Securing Healthcare Communication Using Onion and Garlic Routing

Submitted By

Shruti B. Vaghadia

22MCES17

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF TECHNOLOGY, INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2024

Securing Healthcare Communication Using Onion and Garlic Routing

Major Project - II

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering (Cyber Security)

Submitted By

Shruti B. Vaghadia

(22MCES17)

Guided By

Dr. Jitendra Bhatia

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF TECHNOLOGY, INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2024

Certificate

This is to certify that the major project entitled **Securing Healthcare Communication Using Onion and Garlic Routing** submitted by **Shruti B. Vaghadia (22MCES17)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering (Cyber Security) of Nirma University, Ahmedabad, is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-II, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Jitendra
24/5/24

Dr. Jitendra Bhatia
Guide & Associate Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Vijay Ukani
Associate Professor,
Coordinator M.Tech - CSE (Cyber Security)
Institute of Technology,
Nirma University, Ahmedabad

Bhavsar

Dr. Madhuri Bhavsar
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr Himanshu Soni
Director,
School of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Shruti B. Vaghadia**, Roll. No. **22MCES17**., give undertaking that the Major Project entitled "**Securing Healthcare Communication Using Onion and Garlic Routing**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering (Cyber Security)** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made.It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student
Date: 24|5|2024
Place: Ahmedabad

24/5/24
Endorsed by
Dr. Jitendra Bhatia
(Signature of Guide)

Acknowledgements

I want to extend my heartfelt appreciation to everyone who has been a pillar of support during the progression of this project.

A special acknowledgment goes to **Dr. Madhuri Bhavsar**, Head of the Department at the Department of Computer Science and Engineering, Institute of Technology, Nirma University, and **Dr. Vijay Ukani**, MTech in Computer Science & Engineering (Cyber Security), for granting permission and providing essential facilities for the systematic execution of the project.

I am deeply grateful to my supervisor, **Dr. Jitendra Bhatia**, for their invaluable guidance and unwavering support. **Prof. Malaram Kumar** deserves special thanks for their consistent guidance and encouragement. Their expertise and constructive feedback played a pivotal role in helping me overcome challenges and make informed decisions.

A sincere thank you also goes to my friends and family for their constant love, support, and inspiration throughout this journey. Their unwavering confidence in my abilities served as a driving force, motivating me to work diligently on this project.

Shruti B. Vaghadia
22MCES17.

Abstract

Internet of Medical Things (IoMT) refers to the network of medical devices and applications connected to the healthcare IT systems through the Internet. IoMT is crucial in modern healthcare, enabling remote patient monitoring, data-driven decision-making, and improved patient outcomes. Focused on enhancing the security of the IoMT, this paper explores the integration of blockchain technology and privacy-preserving techniques, specifically onion and garlic routing. The research discusses blockchain's background in healthcare and the privacy-enhancing capabilities of onion and garlic routing. Findings encompass an in-depth analysis of blockchain-based security frameworks, the role of privacy-preserving techniques in IoMT, and the synergistic integration of blockchain and onion and garlic routing techniques. Findings are supported by a case study of the investigative experiment that highlights the advantage of having a routing method framework over traditional ones. Also provided case study, in which, the framework to develop IoT context aware security solutions for the detection of malicious traffic in the IoT use cases. The dataset that was generated by the IoT flock tool will help researchers to develop more robust security context-aware solutions specially for the IoT healthcare environment. The advantages identified include heightened data security, transparency, and tamper resistance. The paper concludes with insights into the evolving landscape of IoMT security, acknowledging the various trade-offs and suggesting future research directions.

