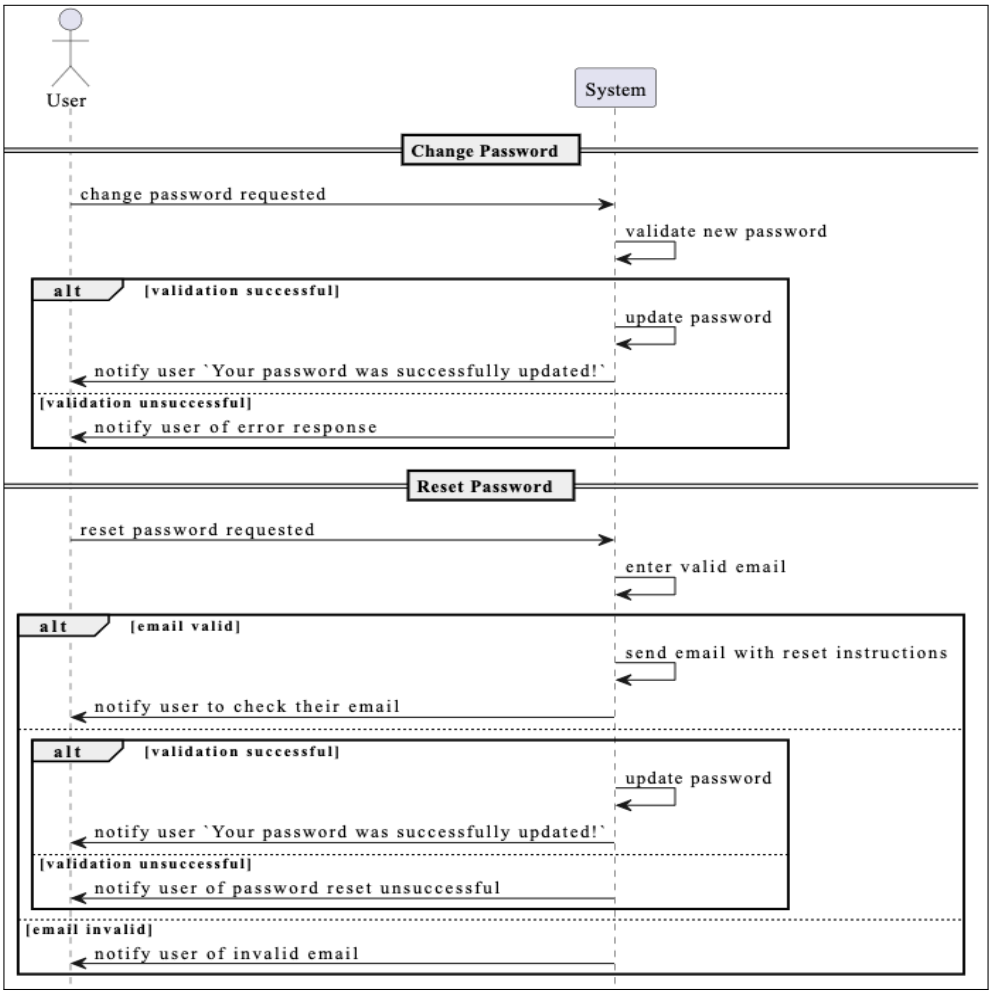


Figure 6.18 : Notification of Change and Reset Password

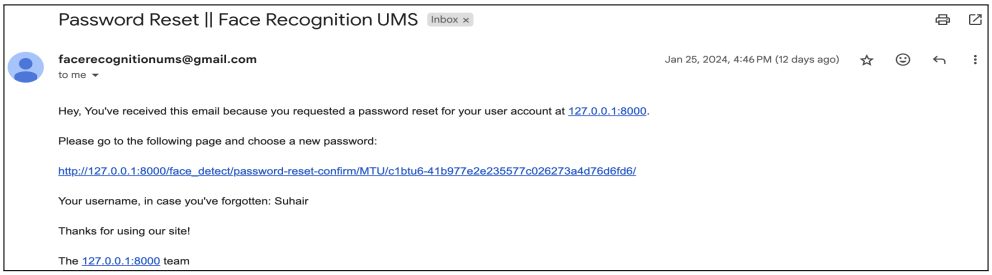


Figure 6.19 : Password Reset

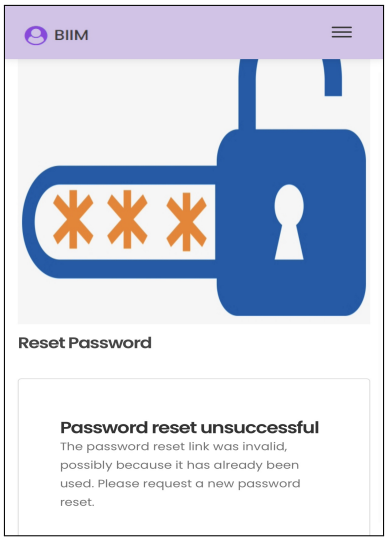


Figure 6.20 : Password Reset Unsuccessful

Algorithm 12 Notification of Change Password Process

```
1:  procedure PASSWORDMANAGEMENT(request)
2:      if change password requested then
3:          validate new password
4:          if validation successful then
5:              update password
6:              notify user 'Your password was successfully updated!'
7:          else
8:              notify user of error response
9:          end if
10:     else if reset password requested then
11:         enter valid email
12:         if email valid then
13:             send email with reset instructions
14:             notify user to check their email
15:         else
16:             notify user of invalid email
17:         end if
18:     end if
19: end procedure
```

6.6 The Working of the OD System

The system, as illustrated in Figure 6.21, focuses on the interactions between organizations and users, which involve the sharing of information with trusted organizations. As organizations navigate the process of accessing user information, the OD system prioritizes user privacy and consent, ensuring control over personal data. Transparency embedded in the notification system keeps all parties informed, which ensures trust and integrity and promotes identity management.

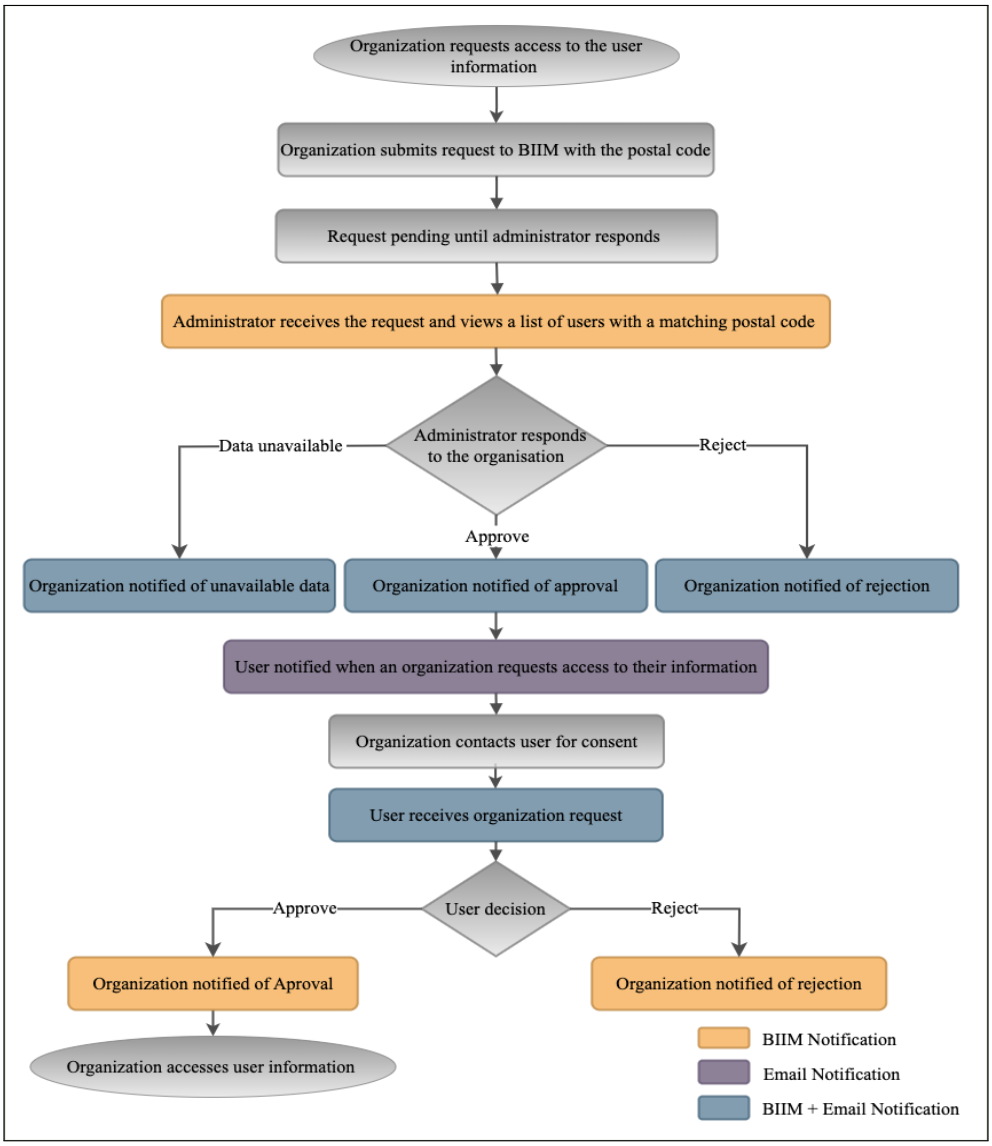


Figure 6.21 : Overview of the OD System Notifications

6.6.1 OD System

BIIM enhances organizational efficiency by enabling access to user information. In the operational context of the organization account, notifications are generated in response to various activities such as registration, logging and updating profiles, or changing passwords, as demonstrated in the UD system.

- The organization is not responsible for managing any user identities.
- The organization has a postal code to initiate a request.
- The organization only grants access to user information upon receiving user permission.

The OD system process includes several sequential steps that aim to facilitate data sharing while protecting privacy protocols, as illustrated in Figure 6.22. The organization initiates the procedure by submitting a request to BIIM, specifying the user's postal code as a reference point, as shown in Figure 6.23, and the request remains pending until the administrator responds, as shown in Figure 6.24. The administrator receives the request, as illustrated in Figure 6.25, and all users with the same postal code are listed. The administrator is tasked with responding to the request and sharing that a user or multiple users have the same postal code, with potential actions including approval, notification of data unavailability, or rejection, as illustrated in Figure 6.26.

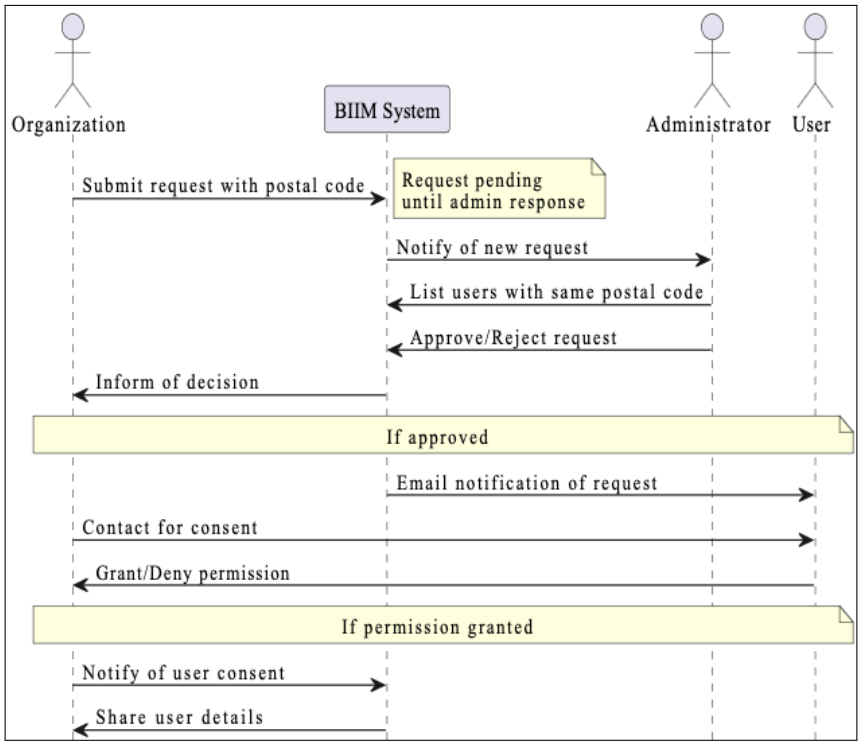


Figure 6.22 : Organization Requests Access User Information

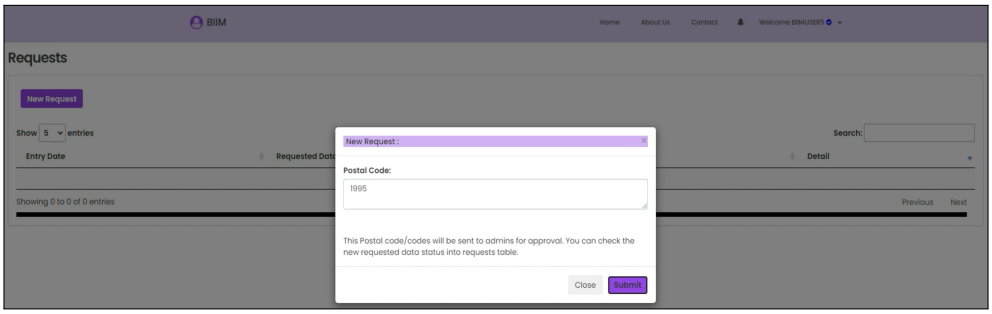


Figure 6.23 : Organization Enters Postal Code for New Request

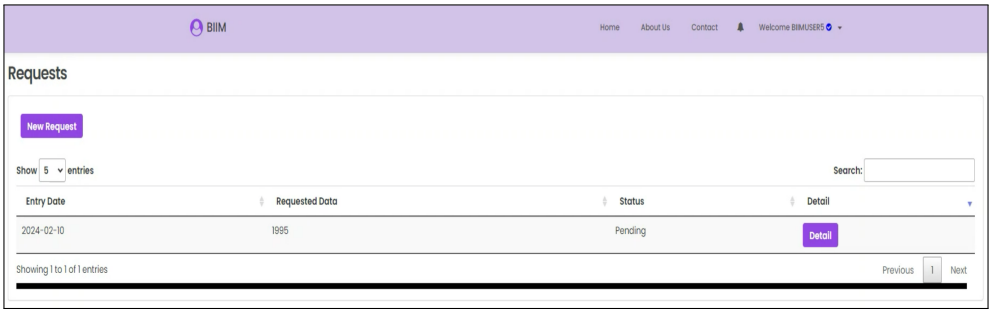


Figure 6.24 : Organization's Request Pending/ Awaiting Admin Action

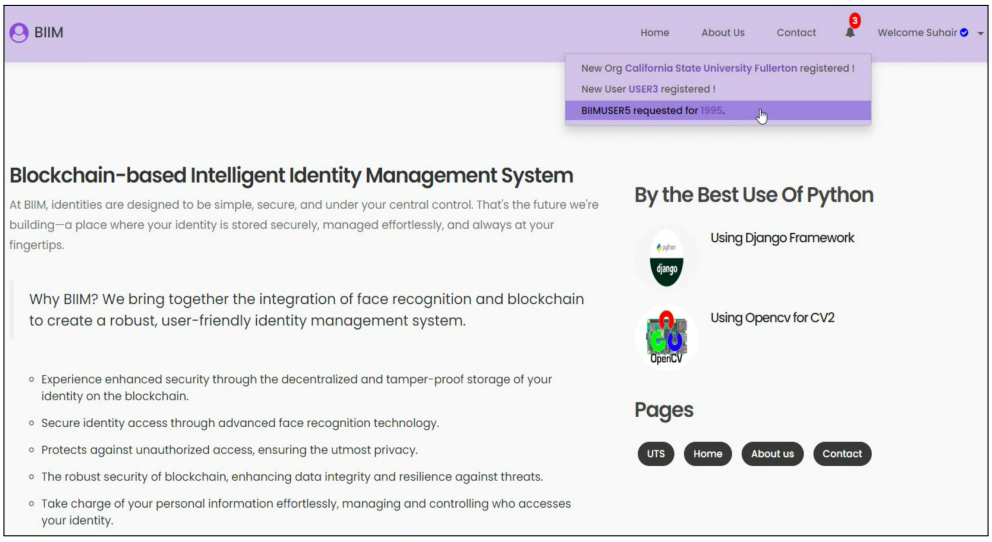


Figure 6.25 : Admin Receives Organization Request

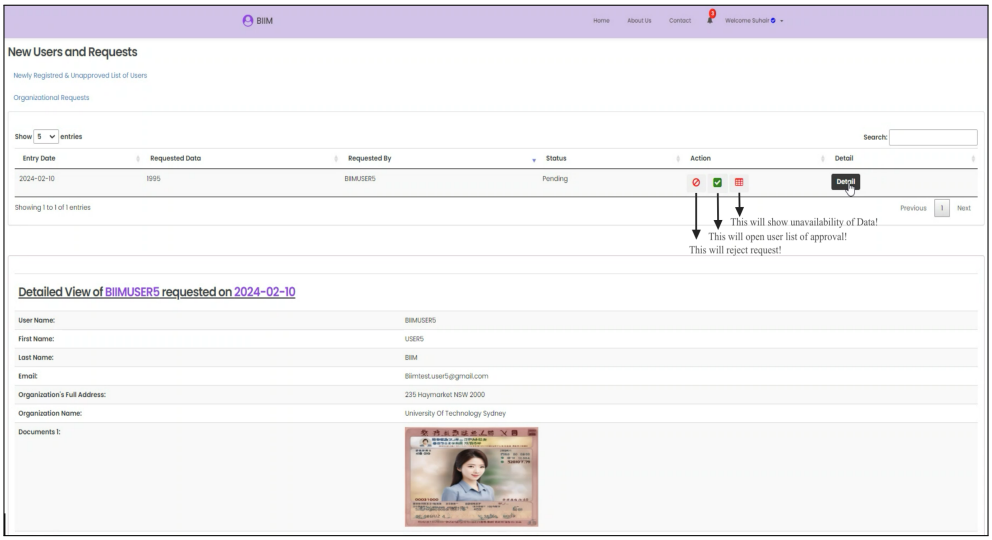


Figure 6.26 : Admin Views Organization Details and Take Action

The administrative decision and notification workflow are governed by Algorithm 13, which formalizes how the system automates approval, rejection, and data unavailability notifications to both the organization and the concerned users. If the request is approved, as illustrated in Figures 6.27, 6.28 and 6.29, the organization is promptly informed, as shown in Figure 6.30, concomitant with sending an email to the user revealing the identity of the requesting organization, as shown in Figure 6.31.

