الجمهورية الجزائرية الديمقراطية الشعبية

Democratic People's Republic Of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry Of Higher Education And Scientific Research

جامعة العربي التبسي - تبسة

University Larbi Tebessi – Tebessa –

Faculty of Science and Technology

Département of Electronic and Telecommunication



le 16/06/2025

DISSERTATION

Presented for the obtaining of the **Academic Master's degree**

In : Telecommunications

Speciality : Network and Telecommunications

By : Gouasmia Aya and Rabah Malak

Subject

Blockchain-Enabled Biometric Template Protection: A secure Authentication Framework

Presented and evaluated on 10/06/2025, by the jury composed of :

Ms. Hanane DJELAB	MCA	President
M. Abdallah MERAOUMIA	Prof.	Supervisor
Ms. Chaima AOUICHE	MCB	Examiner

Promotion : 2024/2025

ACKNOWLEDGEMENTS

First of all, our most sincere praise and thanks go to Almighty God for his countless blessings, especially for the patience, strength and perseverance that he has given us throughout this memory. It is through His mercy and support that we have been able to complete this work.

Secondly, we would like to thank our supervisors, **Professor ABDALLAH MERAOUMIA** and **Dr. YACINE BELHOCINE**. For their constant support, availability, scientific rigor and sound advice have been a valuable source of learning for us. Their confidence and encouragement have allowed us to progress and give our best.

We also thank the members of the jury for agreeing to evaluate our work, and all the teachers who, over the years, have contributed to our academic and personal formation.

Family, friends, colleagues – you have been the refuge in times of turbulence. Thank you for your discreet sacrifices, your encouragement, and this light that you have maintained even when ours was flickering.

To all those whose conversations, fleeting advice or mere presence have nourished this project: this achievement is also yours.

G. Aya et R. Malak

الحمدالله عدد ما أنعم علينا

وعدد مازرع في قلوبنا أملا وعدد مامهد لنا السبل لنصل.

اليوم ... أقف وأنا أحمل بين يدي ثمار أعوام من السعي ومشاعر لا توصف.

ليال سهرت وأيام مضت بين تعب وأمل. لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون لم يكن

الحلم قريبا ولا الطريق كان محفوفا بالتسهيلات لكني فعلتها ...

أما بعد ...

أهلا بمن شاركني فرحة عمري وسعى ليكون جزءا من يومي الأجمل.

أهلا بمن زاد حضوره المعنى وزين اللحظة وخلدها في ذاكرتي هذا اليوم ليس عاديا هذا يوم النهاية والبداية يوم نطوي فيه صفحة لتفتح بعدها فصول جديدة نحمل فيها ماتعلمناه وما عشناه ونمضي بثقة أكبر.

أهدي تخرجي الى روح أبي الغالية...الذي غاب جسده ولم تغب روحه عني لحظة الى من علمني

أن الطموح لا حدود له وأن الإصرار طريق النجاح هذا الإنجاز ثمرة غرسك وعبير دعائك ونور سيرتك أتمنى أن تصلك مشاعري وتفتخر بمن حملو اسمك أثبتو أنك خير مربي وخير معلم وخير أب وخير فقيد.

أهدي تخرجي الى جنة فوق الأرض أمي...الى من علمتني الأخلاق قبل الحروف الى الجسر الصاعد بي الى الجنة الى الداعمة الأولى في حياتي واليد الخفية التي تبتعد عن طريقي الأشواك والمصاعب.

أهدي تخرجي الى ملهمي ونجاحي أخواتي واخواني...من ساندني بكل حب عند ضعفي وأزاح عن طريقي المتاعب سندي وكتفي الذي أستند عليه دائما طالما كانوا الظل لهذا النجاح.
الى صديقاتي ...من تقاسمتم معي اللحظات الحلوة والمرة وكنتم لي اخوة قبل أن تكونوا أصدقاء شكرا لذكرياتكم الجميلة.

(ممتنة اليكم جميعا ماكنت أصل لولا فضلكم علي من بعد الله)

Gouasmia Aya

بسم اللَّه الرَّحمان الرَّحيم

{يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ}

أُهدي تخرجي هذا إلى:

لمن استنزف من روحه قُبَالَ مثولي أمامكم هنا ...لمن أفنى عمره ليجعل من طريقي وردًا ...لمن سهر تعبًا لأنام على وساد الراحة ...لمن كان حضوره الصامت اطمئنانًا ...أبي عزيز الروح... زادني ارتباط اسمي باسمك فخرًا .

لمن حملتني بين طيّات قلبها قبل الأحضان ...لمن كانت لي نبع قوة، ثقة، وأمان ...لمن علمتني أن لا يأس مع الحياة، ولا حياة مع اليأس ...أمي غلا الروح... يكفيني شرفًا أنني قطعة منكِ، يا قطعة من قلبي .إلى أختاي، حبيبتا قلبي، أنيستا حياتي ...لمن كانتا مداد الصبر في مسيرتي، وملجأً ساكنًا لروعاتي" ...هندة صنية"، أدامكما الله فرحة في حياتي.

إلى سندي في هذه الحياة ...إلى من أعلو شامخة حين تذكر أسماءهم ...إلى إخوتي: "تقي الدين &عبد الحليم &كمال ..." سر قوتي وحلو حياتي... كفاني عزَّة أن رزقت بكم إخوة....حفظكم الله، ولا أراني فيكم مكروهًا.

إلى صديقاتي، رفيقات الروح، ساكنات القلب، مبهجات الحياة ...إلى من جمعتني بهنّ لحظات صدق أمتنُ لها: "آية – منار – سهام – وصال – إسراء – عزيزة ..." جمعني الله وإياكن في جناته.

إلى كل من كان لي من وقته حصة لمواساتي في هذا ...المسار أهلاً كانوا، أحبة، أم أصدقاء...

Rabah Malak

Table of Contents

Acknowledgment I
Dedication II
Table of contents IV
List of figures VI
List of tables VII
List of Abbreviations VIII
Abstract X
General Introduction 1

Chapter I: Information Security in the Digital Age

Introduction 5
I.1 Information Security 5
I.1.1 Core principles 5
I.1.2 Cryptographic Techniques 6
I.1.3 Steganography 7
I.1.4 Watermarking 7
I.2 Blockchain Technology 7
I.2.1 Blockchain Principles 8
I.2.2 Core Components 8
I.2.3 Types of blockchain 11
I.2.4 Consensus Mechanisms 12
I.3 Biometric Technologies 13
I.3.1 Biometrics Categories 13
I.3.2 Biometric System 15
I.3.3 Biometrics in Information Security 16
I.4 Security Threats 17
I.4.1 Threat in Biometric Systems 17
I.4.2 Attacks in Blockchain Networks 18
Conclusion 19

Chapter II: Innovative Approaches to Enhance Protection

Introduction 21
II.1 Reinforcing Security 21
II.1.1 Secure Identity Management 22
II.1.2 Decentralized Control 23
II.1.3 Biometrics for Multi-Factor Authentication 23
II.2 Biometric Revocability 24
II.2.1 Biometric Revocation Techniques 25
II.2.2 Fuzzy Vault and Fuzzy Commitments 25
II.2.3 Biometric Hashing and Encryption 26
II.3 **Proposed System** 26
II.3.1 User Authentication Phase (UAP 28

II.3.2 Data Validation Phase (DVP) 28
II.3.3 Blockchain Integration Phase (BIP) 28
II.4 Materials and Methods 29
II.4.1 Contrast Limited Adaptive Histogram Equalization 29
II.4.2 Steerable filter 29
II.4.3 Histogram of Oriented Gradients 29
II.4.4 Self-attention 30
II.4.5 FDA Optimizer 30
II.4.6 Ethereum Blockchain 31
II.4.7 Ganache Blockchain 31
II.4.8 InterPlanetary File System 31
II.4.9 Smart Contracts 32
II.5 Biometric Feature Extraction Approach 32
II.6 Blockchain-Enabled Dual-Layer Template Protection Framework 34
Conclusion 35

Chapter III: ***Experimental results***

Introduction 37
III.1 Biometric System Configuration 37
III.1.1 FKP Region Of Interest Extraction 38
III.2 Blockchain Configuration 42
III.3 Biometric System Performance Evaluation 42
III.3.1 Preliminary results 43
III.3.2 Overall System Performance 46
III.3.3 Optimized System Performance 47
III.3.4 Multi-Modality System Performance 48
III.3.4 Biometric System Security Evaluation 49
Conclusion 50

General Conclusion 52

Bibliography 54

List of figures

Figures		Page
I.1	Blocks structure	10
I.2	Construcing a Merkle Tree	11
I.3	Different biometric modalities	13
I.4	Physiological Biometrics	14
I.5	Behavioral Biometrics	14
I.6	Authentication of a person in a biometric system	15
I.7	Authentication of a person in a biometric system	16
II.1	Proposed system using blockchain and biometrics	27
II.2	Proposed Biometric Feature Extraction system	33
III.1	Filtering and down-sampling of finger image	39
III.2	Determining the X axis	39
III.3	Extracted sub-image before ROI extraction	39
III.4	Image of the contours obtained	40
III.5	Curves on the finger image.	40
III.6	Image obtained by applying convex direction coding	40
III.7	Determining the Y axis	41
III.8	ROI location in the finger image	41
III.9	ROI extraction from finger image	41
III.10	Impact of Filter Size and Filter Number with HOG Regions =9 on Biometric System Performance	44
III.11	Impact of Filter Size and Filter Number with HOG Regions =25 on Biometric System Performance	44
III.12	Impact of Filter Size and Filter Number with HOG Regions =49 on Biometric System Performance	45
III.13	Performance of Biometric Identification System, (a) Open-set biometric identification, and (b) Closed-set biometric identification	46
III.14	Optimized of Biometric Identification System, (a) Open-set biometric identification, and (b) Closed-set biometric identification.	47

List of tables

Page

III.1 Multi-Modality Feature Fusion Results 49
III.2 Fuzzy Vault Security Test 49

LIST OF ABBREVIATIONS

The following terms, in alphabetical order, are used in the text.

AIC	**:**	Central Intelligence Agency
DLT	**:**	Distributed Ledger Technology
ID	**:**	IDentity
POW	**:**	Proof of Work
POS	**:**	Proof of Stake
MitM	**:**	Man-in-the-Middle
P2P	**:**	Peer-to-Peer
AI	**:**	Artificial Intelligence
IOT	**:**	Internet of think
PII	**:**	Personally Identifiable Information
GDPR	**:**	General Data Protection Regulation
PINs	**:**	Personal Identification Numbers
IPFS	**:**	InterPlanetary File System
RB-AC	**:**	Role-Based Access Control
UAP	**:**	User Authentication Phase
DVP	**:**	Data Validation Phase
RSA	**:**	Rivest–Shamir–Adleman (public-key cryptosystem)
ECC	**:**	Elliptic Curve Cryptography
CID	**:**	Content Identifier
DVP	**:**	Digital Video Protocol
BIP	**:**	Bitcoin Improvement Proposal

CLAHE : Contrast Limited Adaptive Histogram Equalization

CDF : Cumulative Distribution Function

HOG : Histogram of Oriented Gradients

FDA : Food and Drug Administration

GUI : Graphical User Interface

CLI : Command-Line Interface

DHTs : Distributed Hash Tables

DAGs : Directed Acyclic Graphs

Abstract

Information security has quickly risen to the top of the priority list in the digital world due to our increasing reliance on interconnected operating systems and data sharing over networks for just about everything. Identity proof and access control are fundamental to the protection of our digital assets; thus, this research illustrates a concept to develop an innovative solution utilizing combined biometric and blockchain technologies to provide enhanced user template protection and reliably authenticate user identity.

The system utilizes the extracted biometric traits from finger joint fingerprint images using current methods of image processing such as HOG in conjunction with modern encryption approaches to safeguard the biometric template. Our solution also offered blockchain technology to ensure data integrity and offers a trustworthy and decentralized authentication mechanism. High recognition accuracy and efficiency of the system demonstrate the concept that could provide a solution to persistent security problems that exist today

Key words : Information Security, Biometrics, Template Protection, Blockchain, HOG.

Résumé:

La sécurité de l'information est rapidement devenue une priorité majeure dans le monde numérique en raison de notre dépendance croissante aux systèmes interconnectés et au partage de données via les réseaux pour pratiquement toutes les activités. La vérification de l'identité et le contrôle d'accès sont fondamentaux pour la protection de nos actifs numériques ; ainsi, cette recherche présente une preuve de concept visant à développer une solution innovante combinant les technologies biométriques et la blockchain pour renforcer la confidentialité des données et authentifier l'identité de manier fiable.

Le système exploite les caractéristiques biométriques extraites des images des articulations digitales à l'aide de techniques modernes de traitement d'image, telles que HOG, associées à des méthodes de chiffrement avancées pour protéger le gabarit biométrique. Notre solution intègre également la technologie blockchain afin de garantir l'intégrité des données et d'offrir un mécanisme d'authentification fiable et décentralisé. Le taux de reconnaissance élevée et l'efficacité du système démontrent la validité de cette preuve de concept, qui pourrait répondre aux défis de sécurité actuels.

Mots-clés : Sécurité de l'information, Biométrie, Protection des modèles, Blockchain, HOG.

ملخص

أصبحت أمن المعلومات أولوية قصوى في العالم الرقمي بسبب الاعتماد المتزايد على الأنظمة المترابطة وتبادل البيانات عبر الشبكات في جميع جوانب الحياة. تُعد عملية التحقق من الهوية والتحكم في الوصول أساسية لحماية أصولنا الرقمية؛ ولذلك، يقدم هذا البحث نموذجًا أوليًا لحل مبتكر يجمع بين تقنيات القياسات الحيوية وتقنية البلوك تشين لتعزيز خصوصية البيانات والتحقق من هوية المستخدمين ومصداقيتهم.

يعتمد النظام على استخراج السمات الحيوية من صور مفاصل الأصابع باستخدام تقنيات معالجة الصور الحديثة مثلHOG ، إلى جانب استخدام أساليب تشفير متقدمة لحماية القوالب الحيوية. كما تم دمج تقنية البلوك تشين لضمان سلامة البيانات وتوفير آلية موثوقة ولا مركزية للمصادقة. وتُظهر دقة التعرف العالية وكفاءة النظام فعالية هذا النموذج الأولي الذي يمكن أن يسهم في حل مشكلات الأمان الحالية.

الكلمات المفتاحية: أمن المعلومات، القياسات الحيوية، حماية القوالب، الترابط.

General Introduction

General Introduction

Information security has become a key principle for protecting the private information of individuals and organizations in the face of the rapid digital revolution. Through mechanisms such as symmetric (AES, RC6) and asymmetric (public/private keys) encryption, as well as hash functions (SHA-256), encryption techniques act as a defensive barrier against breaches. [1] However, these technologies also entail limitation, such as computational complexity and key management. Blockchain technology proposes to redefine trust in the digital space through "consensus mechanisms" (e.g., "proof of work" (PoW) and "proof of stake" (PoS)) and to establish digital trust through the decentralization of records and the immutability of transactions. [2] Like any system, it carries risks, such as vulnerabilities in smart contracts or a 51% attack. To secure identity, biometric systems can use behavioral (e.g., voice, gestures) or physiological (e.g., fingerprints, iris) characteristics, but can be vulnerable to biometric template attacks and identity theft. [3]

Chapter two explores in greater deph into the data security and cybersecurity technologies and innovations mentioned in chapter one. It also discusses the potential of blockchain technology, a decentralized and innovative tool for managing digital transactions and data. It explores concepts such as consensus protocols, decentralization, and the integration of new technologies, such as artificial intelligence and the Internet of Things, to better address cyber threats and improve cybersecurity systems.

It also explores how to ensure rights and fairness through developments in digital identity management using biometric identification techniques that offer a higher level of security and privacy. It also recognizes cryptographic activities such as encryption and hashing to ensure the confidentiality and integrity of sensitive information. It addresses the availability of services for smart contract applications deployed on blockchain platforms such as Ethereum, as well as development services such as those used by Ganache developers to create smart contracts and decentralized applications on the Ethereum blockchain.