Abbreviations

IoMT	Internet of Medical Things
IoT	Internte of Things
EHRs	Electronic Health Records
I2P	Peer-to-peer Network
HMAC	Hash-based message authentication codes
UAV	Unmanned aerial vehicle
IoMV	Internet of military vehicles
IIoT	Industrial Internet of Things
SDN	software-defined networking
IBE	Identity-Based Encryption
BIoT	Decentralized Blockchain-based IoT
PBFT	Practical Byzantine Fault Tolerance
Bi-LSTM	Bidirectional long-short term memory

Contents

List of Figures

Chapter 1

Introduction

1.1 Introduction

Internet of Medical Things (IoMT) is a rapidly growing network of interconnected medical devices that collect, transmit, and process patient data. Despite its immense potential to enhance healthcare delivery, IoMT presents several security and privacy challenges. Medical data is extremely private and sensitive, and compromise could harm patients. The Internet of Things (IoT) is a network of tangible things connected by technologies, software, and sensors. It allows users to gather and share information among various devices and systems with the help of Internet. IoT devices can transmit and collect data like humidity, temperature, movement, and location. IoT devices can also collect and automate functions like lighting, heating, and security systems. Large scale patient data collection, transmission, and analysis are made possible via the IoMT. This information can be used to reducing the healthcare costs and help in developing new drugs and treatments and improve the effectiveness and quality of patient care.

Many researchers have proposed various security frameworks and architecture to enhance healthcare data security. Two evolving cryptographic techniques i.e., Onion Routing and Garlic routing, can be applied to improve the security and privacy of data transmission in the IoMT environment. Garlic Routing makes it complex for unauthorized person or attackers to conduct traffic analysis by encrypting and tunneling multiple messages at a same time. For instance, a user wishes to transmit a message to a webpage via garlic routing. The user initially encrypts the message using multiple layers of encryption with a different key. The user then sends the encrypted message to several nodes inside the garlic routing network. After decrypting one layer of encryption, each node sends the data to the next node. Subsequently, the message is sent to the last node, which decrypts the final section of encryption. A network observant attacker can observe that the user is transmitting encrypted messages to several nodes, but they cannot decipher the messages' original recipient or information. It is because the messages are encrypted via multiple layers of encryption and routed across multiple nodes.

Encrypting messages and directing them around several network nodes, onion routing makes it more difficult for attackers to determine the message's point of origin and destination. For example, a user wishes to transmit a message to a webpage via onion routing. The user first encrypts the message through numerous levels of encryption, each using a different key. The user then sends the encrypted message to a network of onion routers. Once every onion router has broken one layer of encryption, it sends the data to the subsequent onion router. The last onion router decrypts the last level of encryption before sending the message through the webpage. An attacker monitoring the network may observe the user transmitting encrypted messages to a series of onion routers. Still, they are unable to decipher the messages' content or destination. It shows that the messages can be routed through several levels of encryption using a network of onion routers. Combining onion and garlic routing can further enhance security and privacy in data transmission. For example, onion routing could route messages encrypted through a network of onion routers, and garlic routing can encrypt and tunnel multiple messages concurrently. As a result, it would be considerably more difficult for attackers to intercept and look through the data in addition to figuring out the messages' origin and destination. Many applications utilize onion and garlic routing, such as VPNs, peer-to-peer networks, and the Tor network.

Garlic Routing and Onion routing are two approaches that can be implemented in increasing the security and privacy of information transmission. But it's very important to remember that this could be better; for instance, attackers could use sophisticated traffic analysis techniques to track the source and destination of messages routed through garlic routing and onion routing. However, attackers might have more difficulty monitoring users' online activities and intercepting their data when employing onion and garlic routing.

This research work proposes create a secure framework for IoMT applications utilizing onion and garlic routing. The proposed framework is also intended in securing IoMT data from unwanted access, alteration, and disclosure. Additionally, it seeks to protect users privacy by stopping attackers from following them around the Internet. Several use cases for the IoMT, including electronic health records (EHRs), telemedicine, remote patient monitoring, medical equipment management, clinical trial data management, and others, can be developed using the suggested secure framework.