Algorithm 13 Submit Admin Response to Organization Request Procedure

procedure SUBMITADMINRESPONSE(***request***)
    upr_id ← **extract from** *request*
    user_act ← **extract from** *request*
    Retrieve ***userPostReqRecord*** using ***upr_id***
    Update ***userPostReqRecord.action_date*** and ***user_act***
    if user_act = 2 then
        Send *'Request rejected'* email
    else if user_act = 1 then
        Send *'Request approved'* email
    else if user_act = 0 then
        Send *'Request data unavailable'* email
    end if
    return Success response
end procedure

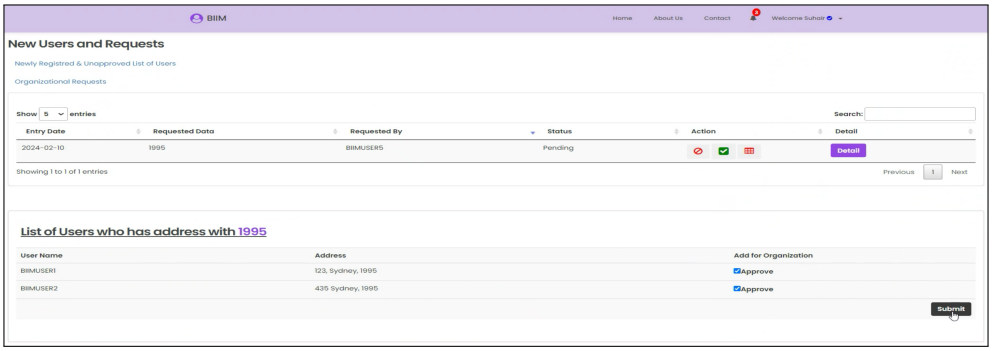


Figure 6.27 : Admin Approves Organization Request

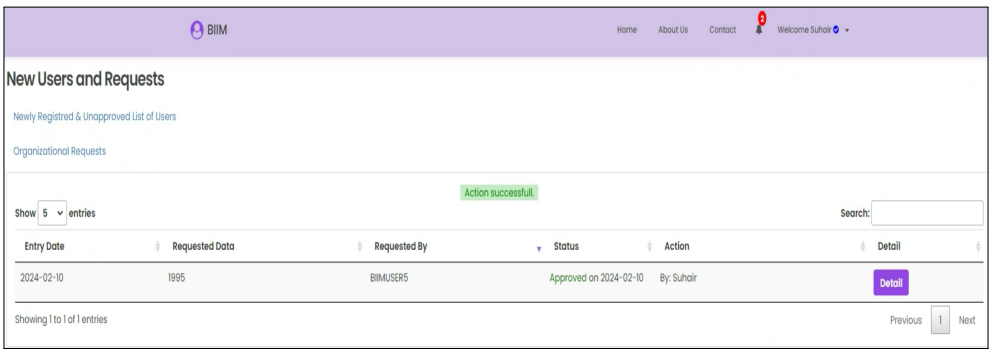


Figure 6.28 : Admin Approves Organization Request- action

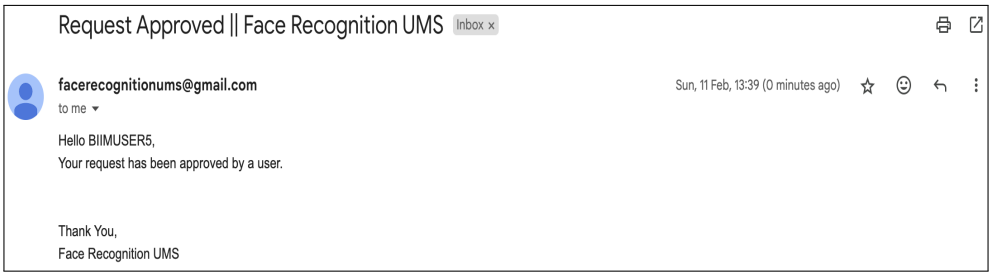


Figure 6.29 : Notification of User Approved Organization Request

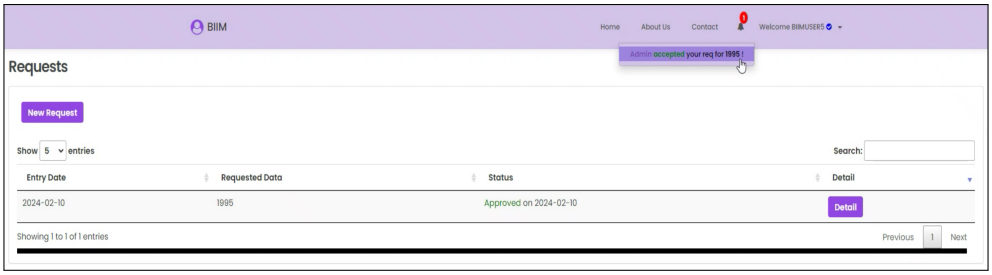


Figure 6.30 : Organization Receives Notification After Admin Approval

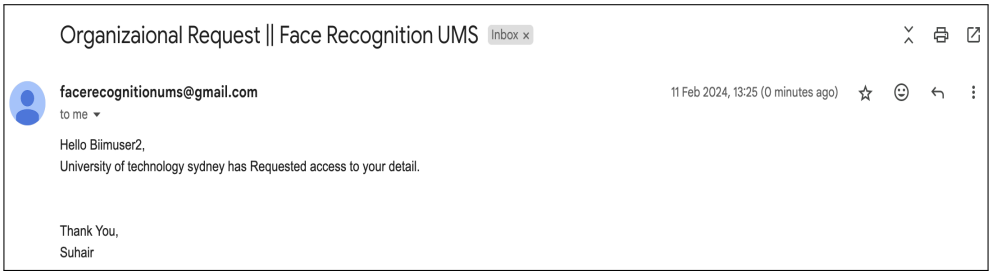


Figure 6.31 : User Receives Notification After Admin Approval

The organization receives a complete list of approved users and directly contacts the designated user, as illustrated in Figure 6.32. This request notifies the user, as shown in Figure 6.33, and requests the user's consent to access the information, as shown in Figure 6.34. The primary logic for this process is articulated through Algorithm 14, which coordinates the automated notification of users upon receipt of organizational access requests. This user-centric approach ensures that people maintain ownership of their personal data.

Algorithm 14 User Notification with Organization Request Procedure

procedure USERNOTIFWITHORGREQST(request)
    Extract user IDs from the request
    Retrieve administrative and organizational details
    if user IDs exist **then**
        for each user ID **do**
            Create Userpostreq entry for each usr_id
            Send notification email to usr_id based on request data
        end for
    end if
    return Success response
end procedure

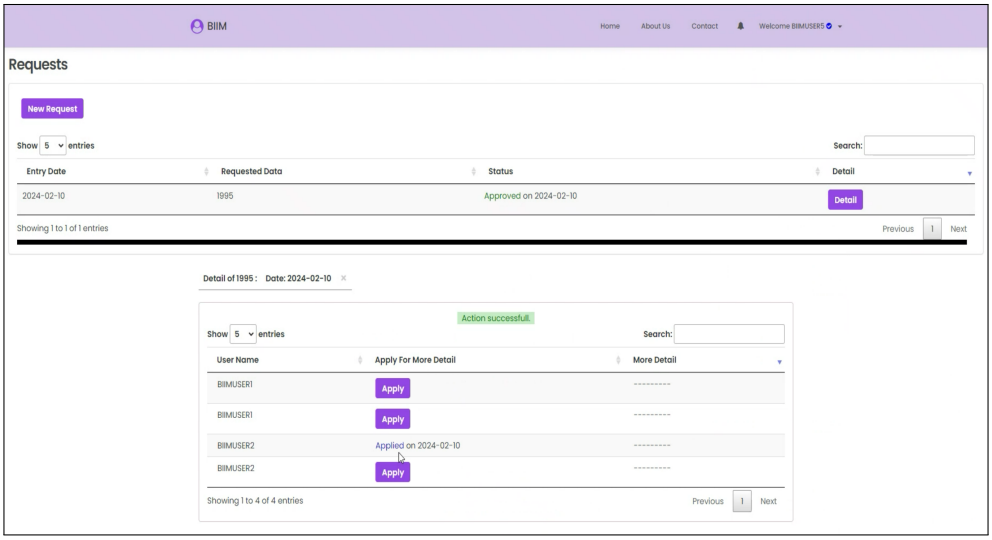


Figure 6.32 : Organization Sends a Request to the User

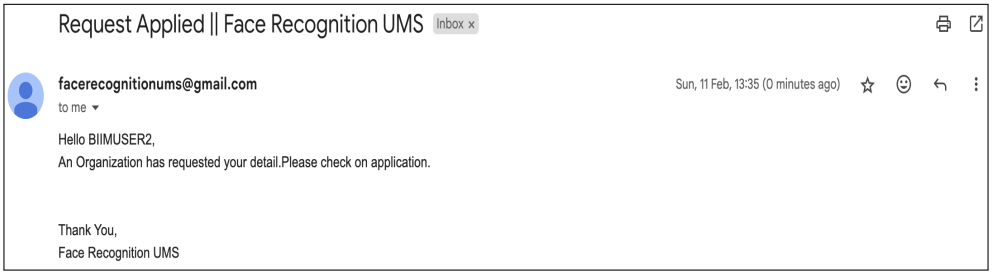


Figure 6.33 : Notification with Organization Request

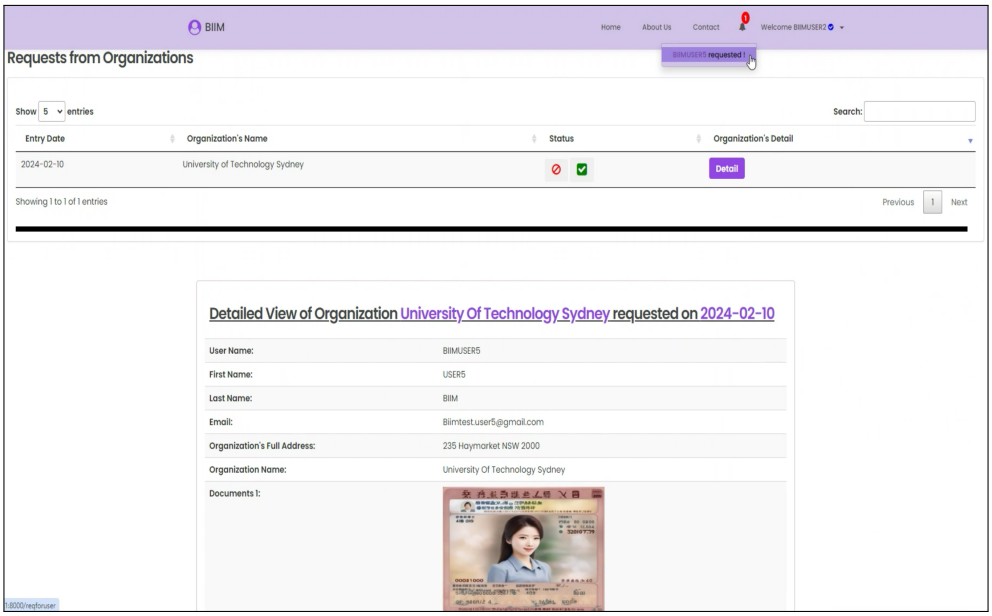


Figure 6.34 : User Receives Organization Request

The user has the discretion to grant or deny permission. If the user rejects the organization's access request, as demonstrated in Figures 6.35 and 6.36, the organization is notified and the request status is updated, as illustrated in Figures 6.37 and 6.38. In contrast, if the user approves the organization's access request, as illustrated in Figure 6.39, the organization is alerted and pertinent user details are shared, as illustrated in Figure 6.40. This facilitates the access of information within the confines of an established privacy framework, as illustrated in Figure 6.41.

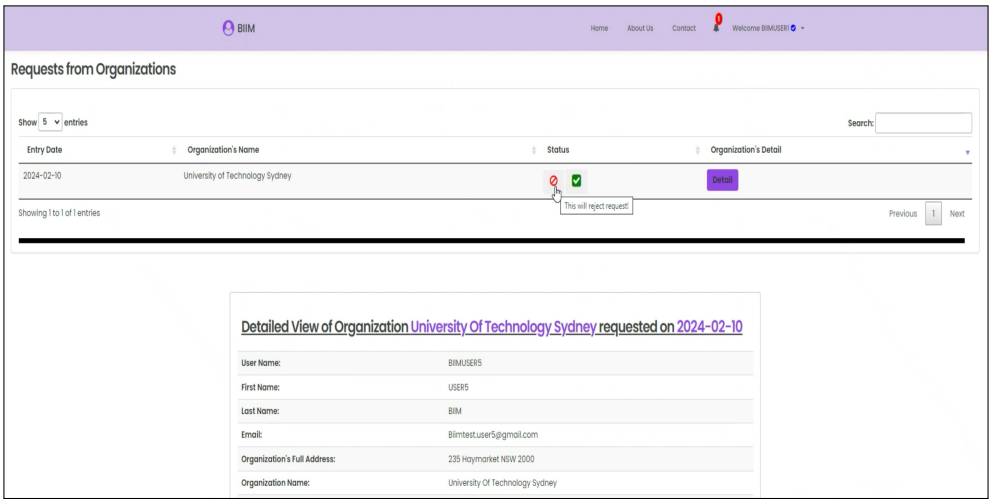


Figure 6.35 : User Rejects Access to Information After Checking Organizational Details