Chapter two highlights the importance of collaboration between various stakeholders within the organization to address common challenges and establish a more secure digital environment. Furthermore, chapter two emphasizes the need for governance frameworks and regulatory provisions to balance the pace of rapid technological advancements with reliable policies to open up an innovative and accessible digital landscape. [4]

With the continued development of information security and digital identity aspects, this research aimed to evaluate the performance of a state-of-the-art decentralized biometric recognition system, designed to improve the security and reliability standards of personal data and digital identities. This research was conducted in a context of growing need for technological solutions combining encryption algorithms, blockchain and biometric recognition methods to secure identity verification procedures, while reducing the risks associated with fraud or data breaches. The empirical analysis methods used in this study measured the system's performance in terms of speed, accuracy and data security, and focused on identifying operational parameters to achieve an optimal balance between efficiency and security. This approach examines how advances in the design of cybersecurity systems, the construction of a state-of-the-art framework that applies advanced investigation methods, scientific conventions and advanced algorithms for identity verification, can make it possible for workers to achieve a reliable and trustworthy identification method in complex digital environments.

The manuscript is organized into three chapters:

Chapter one provides an overview of information security, including the fundamental concepts and methods of watermarking, encryption, and steganography; blockchain technology, including the fundamental elements, types, and consensus mechanisms; and biometric technologies, including the types of biometrics and biometric systems, biometrics in information security, threats in biometric systems, and attacks on Blockchain networks.

Chapter two outlines the growth of the protection of digital systems with a focus on blockchain technologies. The chapter dives into reinforcing information security and biometric revocability. Further still, this chapter presents an architecture for a digital health system that is intended to help instill more secure, trustworthy, privacy-oriented digital systems.

The final chapter illustrates the viability and applicability of our work through step-by-step explanations for experimental design, implementation, and evaluation results. The chapter discusses the dataset that we utilized, the configuration of our blockchain-based system, and the performance metrics which we analyzed to determine accuracy of the proposed system , proving the viability and robustness of our work on realizing secure and privacy-preserving digital ecosystems.

Chapter 1

Information Security in the Digital Age

Summary

This chapter focuses on the risk of cybersecurity in the digital period. It explores three technologies: cryptological processes, blockchain, and biomimetic systems. It focuses on core principles of information security (confidentiality, integrity, and reliable access) and many of the processes involved, such as symmetric and asymmetric counting, hashing, steganography, and digital tattooing. It also points out emerging threats such as hacking and exploits. The chapter closes with the necessity of fully formed cybersecurity solutions that are equal, balanced, robust, and ethical.

Introduction

I.1 Information security

I.2 Blockchain Technology

I.3 Biometric Technologies

I.4 Security Threats

Conclusion

Introduction

This chapter discusses the relevance of information security in the digital age with emphasis on cryptographic techniques, blockchain technology, and biometric systems. It expounds on their security risks and how they ensure data confidentiality, integrity, and availability. Blockchain technology, via its decentralization, revolutionizes trust in digital transactions but faces constraints like consensus protocol manipulation and Sybil attacks. Biometric systems, depending on unique physiological traits, are vulnerable to spoofing and privacy invasion. The chapter demands the implementation of robust security measures to mitigate threats and answer evolving threats in an interdependent world.

I.1 Information Security

Information security, often shortened as InfoSec, is essential to protect sensitive data, whether for individuals or institutions. It entails a range of methods and processes to deter access, use or unauthorized disclosure of information, e.g., protecting data in electronic formats; against all forms of infringement, and also the guarantee of conformity with regulations in force. [1]

It aims to minimize business risks, maximize returns on investments, exploit opportunities, and ensure business continuity. Information security considers the integrity, confidentiality, and availability of information resources, regardless of data type. [2]

I.1.1 Core principales

The AIC (Central Intelligence Agency) triad or availability, integrity, and confidentiality are the three basic concepts of security. Every company has special security objectives and

needs, and every security panel, mechanism, and safeguard is enforced to pursue these concepts. [35]

- **Confidentiality:** By preventing unauthorized users from accessing and entering information sources, it prevents information from spreading in an unauthorized manner. To make sure of this, you have to keep an eye on access to data and encrypt it to improve security and protection throughout the transmission or storage process, while giving authorized individuals access to the data and decryption keys.
- **Integrity:** Its main goal is to ensure that data is uncontaminated and clean during both uploading and storage. This entails ensuring that only authorized users make changes.
- **Availability:** Refers to maintaining data accessibility, meaning that an authorized user can access data or information whenever they need to. It may appear to conflict with confidentiality or even be mistaken for it at times. [3]

I.1.2 Cryptographic Techniques

Cryptography is the art and science of protecting information from unwanted person and converting it into a form undistinguishable by its attackers though stored and transmitted. The main aim of cryptography is keeping data secure form unauthorized persons. Data cryptography mostly is the scramble of the content of data, such as text data, image related data and audio, video related data to compose the data illegible, imperceptible or unintelligible during communication or storage. In Encryption, the data, denoted as plaintext, is transformed into illegible gibberish, denoted as ciphertext, with the help of an encryption key. The reverse of data encryption process is called data Decryption. [5]

- **Symmetric encryption:** The most basic type of encryption with a single secret key is a symmetric algorithm. Before sending any messages, the sender and recipient must exchange this key, which is used for both encryption and decryption. With the same secret key, the plaintext can be obtained once the message has been encoded. Therefore, as long as the private key is kept safely and secretly, the message is secure. These algorithms, which include AES, RC6, and Blow Fish, can cipher the message either one block at a time, as in block ciphers, or one bit at a time, as instream ciphers. [4]
- **Asymmetric encryption:** On the other hand, the issue of sharing the secret key can be resolved by asymmetric schemes. An asymmetric scheme is a relatively new type of encryption that uses a pair of keys: (1) a public key that is widely known, and (2) a private key that is kept in private. The message is encrypted using one key, and the

original plaintext can be restored using the other key. In summary, if we use a private key to encrypt the message, the only way to recover the plaintext is to use the corresponding public key. Conversely, if we use a public key to encrypt the plaintext, we will use the secret key to restore the message to its initial value. However, the entire process is computationally demanding, which is the issue. [4]

- **Hash Function:** Hash Function: A cryptographic hash function randomly converts an arbitrary-length binary input into a fixed-length binary output, such as an image. Using a secure hash function (such as SHA-256), it is computationally impossible to reconstruct the input from the output image. Furthermore, there is very little chance that two different inputs will result in the same output. [15]

I.1.3 Steganography

The art of steganography involves concealing the existence of data by transmitting it through seemingly harmless carriers. Steganography and cryptography are generally closely related. Steganography, on the other hand, will conceal the message so that its existence is never known, whereas cryptography jumbles messages to make them difficult for an unauthorized individual to understand. A person or people will not try to decrypt the information if they view the object that contains the hidden information because they will not be aware that it is hidden. [6]

I.1.4 Watermarking

The process of embedding information known as a watermark—also referred to as a digital signature, tag, or label—into a multimedia object so that it can be later identified or extracted to provide information about the object is known as watermarking. The item could be a picture, sound, or video. A visible "seal" over an image to indicate copyright would be a basic example of a digital watermark. The identity of the buyer of a specific copy of the item, however, may be among the extra details included in the watermark. The watermark is either invisibly or visibly embedded, depending on its intended use. [7]

I.2 Blockchain Technology

Blockchain is a way of storing data so that it becomes difficult or impossible to change, hack, or trick the system.

A blockchain is essentially a digital ledger of transactions that is replicated and shared to all the computer systems on the blockchain. Every block in the chain contains a batch of transactions, and with every new transaction on the blockchain, a record of such a

transaction is entered into participant's ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology(DLT).

Blockchain is a type of DLT in which transactions are stored with an immutabal cryptographic signature known as a hash. [8]

I.2.1 Blockchain Principals

Since Bitcoin's advent in 2009, blockchain software architectures that meet various technical, business, and legal design decisions have been developed. Some of the underlying principles are decentralization of information, transparency, and immutability. [38]

- **Decentralization:** For Blockchain transactions to be executed and validated, the majority of participating nodes must concur. These transactions are replicated on every node in a ledger. This eliminates the necessity for intermediaries to exchange and retain transaction data.
- **Immutable:** Each block's hash value is distinct. Every block has both its own hash address and the hash address of the block before it. Because blocks are distributed globally, any node that tries to modify block data must change data everywhere. Furthermore, since a change in one block will result in a different hash value, rendering all subsequent blocks invalid, it must alter every block. As a result, each new block in the blockchain reinforces the previous block's verification. As a result, information on the Blockchain is tamper-proof and irreversible since it can never be changed in an existing block.
- **Transparency:** Only when most of the entities agree with one another can the distributed ledger be changed. Additionally, the networks changes are visible to the public in order to guarantee security and transparency. [16]

I.2.2 Core Components

The block header and the block body are the two components that make up a block. As previously stated, every block is connected to its parent or preceding block to form a chain. The parent block is absent from the first block, also known as the genesis block. In this case, the header of each block contains the hash of that block**.**

1. Block header: The block header stores metadata for a block, including its hash, timestamp, previous block address, number of bits, and nonce. The genesis node is the first

block and has no previous block header address but is considered the first of the blockchain. Previous block addresses verify the completeness and integrity of the blockchain.

The block header, on the other hand, consists of the following data:

- **Version of the block:** This indicates the set of validation rules the block follows in the blockchain. It is a 4-byte integer.
- **Hash of the previous block:** A SHA256 hash of the most recent block is stored in the block header. It is a 32-byte character string. Previous block address facilitates maintaining the integrity of the blockchain.
- **Merkle Root Hash:** Merkle root hash is also a SHA256 hash. It is derived from the hash of each transaction included in the block. It is also a 32-byte character value.
- **Timestamp:** The timestamp is an unsigned integer, 4 bytes long. It is in Unix Epoch Time format. The timestamp of a block must should always be greater than the median of the time stamp of the last 11 blocks and the interval cannot exceed two hours.
- **Target:** A target limit is maintained in encoded format. It is a 4- byte unsigned integer value.
- **Nonce:** Itis a random value that miners alter to generate the hash of block such that the value is lower than the target threshold. It is a 4-byte unsigned integer value. [40]

2. Block body: The body of a block consists of mainly two parts:

2.1. Transaction counter: The transaction counter contains the number of transactions of a block.

2.2. Transaction: A transaction refers to a send-and-receive message between a receiver and a sender to exchange an asset within a blockchain network with the block size determining the number of transactions that it carries. There are certain features of a transaction:

- **Amount:** Amount is the numerical value that a sender must send.
- **Input:** Input basically refers to the definition of the digital asset, who wishes to transfer. Here, the digital asset ought to be completely identified and have values that are unique from other assets.

- **Output:** has the receiver's account information. It has the value of the digital asset and the Identity (ID) of the receiver. Further, the output has some rules which the receiver should not violate to receive the corresponding value.
- **Transaction ID or hash:** Each transaction features a unique hash or transaction ID that serves as the basis for a digital signature based on public-key cryptography. [24]

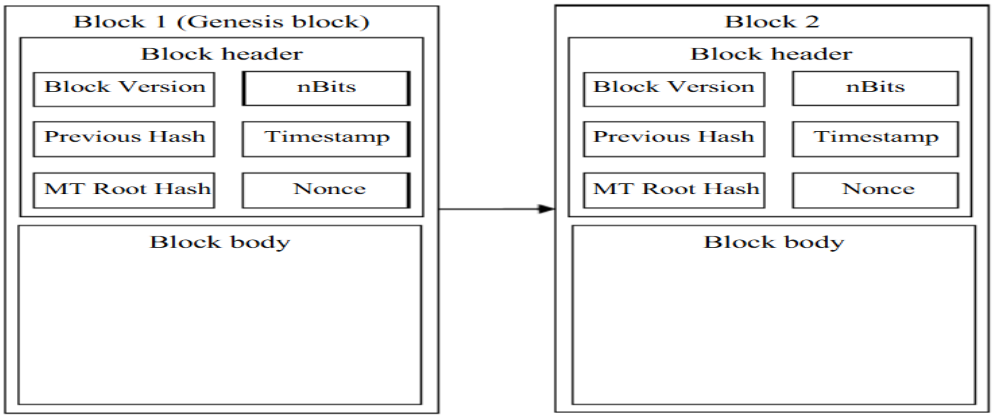


Fig. I.1 Blocks structure [24]

3. Merkle Tree

Representation of Merkle Tree, where hA and hB represent cryptographic hash functions of nodes A and B. h(hA,HB) is the combined hash function of nodes A and B. A, B, C, and D represent the leaf nodes of the Merkle tree.

Are used for efficient storage and authentication of large collections of data. Leaf nodes in the data structure store the blockchain transaction's hash, and non-leaf nodes store cryptographic hashes of labels of their child nodes. The Merkle root, which is the tree's root, stores the hash of all the transactions in a block. Root of Merkle tree is a value of commitment and otherwise can be thought of as a vector commitment. The leaf nodes of the Merkle tree collectively convey the message. Each sister node along the path from leaf node to root node and the leaf nodes form a proof of opening of vector commitment. A traditional blockchain authenticates the consistency and accuracy of data using the opening proof of the Merkle tree. [10]

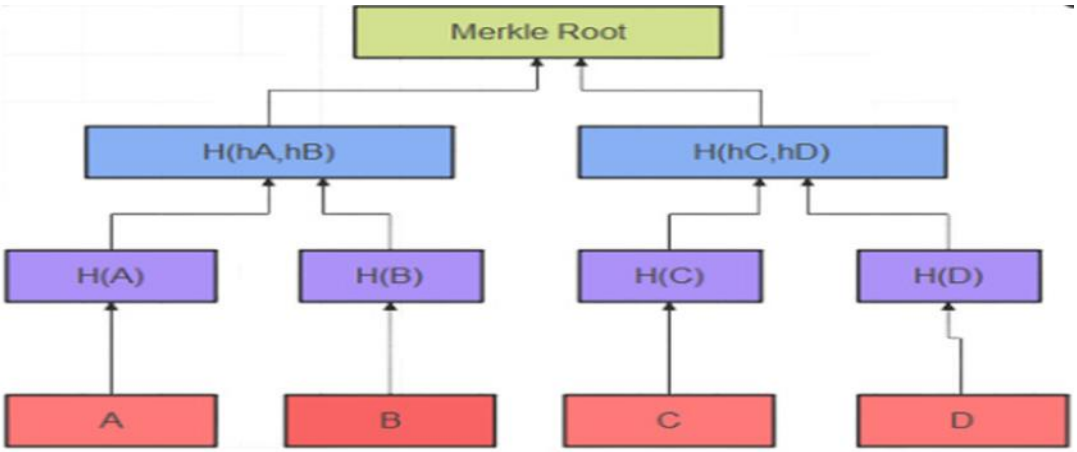


Fig. I.2 Constructing a Merkle Tree [10]

I.2.3 Types of blockchain

There are four different types of blockchain networks depending on demand, preference, and priority. [42]

A brief overview of the four different types of blockchain networks is given below:

1. Private blockchain: Businesses usually use private blockchain networks, which are closed and governed by an organization, to exchange data. These networks' nodes are well-known and rely on trust; they don't check transactions. The network owner makes decisions and the consensus algorithm is not commonly used. The central authority establishes the rules and regulations, which users manage through contracts they sign when they join. Compared to public blockchains like Ripple, private blockchains operate more quickly.

2. Public blockchain: Anyone can join a public blockchain network as a node to mine and take part in the consensus process. In this case, nodes can join, read, and write data into the network without requesting permission from other nodes. Any data can be written to the public blockchain using cryptographic rules, and miners validate transactions. No third parties or developers are interfering with the public blockchain, which is completely decentralized. Nevertheless, this kind of blockchain has slower transaction speeds. One well-known public blockchain network is Bitcoin.