1.2 Motivation

The need to address IoMT security vulnerabilities like unauthorized access, malware and to improve patient privacy and data integrity in healthcare applications has motivated us to do this research work. It recognizes the weaknesses of the current security protocols. It also aims to build a comprehensive and robust security framework specific to the needs of IoMT application by utilizing the onion routing and garlic routing. In addition to enhance patient trust, this framework will help IoMT application, facilitate adherence to healthcare data regulations like Health Insurance and Portability Act - HIPAA and General Data Protection Regulation - GDPR, and eventually help in creating cutting edge advance medical technology.

1.3 Scope of the paper

This research work focuses on improving security in IoMT-based healthcare applications. It introduces a security framework combining garlic and onion routing to enhance data protection, integrity, and availability in the IoMT environment. The scope of the research work includes framework design, performance evaluation, real-world case studies, and future research directions, aiming to advance security in IoMT, build patient trust, and facilitate compliance with healthcare data regulations.

1.4 Research Contribution

- Explored the diverse framework and architectures of blockchain technology implemented in healthcare industry, highlighting their strengths and weakness.
- Examined the role of Onion Routing and Garlic Routing techniques in preserving the privacy and confidentiality of medical data.
- Investigated how blockchain technology and privacy preserving techniques can be collaboratively implemented in creating a comprehensive security framework for IoMT applications.
- In-depth literature survey of various Blockchain-based frameworks for IoMT applications.
- Designed and develop blockchain based secured framework for IoMT applications.
- Developed the simulation model and evaluated the performance of the proposed framework.

1.5 Organization

The rest of the paper is structured as follows. Section II presents the background of the IoT, IoMT, onion and garlic routing. Section III represents related work including literature review. The system model and proposed approach is described in Section IV. Section V presents the results and discussion, and Section VI presents research challenges and future direction. Section VI concludes the paper.

Chapter 2

Background

This section discusses the background in the domain of the proposed work. It covers basics of blockchain technology, onion routing, garlic routing, security mechanism in healthcare and integration of IoMT and healthcare.

2.1 Blockchain Technology

Integrating IoMT into healthcare systems has ushered in a new era of possibilities, offering innovative solutions for patient care, monitoring, and data management. Yet the quick digitization of healthcare procedures has also brought about previously unheard-of difficulties, notably with regard to data security and privacy. The sensitive nature of medical information and the interconnected of medical devices necessitate robust security measures to safeguard patient confidentiality, prevent unauthorized access, and ensure the integrity of healthcare data.

Traditional healthcare systems, mostly relies on centralized databases and communication channels, faces various vulnerabilities such as single points of failure and increased susceptibility to cyber threats. The increasing complexity and frequency of cyberattacks highlight how it is important it is to review and enhance existing security frameworks and architecture of various healthcare system. In this regard, a promising solution toward enhancing the security position of IoMT applications is the integration of blockchain technology with privacy preserving routing methods.

Blockchain technology is a trending and buzz worthy as many companies and industry and taking this technology as feasible option. As blockchain technology is decentralized in nature and that ensure that healthcare data is not stored on single machine but across a network of computers. Secondly healthcare industry faces issues like interoperability and using this technology, seamless exchange of patient information can be shared between various healthcare providers.

Traditional systems are highly susceptible to hacking or data breaches or unauthorized access and this can lead to compromising patient privacy and identity theft. So, in [1] research work, the author has briefly explored the potential implications of implementing blockchain technology in the healthcare industry. The author discusses various challenges and limitations like regulatory compliance like HIPAA and GDPR, scalability and interoperability. The author also discusses the improvement of implementing blockchain technology in healthcare.

Maintaining patient privacy is important in healthcare because patient data confidentiality is not subject to negotiation. Onion routing and garlic routing, cryptographic techniques derived from anonymous communication, offer robust privacy solutions. These techniques layer encrypted data, concealing the source and destination of communication. Onion routing involves the sequential encapsulation of data in multiple layers, each accessible through decryption, while Garlic routing introduces parallel encapsulation, enhancing privacy and security.