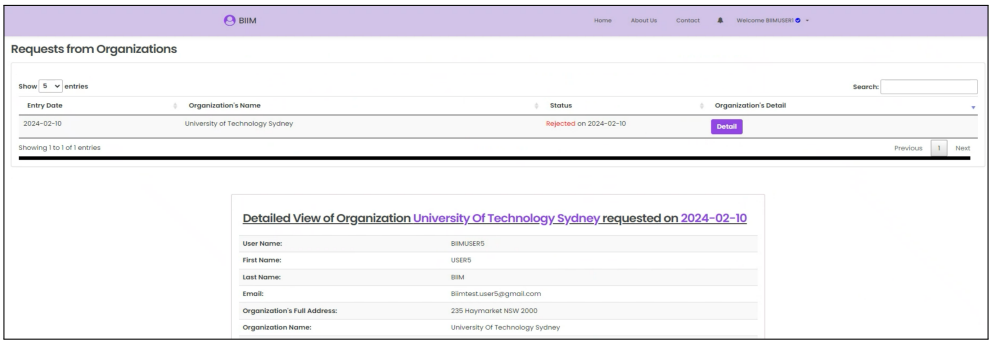


Figure 6.36 : User Rejects Organization Request

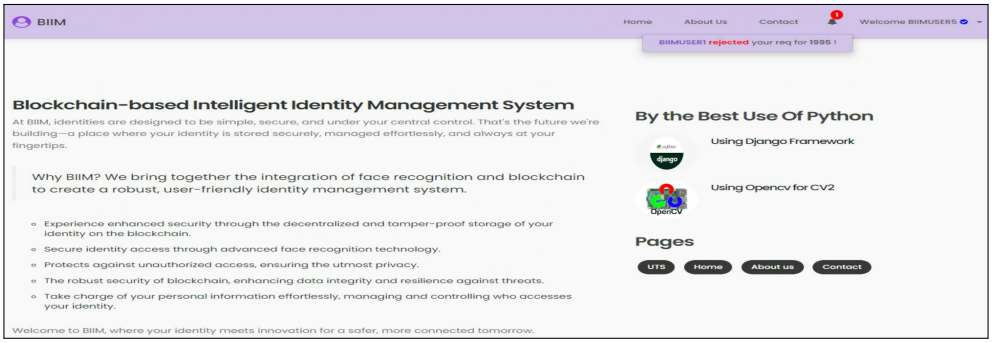


Figure 6.37 : Organization Receives Alert with User Rejection

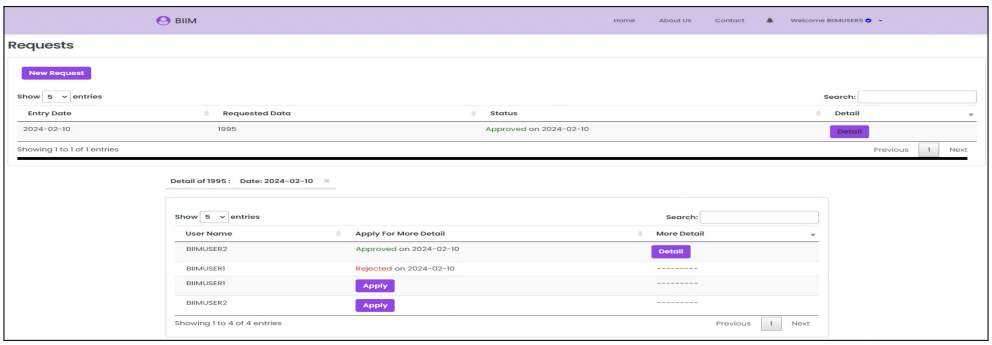


Figure 6.38 : Organization Checks the Requests and Stats

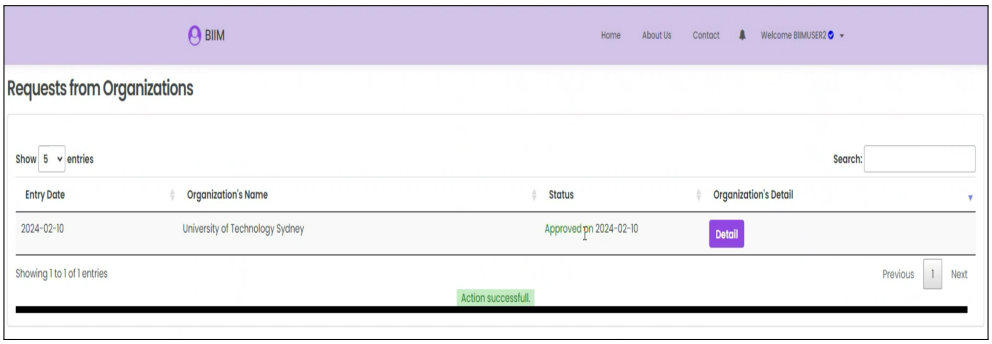


Figure 6.39 : User Approves Access to the Information

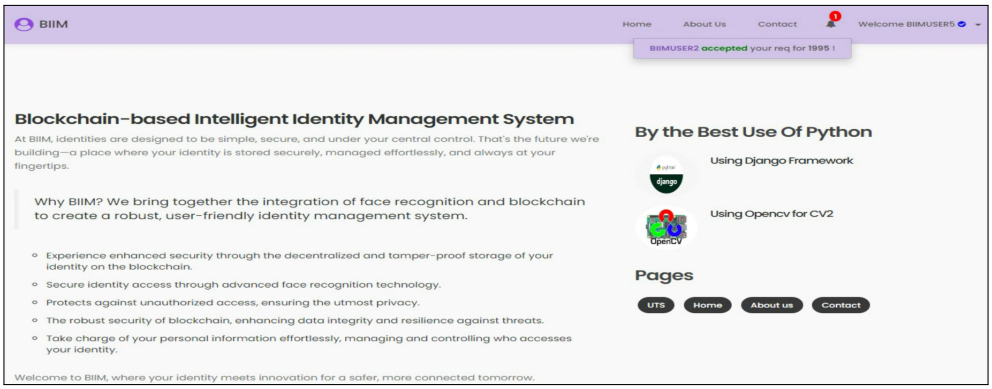


Figure 6.40 : Organization Receives Alert with User Action

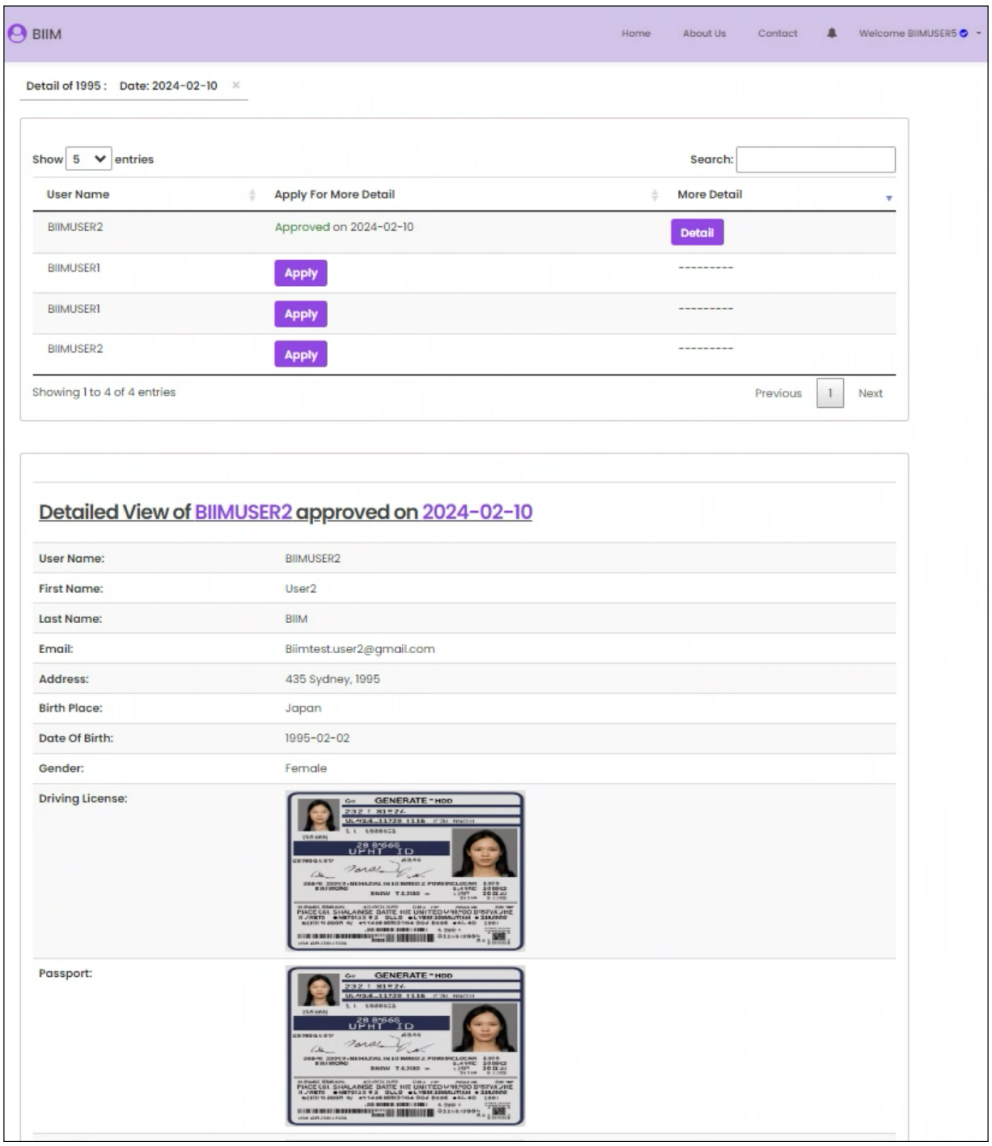


Figure 6.41 : Organization Views User Information

6.7 Implementation

This section presents a detailed overview of the UDOD system's development and integration within the BBIM framework. The UDOD notification subsystem is implemented using the foundational infrastructure, design strategy, and core technologies of the BIIM system described in Chapter 5, Section 5.5. Chapter 6 expands on these foundations by focusing specifically on the notification mechanisms, emphasizing how the algorithms and processes related to user-driven (UD) and organization-driven (OD) notifications operate within the system.

The UDOD subsystem is designed to support real-time notification delivery for critical system and user-related events, including but not limited to user registration, biometric data updates, password changes, and organizational access requests. It employs event-driven mechanisms to trigger notifications and leverages Django's asynchronous capabilities to ensure timely and reliable message dissemination.

Furthermore, the UDOD system enables all notification events to be recorded in a verifiable and fully auditable manner. This design choice ensures transparency, accountability, and trust in user–organization interactions. The implementation illustrates how the UDOD subsystem integrates with the BBIM architecture, empowering users with full control and visibility over their data-related activities. Including these implementation details is essential to demonstrate the practical applicability of the proposed system and to highlight its contributions to privacy-aware decentralized identity management.

6.8 Evaluation of the UDOD System

This section presents a comprehensive evaluation of the UDOD subsystem, focusing on its computational performance, scalability, and functional behavior under realistic operational conditions. The evaluation combines algorithmic analysis, experimental performance testing, and scenario-based validation to assess how effectively the subsystem achieves its design objectives within the BIIM framework.

The analysis emphasizes scalability, efficiency, and user transparency—core attributes

that define the subsystem's ability to deliver privacy-aware and event-driven notifications. Through experimental evaluation, the UDOD subsystem was subjected to a range of user interaction simulations, measuring performance metrics such as SQL transaction time, blockchain commit latency, and overall notification delivery time. These experiments provide empirical insights into how the system performs as user load increases, highlighting its ability to sustain consistent responsiveness and low-latency operation across diverse conditions.

The UDOD notification subsystem functions as a critical component of the BIIM framework, responsible for issuing real-time alerts, processing user access approvals, and ensuring transparency in organizational access requests. Its evaluation places particular emphasis on notification performance, user response handling, and blockchain logging efficiency—all essential for maintaining trust, accountability, and auditability in decentralized identity management.

6.8.1 Evaluation Methodology

The evaluation of the UDOD subsystem adopts a system-driven and experimental approach to verify its functional accuracy and performance efficiency. Considering the subsystem's architecture and objectives, the evaluation focuses on the user consent, event auditing, and blockchain-based notification processing. The system performs as intended, demonstrating stable latency and reliable scalability under varying user and organizational loads. These evaluation methods provide a concise, comprehensive basis for assessing UDOD's performance, transparency, and operational readiness within the BIIM framework.

6.8.2 UDOD Performance Evaluation

The evaluation was conducted by simulating multiple user interactions that triggered notification events, both initiated by users (e.g., profile updates) and by organizations (e.g., access requests to user identities). The UDOD subsystem was tested across multiple user and organization scenarios to evaluate its scalability and performance as usage increased.

A total of seven test groups were used, ranging from 10 to 10,000 users. The system

performance was evaluated based on the following key metrics:

- SQL Time (s): Time required to log notification metadata into MySQL.
- Blockchain Commit Time (s): Time required to store the hashed metadata in BigchainDB in a tamper-evident manner.
- Notification Trigger Time (s): Time required to send an email alert via SMTP.
- Total Time per Event (s): End-to-end latency per notification event.

User Count	Avg SQL Time (s)	Avg Blockchain Time (s)	Email Notification Time (s)	Total Time/ Event (s)
10	0.010	0.340	0.200	0.550
50	0.011	0.344	0.198	0.553
100	0.011	0.338	0.202	0.551
500	0.012	0.345	0.199	0.556
1,000	0.011	0.349	0.197	0.557
5,000	0.011	0.340	0.196	0.547
10,000	0.010	0.339	0.194	0.543

Table 6.1 : Performance Metrics for UDOD Notification Events

The evaluation results of the UDOD subsystem demonstrate its ability to handle real-time notification events with consistent and low-latency performance, even at large scale. Across all user loads, ranging from 10 to 10,000 users, the total processing time per event remained under 0.6 seconds, indicating strong scalability and responsiveness.

A key observation is the stability of both SQL and email notification times, which showed minimal fluctuation as user counts increased. The SQL time remained between 0.010– 0.012 seconds per event, confirming that the InnoDB storage engine efficiently manages transactional metadata under varying load conditions. Similarly, email notification

time, averaging approximately 0.2 seconds, confirms that the SMTP integration is well optimized for asynchronous message delivery.

The most notable performance aspect lies in the blockchain commit time, handled through BigchainDB. The average time of approximately 0.34 seconds to store a hashed record of each notification remained consistent across all user loads. This consistency ensures that even for large-scale deployments (e.g., 10,000 users), the blockchain layer does not introduce prohibitive latency under experimental conditions—an essential requirement for systems that depend on tamper-evident audit trails and real-time responsiveness.

Furthermore, total processing time per event exhibited a slight improvement as the user count increased due to caching and batching optimizations within the asynchronous processing layer. For instance, at 10 users, each event required approximately 0.550 seconds, while at 10,000 users, the time decreased to approximately 0.543 seconds. This observation indicates linear scaling behavior under experimental conditions.

6.8.3 UDOD Algorithm Complexity Analysis

This section analyzes the computational complexity of the key notification and response operations within the UDOD subsystem. Table 6.3 summarizes the complexity and operational characteristics of Algorithms 9- 14 associated with notification and organizational processes.

Algorithm	Complexity	Discussion
Notification of Login Process	$\mathcal{O}(1)$	A simple event-based trigger that does not depend on system size.
Notification of Update Profile Process	$\mathcal{O}(1)$	A database update event, requiring only constant time to execute.
Notification of Change Password Process	$\mathcal{O}(1)$	Sends a confirmation or alert after a password change. Efficient event-based operation.
Submit Admin Response to Organization Request	$\mathcal{O}(1)$	Admin validation and approval are constant-time operations since they involve a lookup and status update.
User Notification with Organization Request	$\mathcal{O}(1)$	Notifies users when an organization requests access to their identity, which is a simple event-driven function.

Table 6.3 : UDOD Algorithm Complexity Analysis

As shown in Table 6.3, the core event-handling logic of the listed algorithms exhibits constant-time behavior $\mathcal{O}(1)$, under operating conditions. These operations, such as login notifications, profile updates, and administrative requests, are event-driven and designed to be independent of system size, providing consistent performance under varying user loads. The constant-time behavior is achieved through the system's event-driven architecture and the use of indexed data access mechanisms. Each notification and administrative action is executed as a single-step event trigger that performs minimal computation and bounded database lookup. The design avoids iterative loops, recursive traversal, or size-dependent searches in the core logic, contributing to stable processing behavior as the number of users and records increases. Furthermore, state updates and message dispatches are implemented as atomic operations, reducing the risk of performance degradation under high load. This architectural approach ensures that the UDOD subsystem maintains predictable and scalable behavior in high-throughput environments, aligning with the design goals of responsiveness and transparency in user consent management.

6.8.4 Functional Validation via Scenario-Based Testing

This scenario validates the UDOD system's implementation by demonstrating the successful execution of notification, consent, and transparency operations within an identity management environment. It further establishes the subsystem's ability to provide real-time awareness and fine-grained control, aligning with privacy-by-design objectives in real-world institutional identity ecosystems.

As presented in Chapter 5, Section 5.8, the scenario involves Bob interacting with the BIIM platform and continuously receiving system-generated alerts through the UDOD subsystem. The overall notification architecture supporting this process is depicted in Figure 6.3, while the registration notification flow is shown in Figure 6.5. During Bob's registration, the system generates OTP notifications, as visualized in Figures 6.6 and 6.7, governed by the notification handling logic defined in Algorithm 9. These notifications establish transparency during the identity creation process. Following registration, Bob's authentication activities are monitored by the UDOD subsystem, which generates real-time login alerts via Algorithm 10. These alerts inform Bob of successful and failed login attempts, reinforcing situational awareness and early detection of unauthorized activity. The scenario further validates notification transparency during profile and credential management operations. When Bob updates personal profile information, the system triggers real-time alerts as per Algorithm 11. Similarly, when Bob changes or resets his password, corresponding alerts are generated following Algorithm 12. These mechanisms demonstrate continuous monitoring and immutable logging of sensitive identity-related operations.

The scenario also highlights organization-driven notification behavior when an external institutional organization (e.g., a university) submits a request to access Bob's identity information. The initiation of this request is illustrated in Figures 6.22, 6.23, and 6.24, while administrative review and decision-making actions are presented in Figures 6.25 and 6.26. The automated decision and notification generation for these actions are governed by Algorithm 13. Once approved, the system issues synchronized notifications to

both the organization and Bob, as shown in Figures 6.29, 6.30 and 6.31. The user-consent phase is validated when Bob receives direct access requests from the university, as illustrated in Figures 6.32, 6.33 and 6.34, where the request notification logic is managed by Algorithm 14. Bob's explicit consent decisions are validated through rejection flows, as depicted in Figures 6.35 and 6.36 and approval flows, as visualized in Figure 6.39. Corresponding organization-side alerts are provided in Figures 6.37, 6.38, 6.40 and 6.41. These interactions confirm that the UDOD subsystem successfully enforces user-centric data governance, enabling Bob to control when and how his personal identity data are shared with institutional service providers.

This scenario confirms that the UDOD system satisfies both functional and non-functional requirements by demonstrating secure notification delivery, transparent user awareness, and consent-driven data exchange. The results validate the subsystem's suitability for scalable deployment in privacy-sensitive, multi-institutional identity management environments.

6.9 Discussion

The findings presented in this chapter confirm that the UDOD subsystem effectively addresses the key limitations identified in Chapter 2, particularly the absence of a decentralized or privacy-aware notification mechanism in identity management frameworks. Existing solutions rely heavily on conventional notification infrastructures—such as Firebase Cloud Messaging (FCM) [39], Apple Push Notification Service (APNs) [10], Amazon Simple Notification Service (SNS) [9], and webhook-based event systems [38]. Although these technologies are effective for general application notifications, they do not provide transparent, user-controlled, or tamper-resistant visibility into identity data-access events. These systems typically operate through centralized intermediaries and do not guarantee end-to-end auditability. In contrast, UDOD introduces a blockchain-enabled, event-driven architecture that supports real-time awareness of identity data-access events while maintaining scalability and computational efficiency.

From a theoretical standpoint, UDOD demonstrates that blockchain can serve as a tamper-evident and transparent trust layer for verifying identity-related activities. By integrating distributed ledger technology with application-level validation logic, the subsystem reduces reliance on centralized intermediaries and enables cryptographically verifiable audit trails. Each access event and corresponding notification is permanently recorded on-chain, ensuring traceability and accountability. This architecture transforms identity management from a static authentication model into a consent-oriented governance framework in which users maintain active oversight over data utilization.

Technically, UDOD's contribution lies in its intelligent event-driven design and algorithmic implementation. The set of Algorithms 9, 10, 11, 12, 13, and 14 ensures that all access events are captured, validated, and recorded across blockchain and database layers with low and predictable processing overhead, exhibiting $\mathcal{O}(1)$ algorithmic complexity for the core event-handling operations. Empirical evaluation confirmed that average processing times remained below 0.6 s across all test groups, comprising 0.01 s for SQL logging, 0.34 s for blockchain commits, and 0.2 s for email notifications. These results demonstrate that the subsystem achieves real-time responsiveness and high operational stability without imposing significant computational overhead.

Architecturally, the UDOD combines two coordinated subsystems: user-Driven and organization-Driven, which enable a balanced approach to managing access events. The UD mechanism governs user-initiated actions, granting individuals the ability to authorize, reject, or monitor identity access requests. The OD mechanism governs organization-initiated events, ensuring that no identity data is disclosed without explicit user consent. This cooperative structure embeds privacy, consent, and accountability directly into the system's operational logic. By encoding these principles into smart contracts, UDOD enforces transparent and verifiable access control across all transactions, operationalizing user-centric governance at the architectural level.

Compared with conventional frameworks, UDOD decentralizes both validation and message dissemination through its integration with BigchainDB. Each notification is hashed

and recorded on-chain in a tamper-evident manner, ensuring integrity and resistance to unauthorized modification. This approach enables proactive, context-aware alerts that empower users to respond before unauthorized access occurs. The result is a transition from reactive data protection to a truly preventive, *privacy-by-design* paradigm—embedding trust, transparency, and accountability within the technical infrastructure itself.

Performance analysis further confirmed that UDOD maintains high efficiency and scalability under varying operational loads. Its optimized notification classification and lightweight encryption minimize latency while preserving full verifiability and data integrity. The approximately linear scalability under experimental conditions between blockchain and database layers validates the practicality of deploying real-time blockchain-based notification systems in production-scale identity environments.

Within the BIIM architecture, UDOD functions as a complementary subsystem to BBIM and FIM. While BBIM ensures biometric authenticity and FIM facilitates cross-domain interoperability, UDOD adds an essential layer of real-time awareness and accountability. These three components create a cohesive, blockchain-enabled identity management system that integrates authentication, federation, and privacy into a unified operational system.

The UDOD subsystem advances decentralized identity management both conceptually and technically. It confirms that blockchain can support scalable, real-time notification mechanisms while promoting a transparent and consent-based system of user governance.

6.10 Conclusion

This chapter highlighted the significance of intelligent, privacy-aware mechanisms for the protection of sensitive identity data. By integrating blockchain and artificial intelligence technologies, the proposed approach enhances user control, transparency, and accountability within the identity management process. The discussion of the UDOD subsystem demonstrated how real-time notifications and structured request–approval workflows contribute to improved visibility and governance of identity-related activities within

the BIIM framework.

The next chapter examines the concept of federated identity and its role in strengthening the overall system architecture. It explores how trusted entities can collaborate to enhance user control, interoperability, and authentication across multiple platforms and organizational domains.

Chapter 7

Federated Identity Management System (FIM)

7.1 Introduction

Over the past few years, digitization has redefined the way information is accessed and organized, leading to an increasing demand for secure and accurate identity management [61]. Traditional identity management systems were developed in a centralized form where one server or central authority authenticates and verifies the real-time user's identities [37]. However, as the process revolves around a central authority, this approach has several problems [81]. To overcome these issues, more sophisticated solutions have been developed. Federated Identity Management System (FIM) constitutes an efficient system for managing multiple digital identities of an individual across different domains within a trusted framework.

Integrating blockchain with FIM offers features such as linearity, scalability, decentralization, time-stamping, identity federation schema support and security features including availability, integrity and privacy [86]. By federated identity schema, we refer to the structured relationship between all digital identities belonging to a single entity across multiple domains, allowing those identities to interoperate securely within a unified trust framework. Ethereum's linearity ensures that the operational steps are executed in their arranged order, preventing any from being skipped. It can also be useful for developing the federation schema. A multi-federation schema ensures that several independent providers have authenticated a given account, which contains enough information to cover the essential certification process steps and can therefore be reused for subsequent applications until it expires [54].

The scientific contribution of the FIM subsystem is situated in the conceptualization

design and implementation of Algorithms 15, 16, 17 and 18 that embed the FIM subsystem within the BIIM framework. The subsystem employs Ethereum and smart contract infrastructures to consolidate multiple virtual identities into a single verifiable identity, securely maintained within a user-controlled digital wallet. Systematic evaluation of the FIM has examined scalability, computational overhead, gas expenditure, and execution time, with results confirming its reliability, efficiency, and applicability in real-world contexts. The social contribution of the FIM subsystem lies in its capacity to unify virtual identities, map them consistently to real-world referents, and ensure their preservation, thereby mitigating fragmentation, reducing security vulnerabilities, and enhancing the usability, transparency, and trustworthiness of digital identity ecosystems. Within the BIIM architecture, the role of the FIM subsystem is situated in its federative functionality and its coherent integration with the BBIM and UDOD subsystems. These subsystems contribute to a comprehensive, user-centric framework for digital identity management.

In the previous chapter, we examined the taxonomy of notifications within the BIIM framework and explored the implementation and operation of the UDOD system. This chapter focuses on the workings of the FIM system, with particular emphasis on its integration with blockchain technology. This integration provides a robust solution to identity verification challenges, ensuring data integrity, security, and privacy. This chapter builds on the architectural foundations of BIIM to present the design, implementation, and evaluation of its federated identity management system. The structure of this chapter is as follows: Section 7.2 introduces the overall system architecture, providing the foundation for subsequent analysis. Section 7.3 examines the working mechanisms of the FIM system. Section 7.4 details the algorithms for achieving the capabilities of the FIM system. Section 7.5 presents the implementation details, and Section 7.6 discusses the evaluation results. Section 7.7 offers a critical discussion of the findings, and finally, Section 7.8 summarizes the key points and concludes the chapter.