3. Consortium Blockchain: The purpose of this blockchain network is to overcome the drawbacks of the private blockchain. In this case, a group of members governs the blockchain network rather than a central authority. In this case, a pre-selected group of nodes controls the consensus mechanism and process and has the power to determine every

aspect of a consortium blockchain network. As a result, multiple entities are in charge rather than just one. Businesses like government agencies, ports, banks, and others need the flexibility to bring in neutral partners or entities, which a consortium offers. [24]

4. Hybrid blockchain: Is a combination of both public and private blockchain. Hybrid blockchain architecture is not available to the world but also offers blockchain functionality such as security, transparency, and integrity. Participants on the hybrid blockchain can decide who can remain on the blockchain or about whose transactions details will be available. This is the best of both worlds and offers a company an opportunity to involve its stakeholders in the best possible way. [12]

I.2.4 Consensus Mechanisms

The consensus mechanism is the most crucial of these fundamental technologies. One could argue that the consensus mechanism is the foundation of a blockchain system and that it is its lifeblood. The degree of trust between nodes in the entire block chain system is primarily determined by the consensus mechanism, which also determines other users' levels of trust in the data on the chain. A collection of techniques known as the "consensus mechanism" helps participants come to a shared understanding. It also refers to the consensus algorithm. [11], The primary ones are:

1. Proof of Work (PoW): It is utilized primarily by Bitcoin, Ethereum, and numerous other public blockchains. It was the first ever consensus mechanism developed. It is always considered the most secure and most reliable of all the consensus mechanisms, although there are scalability concerns. In PoW, miners just compete to see who can find very hard mathematical puzzles using massive machines. The fastest one to come up with the 64-digit hexadecimal number ('hash') wins and has the privilege of creating the new block and affirm the transactions. The successful miner is also rewarded with a predetermined amount of crypto, known as a ‘block reward’. As it requires large amounts of computational resources and energy in order to generate new blocks, the operational costs behind PoW are notoriously expensive. High power consumption is the most common criticism against PoW. It has led many to a more eco-friendly, energy-aware consensus protocols, such as proof of stake (PoS). [12]

2. Proof of Stake (PoS): Within a proof of stake (PoS) system, miners need to own a 'stake' of cryptocurrency in order to be considered for selection randomly to become a

validator. It is not much different than a lottery where the bigger coins you have in your stake, the better your odds. Unlike in PoW where miners are incentivised by block rewards (newly generated coins), those who contribute to the PoS system simply earn rewards. This enables faster and lower-cost transactions. [12]

I.3 Biometric Technologies

Biometrics is an activity to confirm the identity of an individual on the on the basis of morphological, biological and behavioural characteristics of the body human (fingerprint, face, iris., etc.), or otherwise, it enables the identification or authentication of an individual on the grounds of identifiable data and The Commission's own verifiables.

The most common is fingerprint recognition, where multi-spectral sensors provide higher accuracy. Finger veins, palm veins, face, and iris are a few others. Multiple detection techniques are utilized by some systems, but not all. [13]

I.3.1 Biometrics Categories

Nowadays, there exists a large number of biomethic modalities, each with its specifics and its difficulties. Common modalities include face, speech, digital interfaces, eye contour, and eye iris, whereas uncommon modalities include veins, DNA, body odor, ear shape, and stroke. The BIOMET project enables comparative testing of various capteurs and assessment of their fusion performance. [14]



Fig. I.3 Different biometric modalities. [19]

1. Physiological: Physiological biometrics are bodily measurements of the human body, for example face, fingerprint, hand-geometry, ear, iris, retina, DNA, palmprint, hand and finger vein etc. The recognition system that uses physiological traits has a comparatively high accuracy.

In addition, the use of physiological biometrics introduce unwavering identification since the body features are irreplaceable. Fig I.4 illustrates physiological biometric features which can be used in biometric systems for personal verification. [17]

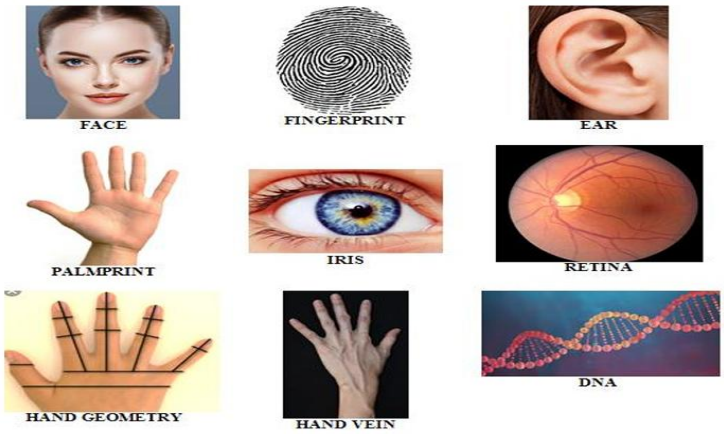


Fig.I.4 Physiological Biometrics [20]

2. Behavioral: Behavioral characteristics are dependent on an act that is performed by a person. On the other hand, behavioral biometrics are dependent on measurements and data extracted from an action and in-are made to measure human body characteristics directly. Fig I.5 shows behavioral biometric characteristics that are used in biometric systems for human verification. [17]

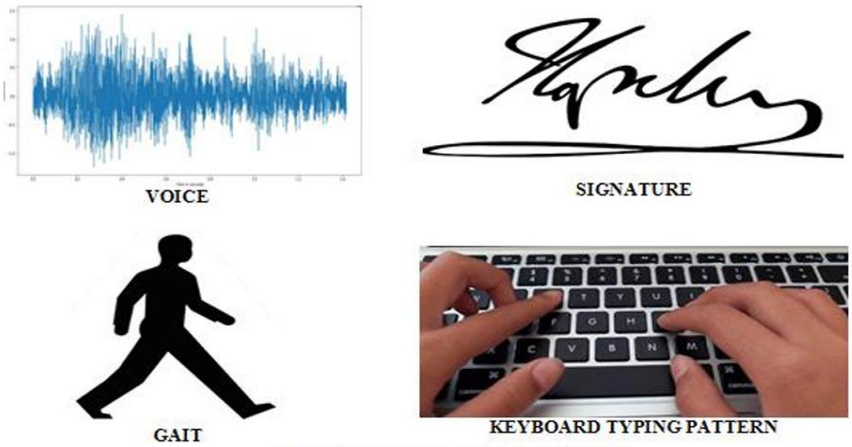


Fig. I.5 Behavioral Biometrics [20]

I.3.2 Biometric System

A biometric system is a system that enables the identification of a particular characteristic of a person using mathematical algorithms and biometric data.

There exist a number of applications of biometric systems. There exist systems that need enroll-ment before users. There are other identification systems that do not need this process. [18]

It consists mainly of two main phases:

1. Enrollment

is a learning phase that aims to collect biometric information about who to identify. Several data acquisition campaigns can be carried out to ensure a certain robustness of the recognition system to temporal variations of the data. During this phase, the biometric characteristics of individuals are captured by a biometric sensor, and then represented in digital form (signatures), and finally stored in the database. The processing related to the enrollment has no time constraint, since it is performed “off-line.” [18]

2. Verification / Identification

❖ **Verification**

In the "one-to-one" comparison mode of verification or authentication, the system verifies an individual's identity by comparing the biometric information they have entered with the biometric template they have stored in the system's database. The system must then respond to the query about the user's identity in this mode. At the moment, a smart card, user name, or personal identification number are used for verification. [18]

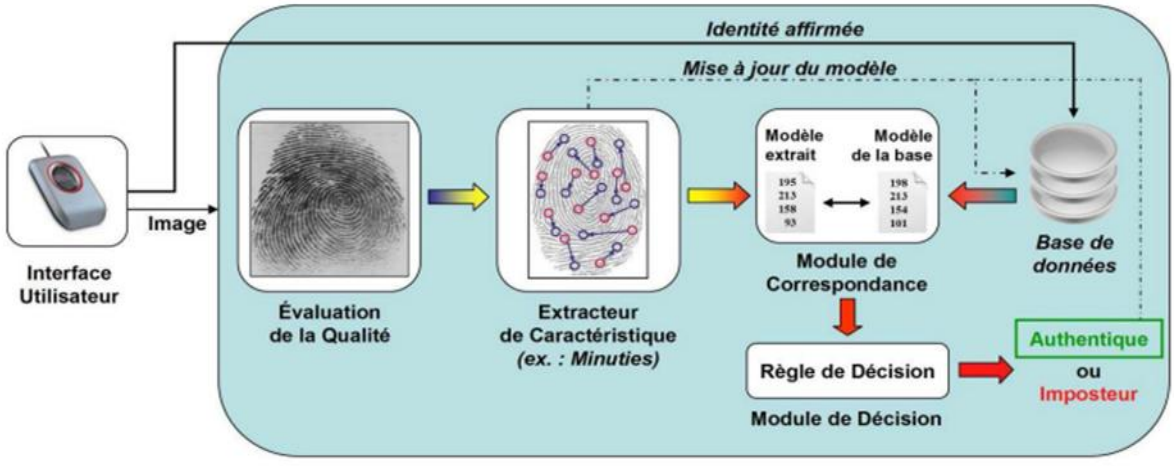


Fig. I.6 Authentication of a person in a biometric system [9]

❖ **Identification**

Positive and negative identification attributes are utilized in user identification. With positive identification, users can verify their identities without necessarily asserting an identity, whereas negative identification, or screening, entails masking true identity with a view to establishing whether the user is the person they purport to be. [18]

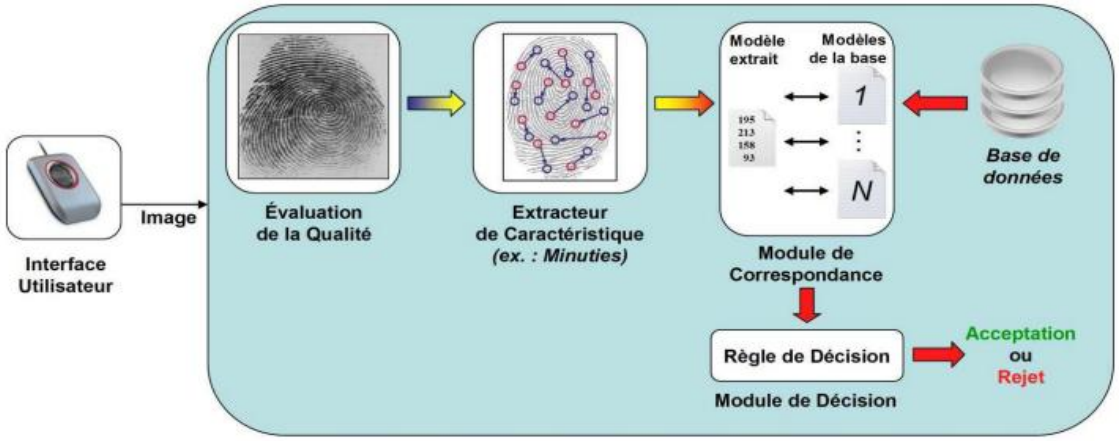


Fig. I.7 Authentication of a person in a biometric system [9]

I.3.3 Biometrics in Information Security

Biometrics in information security utilizes unique biological features like fingerprints, face shapes, or voice to authenticate and verify persons and secure entry to systems or sensitive information. These systems reduce risks of unauthorized access and credential hijacking. Limitations include privacy concerns, vulnerability to spoofing, and recognition algorithm bias. Controls used by organizations include multi-factor authentication and regulatory compliance. [22] [23]

1. Biometric Authentication

Biometric authentication is a consistent process that authenticates the identity of an individual against his/her unique physical or behavioral traits. Biometric authentication is a safer mechanism than traditional password authentication techniques and is significantly used in secure access to secret information and areas. Because they are unique and cannot be altered, biometric traits are best for various uses. [21]

2. Access Control

Biometric authentication is a secure alternative to traditional methods like passwords or keycards through which access control systems can identify individuals based on unique

biological or behavioral traits like fingerprints, faces, or iris. These systems acquire biometric data with sensors, convert it into encrypted templates, and match it against stored records to permit or deny entry. However, risks like presentation attacks and privacy concerns remain. Mitigation strategies are liveness detection and regulatory compliance like GDPR. Advances in artificial intelligence and decentralized storage are making systems increasingly immune to new threats. [25] [26]

I.4 Security Threats

Security risks encompass deliberate attacks, system failure, or human errors posing threats to information assets and leading to data breaches, financial losses, and reputational harm in case they are not adequately controlled. [39]

I.4.1 Threat in Biometric Systems

Biometric systems, due to being founded on distinctive physiological or behavioral traits, have an important part to play in security today. However, they too are susceptible to spoofing, template theft, replay attacks, and insider attacks. It is necessary to comprehend and thwart such threats for maintaining the integrity and reliability of biometric authentication. [43]

1. Spoofing Attacks (Presentation Attacks): These attacks include presenting a fake or replicated biometric characteristic to the sensor for the purpose of imitating an authenticated individual. Attackers often use materials such as gelatin, a silicone mold face mask, or high-resolution images and videos to trick the system. Example: A 3D-printed face mask or fingerprint mold in silicone. [27]

2. Replay Attacks: In this type of attack, an attacker captures biometric data in an authentic session and plays it back to gain unauthorized access. This is particularly common when communication is either unauthenticated or unencrypted. Example: Playing back a recorded voice to pass through a voice authentication system. [28]

3. Template Theft or Leakage: Biometric templates are digital versions of biometric characteristics stored in databases. In the event that such templates are compromised by an attacker, the user's identity is irrevocably lost because biometric traits are not changeable like passwords. Example: Hackers breaking into and pilfering fingerprint templates from a national ID system. [29]

4. Man-in-the-Middle (MitM) Attacks: MitM attacks involve intercepting communication among biometric system components, for instance, between the sensor and matcher. The attacker may alter, inject, or replace data in transit. Example: Altering fingerprint data sent to deceive the system into matching with a forged identity. [30]

5. System Exploits and Bypass Attacks: Attackers may exploit vulnerabilities in the biometric software or operating system to bypass biometric verification altogether. This is accomplished through manipulation of the matching algorithm or even manipulation of stored templates themselves. Example: Manipulating the matching threshold in the backend of the system to force acceptance of an imposter. [25]

6. Insider Threats: These risk factors are due to people inside the company with privileged access to the biometric system. Insiders steal, manipulate, or misuse biometric data for financial or personal gain. Example: An IT administrator exporting fingerprint templates or overriding access privileges. [31]

I.4.2 Attacks in Blockchain Networks

Blockchain networks, being decentralized, are susceptible to security attacks such as Smart Contract Vulnerabilities, 51% attacks, Sybil attacks, and Eclipse attacks. These attacks lead to economic loss, transaction manipulation, or network disruption, necessitating the development of stronger and more secure blockchain-based systems. [43]

1. Majority Attack: Describes an instance where a single party or organization gains control of more than 51% of a blockchain network's hashing power (hash rate). With control, they can dictate transaction verification, revert transactions, and double-spend coins. [32]

2. Sybil Attack: A Sybil Attack is a type of security threat to internet networks in which a single attacker creates and controls multiple fake identities (Sybil nodes) in order to gain an excessively large network presence. It is especially dangerous in decentralized networks where consensus and trust are built on the assumption each identity is an individual, unique participant. [33]

3. Smart Contract Vulnerabilities: Weaknesses in smart contracts refer to security vulnerabilities or flaws in the coding of smart contracts usually written in a language such as Solidity and executed on blockchain platforms such as Ethereum. The weaknesses occur

as a result of errors in logic, design, or implementation, and may be utilized by attackers to trigger unintended behavior such as stealing digital currencies, falsifying accounts, or crashing the system. [34]

4. Eclipse Attack: An Eclipse Attack is a Denial-of-Information attack carried out on peer-to-peer (Peer-to-Peer - P2P) networks, such as Bitcoin or Ethereum, and its goal is to isolate a specific node (or group of nodes) from the network and gain full control over Communications you send or receive. This type of attack differs from traditional attacks aimed at hacking data or cracking encryption; it exploits the structure of the network itself. [36]

Conclusion

With an emphasis on encryption technologies as preventative measures against intrusions, the chapter addresses the opportunities and challenges of digital information security. Despite its susceptibility to network control attacks, it emphasizes how blockchain technology can improve digital trust through decentralization. The chapter also highlights the need for creative solutions like homomorphic encryption to protect data privacy and addresses the shortcomings of biometric systems against sophisticated spoofing techniques. To strike a balance between innovation and the protection of fundamental rights, the study suggests implementing adaptive security strategies based on Zero-Trust models and encouraging interdisciplinary collaboration, such as fusing cybersecurity with AI ethics.