2.2 Onion Routing

In onion routing, it's the server we intend to connect with when the link reaches the intended server within this circuit. After processing our request, it will send the web page that asked back to us over an identical network of nodes. This link is kept between several distinct nodes, i.e., it hops from one server to another. It is called onion routing because every time we hop or visit a server, a new key is generated to encrypt the message we give and the reply we receive.

All of the keys are accessible to the client, but only the keys needed for decryption and encryption on the specific server are accessible to the servers. This procedure is called onion routing because it encrypts your message and requires you to peel off layers of encryption at each hop, much like peeling off an onion.

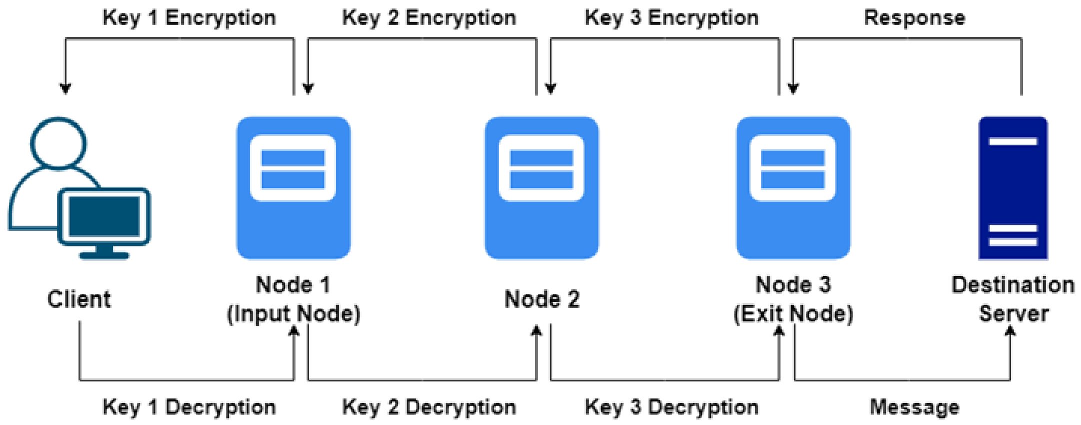

Figure 2.1: Onion Routing

Onion routing is explained with the example in Figure 2.1.

- The client, who possesses all three encryption keys, The request is encrypted thrice, concealing it under three successive layers that need to be sequentially extracted, much to the process of peeling an onion.

- Subsequently, this communication, which has undergone triple encryption, is sent to Node 1, the initial server (Input Node).

- Node 1 just has Node 2's location and Key 1. After decrypting the transmission using Key 1, Node 1 passes it to Node 2. However, Node 2 realizes that the message is still useless due to the presence of two levels of encryption.

- Node 3, also known as the departure node, eliminates the last layer of encryption prior to identifying and transmitting a GET request for the server to its intended target server.

- Once the request for information has been processed, the server will restore the intended site.

- In reverse order, the response traverses the identical nodes, wherein every node applies a distinct layer of encryption using its own key.

- Whenever each of the keys are accessible to the client, it can be decrypted when it eventually reaches them as a triple encrypted response.

In healthcare, patient privacy and trust is very essential. For this, author of [2], explores the integration of blockchain technology with Onion Router Network (Tor) to increase the patient trust and privacy. The authors suggest a cutting edge framework where authors have used distributed ledger, which can be used to verify reliability and integrity of all nodes in the network thereby reduce the risk of compromised or attack communication path. It also outline the advantages and disadvantages, and integration of blockchain technology and anonymous network.

2.3 Garlic Routing

Garlic Routing is also a type of method used for anonymous communication. It is similar to onion routing, just the difference is that it particularly used Invisible Internet Project (I2P) network. In this, multiple messages are referred as cloves which are bundled together in a single encrypted packet i.e. garlic. This will enhance efficiency and privacy of the message.