7.2 FIM System Architecture

Figure 7.1 illustrates the architecture of the FIM subsystem, which leverages blockchain technology to enable secure, decentralized, and interoperable identity federation across domains. The design follows a three-layer Model–View–Controller (MVC) paradigm comprising the *view*, *control*, and *model* layers. Each layer operates autonomously and cooperatively, ensuring modular functionality, structural maintainability, and scalable performance across distributed environments.

The view layer functions as the user interaction interface, enabling access, visualization, and management of federated identities through an intuitive front end. It abstracts complex blockchain processes, delivering a consistent and efficient operational interface for identity retrieval, cross-domain authentication, and credential monitoring. This design not only enhances usability but also advances the system's objective of maintaining user control and transparency in decentralized environments.

The control layer serves as the logical and operational core of the architecture. It orchestrates identity-related processes, including the *Read UID Process*, *Add Identity Process*, *Open URL Process*, and *Delete Identity Process*, as presented in Figure 7.1. Acting as the intermediary between the view and model layers, it validates user operations, routes identity transactions, and enforces compliance with the smart contract logic encoded on the blockchain. By maintaining these validation flows, the control layer ensures integrity, consistency, and policy adherence within federated identity operations. Although it introduces coordination complexity, this layer substantially enhances interoperability and trust among multiple identity providers.

The model layer, also referred to as the storage layer, establishes the blockchain-based data management foundation of the FIM subsystem. It integrates a secure off-chain database with an immutable blockchain ledger to balance performance efficiency and cryptographic assurance. Encrypted identity credentials are maintained within user-controlled digital wallets stored off-chain, while the blockchain immutably records cryptographic proofs of key federated operations such as identity creation, consolidation, and revocation.

The FIM system integrates the PoW consensus algorithm to authenticate and append identity-related transactions onto the blockchain. This ensures that all federated identity operations are validated through a transparent, tamper-resistant, and auditable process, maintaining system integrity without exposing sensitive identity data. This design provides a robust foundation for scalable, trustless, and privacy-preserving identity management within the federated system.

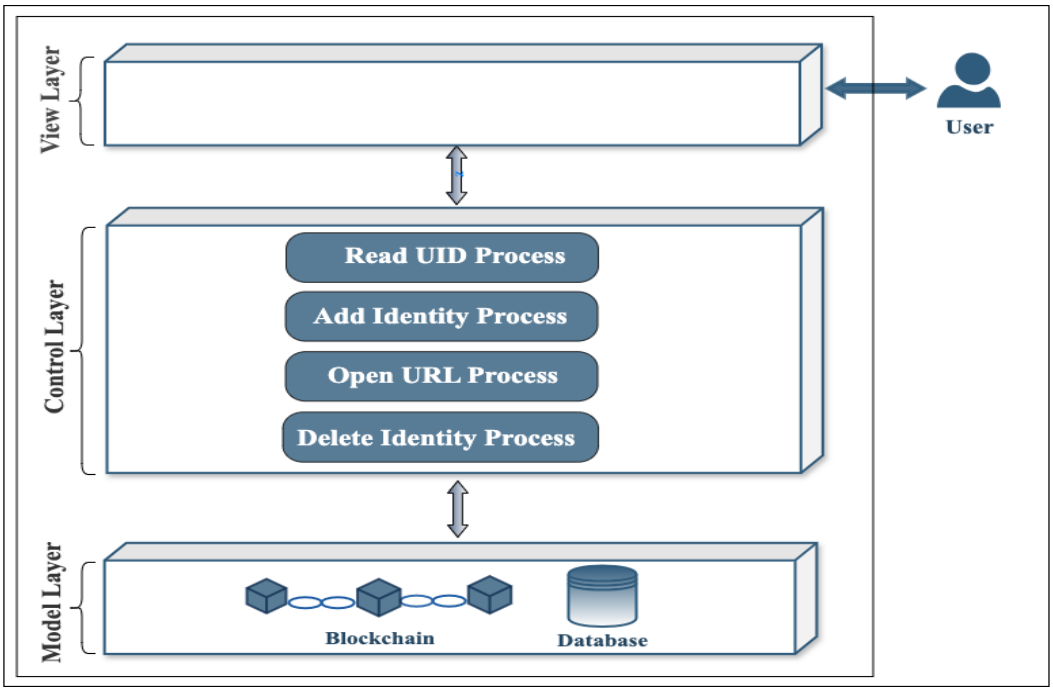


Figure 7.1 : FIM System Architecture

The FIM architecture advances the BIIM framework from isolated biometric verification to a decentralized, federated model of identity governance. By embedding trust directly into its architectural core through smart contracts and consensus mechanisms, the FIM subsystem eliminates reliance on centralized authorities while reinforcing transparency and user sovereignty. Consequently, it operates as a cohesive and interoperable layer that complements the BBIM and UDOD components, collectively enabling secure, scalable, and privacy-preserving identity management systems.

7.3 The Working of the FIM System

As outlined in Chapter 3, the FIM system is a core component of the BIIM architecture. In this thesis, the terms *FIM system* and *FIM subsystem* are used interchangeably to denote the federated identity management capability within BIIM.

Figure 7.2 presents the workflow of the FIM system, offering a structured overview of the authentication and identity federation process from the end-user's perspective. The operational workflow can be summarized as follows. BIIM directs the user to the FIM system interface, which facilitates a connection to the blockchain layer. Through this interface, users are able to execute four primary identity management functions:

- **Reading wallet data:** retrieve and view existing federated identities.
- **Adding a new identity:** append new credentials to the identity wallet.
- **Deleting identity:** remove a federated identity while preserving historical records.
- **Opening a linked URL:** launch a service or application associated with an identity.

Each of these activities is supported by the model layer. For instance, when a new identity is added, the provided credentials are verified, and a token is generated. The transaction is then recorded within a block, validated through a consensus mechanism, and appended to the blockchain. Once confirmed, the block is replicated across all network nodes, ensuring transparency and immutability. Conversely, deleting a federated identity does not alter the user's primary identity; it simply removes the associated federated link. As with identity additions, this operation is immutably recorded on the blockchain. Wallet data consolidates all federated identities, their corresponding tokens, and supporting metadata, enabling users to verify the status of their federated identity at any given time.

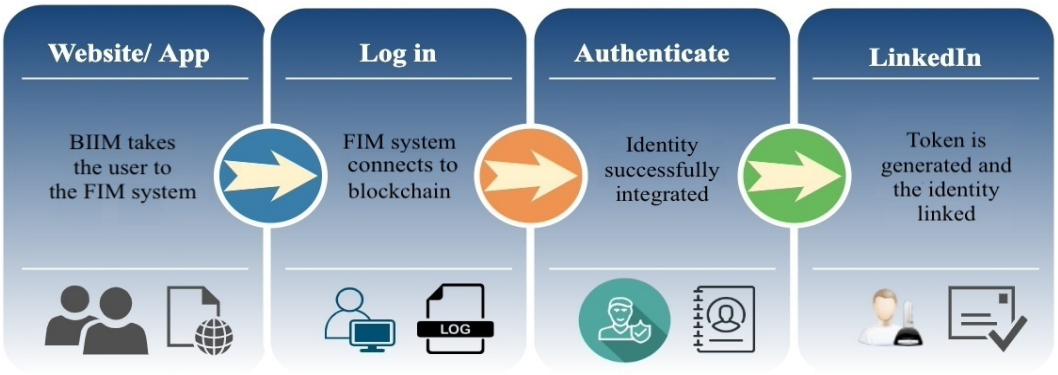


Figure 7.2 : Federated Identity System

Workflow Overview

Figure 7.3 and Figure 7.4 illustrate the operational flow of the FIM system within the BIIM framework. These diagrams delineate the lifecycle of FIM identity operations, encompassing user interaction, interface logic, blockchain execution, and identity wallet updates. Each operation is executed via dedicated smart contract functions on the Ethereum blockchain, ensuring that all interactions are transparent, auditable, and tamper-proof.

Figure 7.3 presents the *contract-level execution flow*, detailing how the application interacts with deployed smart contracts to perform read, write, and delete operations. The diagram captures blockchain confirmations, transaction receipts, and data integrity steps.

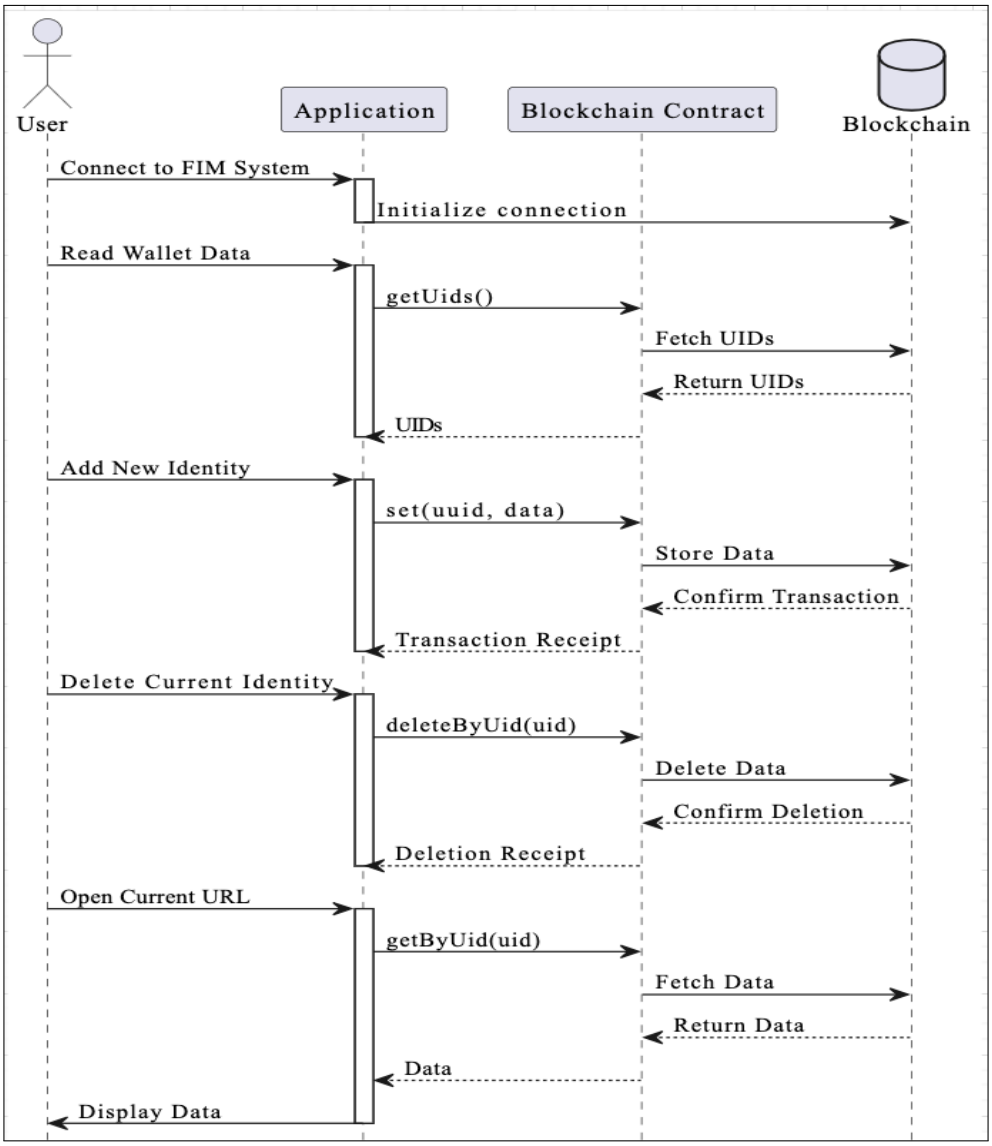


Figure 7.3 : Federated Identity Management System Using Blockchain Technology

Figure 7.4 focuses on the *system-level process flow*, from the user's perspective. It illustrates how the user interface, blockchain network, and identity wallet coordinate to facilitate a coherent and reliable execution of identity lifecycle operations. This higher-level abstraction underscores system usability and highlights the FIM system's interoperability across other systems.

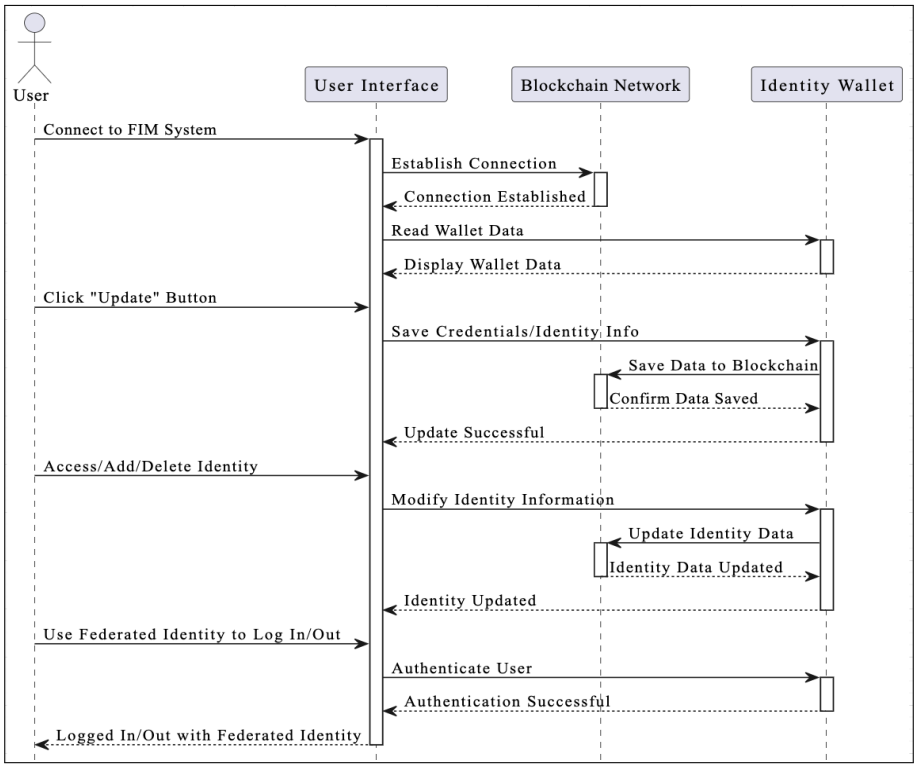


Figure 7.4 : Federated Identity Management Process

Figures 7.3 and 7.4 demonstrate that the FIM system provides a secure and functionally integrated federated identity solution. The smart contract logic and user interface are aligned to support decentralized, real-world identity operations such as reading wallet data, adding or deleting identities, and accessing the linked URL.

7.4 Algorithmic Working of the FIM System

This section presents the algorithmic working of the FIM system and illustrates how the key activities and processes are executed using the system.

Connect to the Blockchain

This fundamental step enables the user to establish a secure connection to the blockchain network via the FIM interface. Once connected, the system ensures a secure link, allowing all subsequent actions to be performed. This process is demonstrated in Figure 7.5.

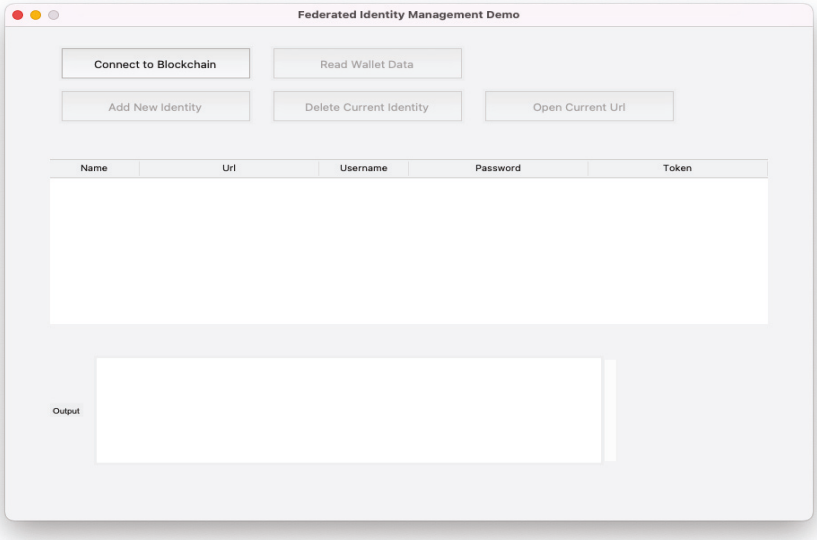


Figure 7.5 : Connect to Blockchain

7.4.1 *Read Wallet Data*

This feature enables the system to retrieve and read data from the user's identity wallet. Once connected to the blockchain network, the system accesses the identity wallet to retrieve the user's encrypted credentials and identity information. Algorithm 15 specifies the procedure for retrieving wallet data, while Figure 7.6 illustrates the implementation outcome, showing the identity information as presented in the system interface.

Algorithm 15 Read UID Process

```
1: function READ_UID
2:     result ← []
3:     for each uid in self.contract.functions.getUids().call() do
4:         result.append(uid)
5:     end for
6:     return result
7: end function
```

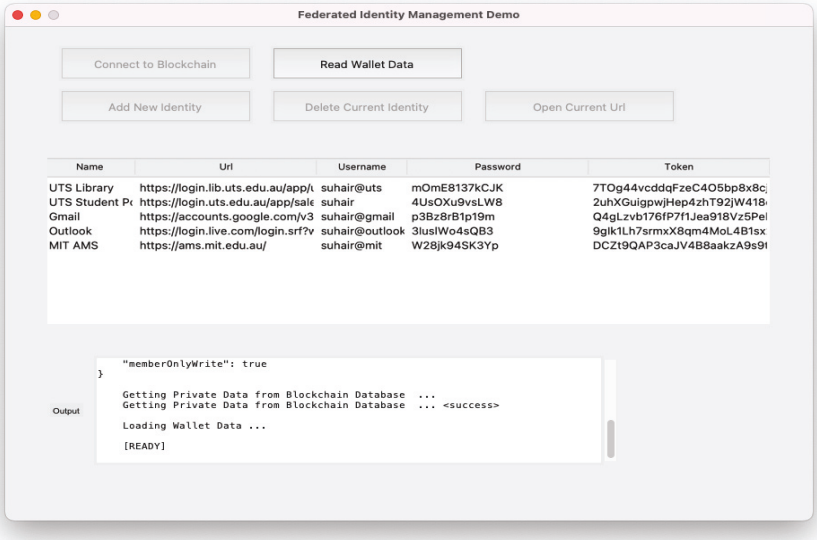


Figure 7.6 : Read Wallet Data

7.4.2 *Add New Identity*

This feature allows users to add a new identity or delete an existing federated link. To add a new identity, the user can save new credentials which are securely integrated into the blockchain-backed system as outlined in Algorithm 16. Each operation is validated by the blockchain network to ensure security and data integrity, with every transaction immutably recorded to maintain a tamper-proof ledger. The implementation of this process is illustrated in Figure 7.7.