Chapter 2

Innovative Approches to Enhance Protection

Summary

This chapter focuses on the importance of emerging technologies such as blockchain and biometrics in maintaining data and system security. It identifies how these technologies aid in creating more effective and secure systems, especially in the health sector, to resist cyberattacks and improve privacy.

Introduction

II.1 Reinforcing Security

II.2 Biometric Revocability

II.3 Proposed System

II.4 Materials and Methods

II.5 Biometric Feature Extraction Approach

II.6 Blockchain-Enabled Dual-Layer Template Protection Framework

Conclusion

Introduction

Blockchain technology has revolutionized the way digital transactions and exchange of data take place by allowing decentralized, secure, and transparent networks. Emerging advancements in blockchain networks are aimed at addressing major limitations like scalability, energy efficiency, and interoperability, which allow large-scale adoption across different industries like finance, healthcare, and supply chains. These advances include the development of novel consensus protocols, layer-2 implementations, and cross-chain communication protocols, all of which come together to widen what blockchain networks can do.

Furthermore, the integration of artificial intelligence (AI) and Internet of Things (IoT) with blockchain is unlocking new opportunities for automation and intelligent decision-making. Governments and regulatory bodies are also increasingly exploring blockchain for secure identity management and transparent public services. As research and innovation continue, blockchain is evolving from a financial tool to a foundational infrastructure for next-generation digital ecosystems.

II.1 Reinforcing Security

Strengthening security is the ongoing activity of establishing and developing policies, procedures, and technological controls for the purpose of protecting systems, networks, information, and individuals against threats and security risks. It involves instituting forward-looking, preventive, and reactive measures to defend against cyberattacks, data theft, or system compromise. This process requires a continuous cycle of threat assessment, risk management, and the implementation of layered defense strategies that align with evolving technologies

and adversarial tactics. Security strengthening also entails promoting a culture of awareness and resilience, ensuring that all stakeholders, ranging from system administrators to end-users, understand their role in maintaining system integrity. Moreover, with the proliferation of advanced persistent threats and sophisticated attack vectors, organizations must embrace adaptive security architectures, such as zero-trust models and behavior-based monitoring systems. These approaches complement traditional security mechanisms by providing more granular access control and real-time threat detection capabilities. Ultimately, the goal is to establish a robust and dynamic defense posture that not only addresses current vulnerabilities but also anticipates future risks through proactive research, investment, and compliance with security standards and regulations [56].

II.1.1 Secure Identity Management

Security solutions and regulations are increasingly influencing personal data privacy, as the exchange of information between various digital agents often remains ambiguous, fragmented, and difficult to monitor. This complexity introduces significant challenges in maintaining the confidentiality and traceability of interactions. One of the key concerns in this context is the erosion of identity anonymity, which is heavily impacted by the degree of linkability of personal data, how easily data from different sources can be associated with a single individual. As digital ecosystems grow, this linkability can lead to unintended privacy breaches.

To counterbalance these privacy concerns, modern frameworks emphasize the need for selective disclosure of Personally Identifiable Information (PII), allowing individuals to share only the necessary attributes without exposing their entire identity profile. Equally important is the ability to track how and when PII is used, enabling greater transparency and accountability in data handling processes. In response, digital identity systems are now being compartmentalized into contextual domains, wherein individuals can manage different facets of their identity separately depending on the service or environment.

Organizations have responded to these evolving privacy demands by implementing customized authentication mechanisms that align with their security and compliance requirements. Furthermore, regulatory frameworks such as the General Data Protection Regulation (GDPR) have introduced enforceable standards for digital rights. These include the right to access, rectify, and erase personal data, thereby ensuring that users maintain ownership and control over their information. GDPR-compliant digital identity solutions not only safeguard user privacy but also foster trust in digital interactions by promoting responsible data governance [44].

II.1.2 Decentralized Control

Access control systems play a critical role in maintaining the security of computing environments by regulating access to system resources and objects. These systems function by evaluating existing security contexts, such as user credentials, roles, and attributes, against defined policies to determine whether an access request should be granted. Traditionally, modern access control mechanisms have relied on the use of reference monitors, which are trusted entities responsible for the enforcement and decision-making process within the system.

A system-wide enforcement model typically involves embedding a reference monitor at the core level of an operating system or across the network infrastructure. This monitor intercepts every request to access system resources, analyzes it according to pre-defined access policies, and either permits or denies the request based on the current security context. This approach ensures a high level of security and reliability, as the enforcement mechanism is integral to the operating system's kernel, making it resistant to tampering or bypassing.

Moreover, in conventional implementations, access control components are centralized and stand-alone, interacting through a unified interface with all system functions and resource managers. This centralization simplifies management and policy updates while also offering transparency to application developers, who do not need to handle security logic explicitly within their applications. However, while effective, such centralized systems can introduce single points of failure and scalability limitations.

To address these concerns, newer models advocate for decentralized control mechanisms, especially in distributed and blockchain-based environments. In these systems, access control decisions and enforcement are distributed across multiple nodes, eliminating reliance on a central authority and enhancing fault tolerance and transparency. This shift toward decentralization aligns with broader trends in cybersecurity and privacy, supporting more resilient and adaptive access control frameworks [45].

II.1.3 Biometrics for Multi-Factor Authentication

Biometric technologies have emerged as a key component in enhancing identity verification systems, especially in the context of multi-factor authentication (MFA). Various biometric modalities have been explored, including DNA sequencing, retinal and iris scans, facial recognition, and fingerprints. Among these, fingerprints are considered the most commercially viable

biometric modality due to their balance between uniqueness, ease of capture, and cost-effectiveness. Their wide adoption in consumer electronics, border security, and corporate access systems further solidifies their role in practical biometric authentication solutions.

Despite their utility, relying solely on fingerprints can pose risks, particularly when low-cost or low-resolution scanners are used. Such devices may produce inconsistent readings or be susceptible to spoofing. Therefore, incorporating fingerprint recognition as part of a broader MFA system, alongside knowledge-based (e.g., PINs or passwords) or possession-based (e.g., security tokens) factors, significantly improves the robustness of authentication mechanisms.

While fingerprints may not inherently offer greater security than traditional PIN codes, they contribute an additional layer of complexity and reduce the risk of credential theft or unauthorized access. In privacy-preserving frameworks, biometric data is especially powerful when integrated with secure processing techniques and protected storage methods, such as cryptographic binding or blockchain-based identity management. These systems can enforce stricter identity verification without exposing personal identifiers, addressing both security and privacy concerns.

Moreover, MFA systems that incorporate biometric verification outperform single-factor solutions, especially in environments requiring high assurance levels. They also align with regulatory demands for secure access and user accountability, making them a preferred choice for modern identity management architectures [45].

II.2 Biometric Revocability

Revocability of biometric data refers to the capacity to invalidate, revoke, or regenerate a biometric template in the event that it is compromised or exposed. This concept is critical because, unlike passwords or tokens, biometric traits such as fingerprints, iris patterns, or facial features are inherently permanent and cannot be changed once leaked. Therefore, the development of revocable or cancelable biometric templates has become a cornerstone in designing privacy-preserving and secure biometric authentication systems.

Cancelable biometrics involve applying intentional, repeatable distortions or transformations to biometric data before storage. If the transformed template is compromised, a new transformation can be applied to the same raw biometric input to generate a different template, thereby achieving revocability without compromising system accuracy. This approach mirrors the concept of resetting a password in traditional authentication systems, making biometric systems more adaptable to real-world security challenges.

Hence, implementing revocable templates contributes not only to the robustness of the system but also aligns with data protection regulations such as the GDPR, which emphasize the user's right to control their personal data, including the ability to withdraw consent or invalidate credentials. The development of revocable biometric mechanisms ensures that privacy and security are preserved even when biometric information is compromised [46].

II.2.1 Biometric Revocation Techniques

Biometric Revocation Techniques are methods to replace compromised biometric data, ensuring security and privacy by invalidating existing templates and issuing new ones without revealing the original data. [46]

- **Cancelable Biometrics:** Cancelable biometrics involve creating biometric templates that are explicitly alterable or revocable in th event of compromise. The templates are rendered reissue able to enable secure replacement without putting original data at risk.
- **Bio-Enrollable Biometrics:** This approach translates biometric data into a version that can be regenerable or re-encrypted so that revocation and updating of biometric templates are feasible.
- **Template Update and Re-issue:** This approach involves periodic updating or re-issuance of biometric templates to prevent long-term vulnerability, especially after a breach or compromise. [46]

II.2.3 Fuzzy Vault and Fuzzy Commitments

Are key binding biometric cryptosystems that obtain secure sketches from a biometric template, storing them in a database as an alternative. [58]

1. Fuzzy Commitments: The Fuzzy Commitment scheme is a cryptographic primitive designed to bind a secret to biometric or noisy data in such a way that the secret can only be retrieved if a sufficiently similar version of the original data is provided. Unlike traditional cryptographic commitments that require exact input matches, fuzzy commitment handles variability using error-correcting codes. The core idea is to encode a secret as a codeword using an error-correcting code and then combine it with the biometric template using bitwise XOR. During verification, if the user presents a close approximation of the original biometric data, error correction is used to recover the original codeword and thus the secret.[47]

Let the secret ($s \in \{0,1\}^k$) be encoded into a codeword ($c \in \{0,1\}^n$) using an error-correcting code ($\mathcal{C}$). Let ($x \in \{0,1\}^n$) be the biometric template. The commitment is formed by computing:

$$\text{commit} = (h(s), c \oplus x) \tag{II.1}$$

Here, $(h(s))$ is a hash of the secret (used for verification), and ($\oplus$) denotes bitwise XOR. To verify, a user provides a biometric sample (x'). The system computes:

$$c' = (c \oplus x) \oplus x' = c \oplus (x \oplus x') \tag{II.2}$$

If the Hamming distance $(d_H(x, x'))$ is within the correctable limit of the code, error correction is used to recover the original (c), and then (s) is decoded from (c). If ($h(s)$) matches the stored hash, the secret is verified.

2. Fuzzy Vault: The Fuzzy Vault scheme is a cryptographic construct designed to securely bind a secret (such as a cryptographic key) with an unordered set of biometric features or noisy data points. Unlike traditional encryption methods, the fuzzy vault accommodates imprecision or variability in the input, making it highly suitable for biometric authentication systems where exact matching is not feasible. The core idea is to "lock" a secret polynomial with a genuine feature set and then "hide" this set among a larger number of chaff points to obfuscate the true data. During authentication, if a user provides a set that sufficiently overlaps with the genuine set, the original secret can be recovered through polynomial interpolation.[47]

Let $(S \in F_q)$ be the secret to protect, encoded as a polynomial $(P(x))$ of degree (k), such that:

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k \tag{II.3}$$

Let $(A = \{x_1, x_2, \ldots, x_t\})$ be the genuine set of biometric features (where ($t > k$)). The vault is constructed by evaluating the polynomial on each element of (A):

$$\mathcal{G} = \{(x_i, P(x_i)) \mid x_i \in A\} \tag{II.4}$$

To hide the genuine points, a set of chaff points $(\mathcal{C} = \{(x_j, y_j)\})$ is generated such that $(x_j \notin A)$ and $(y_j \neq P(x_j))$. The final vault is the union:

$$\mathcal{V} = \mathcal{G} \cup \mathcal{C} \tag{II.5}$$

During decoding, if a user presents a set (B) with sufficient overlap with (A), the corresponding pairs $((x_i, y_i) \in \mathcal{V})$ can be used to reconstruct $(P(x))$ via polynomial interpolation. If at least (k + 1) correct point pairs are recovered, the polynomial (and thus the secret (S)) can be reconstructed.

II.3 Proposed System

The digital health system shown in Figure 1 uses a decentralized design and biometric authentication for security. It is built with a private blockchain and the InterPlanetary File System (IPFS), which stores medical files across different network computers. Only selected nodes,

like big hospitals or major clinics, are allowed to check and add new records to the blockchain. Other users, such as patients, doctors, and labs, can only send data or read records but cannot approve or add anything to the blockchain. The system uses access rules and agreement methods (consensus) to control how each type of user can work with the network.

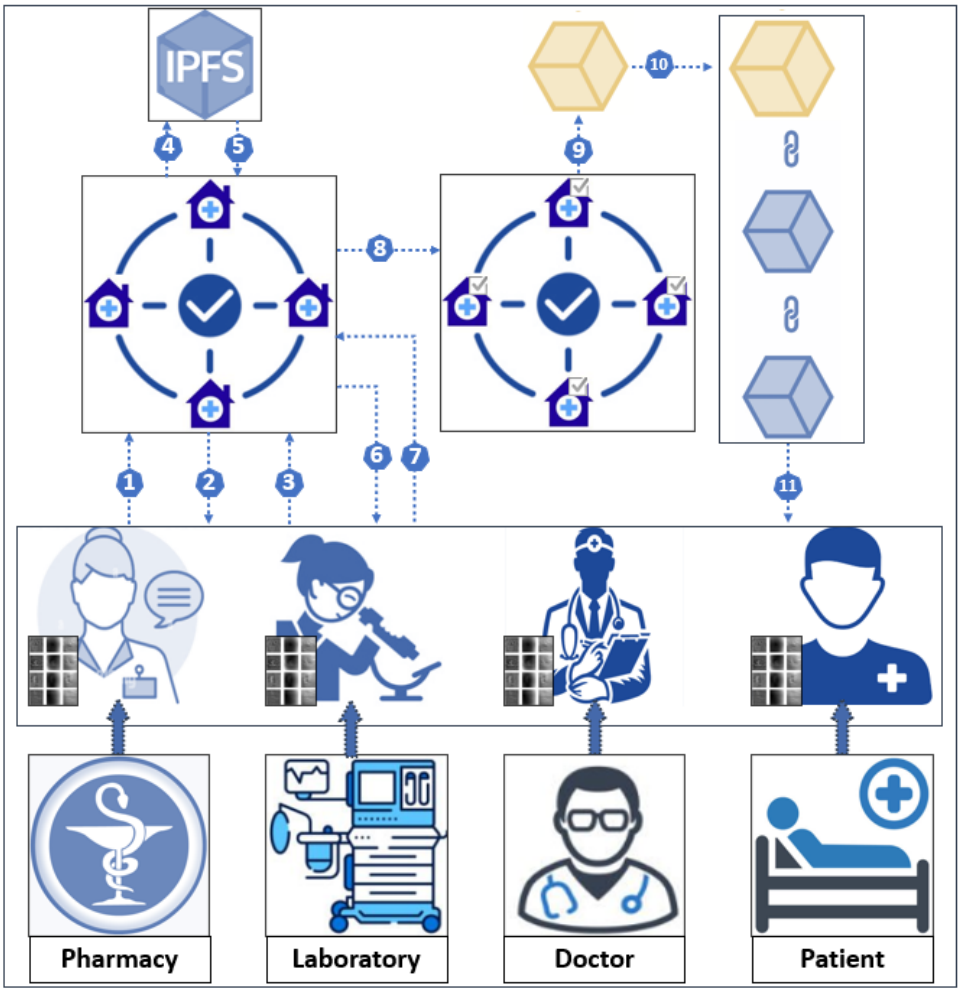


Fig. 1 Proposed system using blockchain and biometrics

In the proposed system, certain trusted nodes are responsible for both checking transactions and managing who can use the system. They verify each user's identity through a decentralized biometric method, using biometric data that is securely stored on IPFS. If a user's biometric data is ever compromised, it can be canceled and replaced with new data, keeping the system secure. This also helps organize users into different roles like patients, doctors, or pharmacists, so that each person can only access the data they are allowed to see. To keep the system secure and efficient, it follows three main steps: first, verifying the user's identity with biometrics; second, checking that the data is correct and follows the rules; and third, saving the verified data to the private blockchain to protect it from being changed or tampered with.