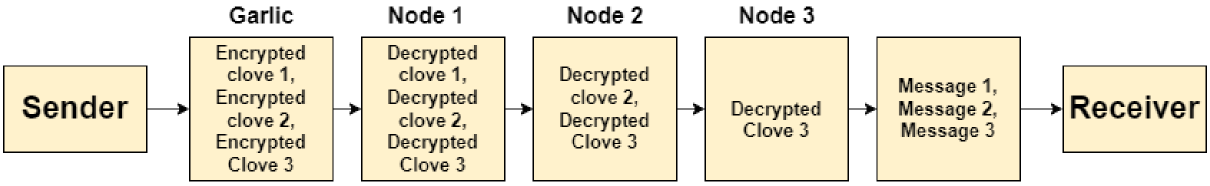
Sender
Garlic
Encrypted clove 1, Encrypted clove 2, Encrypted Clove 3
Node 1
Decrypted clove 1, Decrypted clove 2, Decrypted Clove 3
Node 2
Decrypted clove 2, Decrypted Clove 3
Node 3
Decrypted Clove 3
Message 1, Message 2, Message 3
Receiver

Figure 2.2: Garlic Routing

Garlic routing is explained with the example in Figure 2.2.

- Sender creates a bundle called garlic with three different messages.

- Sender encrypts each message with the public key of selected node in the desired path. Sender encrypts message 1 with node 1 public key and it becomes encrypted clove 1. Just like this, encrypted clove 2 and encrypted clove 3 is created.

- Sender sends whole garlic (three encrypted clove).
- Node 1 uses it private key and decrypt the encrypted clove 1. Node 1 won't able to decrypt encrypted clove 2 and encrypted clove as it doesn't have it's private key.
- This process is repeated for Node 2 and Node 3 and by this decrypted clove 2 and decrypted clove 3.
- Finally, the receiver will get the decrypted message.

Industrial Internet of Things (IIoT) is an extension and application of IoT where this technology and concepts in used in industrial environments. This technology targets machinery or infrastructure of various industrial unlike traditional IoT technology which focus on smart homes and wearable devices. In [3], authors uses deep learning techniques with garlic routing, to ensure the privacy and security in data transmission. The GRADE framework which is also known as Blockchain and garlic routing based secure data exchange framework. The paper also provide a detailed explanation of GRADE framework, addressing the security challenges in IIoT network.

2.4 Healthcare

The history of healthcare is a fascinating journey marked by significant milestones, paradigm shifts, and advancements that have shaped the way we have approach for wellness and disease management. From the ancient practices i.e., using herbal remedies and ritualistic healing to the advance, sophisticated, technology driven healthcare systems of today, the evolution of healthcare can be divided into different eras. This journey, from healthcare 1.0 to 4.0, captures the revolutionary changes in medical understanding, treatment methodologies, and the integration of digital tools and technologies. In this analysis, we will delve into each stage of healthcare evolution, tracing the evolution from traditional healthcare to the modern, digitally driven healthcare.

Healthcare 1.0: Ancient and Traditional Medicine (Prehistoric times to 19th century)

- Early humans relied on herbal remedies, rituals, and tribal medicine.

- Ancient civilizations like Egypt, China, Greece, and India developed various medical practices.
- Hippocrates, known as the "Father of Medicine," introduced the concept of the four humors.

Healthcare 2.0: The Age of Scientific Medicine (19th century to mid-20th century)

- The discovery of germs by Louis Pasteur and the development of the germ theory of disease.
- Advancements in surgery, anesthesia, and antiseptics (Joseph Lister).
- The establishment of medical schools and the professionalization of healthcare.

Healthcare 3.0: The Rise of Modern Medicine (Mid-20th century to late 20th century)

- Antibiotics revolutionized the treatment of bacterial infections (penicillin discovery by Alexander Fleming).
- The development of vaccines for widespread disease prevention (polio, measles, etc.).
- The proliferation of imaging technologies in medicine (X-rays, MRI, CT scans).