Algorithm 16 Add Identity Process

```
1: function ADD_IDENTITY
2:     input ← { 'name': name_entry.get(), 'url': url_entry.get(), 'username': username_entry.get(),
   'password': password_entry.get(), 'token': token_entry.get() }
3:     add_data()
4:     transaction ← add_uid(_uid)
5:     transaction_hash ← send_raw_transaction
6:     update_view()
7:     sub_window.destroy()
8: end function
```

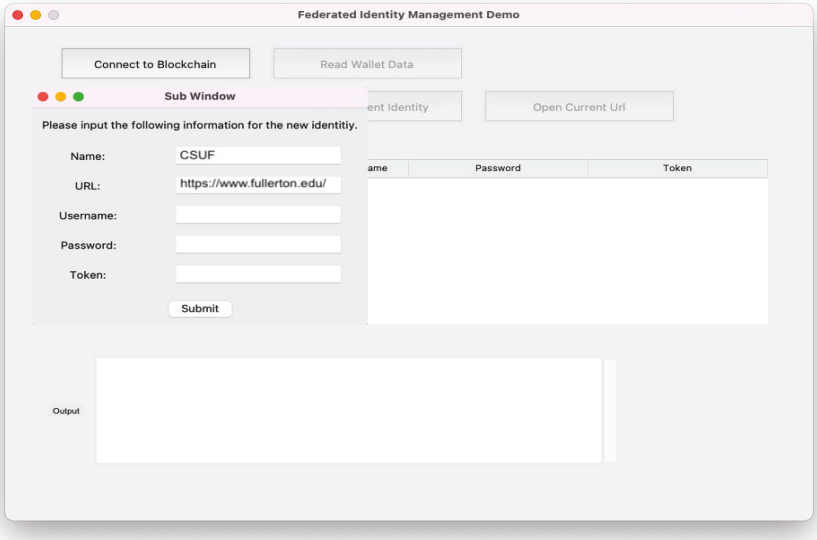


Figure 7.7 : Add Identity

7.4.3 *Delete Current Identity*

This feature enables users to delete or revoke a federated identity without affecting their primary identity within the BIIM framework. Algorithm 17 defines the sequence of operations required to securely execute the deletion process. Each deletion request is authenticated and verified by the blockchain network, ensuring that only legitimate transactions are processed. All deletion records are permanently stored on the blockchain, preserving system transparency and traceability while maintaining data integrity.

Algorithm 17 Delete Identity Process

```
1: function DELETE_IDENTITY
2:     _cur_row ← get_selected_row()
3:     _uid ← _cur_row[]
4:     transaction ← delete_uid(_uid)
5:     transaction_hash ← send_raw_transaction
6:     update_view()
7: end function
```

7.4.4 *Open Current URL*

This feature provides users with direct access to URLs associated with their federated identities. When a user selects an identity record, the system retrieves the corresponding URL, enabling access to external resources linked to their identity management activities. Algorithm 18 specifies this functionality, ensuring that each identity record is correctly linked to its associated web resource. The outcome of this process is illustrated in Figures 7.8 and 7.9, which show how the system interface executes the opening of linked URLs.

Algorithm 18 Open URL Process

```
1: function OPEN_URL
2:     _cur_row ← get_selected_row()
3:     print(_cur_row)
4:     web_browser.open(_cur_row[])
5: end function
```

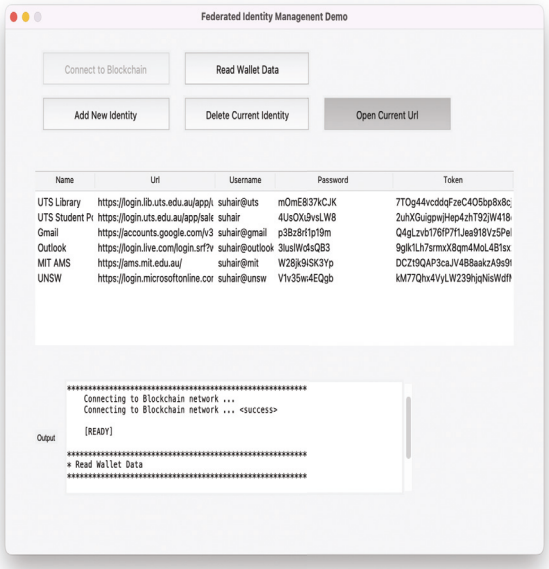


Figure 7.8 : Open Current URL

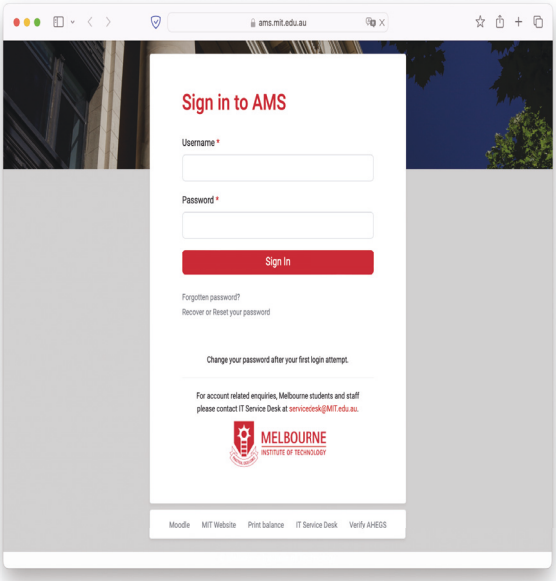


Figure 7.9 : URL

7.5 Implementation

This section describes the implementation of the FIM subsystem within the BIIM framework. It outlines how the conceptual design is translated into a working system through the development of core functionalities, algorithms, and smart contract operations. The focus is on demonstrating the technical realization of identity integration, verification, access, and revocation, thereby showing how the proposed model is operationalized in practice.

7.5.1 Implementation Requirements:

In implementing the FIM system, we employ the *Ethereum blockchain platform*, a widely adopted framework for developing smart contract-based systems due to its decentralization, security, and programmability. Under certain conditions, Ethereum guarantees high availability, immutability, and transparency [68]. However, constraints exist with respect to storage, data transmission, and the execution of Ethereum-based smart contracts, as the gas limit imposes restrictions on the size and complexity of transactions [20]. Table 7.1 summarizes the hardware and software specifications used during the experimental evaluation of the FIM system.

Type	**Description**
CPU	Apple M1 Max
RAM	64 GB
SSD	1 TB
Operating System	macOS Sonoma 14.5

Table 7.1 : Experiment Environment

Smart contracts form the backbone of the FIM subsystem, addressing critical security requirements related to identity token generation, verification, and lifecycle management. These self-executing programs are embedded within the Ethereum blockchain and automatically enforce predefined rules without human intervention [84]. By encoding contract logic directly on-chain, smart contracts eliminate the need for third-party intermediaries while ensuring that identity transactions are tamper-proof, transparent, and verifiable.

We also employed smart contracts to address critical security concerns related to the verification of authentication tokens. These smart contracts generate tokens and verify the user's identity. Smart contracts are self-executing programs that operate without human intervention. They are ledger-based contracts coded into a blockchain, defining rules and penalties similar to traditional contracts. However, unlike traditional legal agreements, smart contracts automate the processes of enforcement and verification. By removing the need for intermediaries, smart contracts reduce the risk of tampering, improve execution speed, and enhance overall trust in the system [84].

Ethereum's deterministic execution and linear state transitions ensure that each identity-related transaction—such as creation, revocation, or federation—can be independently audited and reproduced across network nodes. This deterministic behavior supports verifiability in a decentralized context and guarantees consistent outcomes across the blockchain. Additionally, smart contracts are programmed with a defined set of conditions and stored in a public, immutable ledger. Every participant in the network maintains a synchronized copy of the contract, making them publicly accessible, cryptographically unforgeable, and resistant to unauthorized modification [62].

Solidity, a programming language tailored for writing smart contracts on Ethereum, is employed in our implementation. Solidity is statically typed, features a syntax similar to JavaScript, and compiles contracts into EVM bytecode. Multiple Ethereum development environments exist, such as Remix, Atom, and Visual Studio Code. For this research, Remix[9] was selected due to its simplicity and comprehensive features, including a browser-based compiler, debugging tools, gas estimation, and the ability to import existing contracts [74].

For local development and testing, Ganache CLI[10] is used to provide a large set of pre-funded accounts for immediate use [58]. Furthermore, MetaMask[11] is integrated as a digital wallet and browser extension to manage private keys and facilitate interactions

[9] https://remix.ethereum.org/

[10] https://archive.trufflesuite.com/ganache/

[11] https://metamask.io/

with the Ethereum blockchain, ensuring the secure and efficient handling of transactions throughout the development process.

Python is utilized as the primary programming language for the implementation of the FIM subsystem. Known for its efficiency, readability, and extensive use in data analysis, Python was chosen for its ability to handle complex backend processes such as managing interactions with the Ethereum blockchain [88]. Its simplicity and versatility make it well-suited for integrating blockchain functionality, smart contract interactions, and testing environments, including MetaMask and Ganache. Additionally, a proof-of-work demonstration was conducted to showcase the use of Python in designing and implementing the FIM authentication system, highlighting its role in facilitating blockchain-based operations with precision and reliability.

The complete source code for the implementation of the FIM system is hosted on GitHub. This repository provides access to the source code and all necessary dependencies, allowing for replication and further development by other researchers and practitioners. For detailed access, the project files can be found at Federated Identity Repository, where all the project files are organized and maintained.

7.5.2 Implementation Process

The implementation process for deploying smart contracts on the Ethereum blockchain involves several steps. To ensure accuracy and clarity, the following detailed explanation is provided.

Step 1: Write and Deploy Code on Remix

The process starts by writing the smart contract code in Remix, a widely used Solidity IDE [74], as illustrated in Figure 7.10.

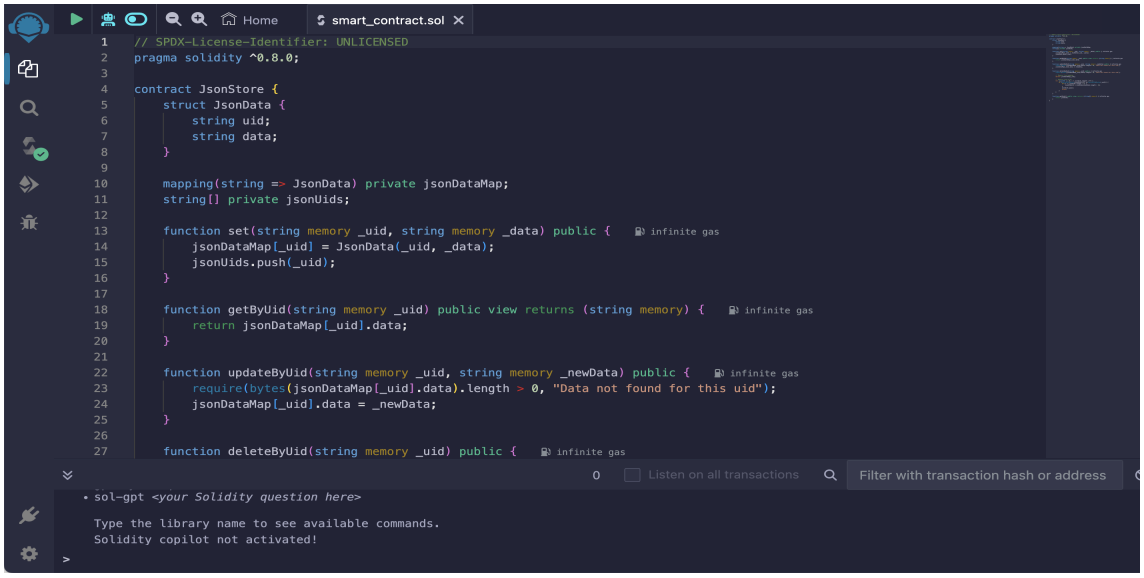


Figure 7.10 : Deploy Code on Remix

Step 2: Select the Appropriate Compiler Version

In Remix, we select the appropriate Solidity compiler version that matches the version used in our smart contract, as shown in Figure 7.11. This ensures compatibility and successful compilation.

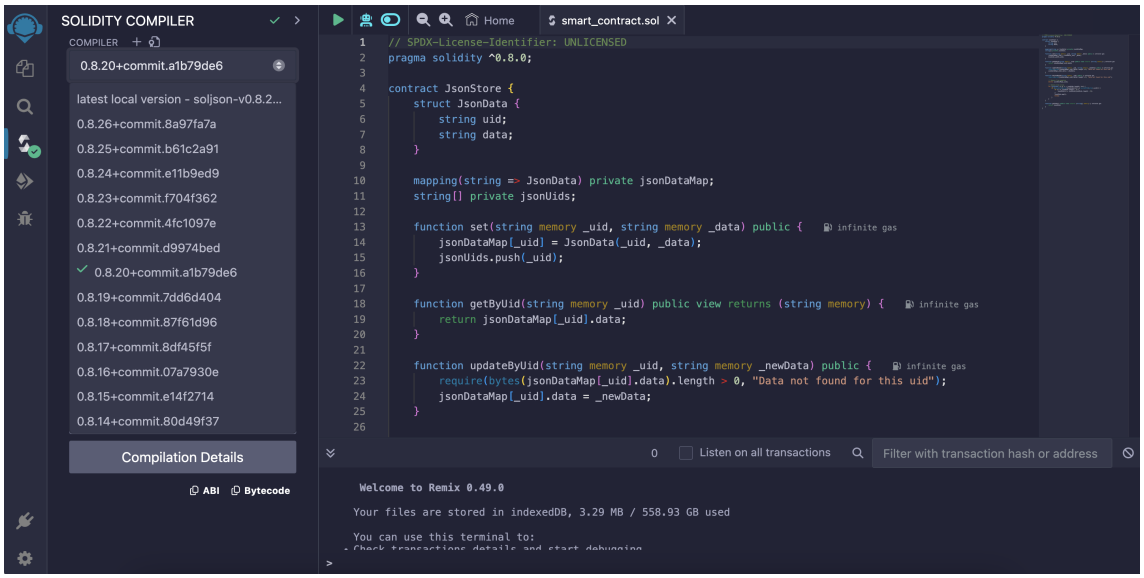


Figure 7.11 : Select Appropriate Compiler Version

Step 3: Compile the Smart Contract

We compiled the smart contract in Remix, as shown in Figure 7.12. If there are no

syntax errors, the contract compiles successfully, generating the necessary bytecode and Application Binary Interface (ABI).

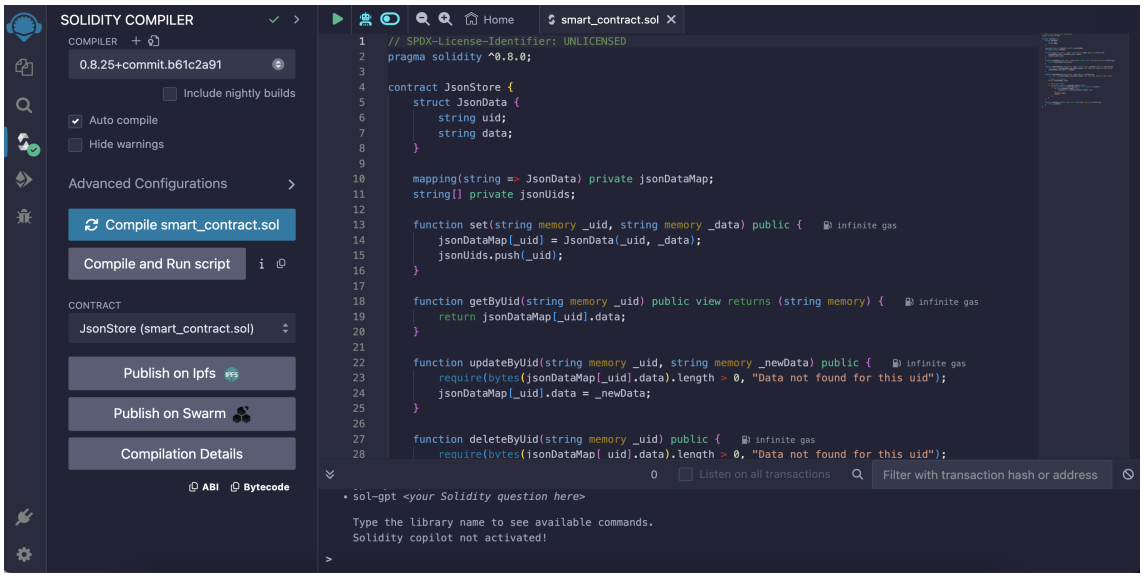


Figure 7.12 : Smart Contract Successfully Compiled on Remix

Step 4: Connect MetaMask for Deployment

We chose MetaMask as the environment for deploying the contract, as shown in Figure 7.13. MetaMask is a browser extension that serves as an Ethereum wallet, which enables us to interact with the Ethereum blockchain.

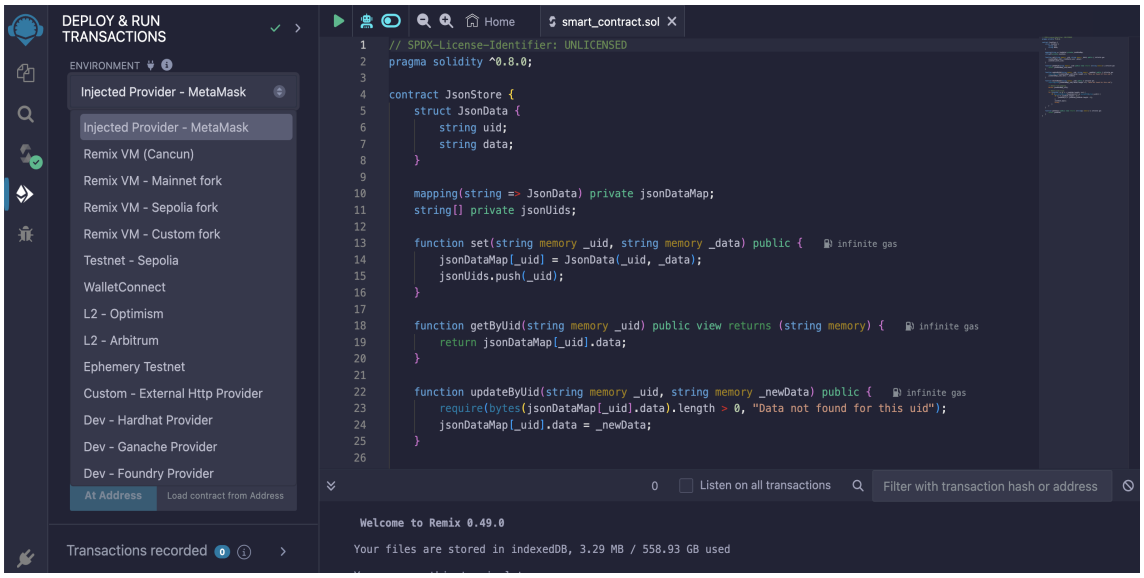


Figure 7.13 : Select MetaMask on Remix for Deployment

Step 5: Deploy Smart Contract Using MetaMask

MetaMask prompts us to confirm the deployment transaction to ensure we are connected to a test account, as shown in Figure 7.14.