II.3.1 User Authentication Phase (UAP)

The User Authentication Phase (UAP) uses blockchain, IPFS, and smart contracts to create a secure, role-based access control system. This makes sure that only the right users, such as patients, doctors, or pharmacists, can access the system, while keeping all data safe and unchanged. In Step 1, the user sends a service request to admin nodes. In Step 2, the admin nodes reply with a public key, which the user uses to encrypt their biometric data (like fingerprints or face features). In Step 3, the encrypted biometric data is sent to the admin nodes. Then, in Step 4, the admin nodes retrieve the user's saved biometric model from IPFS using a unique ID. Step 5 brings back the model from IPFS to compare with the user's new biometric data. If the match is successful, the user is given access based on their role. If it fails, access is denied, and the user is informed (Step 6). Once the user finishes their task, the session ends securely in Step 7. This process ensures strong privacy, prevents tampering, and uses blockchain to track all access and data actions in a transparent and unchangeable way.

II.3.2 Data Validation Phase (DVP)

In Step 8, the blockchain checks if the data uploaded by the user is correct and follows the system's rules. It looks at the data's format and structure to make sure it meets all required standards. This check is done automatically using a smart contract, which acts like a rule enforcer. If the system sees that a new block is needed to store the data, the smart contract sets a signal to start creating one. In Step 9, once that signal is active, the system begins building the new block. It collects and organizes the validated data based on fixed rules, with the smart contract helping to structure everything properly. After the block is ready, it goes through a final check (called consensus) before being added to the blockchain. This process, handled by smart contracts, ensures that all data added to the blockchain is accurate, secure, and recorded in a way that cannot be changed.

II.3.3 Blockchain Integration Phase (BIP)

In the final part of the process, Step 10 adds the new block to the blockchain. A group of decentralized nodes checks the data and its details, and once they all agree (reach consensus), the block is added permanently. This makes sure the data cannot be changed and stays secure. Then, in Step 11, the user is notified by the smart contract. The system sends a message that includes the block hash, the transaction ID, and a confirmation that the data has been safely recorded. This update gives the user real-time proof that their data is stored, protected from tampering, and easy to find later if needed.

II.4 Materials and Methods

This subsection outlines the material requirements for implementing and testing the proposed System.

II.4.1 Contrast Limited Adaptive Histogram Equalization

Contrast Limited Adaptive Histogram Equalization (CLAHE) is an image enhancement technique that improves local contrast by applying histogram equalization to small regions (tiles) of an image rather than the entire image. Unlike standard histogram equalization, CLAHE limits contrast amplification to prevent noise over-enhancement by clipping the histogram at a predefined threshold [49]. For each tile, the histogram is clipped, and excess pixels are redistributed uniformly. The output intensity mapping function for a pixel with intensity (r) in a tile is given by the cumulative distribution function (CDF) of the clipped histogram:

$$s = CDF_c lip(r) = \sum_{i=0}^{r} \frac{h_{clip}(i)}{N} \quad \text{(II.6)}$$

II.4.2 Steerable filter

Steerable filters are a class of orientation-selective filters that allow efficient computation of filter responses at any orientation using a linear combination of a set of basis filters. This property makes them especially useful for edge detection, texture analysis, and feature extraction in images [57]. A steerable filter (G_θ) at an arbitrary angle (θ) can be expressed as a weighted sum of basis filters (G_{θ_k}):

$$G_\theta(x,y) = \sum_{k=1}^{n} a_k(\theta) G_{\theta_k}(x,y) \quad \text{(II.7)}$$

where ($G_{\theta_k}(x,y)$) are the basis filters precomputed at fixed orientations (θ_k), and ($a_k(\theta)$) are the steering coefficients that depend on the desired angle (θ). This formulation enables continuous orientation tuning while reducing computational cost.

II.4.3 Histogram of Oriented Gradients

Histogram of Oriented Gradients (HOG) is a feature descriptor used in computer vision and image processing for object detection. It captures the structure or shape of objects by computing the distribution of gradient orientations in localized regions of an image. The image is first divided into small spatial regions called cells, and for each cell, a histogram of gradient directions is calculated. The gradient magnitude ($M(x,y)$) and orientation ($\theta(x,y)$) at each pixel are computed as:

$$M(x,y) = \sqrt{\left(I_x(x,y)\right)^2 + \left(I_y(x,y)\right)^2} \quad \text{(II.8)}$$

$$\theta(x,y) = \arctan\left(\frac{I_y(x,y)}{I_x(x,y)}\right) \quad \text{(II.9)}$$

where (I_x) and (I_y) are the image gradients in the horizontal and vertical directions, respectively. The histograms from all cells are then normalized over larger blocks to ensure illumination invariance. HOG features are widely used for detecting objects like pedestrians and vehicles due to their robustness and efficiency.

II.4.4 Self attention:

Self-attention is a core component in Transformer architectures, allowing a model to weigh the importance of different elements in a sequence relative to each other [50]. Unlike traditional models that process sequences in a fixed order, self-attention computes interactions between all positions simultaneously. Given an input sequence represented as a matrix ($X \in R^{n \times d}$), the self-attention mechanism projects (X) into queries (Q), keys (K), and values (V) through learned linear transformations. The attention output is computed as:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^{\top}}{\sqrt{d_k}}\right)V \tag{II.10}$$

where ($Q = XW^Q$), ($K = XW^K$), and ($V = XW^V$) are the query, key, and value matrices, respectively, and (d_k) is the dimension of the keys. The dot-product attention scores determine how much each part of the input should attend to every other part, enabling the model to capture dependencies regardless of distance in the input sequence.x²

II.4.5 FDA Optimizer

Flow direction algorithms are used in hydrological and terrain analysis to determine the direction water would flow across a digital elevation model (DEM) [52]. Optimizing these algorithms improves both computational efficiency and the accuracy of flow modeling. A commonly used method is the D8 (Deterministic Eight) algorithm, where each cell in a grid flow to one of its eight neighbors with the steepest descent. The flow direction ($D(i,j)$) from a cell at position ((i,j)) is given by:

$$D(i,j) = \arg\min_{(m,n)\in\mathcal{N}(i,j)}\left(\frac{Z(i,j)-Z(m,n)}{d_{(i,j),(m,n)}}\right) \tag{II.11}$$

where ($Z(i,j)$) is the elevation at cell ((i, j)), ($\mathcal{N}(i,j)$) is the set of neighboring cells, and (d) is the distance between cells (1 for orthogonal, ($\sqrt{2}$) for diagonal). Optimizations may involve using multi-flow direction (MFD) models, parallel computing, or improved edge-case handling to enhance accuracy and reduce runtime in large-scale terrain datasets.

II.4.6 Ethereum Blockchain

Ethereum is a decentralized, open-source blockchain platform that enables the execution of smart contracts, self-executing code stored and run on the blockchain without the need for a central authority. Unlike Bitcoin, which is primarily designed for peer-to-peer financial transactions, Ethereum supports a wide range of decentralized applications (dApps) through its Turing-complete Ethereum Virtual Machine (EVM). Transactions and contract executions are verified by a distributed network of nodes, and all records are stored immutably on the blockchain. Ethereum uses a native cryptocurrency called Ether (ETH) to incentivize participants and pay for computational operations via gas fees. Since its upgrade to Ethereum 2.0, the platform has transitioned from Proof of Work (PoW) to Proof of Stake (PoS), improving scalability, energy efficiency, and transaction throughput, making it more suitable for modern decentralized systems, including healthcare, finance, and identity management applications [54].

II.4.7 Ganache Blockchain

Ganache is a personal, in-memory Ethereum blockchain used primarily for development and testing of decentralized applications (dApps) and smart contracts. It allows developers to simulate a blockchain environment locally, offering fast and deterministic control over transactions, accounts, and mining processes without the need for real network deployment. Ganache provides features such as customizable gas costs, block times, and account balances, enabling efficient debugging and testing workflows. It supports both a graphical interface (Ganache UI) and a command-line version (Ganache CLI), making it versatile for various development needs. As part of the Truffle Suite, Ganache integrates seamlessly with smart contract compilation and migration tools. Its ability to instantly mine blocks and inspect the blockchain state makes it an essential tool in the development lifecycle, particularly useful in academic and research environments for experimenting with blockchain logic before deployment to a live Ethereum testnet or mainnet. [55]

II.4.8 InterPlanetary File System

The InterPlanetary File System (IPFS) is a peer-to-peer distributed file storage protocol designed to make the web more decentralized, resilient, and efficient. Instead of addressing files by location (such as URLs), IPFS identifies them based on their content using cryptographic hashes. When a file is added to IPFS, it is divided into smaller blocks, each hashed and linked using a Merkle Directed Acyclic Graph (Merkle DAG). This structure ensures content integrity and enables deduplication. Files can be retrieved from any peer on the network that hosts the corresponding hash, improving redundancy and fault tolerance. IPFS is particularly well-suited

for blockchain-based systems, as it allows large data files (such as biometric templates, medical records, or images) to be stored off-chain while retaining verifiable references on-chain through their unique Content Identifier (CID). This reduces on-chain storage costs and enhances scalability and privacy.

II.4.9 Smart Contracts

Smart contracts are self-executing digital agreements deployed on a blockchain that automatically enforce rules and conditions without requiring intermediaries. They consist of code written in programming languages like Solidity (for Ethereum), and once deployed, they operate autonomously and immutably. Each contract is identified by a unique address and responds to transactions that meet predefined conditions. Smart contracts are widely used for various applications such as decentralized finance (DeFi), identity verification, supply chain management, and secure access control. In Ethereum, smart contracts run on the Ethereum Virtual Machine (EVM), where every function call and transaction is validated by the network and permanently recorded on the blockchain. This ensures transparency, tamper-resistance, and auditability. In privacy-sensitive systems, smart contracts can be designed to handle access permissions, trigger events, and interact with off-chain data (e.g., via oracles or IPFS), forming a critical component of decentralized application logic.

II.5 Biometric Feature Extraction Approach

One of the most important steps in any pattern recognition system is feature extraction, which means identifying the most useful information from an image or data input. The quality of these features has a major impact on how accurately the system can recognize patterns, such as faces, fingerprints, or other objects. There are different ways to extract features. Some methods use traditional machine learning, where features are selected manually or based on predefined rules. Others use deep learning, which allows the system to automatically learn the most important features from the data.

A key benefit of deep learning is that the classifier, the part of the system that decides what a pattern is, can also take part in choosing and improving the features during training. In this way, the classifier doesn’t just make predictions but also helps adjust the feature extraction process to get better results. It acts like an expert that fine-tunes how features are selected, making the system smarter over time.

In our system, we followed this deep learning principle by including an optimization step. This step allows the classifier to guide and improve the feature extraction method during training.

As a result, the system becomes more accurate in recognizing patterns, because the features it uses are better suited to the task. This combined approach helps boost the overall performance and reliability of the system.

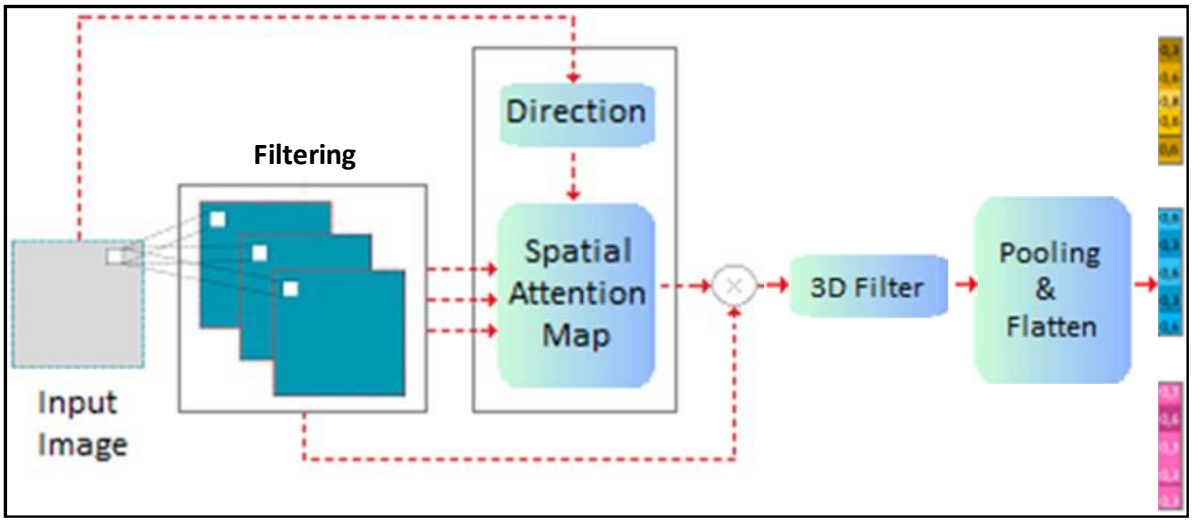


Fig. 2 Proposed Biometric Feature Extraction system

To enhance the quality and robustness of feature extraction, a multi-step directional filtering framework is proposed. This approach combines steerable filtering, spatial attention mechanisms, and 3D Gaussian filtering to generate a high-quality, compact feature vector suitable for biometric recognition.

► **Step 1:** In the first step, the input image $(I(x,y))$ is passed through a set of (N) steerable filters, each parameterized by a distinct orientation (θ_i) and scale (σ_i). The steerable filter response $(F_i(x,y))$ for each configuration is given by:

$$F_i(x,y) = I(x,y) * G_{\theta_i,\sigma_i}(x,y), \quad i = 1,2,\dots,N \tag{II.12}$$

where $(G_{\theta_i,\sigma_i}(x,y))$ represents a directional Gaussian filter kernel, and ($*$) denotes convolution. This process yields (N) filtered feature maps that capture directional information at multiple scales and orientations.

► **Step 2:** In step 2, the input image undergoes gradient computation in the horizontal and vertical directions to capture edge structures and directional cues. These gradients, denoted as $(\nabla_x I) and (\nabla_y I)$, are computed using:

$$\nabla_x I = \frac{\partial I}{\partial x}, \quad \nabla_y I = \frac{\partial I}{\partial y} \tag{II.13}$$

The gradient components are then fed into a spatial attention module, which generates an attention map ($A(x, y)$). This map highlights salient regions in the image that contain meaningful directional features. Simultaneously, the previously obtained filtered feature maps \($F_i(x, y)$) are also input into this attention module, allowing the system to fuse gradient-based saliency with orientation-specific features.

► **Step 3:** In the third step, each filtered image is element-wise multiplied by the attention map:

$$\widetilde{F_i}(x, y) = F_i(x, y) \cdot A(x, y) \tag{II.14}$$

This operation enhances the original filtered outputs by weighting them with attention-driven importance scores. The set of refined feature maps ($\{\widetilde{F_i}\}$) is then aggregated using a 3D Gaussian filter, ($G_3(x, y, i)$), which performs smoothing across spatial and directional dimensions:

$$F_{\text{enh}}(x, y) = \sum_{i=1}^{N} \widetilde{F_i}(x, y) * G_3(x, y, i) \tag{II.15}$$

This filtering produces a single enhanced feature map (F_{enh}) that combines multi-directional features into a unified representation.

► **Step 4:** Finally, in the fourth step, (F_{enh}) is passed through a pooling layer to reduce spatial dimensions while retaining essential information. The resulting feature map is flattened into a one-dimensional vector. To generate a compact and discriminative feature descriptor, the Histogram of Oriented Gradients is computed on the enhanced image. The HOG descriptor captures the distribution of gradient orientations within localized regions, providing a robust representation for classification or matching.

This multi-step framework is particularly suited for biometric applications, as it preserves direction-sensitive features, focuses on salient regions, and compresses information into a low-dimensional yet powerful descriptor.