Healthcare 4.0: Digital Revolution (Late 20th century to early 21st century)

- Adoption of EHR to digitize patient information.
- Telemedicine and telehealth initiatives started to connect patients with healthcare providers remotely.
- The use of computers and technology in medical research, diagnosis, and treatment planning.

Each of these stages represents a significant shift in the approaches, technologies, and paradigms within the healthcare sector as shown in the Figure 2.3. The transition from 1.0 to 4.0 highlights the progression from ancient and traditional practices to the incorporation of digital technologies and data-driven strategies in modern healthcare. Keep in mind that these are generalizations, and the actual evolution of healthcare is more complex and nuanced.

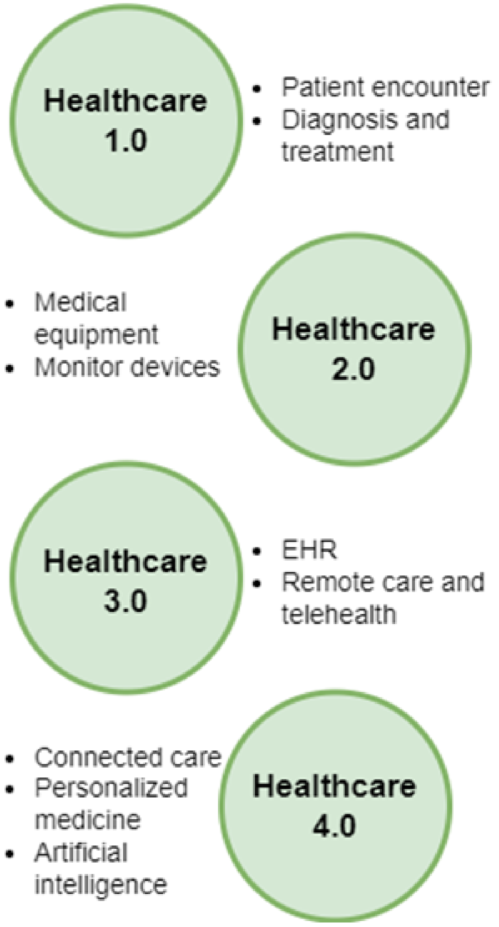

Figure 2.3: Evaluation of Healthcare

2.5 Integration of IoMT and Healthcare

IoMT is a key component of the modern healthcare landscape and falls under the broader category of Healthcare 4.0 or the Digital Revolution in healthcare. Healthcare 4.0 represents the integration of digital technologies, connectivity, and data-driven approaches into healthcare systems. The term ”IoMT” pertains especially to the internet-connected network of medical devices and applications capable of gathering, transferring, and analyzing healthcare data. The key aspects of IoMT in healthcare include:

- Connected Devices: IoMT involves the use of various connected devices, such as wearable fitness trackers, smart medical devices, and remote patient monitoring systems.

- Data Collection and Monitoring: Real time health data is gathered by various IoMT devices, allowing for ongoing patient observation. In addition to other pertinent health metrics, this information may include vital signs, activity levels, and adherence to medications.

- Remote Patient Monitoring: The IoMT enables medical practitioners to remotely monitor the well-being of the patient they treat. This is especially helpful for postoperative care, maintaining chronic illnesses, and other circumstances where ongoing observation is important.

- Enhanced Diagnostics: By utilizing linked medical imaging equipment, sensors, and diagnostic instruments, IoMT helps to improve diagnostics as well as more precise diagnosis and treatment may result from this.

- Telemedicine and Telehealth: IoMT is a key component for both telehealth and telemedicine usage, enabling secure network-based health related data transmission, virtual consultations, and remote healthcare services.