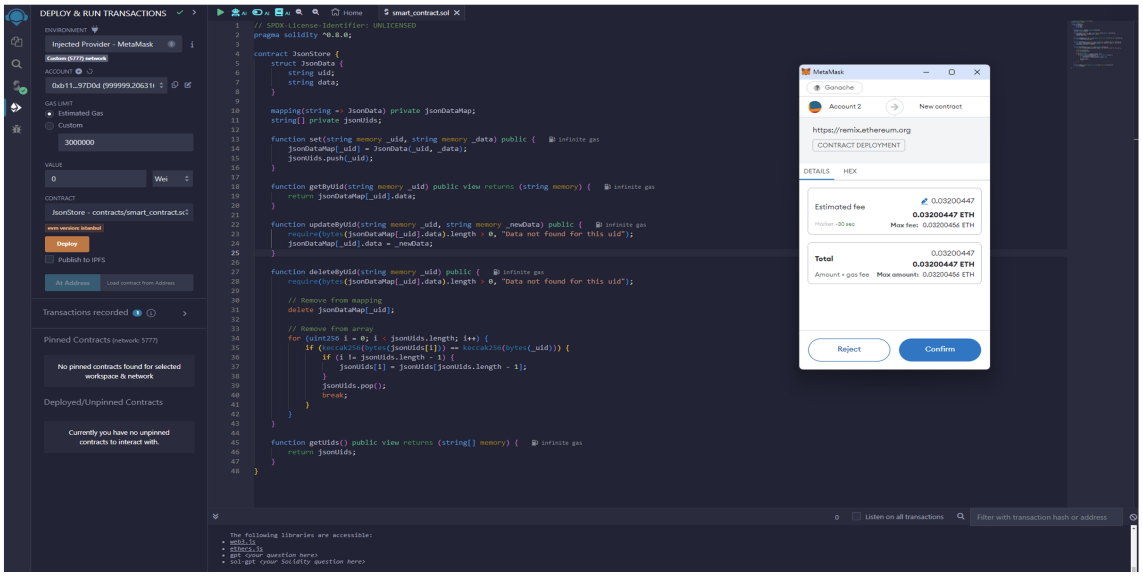


Figure 7.14 : Smart Contract Deployment Using MetaMask with Test Account

Step 6: Confirm Deployment on Local Ethereum Network

After confirming the transaction, the smart contract is deployed on the local Ethereum test network provided by Ganache, as shown in Figure 7.15. Remix displays a confirmation message indicating successful deployment.

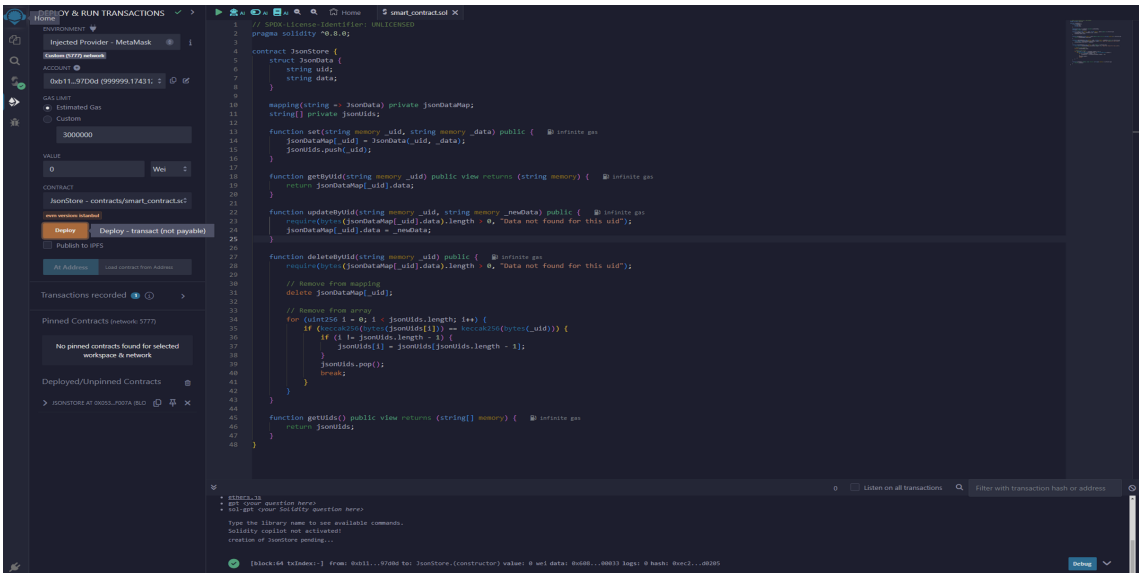


Figure 7.15 : Smart Contract Successfully Deployed on the Local Ethereum Test Network

Step 7: Acquire Deployed Smart Contract

Copy the address of the deployed smart contract:

0x053F90c10282c9076D12Aa5016176e63319f007A

Step 8: View Ganache Test Accounts

We use Ganache to view the list of test accounts, as shown in Figure 7.16. Ganache provides a set of pre-funded accounts for testing purposes.

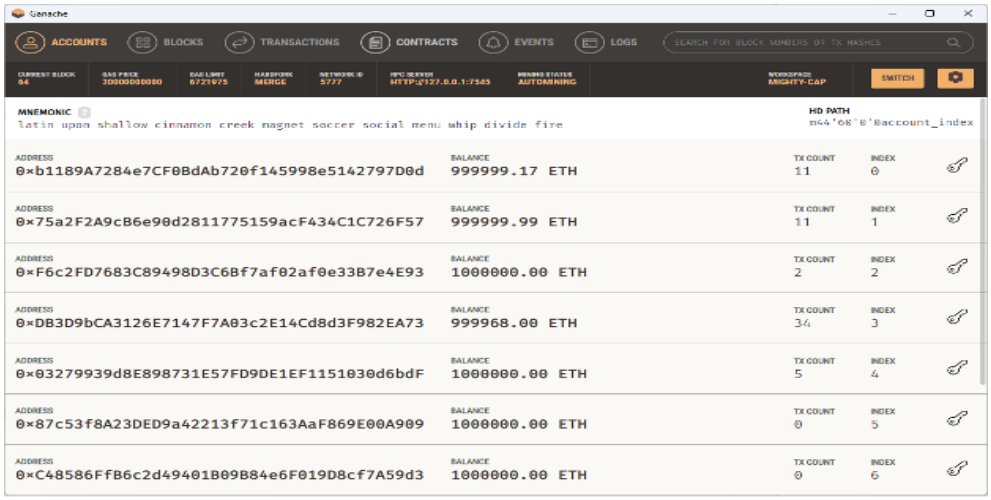


Figure 7.16 : Ganache Test Accounts

Step 9: Acquire Test Account's Private Key

A copy is made of the private key of one of the test accounts from Ganache, as shown in Figure 7.17. This key used to import the account into MetaMask.

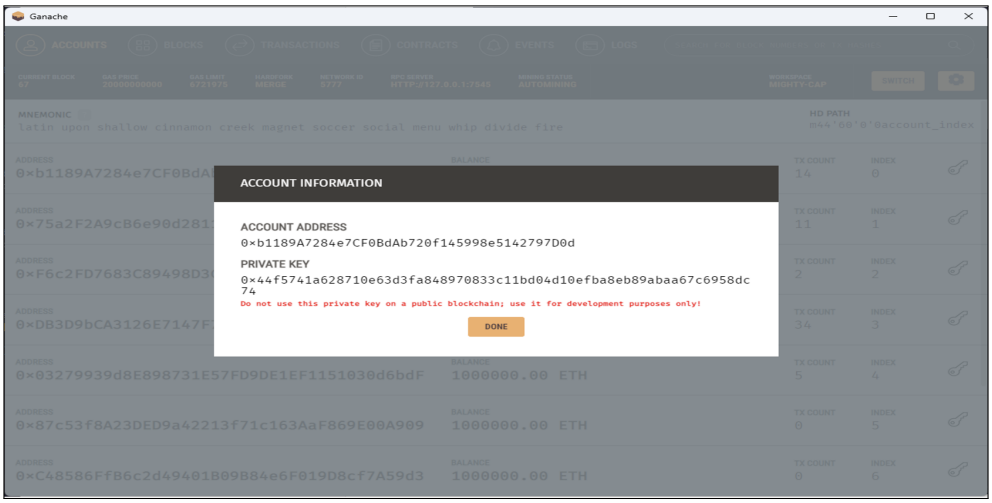


Figure 7.17 : Acquire Test Account's Private Key

Step 10: Setup Ganache Test Network on MetaMask

In MetaMask, we set up a new network connection to the Ganache test network. We enter the RPC URL provided by Ganache, along with the chain ID and other necessary details, as shown in Figure 7.18

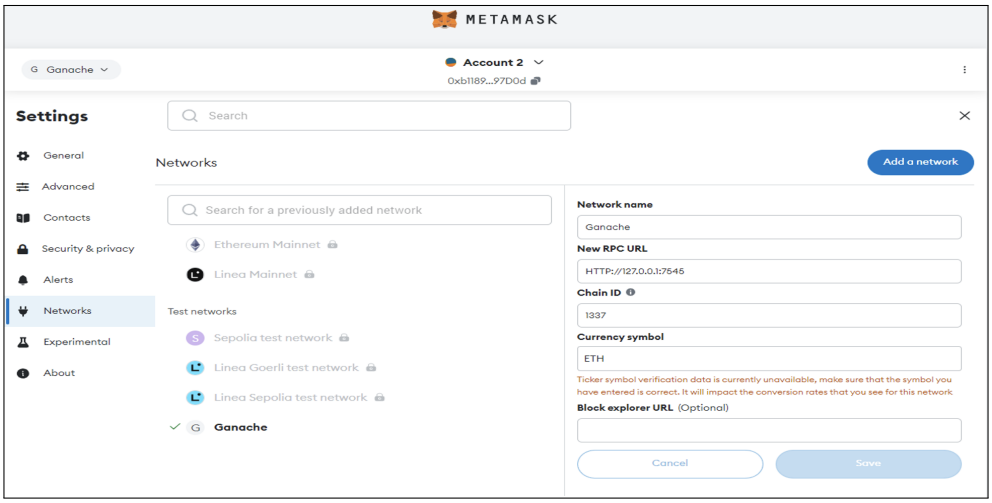


Figure 7.18 : Setup for the Ganache Test Network on MetaMask

Step 11: Import Test Account to MetaMask

We use the private key obtained from Ganache to import a test account into MetaMask, as demonstrated in Figure 7.19. This allows MetaMask to interact with the local Ethereum test network and the deployed smart contract.

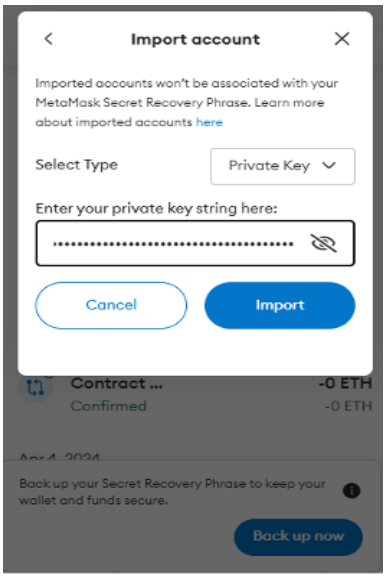


Figure 7.19 : Import Test Account to MetaMask

7.6 Evaluation of the FIM System

This section evaluates the performance and effectiveness of the FIM system through a combination of empirical benchmarking and algorithmic analysis. By integrating both system-centric and user-centric perspectives, the evaluation offers a comprehensive understanding of the system's capabilities. The analysis considers key metrics such as scalability, computational efficiency, and security, while also highlighting the system's role within the broader BIIM framework. The evaluation is carried out through two complementary approaches: experimental testing and system-driven analysis. Given the nature of the system, the emphasis is placed on system-driven evaluation to verify that the implemented functionalities operate as intended and align with the design objectives.

7.6.1 FIM Experimental Evaluation

The evaluation results demonstrate the performance and cost implications of this process. Table 7.2 highlights the time consumption, average time per record, and gas cost for processing varying numbers of records, from 10 to 10,000. As the number of records increases, the total time consumption and gas cost increase, indicating a proportional relationship. Time consumption values represent the time taken to process the specified records, which may include system overhead and other factors that influence processing time. However, the average time per record remains relatively stable, suggesting efficient and scalable performance. This consistency points to the system's ability to handle larger datasets without significant degradation in processing speed. The cost of gas, which represents the computational expense, also increases with the number of records, which is essential for budgeting in blockchain applications. Overall, the results affirm that using these tools for identity management on the blockchain is efficient, scalable, and predictable in terms of performance and cost. This evaluation assesses the time consumption and gas cost implications associated with identity operations.

Number of records	Time consumption (sec)	Avg. time consumption per 1 record	Total gas cost (Gwei)
10	0.778096199	0.0778096199	0.3737488
50	3.718056202	0.07436112404	1.868744
100	6.713336945	0.06713336945	3.737488
500	36.428756	0.072857512	18.68744
1000	73.3505578	0.0733505578	37.37488
5000	470.1641111	0.09403282222	186.8744
10000	1227.766962	0.1227766962	373.7488

Table 7.2 : Evaluation Results

If the gas cost per record remains constant (0.03737488), the total gas cost for records can be calculated as:

Total gas cost = Gas cost per record × Number of records

To evaluate the average time consumption per record, we use the following equation:

$$\text{Avg. time consumption per record} = \frac{\text{Time consumption}}{\text{Number of records}}$$

This metric provides valuable insights into how the system behaves as the workload increases. Understanding this relationship is particularly critical in blockchain environments, where computational effort directly translates into gas costs and monetary expenses. Analyzing these trends helps in budgeting and highlights the need for robust optimization strategies to maintain cost-effectiveness as the dataset grows.

7.6.1.1 Gas Cost vs. Number of Records

Figure 7.20 illustrates the correlation between the volume of records and their associated gas costs. The data confirms that while the system is highly efficient for smaller datasets, the increasing computational expense of larger records necessitates proactive cost management. These findings are essential for evaluating the system's economic viability

and identifying potential areas for further optimization.

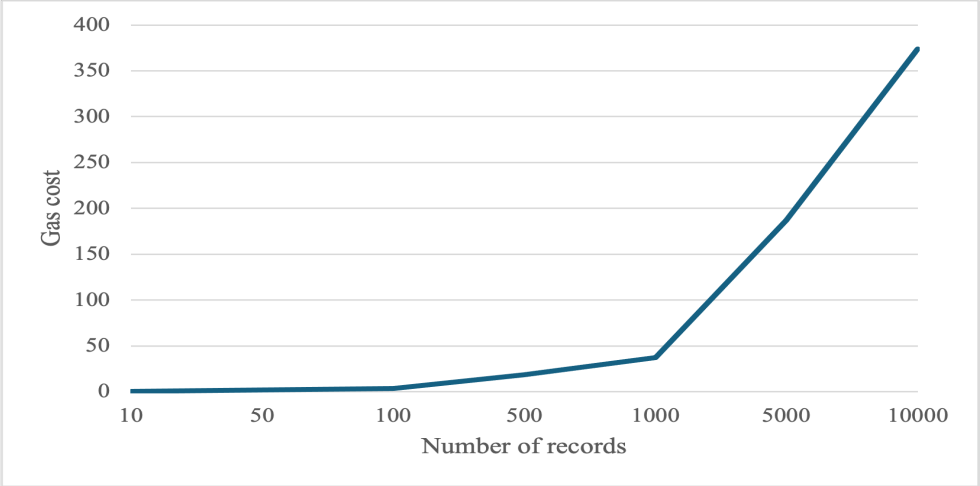


Figure 7.20 : Gas Cost vs. Number of Records

Figure 7.20 shows that there is a significant increase in gas costs as the number of records exceeds 1000. This sharp rise illustrates the need for efficient scaling strategies in blockchain systems. The rise in gas costs can be attributed to various factors, including increased data storage requirements, transaction complexity, network congestion, smart contract execution inefficiencies and block gas limits. As the number of records grows, the demand for data storage across multiple network nodes increases, thereby raising costs. The complexity of transactions also escalates, necessitating more computational steps to verify and store each record, which in turn, increases gas costs. Network congestion further drives up gas prices as users compete to prioritize their transactions. Smart contract execution costs rise significantly with more records, particularly when contracts contain loops or operations that scale with dataset size. Ethereum's block gas limit, which restricts the maximum gas per block, is reached more frequently with higher record counts, necessitating multiple blocks and leading to higher costs.

7.6.1.2 Time Consumption vs. Number of Records

Figure 7.21 illustrates the linear relationship between the number of records and time consumption in the FIM system. As the number of records increases, so does the time

required for operations, as shown by the dotted trend line. This strong positive correlation confirms that the system's performance scales predictably with data volume, facilitating reliable capacity planning. For instance, doubling the number of records from 6,000 to 12,000 approximately doubles the time consumption. Understanding this relationship helps identify optimization strategies to manage larger datasets more efficiently.

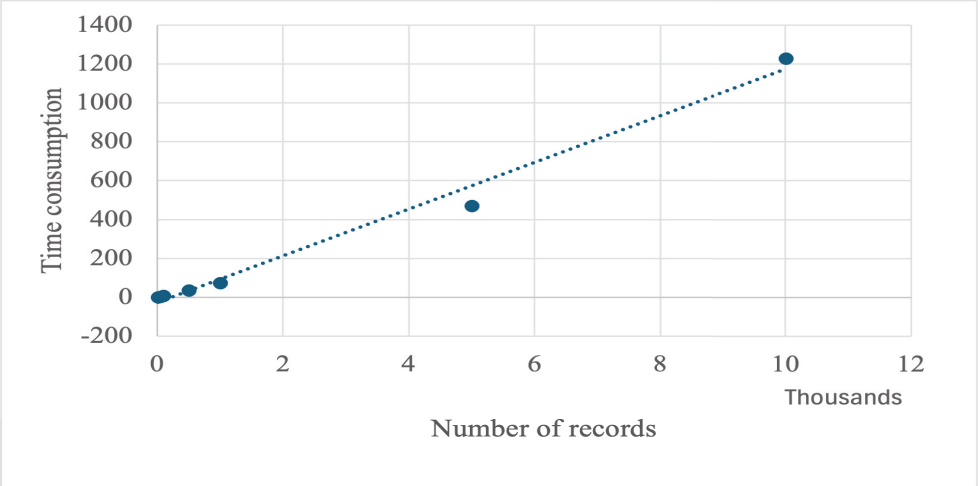


Figure 7.21 : Time Consumption vs. Number of Records

Based on Figure 7.21 and the evaluation of the data points, we can derive the equation:

Given the points (0, 0) and (10, 1200):

1. Determine the slope (m):

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1200 - 0}{10 - 0} = 120$$

2. Determine the Y-intercept (b): Since one of the points is (0, 0), the y-intercept b is 0.

3. Form the Equation:

$$y = mx + b$$

This means time consumption (y) can be calculated using the equation:

$$y = 120x$$

where x is the number of records (in thousands).

The evaluation equation is:

$$\text{Time consumption} = 120 \times \text{Number of records (in thousands)}$$

Interpretation:

- For 1,000 records: $y = 120 \times 1 = 120$ units of time.
- For 5,000 records: $y = 120 \times 5 = 600$ units of time.
- For 10,000 records: $y = 120 \times 10 = 1200$ units of time.

This linear equation allows us to predict the time consumption based on the number of records, facilitating performance evaluation and capacity planning.

7.6.2 FIM Algorithm Complexity Analysis

This section analyzes the algorithmic complexity of our system's core FIM operations. Table 7.4 summarizes the computational complexity, expressed using $\mathcal{O}$ (Big-O) notation, of Algorithms 15- 18, which implement the primary FIM operational processes.

Algorithm	**Complexity**	**Discussion**
Read UID Process	$\mathcal{O}(1)$	Reads a unique identifier for authentication, requiring a single lookup operation.
Add Identity Process	$\mathcal{O}(1)$	Inserts a new identity record into the system, making it a constant-time operation.
Open URL Process	$\mathcal{O}(1)$	Opens an associated identity-linked URL, requiring minimal computation.
Delete Identity Process	$\mathcal{O}(1)$	Deletes a user identity, requiring a single database operation.