II.6 Blockchain-Enabled Dual-Layer Template Protection Framework

To ensure robust protection of biometric templates, our system integrates a dual-layered security mechanism that leverages both fuzzy vault cryptography and blockchain technology. The primary objective is to prevent unauthorized access, manipulation, or leakage of sensitive biometric data, which are key concerns in modern digital identity systems. In the first layer, the fuzzy vault scheme conceals the genuine biometric features by encoding them as coefficients

of a secret polynomial and binding them with numerous chaff points. This approach offers resilience against brute-force and correlation attacks by obfuscating the true template among a sea of decoys. However, to further enhance the security and traceability of these protected templates, the second layer employs a private blockchain network. Instead of storing the raw biometric data, only the encoded polynomial (i.e., the fuzzy vault secret) is recorded in the blockchain. This immutable ledger ensures that once a template is committed, it cannot be altered or tampered with, while also maintaining transparency and auditability. By combining fuzzy vault with the decentralized, tamper-resistant nature of blockchain, the system offers a powerful template protection framework that upholds both user privacy and data integrity in a secure, scalable manner.

II.7 Conclusion

It is clear from this chapter that continuous technological innovation is crucial towards improving data protection and safeguarding digital systems, especially in the face of rising cyberattacks. Blockchain and biometric technologies are excellent tools for building flexible, open, and safe systems on the foundation of sophisticated techniques such as encryption, decentralized control, and smart contracts. Combining these technologies is able to achieve very high security levels while protecting the privacy of users and operational efficiency, providing a secure, integrated digital space. This combination ultimately contributes to the development of smart, autonomous systems reacting to the demands of the digital age, particularly in the field of healthcare.

Chapter 3

Experimental results

Summary

Biotechnologies are more often applied across a variety of uses because of their useful influence on the level of security of information systems. In this chapter, we presented the outputs of our experimentation on a model database of finger joint fingerprints. Our outputs, show that how effective our proposal is, compares well with many state-of-the-art research. By demonstrating the performance and effectiveness of our biometric encryption system, we hoped to provide useful information of the potential uses and impact, as it applies to improving security levels in numerous areas.

Introduction

III.1 Biometric System Configuration

III.2 Blockchain Configuration

III.3 Biometric System Performance Evaluation

Conclusion

Introduction

In this chapter, we describe the experiments carried out to test the performance and security of the proposed system. The goal of these experiments is to find out how well the system works in providing a safe and efficient way to share and manage data. The evaluation mainly focuses on two important components of the system. First, we look at how accurately the biometric authentication can verify user identities. Second, we study how the blockchain technology helps keep health data secure, tamper-proof, and well-distributed.

To make the testing more organized, we measure the technical performance of both the biometric system and the blockchain. This includes checking how quickly and accurately the system can identify users and how well the blockchain handles data transactions. And we focus on the security aspects, including how resistant the biometric system is to attacks and how the blockchain ensures data integrity and access control.

These experiments help us understand how effective is our proposed system, where protecting sensitive information and ensuring accurate access control are critically important.

III.1 Biometric System Configuration

The biometric system in our project is designed to work in different modes, mainly authentication and recognition. In recognition mode, the system can operate in two ways: closed-set (where all users are already registered in the system) and open-set (where the person being

recognized might not have been registered before). Our proposed system is capable of working effectively in both modes, but for a more thorough evaluation, we chose to focus on the recognition mode under both open-set and closed-set conditions.

To evaluate the performance of the proposed biometric identification system, we used the Finger-Knuckle-Print (FKP) dataset developed by the Polytechnic University of Hong Kong (PolyU). This academic dataset includes a total of 7,920 images collected from 165 individuals, consisting of 125 men and 40 women. Among the participants, 143 individuals are aged between 20 and 30, while the remaining 22 fall within the 30 to 50 age group.

The data collection process was carried out in two separate sessions to help test the system's stability over time. In each session, every participant was asked to provide 6 images for each of the following four fingers: Left Index Finger (LIF), Left Middle Finger (LMF), Right Index Finger (RIF), and Right Middle Finger (RMF). This resulted in a total of 48 images per subject across all four finger types. The use of multiple fingers and repeated sessions helps ensure a robust evaluation of the system's recognition accuracy and reliability under varying conditions.

III.1.1 FKP Region Of Interest Extraction

The Finger-Knuckle Print also presents a unique characteristic for each individual. It remains unchanged over time, is easy to capture, digitize, and store.

Once the coordinate system is established, the central part (Region of Interest - ROI) is segmented. To extract the ROI containing the textures around the joint, we use the algorithm described in [60]. This operation aims to eliminate the background (reduce image size) and obtain more accurate results.

► **Filtering and Down sampling:** Each image in the database has a size of 768×576 pixels with a resolution of 400 dpi. It is unnecessary to use this resolution for feature extraction (a lower resolution can still effectively represent the primary and secondary lines around the joint). Consequently, the finger image undergoes a filtering operation followed by a down-sampling operation. The goal of filtering is to reduce noise in the image. A low-pass filter (e.g., Gaussian filter) can be applied to reduce this noise and improve the quality of the original image. The down-sampling operation reduces the image resolution to 150 dpi, which significantly lowers computation costs by reducing data volume. We denote the resulting image as **ID**. This step's result is shown in Figure 1.

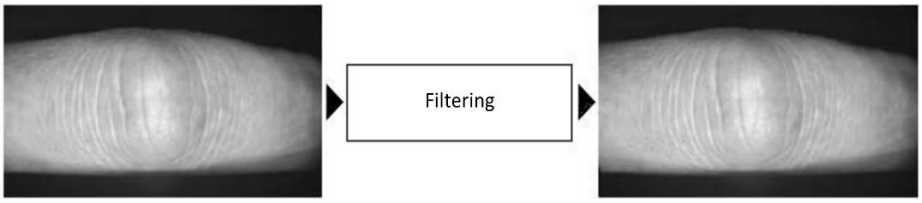


Fig 1. Filtering and down-sampling of finger image.

► **Determination of the X-Axis:** Once the fingerprint image has been filtered and down sampled, the algorithm determines the horizontal X-axis. The lower boundary of the finger can be easily extracted using a Canny edge detector. The Canny filter is chosen for its advantages (good detection and localization). This lower boundary is relatively consistent across images because all fingers are placed on the base block during image acquisition. By approximating this boundary as a straight line, the X-axis is defined. Figure 2 illustrates the X-axis along the finger's lower edge.

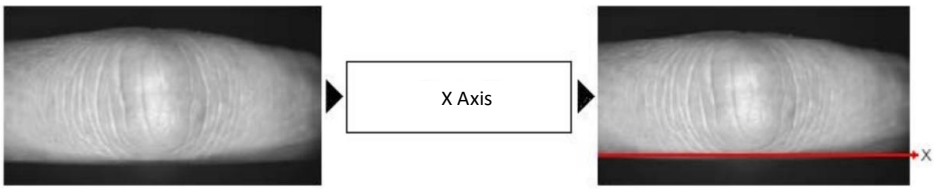


Fig 2. Determining the X axis.

► **Sub-Image Extraction:** Only part of the finger image contains useful information for biometric identification. Therefore, we first extract a sub-image IS from the original image. The left and right boundaries of IS are empirically fixed values, while the top and bottom boundaries are estimated based on actual finger boundaries. Figure 3 shows an example of a sub-image, which is then used to calculate the Y-axis.

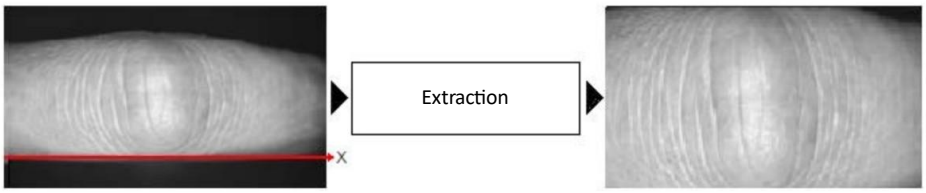


Fig 3. Extracted sub-image before ROI extraction.

► **Contour Detection:** By applying the Canny edge detector to image IS, we obtain the contour image IE. See Figure 4 for an example.

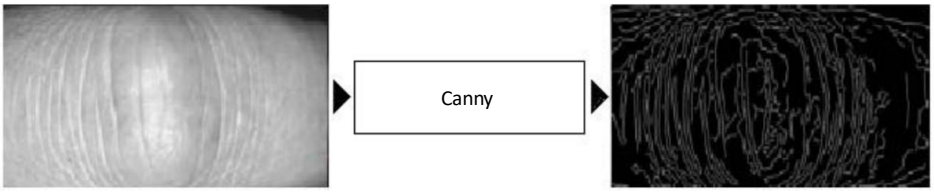


Fig 4. Image of the contours obtained.

► **Convex Direction Encoding:** Based on the curvature characteristics of the contours in image IE, we can encode IE to produce a coded image ICD, representing the convex directions of curves. At this step, each pixel in IE is assigned a code to represent its local (convex) direction. Based on observation, an ideal model of finger image curves is shown in Figure 5.

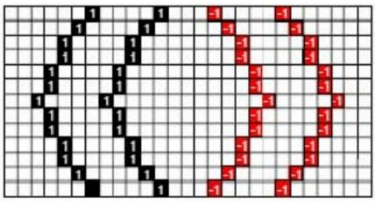


Fig 5. Curves on the finger image.

In this model, curves are either convex to the left or to the right. Pixels on left-convex curves are coded as "1", right-convex as "-1", and all others as "0". Figure 6 shows these convex directions in ICD.

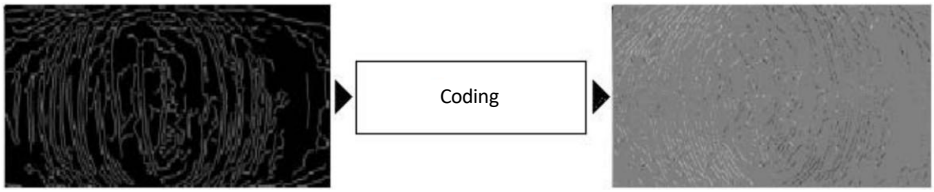


Fig 6. Image obtained by applying convex direction coding.

► **Determination of the Y-Axis:** In a finger image, most curves on the left side are directed to the left and those on the right to the right. However, there is a small zone around the joint where clear convex directions are absent. From this observation, we define a convexity magnitude **%** as:

$$\%(x) = \left| \sum_{W} ICD \right|$$

where x is the horizontal position (i.e., a column), and W is a symmetric window centered at x, with height equal to the image height and width d = 35 in our case. The convexity magnitude % reaches its minimum near the center of the joint. The window W moves from left to right across different x values. The Y-axis is defined as:

$$\mathbf{Y} = arg\min_{x}[\%(x)]$$

This position defines the Y-axis. Figure 7 shows the Y-axis on the finger image.

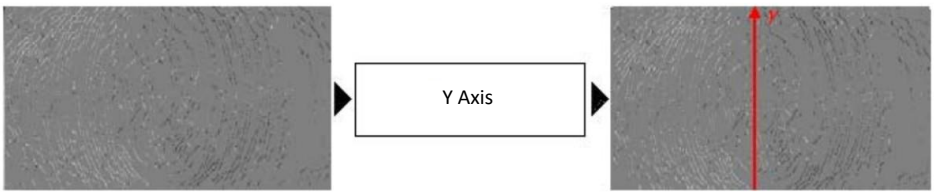


Fig 7. Determining the Y axis.

► **ROI Localization:** After localizing the X and Y axes, we define a region in the image ID, named IROI, representing the region of interest. According to Figure 8, the ROI, with a fixed size, is extracted from the image ID.



Fig 8. ROI location in the finger image.

► **ROI Extraction:** A rectangular region cantered on the Y-axis (see Figure 9), with fixed dimensions (110×220 pixels), is extracted as the ROI. It contains most of the fingerprint information.

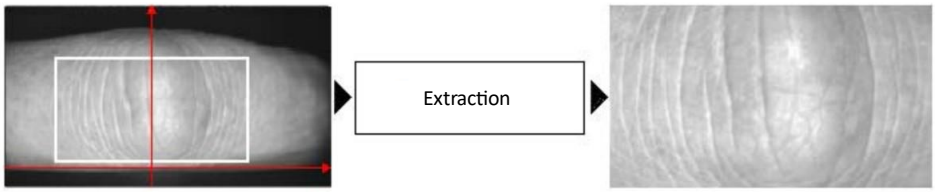


Fig 9. ROI extraction from finger image.

Finally, the methods for locating the X and Y axes and extracting the ROI can effectively align different finger images by normalizing the area used for further biometric feature extraction. These operations significantly reduce variations caused by different finger placements during acquisition.

III.2 Blockchain Configuration

To build a secure and well-organized system, we used Ganache to set up a local blockchain network. Ganache provides a stable environment that allows developers to write, test, and deploy smart contracts without connecting to a live network. The blockchain was configured with a Network ID of 5777, an RPC server at http://127.0.0.1:8545, a gas limit of 6,721,975, and a chain ID of 1337. These settings helped us run smooth and repeated tests during development before deploying the system to a public blockchain.

To simulate a real healthcare environment and implement role-based access control, we created 300 user accounts. Out of these, 200 accounts were assigned to patients, who are the main users of the system. The remaining 100 accounts were divided among different healthcare roles: 40 doctors, 20 laboratories, 15 pharmacists, 15 clinics, and 10 hospitals. This realistic distribution ensures that each type of user has proper access permissions, in line with their professional responsibilities. For decentralized and permanent storage, we used IPFS via the public gateway at https://ipfs.tech/ipfs/, with API calls made securely over HTTPS at ipfs.tech:5001. In our system, we store only content identifiers (CIDs) on the blockchain, instead of the actual health data. This reduces storage costs on the blockchain and improves the system's speed, security, and scalability.

We used the Truffle framework to write and deploy smart contracts. The development environment was connected to our local Ganache instance at 127.0.0.1:8545. The contracts were written in Solidity version 0.6.x, which offers modern Ethereum features and better security. To allow the front-end application to interact with the blockchain, we used Web3.js, a JavaScript library that helps perform transactions such as biometric data upload, verification, and retrieval. Overall, these technologies and configurations were chosen to follow best practices in blockchain-based systems. They support strong security, clear access control, and reliable data integrity, all critical requirements for managing sensitive healthcare data in a decentralized system.

III.3 Biometric System Performance Evaluation

In this subsection, we evaluate the overall efficiency and security of the proposed system. The assessment focuses on three main areas. First, we examine the system's access control

performance, specifically its ability to accurately recognize and authenticate authorized users. Second, we analyze how effectively the blockchain infrastructure supports the secure and consistent distribution of services across the network. Finally, we conduct a security evaluation by simulating both common and high-risk cyberattacks to test the system's resilience and robustness under potential threat scenarios

In this section, we assess the performance of the biometric system using a structured experimental approach. The dataset is split into two parts: 60% is used for training the system, and 40% is used for validation. To clearly demonstrate the effectiveness of each stage, the evaluation process is divided into three main experiment sets.

The first set focuses on a single biometric modality, where we conduct an empirical study to identify the optimal filter size and number. The second set investigates how the selected filter parameters affect all modalities, providing a broader view of the system's performance. Finally, the third set aims to enhance accuracy by optimizing the filter parameters during the filtering stage.

This three-stage evaluation helps us understand the contribution of each component and accurately measure the system's efficiency under various conditions.

III.3.1 Preliminary results

In this section, we systematically evaluate the performance of the proposed Finger Knuckle Print (FKP) recognition system under varying parameter configurations. Specifically, we analyse how different numbers of Steerable filters, filter sizes, and Histogram of Oriented Gradients (HOG) region partitioning strategies affect the recognition accuracy. The number of Steerable filters used ranges from *2* to *6*, i.e., [2,3,4,5,6], allowing us to examine the trade-off between spectral diversity and computational cost.

For each filter configuration, we test multiple filter sizes selected from an odd-sized kernel range $[19x19,21x21,23x23,25x25,27x27,29x29,31x31]$which ensures symmetry and consistency in spatial frequency response. Furthermore, the extracted ROI is divided into different numbers of sub-regions for HOG feature computation, specifically using *9*, *25*, and *49* blocks. This variation in region granularity allows us to assess the impact of local texture detail resolution on feature representation quality. The goal of these experiments is to identify the optimal combination of parameters that yields the best balance between recognition performance and computational efficiency.