- Data Analytics and AI: IoMT generates data in enormous quantity and Data Analytics and Artificial Intelligence are two techniques that can be use in this case. This analysis can provide valuable insights into patient health trends, support clinical decision-making, and contribute to predictive analytics for preventive care.

IoMT is a transformative force in healthcare, offering opportunities to enhance patient care, improve efficiency, and enable more proactive and personalized healthcare approaches. It is part of the broader movement toward digitization and connectivity within the healthcare ecosystem, contributing to the ongoing evolution of healthcare delivery. Authors of [4], explores the probable chances of integration of IoMT applications in the development of advance smart healthcare system. The authors has also did a systematic review of various IoMT applications and impact on healthcare delivery, remote monitoring system. The main focus is to make healthcare system to create more patient centric, technology based and efficient advanced healthcare environments.

Chapter 3

Related Work

This survey represents the state of art in IoMT domain. Research in this domain are explained as per taxonomy in Table 3.1, 3.2 and 3.3. Explored research work in three key aspects: Blockchain Technology, Onion Rounting and Garlic routing, and the Integration of Onion and Garlic routing with blockchain technology. Highlighted the significance of each in enhancing healthcare security. Referenced relevant Figure 3.1 to illustrate key concepts.

3.1 Literature Review

Health information analysis is the process of examining and analysis data related to various healthcare data i.e. patient health records, clinical trails and laboratory results. So in [5], authors have presented a detailed and comprehensive framework for securing

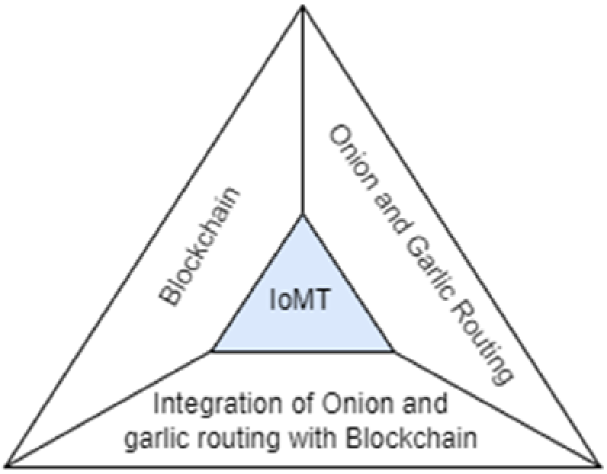

Figure 3.1: Literature Review

health data management and data analysis in respect to IoMT. By integration blockchain technology, this framework will ensure tamper proof, transparent access control and also thereby address data security and trustworthy healthcare applications.

Table 3.1: Literature Review - Blockchain based security framework for IoMT applications

Author	Year	Objective	Tools and Technology Used	Challenges	Future Scope
Dilawar N. et. al. [6]	2019	Implementing robust encryption protocols for enhancing security in IoMT data transmission.	Blockchain, P2P communication, PoW, Access Control	Integration, Scalability, Privacy concerns	Enhanced Security measures and interoperability
Kumar R. et. al. [7]	2021	Security and Privacy based framework for IoMT applications using blockchain.	Blockchain, File System	Security, Privacy	Privacy Enhancement
Egala B. S. et. al. [8]	2021	Fortified-Chain: A blockchain based framework for security and privacy assured IoMT for effective access control	Blockchain, Regulatory Framework	Security, Access Control, Privacy	Privacy Measures
Mallick S. et. al. [9]	2021	EMRI: Scalable and Secure Blockchain based IoMT framework	Blockchain	Scalability, Security, Transaction Efficiency	Scalability
Rahmani M. K. et. al. [10]	2022	Blockchain based trust management framework for IoMT applications.	Blockchain, Cloud Computing	Trust Management, Scalability, Security	Enhanced Scalability, Trust Models
Mallick S. R. et. al. [11]	2022	Integration of Blockchain Technology with fog computing and IoMT framework.	Blockchain, Fog Computing, IoMT	Integration, Security, Complexity	Optimization, Standarization
Rafique W. et. al. [12]	2023	Securemed: A blockchain based privacy preserving framework	Blockchain	Security, Scalability, Privacy Preservation	Enhanced Privacy, Real World Implementation
Alshammari B. M. et. al. [13]	2023	AIBPSF-IoMT: AI and Blockchain based predictive security framework for IoMT technologies.	Blockchain, Artificial Intelligence	Predictive, Security, Integration, Scalability	Advance AI, Integration
Alshammari R. A. et. al. [14]	2023	Resilient Security framework using TNN and Blockchain using TNN and Blockchain for IoMT applications.	Blockchain, Trained Neural Networks	Resilience, Integration, Complexity	Integration
Wazid M. et. al. [15]	2023	BACK-EHA: A framework blockchain based security solution for IoMT based healthcare applications.	Blockchain	Security, Integration	e-Health application, Security