Table 7.4 : FIM Algorithm Complexity Analysis

These operations achieve constant-time performance through the use of indexed data

mappings and single-step smart contract calls. The absence of iterative loops or dynamic data traversal ensures the system's performance is resilient to identity volume. No operation relies on iteration or data traversal. All functions leverage direct index access or one-step state updates, ensuring computational stability regardless of identity volume. All operations run in $\mathcal{O}(1)$, meaning they perform constant-time work irrespective of the number of users or stored records. This efficiency results from the architectural decision to implement smart contract functions as single-step calls without iterative loops or data-dependent traversal. For instance, the `read_uid`, `add_identity`, and `delete_identity` operations each interact with indexed mappings on the blockchain, enabling direct lookups or state changes rather than scanning entire datasets. As a result, execution time and gas cost remain predictable and low, ensuring that user experience is not degraded even as the number of stored identities increases. This design aligns with the FIM system's goal of delivering low-latency, scalable identity management in decentralized environments.

7.6.3 Functional Validation via Scenario-Based Testing

This scenario validates the FIM system's implementation by demonstrating the successful execution of identity lifecycle operations within a live environment. It further establishes practical interoperability with existing institutional systems, aligning with deployment objectives in real-world contexts.

As presented in Chapter 5 Section 5.8, the scenario involves a user (Bob) accessing a university portal through the BIIM platform. The overall federated identity architecture supporting this process is depicted in Figure 7.1 and the blockchain-enabled identity flow is detailed in Figure 7.3. The process begins with identity integration through the FIM interface, where the user registers a new service identity via the interface shown in Figure 7.7, initiating the *Add_Identity* procedure as defined in Algorithm 16. Following registration, the system retrieves the federated identity by executing the *Read_UID* process described in Algorithm 15, as illustrated in Figures 7.5 and 7.6. The retrieved identity record is subsequently used to generate a blockchain-backed authentication token that is cryptographically linked to the user's wallet, consistent with the federated operational flow

presented in Figure 7.4. Once verified, the *Open_URL* process detailed in Algorithm 18 is executed to enable secure redirection and access, as demonstrated in Figures 7.8 and 7.9. This mechanism allows Bob to securely access the university portal without redundant credential entry, thereby ensuring both efficiency and security. Should Bob choose to revoke access, the system executes the *Delete_Identity* procedure defined in Algorithm 17, ensuring the secure removal of the federated association from the FIM system, with the revocation transaction permanently recorded on the blockchain.

This scenario confirms that the FIM system satisfies both functional and non-functional requirements by demonstrating secure identity creation, retrieval, authentication, and revocation. These results validate the system's suitability for scalable deployment across multi-domain institutional environments.

7.7 Discussion

The results presented in this chapter substantiate the claim that the proposed FIM system addresses the theoretical and practical deficiencies identified in Chapter 2, particularly the lack of a blockchain-enabled framework supporting secure, user-controlled identity federation. While earlier studies have explored self-sovereign identity and blockchain-based authentication within single administrative domains, they have not resolved the challenge of cross-domain interoperability under user control [5]. The FIM system responds to this gap by integrating federated identity functionality within a distributed blockchain infrastructure, reconciling interoperability, verifiability, and user autonomy.

From a theoretical perspective, the FIM system demonstrates how blockchain can function as a distributed trust fabric for federated identity systems. By replacing hierarchical, provider-centric architectures with decentralized consensus mechanisms, it reconfigures trust— shifting it from institutional intermediaries to cryptographically verifiable smart contracts. Each identity operation is immutably recorded on-chain, ensuring traceability, verifiability, and non-repudiation. The system's layered architecture consisting of view, control, and model layers, enhances reliability by enforcing a clear separation of concerns

and supports modular scalability across heterogeneous digital environments.

Empirical results confirm the viability of this system. The evaluation shows a linear relationship between computational cost and data volume, indicating maintained scalability without exponential resource use. The constant-time complexity $\mathcal{O}(1)$ of the core algorithms demonstrates computational stability regardless of identity volume. The proportional increase in gas expenditure reflects Ethereum's deterministic transaction model, confirming predictable and manageable costs under realistic deployment conditions. These findings validate that a properly implemented blockchain infrastructure can meet the operational demands of federated identity management at scale.

Traditional federated identity systems such as SAML, OpenID Connect, or OAuth 2.0 rely on centralized identity providers, reproducing asymmetries of control and surveillance [66]. In contrast, the FIM system restores decision-making authority to users through a self-managed digital wallet embedded within the blockchain. This design grants individuals exclusive control over the disclosure and revocation of their credentials, reinforcing principles of data sovereignty and privacy preservation.

Within the BIIM architecture, the FIM system plays an integrative role. It extends the biometric verification mechanisms of the BBIM system and complements the transparency and accountability features of the UDOD system. Through this layered integration, the FIM system achieves its primary objective of secure identity federation while strengthening the coherence and functionality of the BIIM architecture.

These outcomes position the FIM system as a technical and conceptual advancement in federated identity management. The findings demonstrate that decentralized infrastructures can support interoperable identity federation while preserving user control, thereby establishing blockchain as a viable foundation for next-generation digital identity systems.

7.8 Conclusion

This chapter focused on the importance of a federated identity management system and robust authentication procedures across various platforms. Our approach facilitates

the secure linking and storage of multiple identities within a digital wallet, ensuring users maintain control over their personal information. We also detailed the technical flow of our system, illustrating how Ethereum provides a tamper-proof ledger. This combination of technologies enhances the transparency and security of the authentication process.

The next chapter provides a comprehensive conclusion to the thesis, summarizing the key findings and contributions of this research. Additionally, we discuss future directions for the implementation and development of advanced identity systems.

Chapter 8

Conclusion

8.1 Introduction

The previous chapter discussed the significance of a federated identity management system and implemented robust authentication procedures, detailing how our approach securely links and stores multiple identities within a digital wallet. As the final chapter, this section transitions from the specific focus on federated identity to provide a holistic overview of the entire thesis, addressing the integration of all BIIM subsystems.

The primary objective of this research has been to develop a highly reliable and robust identity management framework using innovative blockchain technology. By integrating biometric-based identifiers (BBIM), user-driven document management (UDOD), and federated identity (FIM), this technology empowers users to exercise vigilant control over the accessibility and management of their personal data. Ultimately, this research aims to revolutionize identity verification and establish a secure foundation for protecting user privacy in an increasingly interconnected digital world.

The structure of this chapter is as follows: Section 8.2 provides a comprehensive summary of the thesis. Section 8.3 explains the problems addressed in the thesis. Section 8.4 highlights the key accomplishments of the research. The comprehensive implications of BIIM are discussed in Section 8.5. Then, Section 8.6 covers the limitations encountered during the study. Finally, Section 8.7 outlines potential directions for future research, building on the findings of this thesis.

8.2 Thesis Summary

Integrating biometrics with blockchain technologies to address niche issues in identity management is the fundamental objective of this thesis. The purpose of this integration is to provide a reliable user-centric identity management system. This system will improve users' privacy and security while enabling them to maintain a self-sovereign identity. By utilizing the immutability of blockchain technology, the system ensures the protection of biometric data and maintains the integrity of the information. Moreover, the independence from geographical boundaries is one of the key features of a blockchain ecosystem. It ensures secure and universal authentication of the user identity, thus making it possible to perform the verification at any time and from any location.

BIIM is the essential framework that provides individuals with self-sovereignty and privacy when managing and controlling their digital identities. The BIIM system is designed to make it possible to store and maintain user identities securely. Through its robust features and functionalities, the BIIM framework empowers users with granular control over their personal information, enabling them to decide when, how and with whom their data is shared, fostering confidence and trust. BIIM not only safeguards user privacy, it also ensures that identities are protected holistically.

One of the critical aspects of BIIM is its ability to enable users to manage their identities independently. This means that individuals have full authority over the flow of their personal data, giving them the freedom to disclose or withhold information from any third party. Moreover, while BIIM provides users with the utmost privacy, it also incorporates the mechanisms that allow authorized government entities to access the necessary information under specific legal conditions. This ensures that law enforcement agencies and other authorized bodies can fulfill their duties effectively without compromising the privacy rights of individuals. The BIIM system achieves remarkable capabilities by effectively implementing the BBIM, UDOD, and FIM subsystems:

The BBIM system is designed to securely store and compare biometric data, ensuring protection from unauthorized access. This system guarantees that sensitive personal

information is managed with the highest standards of care and security.

The UDOD system, on the other hand, plays a role in enhancing user privacy within the BIIM system. It provides proactive privacy-aware notifications, empowering users with real-time information about their interactions within the system and between different entities. These notifications serve as an added layer of protection, allowing individuals to stay informed and make decisions.

Furthermore, the FIM system simplifies user access to various platforms by consolidating credentials into a single, secure digital identity. This not only enhances user convenience, but also mitigates the risk of identity theft and unauthorized access to personal accounts. Users can navigate confidently through different platforms without needing multiple usernames and passwords, enhancing their digital experience while maintaining optimal security.

8.3 Problems Addressed in this Thesis

8.3.1 Research Problem 1: Comprehensive Framework

The current literature lacks a holistic approach that integrates biometrics, blockchain technology, AI-driven notifications, and federated identities into a single framework for identity management. While each component has been studied separately, a significant gap exists in creating a unified system that leverages all these technologies to enhance identity management solutions.

8.3.2 Research Problem 2: Secure and Scalable Storage of Biometric Data

There is a clear gap in the research regarding the secure and scalable storage of biometric data within the blockchain. Although biometric authentication is highly secure, the literature does not sufficiently address methods for reliably storing biometric information on the blockchain to strengthen the security of identity management systems.

8.3.3 Research Problem 3: Proactive Notification Systems

Existing research does not sufficiently cover the development of intelligent notification systems that alert users before any changes or access to their identity details occur. This gap points to the need for systems that provide real-time alerts, enhancing user awareness and control over personal information.

8.3.4 Research Problem 4: Integration of Federated Identities with Blockchain

The literature lacks comprehensive strategies for integrating federated identities with blockchain technology using AI-driven methods. There is a significant gap in creating a system that combines various identity management platforms into a cohesive, biometrics-driven blockchain-based solution.

8.3.5 Research Problem 5: Evaluation and Validation of Comprehensive Identity Management Systems

There is a notable lack of evaluation and validation methods for integrated identity management systems that combine blockchain, biometrics, AI-driven notifications, and federated identities. Effective evaluation and validation are important to ensure these systems meet their objectives and perform reliably, which requires thorough testing and assessment to identify improvements and confirm their effectiveness.

8.4 Thesis Achievements

The accomplishments of this thesis are summarized as follows:

1. This work offers a comprehensive review of the literature in the area of identity management. More details can be found in Chapter 2.

2. This work proposes the BIIM framework that enables the reliable and intelligent storage and management of user identities on the blockchain layer, which comprises the following subsystems:

2.1 BBIM system, which is responsible for storing biometric information on top of the blockchain layer. More details can be found in Chapter 5.

2.2 UDOD system, which is an intelligent privacy-aware measure to inform the owner of the information if the information has been accessed. More details can be found in Chapter 6.

2.3 FIM system, which is responsible for integrating federated identities into the developed biometrics-driven blockchain-based identity management system. More details can be found in Chapter 7

8.5 Comprehensive Implications of the Blockchain-Based Identity Management System

8.5.1 Implications for Research

The BIIM system is a novel framework that stores identity information on the blockchain. It includes three critical subsystems: BBIM, UDOD, and FIM. This innovative approach to identity management has profound implications for research.

1. **Blockchain Security:** The use of blockchain for storing user data and biometrics in the BBIM subsystem presents opportunities to explore advanced security mechanisms. Researchers can investigate new blockchain algorithms and protocols to further enhance data protection.

2. **Privacy Preservation:** The BBIM subsystem's method of securely storing biometric data and valid IDs offers a rich area for research into privacy-preserving techniques within blockchain environments, balancing transparency and confidentiality.

3. **User-Centric Control:** The UDOD notification system, which alerts users of access attempts and allows them to accept or reject requests, invites studies into user-centric control mechanisms and their impact on user trust and system usability.

4. **Scalability Solutions:** As the BIIM system scales, future research can focus on overcoming the scalability challenges associated with blockchain-based identity management, aiming to ensure robustness and efficiency for a large number of users.

5. **Regulatory Compliance:** The implementation of blockchain-based identity systems across different jurisdictions poses regulatory challenges. Researchers can explore legal frameworks and compliance strategies to facilitate the global adoption of such systems.

8.5.2 Implications for Practice

The BIIM system offers numerous practical benefits for organizations and users, enhancing security and operational efficiency.

1. **Enhanced Security:** The BBIM subsystem's use of blockchain to store user data and biometrics significantly reduces the risk of identity fraud. This high-security approach is crucial for sectors such as banking and healthcare.

2. **User Empowerment:** The UDOD notification system empowers users by giving them control over their personal information. Users receive alerts when access is attempted and can approve or reject requests from organizations, ensuring their privacy and autonomy.

3. **Operational Efficiency:** Organizations can streamline their identity verification processes using the BIIM system, reducing the time and cost associated with manual checks and increasing overall efficiency.

4. **Accessibility:** The BIIM system allows users to manage all their identities in one place, simplifying the management process and ensuring consistency across various platforms.

5. **Interoperability and Integration:** The BIIM system's design ensures interoperability with existing identity management solutions, facilitating broader adoption and smoother integration for organizations upgrading their security infrastructure.

8.5.3 Implications for Society

The BIIM system has significant societal implications, particularly in enhancing security and trust in digital interactions.

1. **Reduction in Identity Fraud:** The secure and tamper-proof method for managing identities through blockchain technology in the BBIM helps to reduce identity theft and fraud, contributing to a safer digital environment.

2. **Enhanced Online Safety:** The BIIM system's robust security measures increase public confidence in online transactions and interactions, encouraging greater digital participation.

3. **Community Trust:** Secure identity verification through the BIIM system enhances community trust, as individuals and organizations can be confident in the authenticity of identities. This trust is crucial for building robust social and economic networks.

4. **Transparency and Accountability:** The transparent and auditable transaction records maintained by the BIIM system ensure accountability and build trust in digital interactions, benefiting individuals and organizations.

8.6 Thesis Limitations

Despite the significant contributions of this research, several limitations and challenges emerged during the development and evaluation of the BIIM framework.

1. **Inclusivity and Accessibility in Biometric Systems**

   Biometric technologies face inherent challenges in accommodating individuals with disabilities or users whose biometric attributes fail to register reliably. For example, certain medical conditions or physical limitations may prevent consistent biometric capture. This limits the universal applicability of BIIM and underscores the need for more inclusive identity verification mechanisms.

2. **Blockchain Scalability and Maturity**

   Scalability remains a central limitation of our current solution. Blockchain networks, while offering immutability and transparency, are constrained by limited transaction throughput and high costs during periods of network congestion. Moreover, the use of proof-of-work consensus in this research introduced an average delay of approximately ≈ 1.2 seconds per user, which becomes significant at scale. Due to the costs and latency, future work should develop intelligent approaches to address these gaps.

3. **Layered Blockchain Complexity**

   This research focused primarily on a Level-1 blockchain implementation. However, comparisons with Level-2 infrastructures were beyond the scope of this work. As a result, the analysis does not capture how alternative blockchain layers might improve scalability, reduce gas costs, or enhance real-world usability.

4. **Usability Testing**

   Due to time constraints, practical usability testing was not performed. While functional validation was achieved in simulated environments, real-world deployment involving end users was outside the scope of this study. Consequently, issues such as user adoption challenges, interface design, and governance are crucial issues for future investigation and research attention.

5. **Evaluation Constraints**

   The framework was primarily tested in controlled environments. Real-world deployments may introduce additional complexities, including heterogeneous devices, malicious adversaries, governance challenges, and socio-legal considerations that were beyond the scope of this research.

8.7 Future Research Directions

Building on the limitations identified above, we outline several promising directions for advancing the BIIM framework:

1. **Enhancing Trust Mechanisms**

   Implement a smart contract–based trust scoring feature that correlates a user's trust score with the quantity, diversity, and provenance of submitted identity documents and/or biometrics. Such a mechanism can incentivize users to maintain robust, verifiable identities and enable relying parties to apply risk-adjusted policies.

2. **Migration to Lightweight Consensus Protocols**

   The use of proof-of-work (PoW) introduces latency and inefficiency. Future implementations should adopt lightweight consensus protocols such as proof-of-authority (PoA) or explore permissioned frameworks (e.g., Tendermint), which can substantially reduce confirmation time and improve system performance and scalability.

3. **Exploring Layer-2 Blockchain Solutions**

   Investigate Layer-2 infrastructures (e.g., Polygon, Arbitrum, Optimism) to reduce gas expenditure and improve transaction throughput. Comparative studies between Layer-1 and Layer-2 platforms should quantify trade-offs in latency, cost, and security assumptions to guide real-world deployment choices.

4. **Usability Testing and Real-World Deployment**

   Conduct structured usability studies and pilot deployments in domains such as healthcare, finance, and smart-city services. Field evaluations will surface issues related to user adoption, interface design, governance, and operational robustness that are not fully captured in controlled environments. The system can be delivered through a scalable, cloud-based Software-as-a-Service (SaaS) deployment model to support reliable access by end users.

5. **Mechanisms for Biometric Inclusivity**

   Expand support for multi-modal biometrics (e.g., fingerprints, face, voice, and behavioral traits) and provide accessible fallbacks. Incorporate privacy-preserving techniques such as secure multi-party computation (SMPC) and zero-knowledge proofs (ZKPs) to improve inclusivity while mitigating spoofing and model inversion risks.

6. **Privacy-Preserving Regulatory Compliance**

   Explore cryptographic mechanisms such as homomorphic encryption and selective-disclosure credentials to reconcile user sovereignty with compliance requirements (e.g., KYC/AML, GDPR). Policy-aware attestations can enable lawful verification while minimizing exposure of sensitive attributes.

7. **Integration with Emerging Technologies and Applications**

   Extend BIIM to interoperate with emerging technologies and applications such as IoT ecosystems, decentralized finance (DeFi) platforms, and smart-city infrastructures. Providing a standards-aligned API/SDK can facilitate secure, interoperable, and scalable deployments.

Bibliography

[1] Ahmed, K., Saraya, S. F., Zaki, J., and Ali-Eldin, A. M. T. (2023). A blockchain self-sovereign identity for open banking secured by the customer's banking cards. *Future Internet*. DOI: 10.3390/fi15060208.

[2] Alamri, B., Crowley, K., and Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in health iot. *Italian National Conference on Sensors*. DOI: 10.3390/s23010218.

[3] Alanzi, H. and Alkhatib, M. (2022). Towards improving privacy and security of identity management systems using blockchain technology: A systematic review. *Applied Sciences*, 12(23):12415. DOI: 10.3390/app122312415.

[4] Alkharashi, A. and Mathkour, H. (2020). Federated identity management systems: A review of features, challenges, and future directions. *IEEE Access*, 8:198471–198490. DOI: 10.1109/ACCESS.2020.3033799.

[5] Allen, C. and McCorry, P. (2021). Self-sovereign identity: Foundations, applications, and challenges. *IEEE Access*, 9:17443–17457.

[6] Alpár, G., Hoepman, J.-H., and Siljee, J. (2011). The identity crisis: Security, privacy and usability issues in identity management. *arXiv preprint arXiv:1101.0427*. DOI:10.48550/arXiv.1101.0427.