The experimental results reveal significant insights into the effects of filter size, number of filters, and HOG region granularity on the recognition error rate of the Finger Knuckle Print (FKP) system.

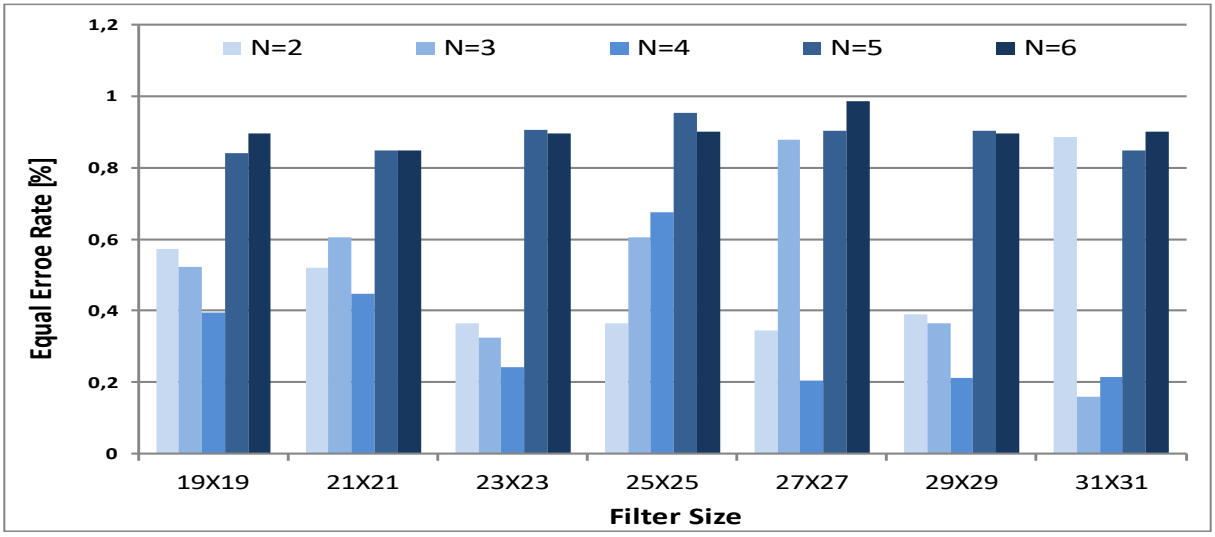


Fig 10. Impact of Filter Size and Filter Number with HOG Regions =9 on Biometric System Performance

The coarsest HOG configuration, with only *9* regions, results in the highest overall error rates. exhibit elevated error values, particularly at smaller filter sizes. For instance, at 19×19 records a high error of 0.5721, and in 27×27 reaches 0.8782. Interestingly, some localized improvements are noted—for example, at 27×27 yields a relatively low error of 0.2049—but these are inconsistent across runs. a near-complete degradation in performance with error rates consistently exceeding \$0.84\$, and reaching up to 0.9857 at 27×27. This sharp decline in accuracy indicates that the low number of HOG regions fails to capture sufficient local structural detail in the ROI, especially when paired with complex or larger filters.

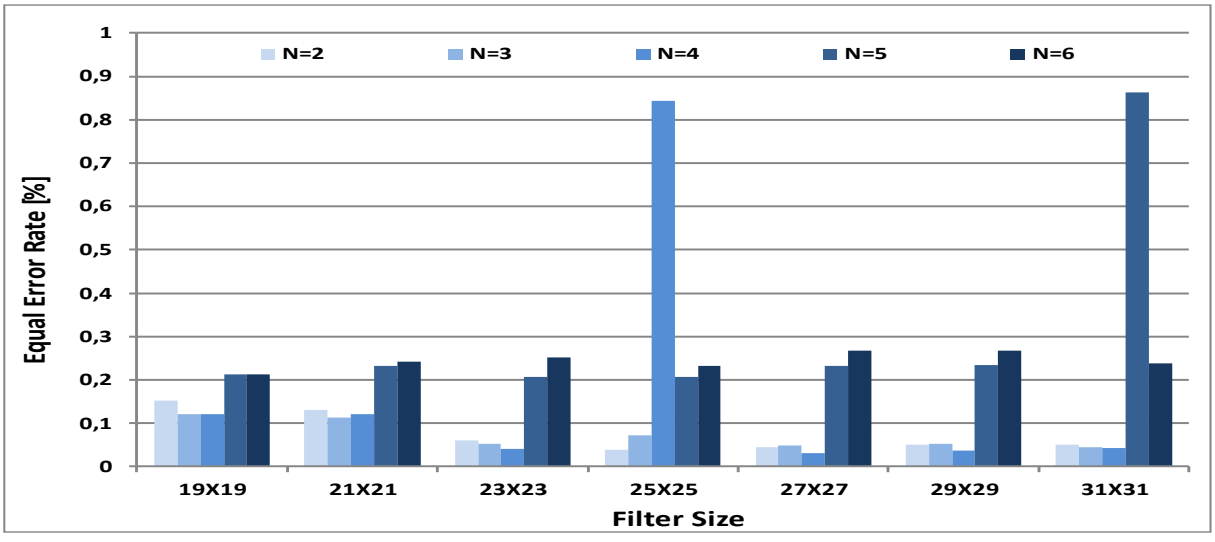


Fig 11. Impact of Filter Size and Filter Number with HOG Regions =25 on Biometric System Performance

A substantial improvement in performance is observed when the number of HOG regions is increased to to 25. In this configuration, all five experimental runs exhibit significantly lower error rates across most filter sizes. Notably, 25×25 achieves a minimum error of 0.0387, while 31×31 and 27×27 reach their lowest errors of 0.0454 and 0.031, respectively. These results suggest that the 25-region HOG division offers a favorable balance between local feature resolution and spatial generalization. For most filter sizes benefit from this configuration, maintaining acceptable error rates under 0.27, with only a single anomaly at 31×31 reaching a peak error of 0.863. This spike is likely due to a compounded effect of large filters and insufficient generalization, possibly causing feature misalignment or over-smoothing.

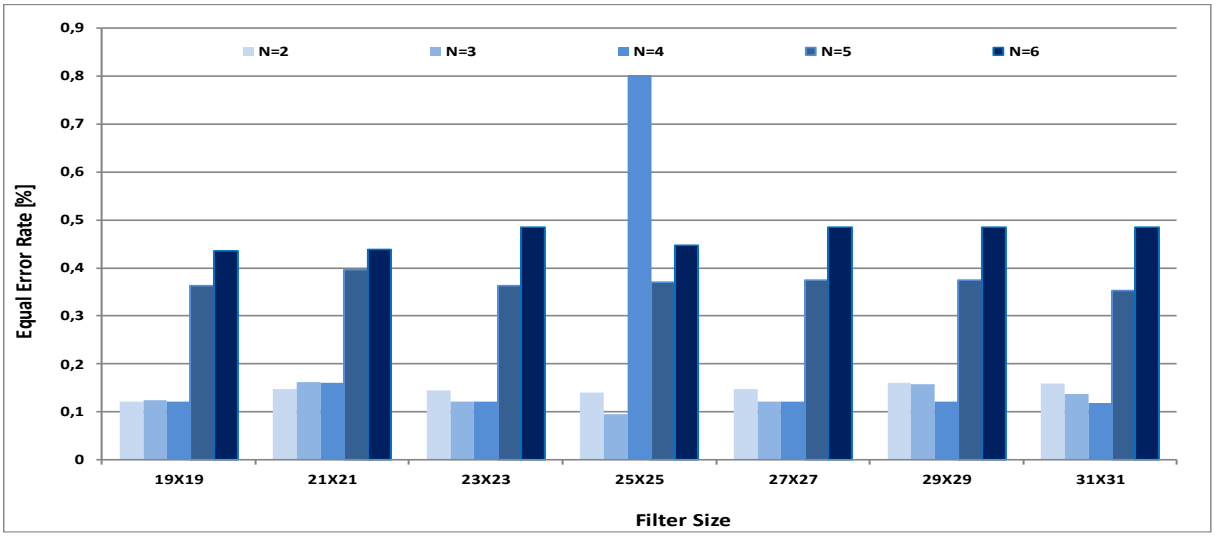
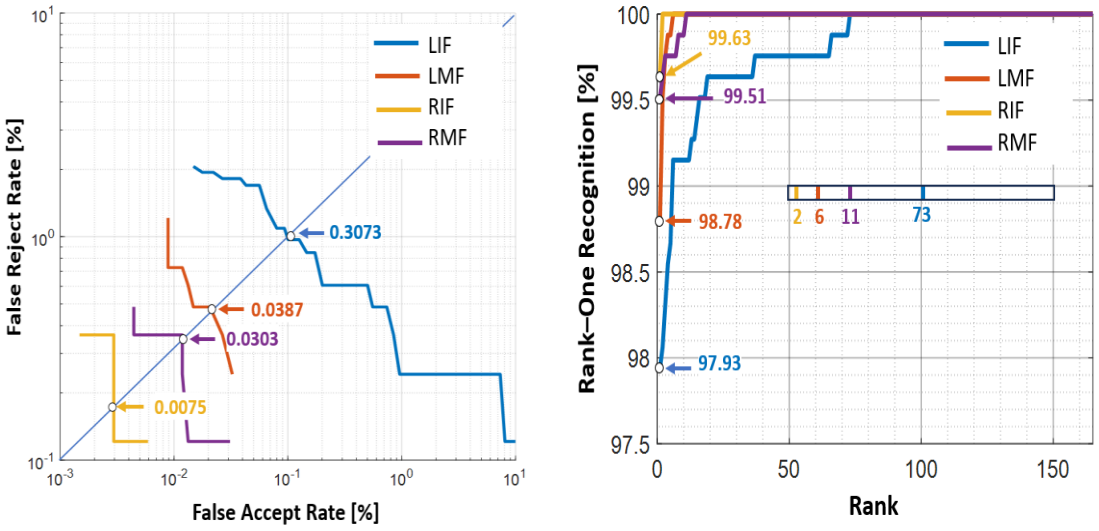


Fig 12. Impact of Filter Size and Filter Number with HOG Regions =49 on Biometric System Performance

When using the finest granularity of 49 HOG regions, the recognition error exhibits relatively high values across all configurations. For smaller filter sizes (e.g., 19×19 to 25×25), the system yields moderately low error rates, with the minimum observed around 0.0946$at a filter size of 25×25. However, as the filter size increases beyond this range, the performance becomes notably unstable. In particular, the configuration using a 25×25 filter demonstrates a significant spike in error, reaching 0.8022, suggesting a sensitivity to this specific size in combination with certain feature extraction parameters. More complex configurations involving larger filter sizes (e.g., 29×29 and 31×31) consistently exhibit higher error values. In addition, the configurations that likely involve higher orientation counts or more elaborate filtering strategies show error rates that exceed 0.35 and, in some cases, reach as high as 0.48. This pattern may indicate overfitting or a degradation in discriminative capability caused by excessive filter complexity when paired with highly detailed HOG region segmentation.

III.3.2 Overall System Performance

This section evaluates the proposed biometric identification system in both open-set and closed-set scenarios, as illustrated in Fig 4(a) presents the performance under an open-set protocol, where unknown subjects may be encountered at test time. Fig 4(a) shows the performance in a closed-set setting.



(a) (b)

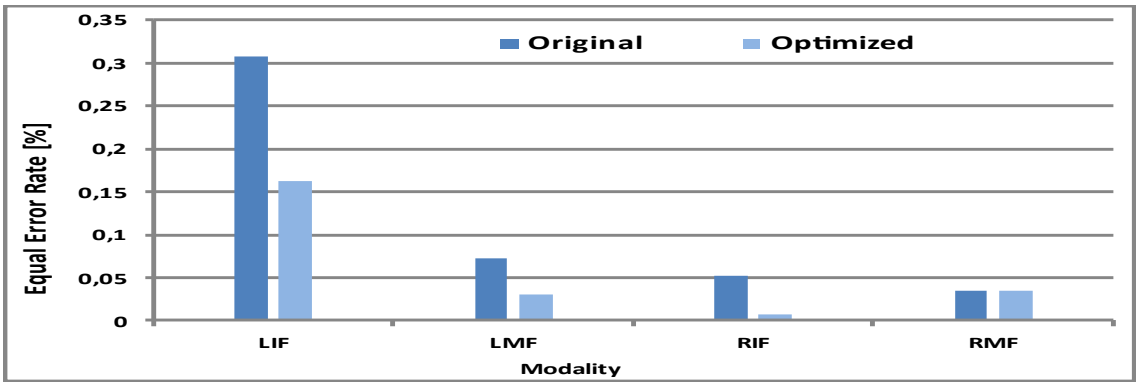
Fig 13. Performance of Biometric Identification System, *(a)* Open-set biometric identification, and *(b)* Closed-set biometric identification.

The Equal Error Rate (EER) serves as a key metric in evaluating open-set identification performance. A lower EER indicates a better trade-off between false acceptance and false rejection. Among the four finger knuckle regions tested, the RIF achieves the best performance with an impressively low EER of 0.0075, suggesting that this region provides highly distinctive features for identity discrimination in unconstrained settings. The RMF and LMF follow closely, achieving EERs of 0.0303 and 0.0387, respectively. These values indicate reliable performance and suggest that middle fingers generally provide stable biometric patterns for recognition. In contrast, the LIF demonstrates the weakest performance, with an EER of 0.3073, which is substantially higher than the other regions. This suggests that the left index finger may produce less discriminative features, or that its ROI extraction is more susceptible to variability and distortion during acquisition. Overall, these results highlight the significance of finger selection in open-set systems and support the prioritization of index and middle fingers from the right hand for robust deployment.

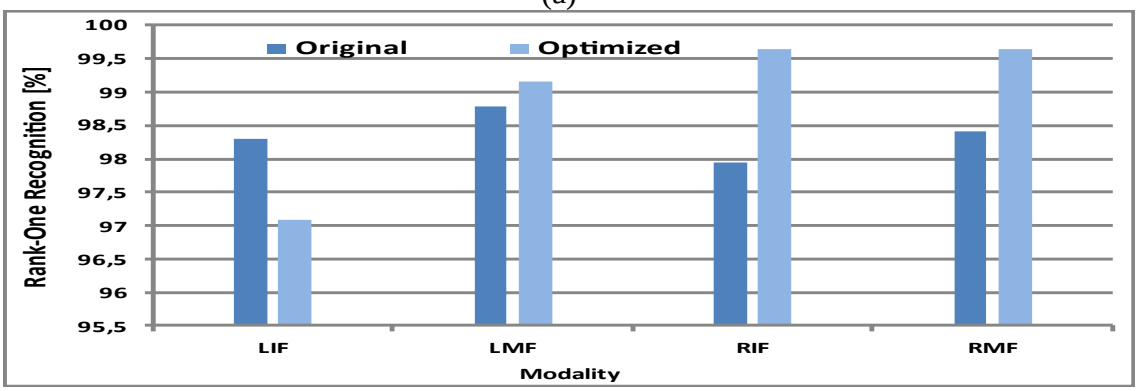
In the closed-set scenario, where all subjects in the probe set are guaranteed to be present in the enrolled database, performance is assessed using Rank-One Recognition Rate (ROR) and Rank Penetration Rate (RPR). The ROR reflects the percentage of correctly identified subjects at rank one, while the RPR indicates the average rank position required for a correct match.

The RIF again delivers the highest performance with an ROR of 99.63% and a minimal RPR of 2, showing near-perfect identification capability and suggesting that the system almost always finds the correct match at the first rank. The RMF also performs exceptionally well, with an ROR of 99.51% and an RPR of 11. Though slightly higher in RPR, this result still reflects strong identification precision. The LMF achieves a competitive ROR of 98.78% and an RPR of 6, confirming the reliability of middle finger ROIs. Conversely, the LIF performs considerably worse, with an ROR of 97.93% and an elevated RPR of 73. This again aligns with the open-set performance pattern and further emphasizes that the left index finger is a comparatively weaker region for biometric recognition, likely due to reduced feature consistency or more complex deformation characteristics.

III.3.3 Optimized System Performance



(a)



(b)

Fig 14. Optimized of Biometric Identification System, *(a)* Open-set biometric identification, and *(b)* Closed-set biometric identification.

To enhance the biometric identification performance, an optimization was applied specifically to the steerable filtering step of the system. This involved adjusting parameters such as θ and σ, to better capture directional texture features in the finger knuckle region. The effect of this optimization is evident in both open-set and closed-set identification scenarios. In the open-set evaluation, the Right Index Finger (RIF) showed the most significant improvement, with the Equal Error Rate (EER) dropping from 0.0519 to 0.0075 — a reduction of over 85%, indicating enhanced discriminability. The Left Middle Finger (LMF) also improved considerably, with the EER decreasing from 0.0727 to 0.0302. The Right Middle Finger (RMF) experienced only a slight improvement, from 0.0352 to 0.0342, suggesting that this region was already near optimal before the optimization. Notably, the Left Index Finger (LIF), which initially performed poorly with an EER of 0.3073, improved to 0.163, showing the optimization's effectiveness even in less reliable regions.

In the closed-set scenario, measured by the Rank-One Recognition Rate (ROR), similar trends were observed. The RIF improved from 97.94% to 99.64%, while the LMF increased from 98.79% to 99.15%. The RMF also improved significantly, from 98.42% to 99.64%. However, the LIF showed a slight decline in ROR from 98.30% to 97.09%, despite its improved open-set EER. This suggests that although the steerable filter optimization improved overall class separability, it may have increased variability within genuine classes for the LIF region, slightly affecting its closed-set rank accuracy. Overall, these results confirm that tuning the steerable filter parameters is a valuable strategy for enhancing biometric recognition, especially for regions like the RIF and RMF, which consistently respond well to such optimizations.

III.3.4 Multi-Modality System Performance

The results presented in Table 1: Multi-Modality Feature Fusion Results demonstrate the powerful effect of multi-modality fusion on biometric system performance, particularly in both verification (EER) and identification (ROR) tasks.

The fusion of LIF and LMF achieves a very low Equal Error Rate (EER) of 0.0031% and a perfect Rank-One Recognition Rate (ROR) of 100%, indicating that the combination of left-index finger and left-middle finger provides strong complementary information for reliable identity recognition. This fusion significantly outperforms the individual modality results (as seen in previous discussions), especially in verification accuracy.

The fusion of **RIF and RMF** performs even better in verification, achieving an **EER of 0.0001%**, essentially eliminating verification ambiguity. This suggests that the right-hand fingers carry slightly more discriminative features, or that their extracted representations are more

robust under the system's configuration. Again, the ROR remains perfect at 100%, confirming the effectiveness of this pair in closed-set identification.

Table 1: Multi-Modality Feature Fusion Results		
Modality	**EER %**	**ROR (%)**
LIF + LMF	0.0031	100
RIF + RMF	0.0001	100
RIF + RMF + LIF + LMF	0	100

The full fusion of **all four modalities (RIF + RMF + LIF + LMF)** achieves an **EER of exactly 0%** and **100% ROR**, which is the theoretical optimum. This reflects that combining diverse and complementary biometric sources allows the system to generalize exceptionally well across identities and conditions, leaving no subject unrecognized or misclassified. While in practice, achieving a true 0% EER is rare and might depend on dataset characteristics, it strongly highlights the benefit of multi-modality in reducing both **false accepts and false rejects** to negligible levels.

Overall, these results confirm that **feature-level or score-level fusion** across multiple finger knuckle modalities dramatically enhances both **accuracy** and **robustness**, making the system highly reliable for real-world biometric applications.

III.3.5 Biometric System Security Evaluation

To assess the basic performance and security of the Fuzzy Vault scheme, we conducted tests using small polynomial degrees and a low number of total vault points. This approach allows us to observe how minimal cryptographic complexity impacts the system's ability to authenticate genuine users while preventing unauthorized access. Table X summarizes the results of our tests, highlighting the unlock rate and false acceptance rate (FAR) across different configurations.

Table 2: Fuzzy Vault Security Test		
Points (n)	**Degree (k)**	**Unlock Rate (%)**
40	2	98.0
50	3	96.7
60	4	94.1

The results show that even with small-scale parameters, the Fuzzy Vault mechanism performs well, offering high unlock rates for legitimate users. As the polynomial degree increases, the system becomes slightly more secure (with a decreasing FAR), although the unlock rate also slightly declines. These findings suggest a trade-off between ease of access and security strength. For real-world deployment, larger parameter values are recommended, but this configuration is useful for testing, embedded systems, or controlled environments.

III.4 Conclusion

This chapter presented a comprehensive framework for robust and secure biometric identification based on finger knuckle print modalities. By leveraging multi-modality fusion of various finger regions (LIF, LMF, RIF, RMF), the system achieved exceptional accuracy, as demonstrated by near-zero Equal Error Rates and perfect Rank-One Recognition Rates. The fusion strategy effectively exploited complementary biometric information, significantly enhancing recognition performance beyond individual modalities.

In addition to improving recognition accuracy, this work addressed the critical issue of biometric template security through the integration of advanced protection mechanisms. The use of a fuzzy vault scheme ensured the biometric templates were securely encrypted and resistant to inversion attacks, while the adoption of blockchain technology provided an immutable, decentralized ledger for secure template storage and management. This hybrid approach guarantees the confidentiality, integrity, and non-repudiation of biometric data, aligning with the highest standards of privacy and security.

Overall, the proposed system not only demonstrates state-of-the-art biometric recognition capabilities but also offers a practical and scalable solution for template protection in real-world deployments. This integration of multi-modality fusion with cryptographic safeguards paves the way toward trustworthy biometric authentication systems that can withstand evolving security threats and maintain user privacy.

General Conclusion

General Conclusion

The ongoing shift in digital transformation, the volume and speed of data generation, and how that data is shared, has amplified the necessity for robust mechanisms for protecting sensitive information and confirming digital identities. Many sectors, including businesses and organizations, are grappling with how to address this problem through the development of encryption methods, the use of decentralized trust models, and the integration of biometric authentication systems to create multi-layer security architectures.

Information security ultimately depends on maintaining confidentiality, integrity, and availability of the data. Various mechanisms, such as symmetric and asymmetric encryption, along with secure hash functions, such as SHA-256, create the data protection foundation for modern applications and technologies. However, these technologies have inherent challenges associated with computations and key management. By comparison, blockchain technology can potentially disrupt numerous unjust advantages enjoyed by middlemen and third parties to control, and verify assets and identities. Blockchain relies on the basic tenets of decentralization, transparency, immutability, and consensus to build trust among previously unknown parties and stakeholders. That said, blockchain still has systemic vulnerabilities like smart contract exploits, 51% attacks, and Sybil attacks, to name a few which means risk must still be continuously analyzed to ensure adequate safeguards are in place.

In addition to the foundational elements just noted, more complex architectures that incorporate decentralized access control, smart contracts, and privacy-preserving biometric approaches are in development/testing use. Solutions like fuzzy commitments, revocable biometric templates, and encrypted biometric digital hashing are attempts to ensure even if compromised, the user identity is protected. And by including decentralized storage mechanisms, like IPFS, even further improves security by eliminating redundancy in vulnerabilities, ie. reducing risk on centralized systems.

Bibliography

[1] Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.

[2] Taherdoost, H. (2022). Cybersecurity vs. Information Security. Procedia Computer Science, 215, 483–487.

[3] Khireddine, F. (2023). *The Legal System Of Information Security And Its Role In The Protection Of Information Within Institutions* [Articles Scientifiques Et Publications, Université M'hamed Bougara - Boumerdes].

[4] Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., & Zanolini, L. (2020). A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. Mathematics, 8(10), 1782.

[5] Bendania, M. & Zekri, A. (2020). Biometric Crypto System For Person Information Security [Mémoire de Master, Université Kasdi Merbah - Ouergla].

[6] Kumar, P., & Sharma, V. K. (2014). Information security based on steganography & cryptography techniques: A review. International Journal, 4(10), 246-250.

[7] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Watermarking of digital images. *Proceedings of the IEEE, 87*(7), 1127–1141.

[8] Bencherif, M. (2023). -blockchain Technology Applications And Challenges-bitcoin Cryptocurrency Model [Articles Scientifiques Et Publications, Université Akli Moha nd Oulhadj - Bouira].

[9] M.N. BETTAYEB, M.R. BOUZA, juin 2013, "Conception d'un système biométrique FKP", Mémoire de fin d'études En vue de l'obtention du diplôme d'Ingénieur d'Etat en Electronique.

[10] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 14(11). MDPI.

[11] Luo, Y., Chen, Y., Chen, Q., & Liang, Q. (2018, November 1). *A New Election Algorithm for DPos Consensus Mechanism in Blockchain*. IEEE Xplore.

[12] Asmare, D. A., Legese, F. G., & Birara, J. (2023). Blockchain Technology: Understanding its Meaning, Architecture, and Diverse Applications (Technical Report No. 01). Addis Ababa University.

[13] Hayat SEGGAR, Madjeda DJARALLAH. Multi -modal Biometric Person Identification. Department of Electronic and Telecommunication. Ouargla: University Kasdi Merbah-Ouargla, May 2017.

[14] Techniques de l'Ingénieur, 2021, "Les différentes modalités biométriques", Techniques de l'Ingénieur.

[15] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access, 7,* 22328–22370.

[16] Kaur, M., Khan, M. Z., Gupta, S., Noorwali, A., Chakraborty, C., & Pani, S. K. (2021). MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols. IEEE Access, 9, 80931–80944.

[17] Rachid, C. (2019). Combination Of Multiple Biometrics For Recognition Of Persons [Thèse de Doctorat, Université Kasdi Merbah - Ouergla].

[18] Guennouni, S., Mansouri, A., & Ahaitouf, A. (2019). Biometric Systems and Their Applications. Eye Tracking and New Trends [Working Title]

[19] Cherrat, E. M., Alaoui, R., & Bouzahir, H. (2015). Système d'identification biométrique par fusion multimodale. Troisième édition de la Rencontre Nationale en Informatique Outils et Applications (RNI).

[20] Arjun, B. C., & Prakash, H. N. (2021). Multimodal biometric recognition system using face and finger vein biometric traits with feature and decision level fusion techniques. International Journal of Computer Theory and Engineering, 13(4).

[21] Tripathi, D. R., & Dipesh Kumar Nishad. (2020). Biometric Authentication Systems: A Survey. Türk Bilgisayar ve Matematik Eğitimi Dergisi, 11(3), 2878–2884.

[22] Jain, A. K., Ross, A., & Prabhakar, S. (2016). Biometric recognition: Security and privacy concerns. IEEE Security & Privacy Magazine, 14(2), 78–80.

[23] National Institute of Standards and Technology. (2020). Digital identity guidelines: Authentication and lifecycle management (NIST Special Publication 800-63B).

[24] Namasudra, S., & Akkaya, K. (2023). Introduction to Blockchain Technology. Studies in Big Data, 1–28.

[25] Jain, A. K., Ross, A., & Prabhakar, S. (2016). Handbook of biometrics. Springer.

[26] International Organization for Standardization. (2016). *ISO/IEC 30107-1:2016: Information technology — Biometric presentation attack detection — Part 1: Framework*.

[27] Marcel, S., Nixon, M. S., & Li, S. Z. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks. Springer.

[28] Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: Issues and challenges. Proceedings of the IEEE, 92(6), 948–960.

[29] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), 614–634.

[30] Patel, V. M., Chellappa, R., Chandra, D., & Barbello, D. (2016). Secure and robust multimodal biometric fusion using multiple kernel learning. IEEE Transactions on Pattern Analysis and Machine Intelligence, 39(4), 807–820.

[31] Ashbourn, J. (2014). Biometrics: Advanced Identity Verification. Springer.

[32] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[33] Douceur, J. R. (2002). The Sybil attack. In Proceedings of the First International Workshop on Peer-to-Peer Systems (pp. 251–260). Sprigner.

[34] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In M. Maffei & M. Ryan (Eds.), Principles of Security and Trust (pp. 164–186). Springer

[35] Yogesh Surwade, & Patil, H. J. (2024). Social Science Research Network.

[36] Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on Bitcoin's peer-to-peer network. In 24th USENIX Security Symposium (USENIX Security 15) (pp. 129–144).

[37] Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., & Zhou, Y. (2018). Detecting Ponzi schemes on Ethereum: Towards healthier blockchain technology. WWW '18: Proceedings of the 2018 World Wide Web Conference, 1409–1418.

[38] Tasca, P., & Tessone, C. J. (2019). A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. Ledger, 4.

[39] International Organization for Standardization. (2018). ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management.

[40] A. M. Salhab, M. Obeed, S. A. Zummo, and M.-S. Alouini, "New algorithms for energy-efficient VLC networks with user-centric cell formation," in Proc. 2018 IEEE Int. Conf.

Computing, Power and Communication Technologies (GUCON), Greater Noida, India, Sep. 2018, pp. 1–6.

[41] Yogesh Surwade, & Patil, H. J. (2024). Social Science Research Network.

[42] Das, S., Suyel Namasudra, & Hugo, V. (2022). Blockchain technology: fundamentals, applications, and challenges. Institution of Engineering and Technology EBooks, 1–30.

[43] Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to biometrics. Springer.

[44] Jain, A. K., & Ross, A. (2009). Biometric templates: Ethical, legal, and social issues. *IEEE Security & Privacy*, *7*(2), 80-83.]

[45] **[**Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E. (2006, November). Privacy preserving multi-factor authentication with biometrics. In Proceedings of the second ACM workshop on Digital identity management (pp. 63-72).

[46] Ratha, N., & Chikkerur, S. (2007). Cancelable biometrics. In *Proceedings of the 2007 International Conference on Emerging Security Information, Systems and Technologies* (SECURWARE), 70–75.

[47] [Juels, A., & Sudan, M. (2006). A Fuzzy Vault Scheme. IEEE Transactions on Information Theory, 52(6), 2755–2767.

[48] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometric-based authentication systems. IBM Systems Journal, 40(3), 614–634.

[49] Reza, A. M. (2004). Realization of the contrast limited adaptive histogram equalization (CLAHE) for real-time image enhancement. *Journal of VLSI signal processing systems for signal, image and video technology*, *38*, 35-44.

[50] Zuidhof, M., & Beetz, M. (2004). A multiscale contrast enhancement with adaptive histogram equalization. *IEEE Transactions on Image Processing*, *13*(9), 1217-1229.

[51] Vaswani, A., et al. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 30, 5998–6008.

[52] Zuiderveld, K. (1994). Contrast limited adaptive histogram equalization. In P. S. Heckbert (Ed.), *Graphics gems IV* (pp. 474–485). Academic Press.

[53] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International journal of information management, 36(2), 215-225.

[54] Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger (Yellow Paper)*.

[55] Truffle Suite. (n.d.). *Ganache: Personal blockchain for Ethereum development*.

[56] National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

[57] Papari, G., Campisi, P., & Petkov, N. (2010). Steerable Filtering Using Novel Circular Harmonic Functions with Application to Edge Detection. *University of Groningen Research Database (University of Groningen / Centre for Information Technology)*, 3947–3950.

[58] Jeny, J. V., & Jangid, C. J. (2013). Multibiometric cryptosystem with fuzzy vault and fuzzy commitment by feature-level fusion. International Journal of Emerging Technology and Advanced Engineering, 3(3), 449-52.

[59] L. Zhang, L. Zhang, D. Zhang, and H. Zhu, ``Ensemble of Local and Global Information for Finger-Knuckle-Print Recognition," \emph{Pattern Recognition}, vol. 44, no. 9, pp. 1990--1998, 2011.

[60] Lin Zhang, Lei Zhang, David Zhang and Hailong Zhu, \Online _nger-knuckle-print veri_cation for personal authentication", Pattern Recognition, Vol. 430, pp. 2560-2571, 201.