[7] Alsayed Kassem, J., Sayeed, S., Marco-Gisbert, H., Pervez, Z., and Dahal, K. (2019). Dns-idm: A blockchain identity management system to secure personal data sharing in a network. *Applied Sciences, MDPI*, 9(15):2953. DOI: 10.3390/app9152953.

[8] Alsobhi, H., Mirdad, A., Alotaibi, S., Almadani, M., Alanazi, I., Alalyan, M., Alharbi, W., Alhazmi, R., and Hussain, F. K. (2021). Innovative blockchain-based applications -

state of the art and future directions. In Barolli, L., Woungang, I., and Enokido, T., editors, *Advanced Information Networking and Applications*, pages 323–335, Cham. Springer International Publishing. DOI: 10.1007/978-3-030-75078-7_33.

[9] Amazon Web Services (2023). Amazon simple notification service (sns): Developer guide. https://docs.aws.amazon.com/sns. Accessed: 31 Jan 2024.

[10] Apple Inc. (2023). Apple push notification service (apns) documentation. https://developer.apple.com/documentation/usernotifications. Accessed: 1 Feb 2024.

[11] Arias Cabarcos, P., Almenárez, F., Gómez Mármol, F., and Marín, A. (2014). To federate or not to federate: A reputation-based mechanism to dynamize cooperation in identity management. *Wireless personal communications*, 75:1769–1786. DOI: 10.1007/s11277-013-1338-y.

[12] Australian FinTech (2022). Baxe partners with idemia and haventec to launch the world's first defi ecosystem secured by facial authentication. [Online]. Available: https://australianfintech.com.au/baxe-partners-with-idemia-and-haventec-to-launch-the-worlds-first-defi-ecosystem-secured-by-facial-authentication/. Accessed on: 25 Sep 2023.

[13] Bai, T., Hu, Y., He, J., Fan, H., and An, Z. (2022). Health-zkidm: a healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*, 22(20):7716. DOI: 10.3390/s22207716.

[14] Belchior, R., Vasconcelos, A., Guerreiro, S., and Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, 54(8):1–41. DOI: 10.1145/3471140.

[15] Bendiab, K., Kolokotronis, N., Shiaeles, S., and Boucherkha, S. (2018). Wip: A novel blockchain-based trust model for cloud identity management. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and*

Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pages 724–729. IEEE. DOI: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126.

[16] Birrell, E. and Schneider, F. B. (2013). Federated identity management systems: A privacy-based characterization. *IEEE security & privacy*, 11(5):36–48. DOI: 10.1109/MSP.2013.114.

[17] Bisogni, F. and Asghari, H. (2020). More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws. *Journal of Information Policy*, 10:45–82. DOI: 10.5325/jinfopoli.10.2020.0045.

[18] Bouras, M. A., Lu, Q., Dhelim, S., and Ning, H. (2021). A lightweight blockchain-based iot identity management approach. *Future Internet*. DOI: 10.3390/fi13020024.

[19] Brandín, R. and Abrishami, S. (2021). Information traceability platforms for asset data lifecycle: blockchain-based technologies. *Smart and Sustainable Built Environment*, 10(3):364–386. DOI: 10.1108/SASBE-03-2021-0042.

[20] Buterin, V. (2016). Ethereum: platform review. *Opportunities and challenges for private and consortium blockchains*, 45:1–45.

[21] Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., and Secundo, G. (2022a). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Information & Management*, 59(7):103508. DOI: 10.1016/j.im.2021.103508.

[22] Centobelli, P., Cerchione, R., Vecchio, P. D., Oropallo, E., and Secundo, G. (2022b). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Information & Management*, 59(7):103508. DOI: 10.1016/j.im.2021.103508.

[23] Chadwick, D. W. and Klingenstein, N. (2016). The permis approach to federated identity and access management. *Computer Standards & Interfaces*, 42:90–103. DOI: 10.1016/j.csi.2015.05.004.

[24] Christensen, D. and Jorgensen, B. (2025). *Identity Theft: Awareness Strategies to Protect Yourself*. New Mexico State University Cooperative Extension Service.

[25] Cocco, L., Tonelli, R., and Marchesi, M. (2021). Blockchain and self sovereign identity to support quality in the food supply chain. *Future Internet*. DOI: 10.3390/fi13120301.

[26] Delgado-Mohatar, O., Fierrez, J., Tolosana, R., and Vera-Rodriguez, R. (2020). Blockchain meets biometrics: Concepts, application to template protection, and trends. *arXiv preprint arXiv:2003.09262*. DOI: 10.48550/arXiv.2003.09262.

[27] DeLiema, M. and Witt, P. (2024). Profiling consumers who reported mass marketing scams: demographic characteristics and emotional sentiments associated with victimization. *Security Journal*, 37(3):921–964. DOI: 10.1057/s41284-023-00401-5.

[28] Deng, J., Guo, J., and Zafeiriou, S. (2019). Arcface: Additive angular margin loss for deep face recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 4690–4699. DOI: 10.1109/CVPR.2019.00482.

[29] Django Software Foundation (2019). The web framework for perfectionists with deadlines. Accessed 20 Aug 2023.

[30] e-Estonia (2023). KSI Blockchain. [Online]. Available: https://e-estonia.com/story/ksi-blockchain/. Accessed on: 05 Sep 2023.

[31] Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., and Xenakis, C. (2023). Inchain: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. *Int. J. Inf. Sec.* DOI: 10.1007/s10207-023-00741-8.

[32] Fernández-Iglesias, M. J., Delgado von Eitzen, C., and Anido-Rifón, L. (2024). Efficient traceability systems with smart contracts: Balancing on-chain and off-chain

data storage for enhanced scalability and privacy. *Applied Sciences*, 14(23):11078. DOI: 10.3390/app142311078.

[33] Feulner, S., Sedlmeir, J., Schlatt, V., and Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets*. DOI: 10.1007/s12525-022-00573-9.

[34] GeeksforGeeks (2023). History of blockchain. [Online]. Available: https://www.geeksforgeeks.org/history-of-blockchain/. Accessed on: 15 Oct 2023.

[35] Ghani, F. A., Shabri, S. M., Rasli, M. A. M., Razali, N. A., and Shuffri, E. H. A. (2020). An overview of the personal data protection act 2010 (pdpa): Problems and solutions. *Global Business and Management Research: An International Journal*, 12(4):559–566.

[36] Ghosh, A., Gupta, S., Dua, A., and Kumar, N. (2020). Security of cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, 163:102635. DOI: 10.1016/j.jnca.2020.102635.

[37] Gilda, S., Jain, T., and Dhalla, A. (2023). None shall pass: A blockchain-based federated identity management system. In *Inventive Computation and Information Technologies: Proceedings of ICICIT 2022*, pages 329–352. Springer. DOI: 10.1007/9789811974021_24.

[38] GitHub Inc. (2023). Github webhooks documentation. https://docs.github.com/developers/webhooks. Accessed: 1 Jan 2024.

[39] Google (2023). Firebase cloud messaging. https://firebase.google.com/docs/cloud-messaging. Accessed: 1 Feb 2024.

[40] Grüner, A., Mühle, A., and Meinel, C. (2021). Atib: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider. *IEEE Access*. DOI: 10.1109/access.2021.3116095.

[41] Han, P., Sui, A., Wu, J., and Wu, J. (2022). Identity management and authentication of a uav swarm based on a blockchain. *Applied Sciences*. DOI: 10.3390/app122010524.

[42] Hinds, J., Williams, E. J., and Joinson, A. N. (2020). "it wouldn't happen to me": Privacy concerns and perspectives following the cambridge analytica scandal. *International Journal of Human-Computer Studies*, 143:102498. DOI: 10.1016/j.ijhcs.2020.102498.

[43] Josang, A. and Pope, S. (2005). User centric identity management. In *Proceedings of the Workshop on Digital Identity Management (DIM'05)*, pages 77–86. ACM. DOI: 10.1145/1102486.1102504.

[44] Kalita, K. P., Kharbhih, J. C., Boro, D., and Bhattacharyya, D. K. (2024). An enhanced blockchain consensus mechanism using proof-of-work and proof-of-stake. In Deka, J. K., Robi, P. S., and Sharma, B., editors, *Emerging Global Trends in Engineering and Technology*, pages 501–511. Springer. DOI: 10.1007/978-981-99-4362-3_46.

[45] Kallela, J. et al. (2008). Federated identity management solutions. In *TKK T-110.5190 Seminar on Internetworking*.

[46] Kassem, J. A., Sayeed, S., Marco-Gisbert, H., Pervez, Z., and Dahal, K. (2019). Dns-idm: a blockchain identity management system to secure personal data sharing in a network. *Applied Sciences*. DOI: 10.3390/app9152953.

[47] Khalil, U., Malik, O. A., Uddin, M., and Chen, C.-L. (2022). A comparative analysis on blockchain versus centralized authentication architectures for iot-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. *Sensors*, 22(14):5168. DOI: 10.3390/s22145168.

[48] Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., and Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and Software Technology*, 51(1):7–15. DOI: 10.1016/j.infsof.2008.09.009.

[49] Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT professional*, 19(4):68–72. DOI: 10.1109/MITP.2017.3051335.

[50] Lai, C., Zhang, P., Chen, Y., Wang, H., and Zhou, W. (2024). Biozero: An efficient and privacy-preserving decentralized biometric authentication protocol on open blockchain. *arXiv preprint arXiv:2409.17509*. DOI:10.48550/arXiv.2409.17509.

[51] Lamport, L., Shostak, R., and Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401. DOI: 10.1145/3335772.3335936.

[52] Lazarova, V. (2023). Working with large objects in application development. *Revista Economică*, 75(2). DOI: 10.56043/reveco-2023-0020.

[53] Lee, S. H. and Yang, C. S. (2018). Fingernail analysis management system using microscopy sensor and blockchain technology. *International Journal of Distributed Sensor Networks*, 14(3):1550147718767044. DOI: 10.1177/1550147718767044.

[54] Lesavre, L., Varin, P., Mell, P., Davidson, M., and Shook, J. (2020). A taxonomic approach to understanding emerging blockchain identity management systems. *arXiv: Cryptography and Security*, pages 57–57. DOI: 10.6028/NIST.CSWP.01142020.

[55] Li, S. Z. and Jain, A. K. (2018). *Encyclopedia of Biometrics*. Springer, 2nd edition. Provides foundational methods in feature extraction, indexing, and optimization for biometric systems.

[56] Liao, C.-H., Guan, X.-Q., Cheng, J.-H., and Yuan, S.-M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems*, 135:450–466. DOI: 10.1016/j.future.2022.05.015.

[57] Lyu, Q., Cheng, S., Li, H., Liu, J., Shen, Y., and Wang, Z. (2022). Nssia: A new self-sovereign identity scheme with accountability. *Cornell University - arXiv*. DOI: 10.48550/arxiv.2206.04911.

[58] López Vivar, A., Castedo, A. T., Sandoval Orozco, A. L., and García Villalba, L. J. (2020). An analysis of smart contracts security threats alongside existing solutions. *Entropy*, 22(2). DOI: 10.3390/e22020203.

[59] Maher, C. A. and Hayes, B. E. (2025). Privacy please: The presence of others and disclosure of identity theft victimization. *Deviant Behavior*, pages 1–20. DOI:10.1080/01639625.2025.2492710.

[60] Maler, E. and Reed, D. (2011). The venn of identity: Options and issues in federated identity management. *IEEE Security & Privacy*, 9(1):16–23. DOI: 10.1109/MSP.2011.2.

[61] Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., Lioy, A., López, D., Santos, H., Gonos, A., et al. (2021). Cybersecurity in ict supply chains: key challenges and a relevant architecture. *Sensors*, 21(18):6057. DOI: 10.3390/s21186057.

[62] Mavridou, A. and Laszka, A. (2018). Tool demonstration: Fsolidm for designing secure ethereum smart contracts. In *Principles of Security and Trust*, pages 270–277. Springer International Publishing. DOI: 10.1007/978-3-319-89722-6_11.

[63] McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., and Granzotto, A. (2016). Bigchaindb: a scalable blockchain database. *BigChainDB*, pages 53–72.

[64] Mohammadzadeh, N., Nogoorani, S. D., and Muñoz-Tapia, J. L. (2021). Decentralized factoring for self-sovereign identities. *Electronics*, 10(12):1467. DOI: 10.3390/electronics10121467.

[65] Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86. DOI: 10.1016/j.cosrev.2018.10.002.

[66] Naik, N. and Jenkins, P. (2017). Securing digital identities in the cloud by selecting an apposite federated identity management from saml, oauth and openid connect. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, pages 163–174. IEEE. DOI: 10.1109/RCIS.2017.7956534.

[67] Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. In *The Ethics of Information Technologies*, pages 141–178. Routledge. DOI: 10.4324/9781003075011.

[68] Omar, I. A., Hasan, H. R., Jayaraman, R., Salah, K., and Omar, M. (2021). Implementing decentralized auctions using blockchain smart contracts. *Technological Forecasting and Social Change*, 168:120786. DOI: 10.1016/j.techfore.2021.120786.

[69] Oracle (2019). Mysql :: Mysql 8.0 reference manual :: 1.3.1 what is mysql? [Online]. Available: https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html. Accessed on: 10 Jan 2024.

[70] Paik, H.-Y., Xu, X., Bandara, H. M. N. D., Lee, S. U., and Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance. *IEEE Access*, 7:186091–186107. DOI: 10.1109/ACCESS.2019.2961404.

[71] Panait, A.-E., Olimid, R. F., and Stefanescu, A. (2020). Identity management on blockchain – privacy and security aspects. *arXiv preprint arXiv:2004.13107*. DOI: 10.48550/arXiv.2004.13107.

[72] Pearson, D. L. (2021). *Chaotic and Unexplored: The Complex Relationship between Security Professionals, Data Breaches, and Malicious Actors*. PhD thesis, University of Fairfax. DOI: 10.6084/m9.figshare.15070371.

[73] Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77. DOI: 10.2753/MIS0742-1222240302.

[74] Rahman, M. M., Tonmoy, M. T. K., Shihab, S. R., and Farhana, R. (2023). Blockchain-based certificate authentication system with enabling correction. *arXiv preprint arXiv:2302.03877*. DOI: 10.48550/arXiv.2302.03877.

[75] Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., Mashat, A., et al. (2022). Blockchain-based trust management framework for cloud computing-based internet of medical things (iomt): a systematic review. *Computational Intelligence and Neuroscience*, 2022. DOI: 10.1155/2022/9766844.

[76] Ratha, N. K., Senior, A., and Bolle, R. M. (2001). Automated biometrics. In Singh, S., Murshed, N., and Kropatsch, W., editors, *Advances in Pattern Recognition*, pages 447–455. Springer Berlin Heidelberg. DOI: 10.1007/3-540-44732-6_46.

[77] Ratzlaff, B. D. (2025). *A life course perspective on childhood adversity, protective factors, and financial fraud vulnerability*. PhD thesis, Kansas State University.

[78] Raul, A. C. (2021). *The privacy, data protection and cybersecurity law review*. Law Business Research Limited.

[79] Sabrina, F., Li, N., and Sohail, S. (2022). A blockchain based secure iot system using device identity management. *Sensors*. DOI: 10.3390/s22197535.

[80] Satybaldy, A., Hasselgren, A., and Nowostawski, M. (2022a). Decentralized identity management for e-health applications: state-of-the-art and guidance for future work. *Blockchain in Healthcare Today*, 5. DOI: 10.30953/bhty.v5.195.

[81] Satybaldy, A., Subedi, A., and Nowostawski, M. (2022b). A framework for online document verification using self-sovereign identity technology. *Sensors*. DOI: 10.3390/s22218408.

[82] Sedlmeir, J., Rieger, J. M., Fridgen, G., and Guggenmos, S. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, 63(5):603–613. DOI: 10.1007/s12599-021-00722-y.

[83] Shahbazi, Z. and Byun, Y.-C. (2021). Integration of blockchain, iot and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors*, 21(4):1467. DOI: 10.3390/s21041467.

[84] Shaker, M., Shams Aliee, F., and Fotohi, R. (2021). Online rating system development using blockchain-based distributed ledger technology. *Wireless Networks*, 27(3):1715–1737. DOI: 10.1007/s11276-020-02514-w.

[85] Sharma, G., Singh, P., Chauhan, N., and Dhiman, G. (2023). A survey on blockchain deployment for biometric systems. *IET Blockchain*, 3(4):251–265. DOI: 10.1049/blc2.12063.

[86] Shuhan, M. K. B., Hasnayeen, S. M., Das, T. K., Sakib, M. N., and Ferdous, M. S. (2023). Decentralised identity federations using blockchain. *arXiv preprint arXiv:2305.00315*. DOI: 10.48550/arXiv.2305.00315.

[87] Soltani, R., Nguyen, U. T., and An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, 2021:8873429. DOI: 10.1155/2021/8873429.

[88] Srinath, K. R. (2017). Python–the fastest growing programming language. *International Research Journal of Engineering and Technology*, 4(12):354–357.

[89] Sullivan, C. and Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*, 33(4):470–481. DOI: 10.1016/j.clsr.2017.03.016.

[90] Sun, J., Yao, X., Wang, S., and Wu, Y. (2020). Blockchain-based secure storage and access scheme for electronic medical records in ipfs. *IEEE Access*, 8:59389–59401. DOI: 10.1109/ACCESS.2020.2982964.

[91] Torky, M. and Hassan, A. R. (2020). Integrating blockchain and the internet of things in a secure healthcare system: A review and roadmap. *Future Generation Computer Systems*, 110:883–897. DOI: 10.1016/j.future.2020.04.047.

[92] Vaz, R., Shah, V., Sawhney, A., and Deolekar, R. (2017). Automated big-o analysis of algorithms. In *2017 international conference on nascent technologies in engineering (ICNTE)*, pages 1–6. IEEE. DOI: 10.1109/ICNTE.2017.7947882.

[93] W3C (2022). Decentralized identifiers (dids) v1.0: Core architecture, data model, and representations. https://www.w3.org/TR/did-core/.

[94] Woodside, J. M., Augustine Jr, F. K., and Giberson, W. (2017). Blockchain technology adoption status and strategies. *Journal of International Technology and Information Management*, 26(2):65–93. DOI: 10.58729/1941-6679.1300.

[95] Xiang, X., Wang, M., and Fan, W. (2020). A permissioned blockchain-based identity management and user authentication scheme for e-health systems. *IEEE Access*. DOI: 10.1109/access.2020.3022429.

[96] Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W. J., and Imran, M. A. (2020). Beeptrace: Blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond. *IEEE Internet of Things Journal*, 8(5):3915–3929. DOI: 10.1109/JIOT.2020.3025953.

[97] Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*. DOI: 10.6028/NIST.IR.8202.

[98] Zhao, B., Guo, Y., and Bi, J. (2020). Efficient parallel processing strategies for deep learning-based biometrics. *IEEE Transactions on Information Forensics and Security*, 15:3447–3460. DOI: 10.1109/TIFS.2020.2986137.

[99] Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE. DOI: 10.1109/BigDataCongress.2017.85.

[100] Zhuang, Y., Shyu, C.-R., Hong, S., Li, P., and Zhang, L. (2023). Self-sovereign identity empowered non-fungible patient tokenization for patient-centric health

information exchange using blockchain technology. *Computers in Biology and Medicine*, 157:106778. DOI: 10.1016/j.compbiomed.2023.106778.