Message Authentication Code (MAC) is a cryptographic technique that ensure authenticity and integrity of message that is transmitted over a network. So in [16], author proposes a secure framework for protecting data transmission. Authors has proposed a framework which is known as Elliptic Curve Menezes–Qu–Vanstone-based message authentication code (ECMQV-MAC) protocol for securing data transmission between various medical devices. Also, utilization of Encrypted K-means clustering based stellar consensus protocol (EKMC-SCP) to ensure data integrity and data confidentiality of medical data using Blockchain Technology that is transmitted over IoMT network.

Two factor authentication (2FA) is a process which is widely used for security in any application that requires two different types of identification like pin, password or security answer before allowing the user to use that application or system. In [17], author proposed a robust and efficient two factor authentication scheme (TFAS) especially designed for blockchain based IoMT application. Authors has used this framework for Physical Unclonable Functions (PUFs) that used to inherent physical variants in manufacturing and materials process for creating unique and unclonable identifiers for various electronic devices. Authors also have applied this framework on a cryptographic techniques i.e. Fuzzy Extractor which can be used in generating stable, reproducible cryptographic keys from noise, non uniform data generated from IoMT applications. The main objective is to enhance the security and authentication process.

Table 3.2: Literature Review - Onion Routing and Garlic Routing in Security

Author	Year	Objective	Tools and Technology Used	Challenges	Future Scope
Li Min, et. al. [18]	2020	Proposed a blockchain technology based decentralized authentication scheme using two way peg protocol for smart communities.	Sidechain Technology, Two way peg protocols, Garlic Routing, Onion Routing	Ensuring decentralized system	Scalability and Efficiency
Cheng Xinga, et. al. [19]	2021	Developed a anonymous communication system using Software Defined Architecture (SDN).	Communication Protocols, SDN	Privacy, Network Management Efficiently	Security Threats
Sankar S, et. al. [20]	2021	To increase security in blockchain based peer to peer network for beyond 5G and IoT	Peer to Peer Network, Blockchain Technology, IoT, Beyond 5G	Integration of Blockchain with IoT	Scalable Blockchain Solutions.
Samuel Omaji, et. al.[21]	2022	Developed a anonymous IoT based e-healthcare monitoring system using Blockchain Technology.	IoT, Blockchain Technology, Garlic Routing, Onion Routing	Data Security and Data Scalability	Interoperability with existing healthcare system
Samuel Omaji, et. al. [22]	2022	Developed a framework GarliChain, privacy based preserving system for smart grid consumers using Blockchain Technology.	Blockchain Technology, Garlic Routing, Smart Grid	Ensuring consumer privacy.	Integration with existing smart grid system
Patel Maitri, et. al. [23]	2023	Developed an framework using AI and Blockchain technology using Onion Routing for securing IoT communications.	AI, Blockchain Technology, Onion Routing. IoT	Scalability, Integration	Advance AI Techniques, Broader IoT applications
Maalavika S., et. al. [24]	2023	Use of garlic routing and AI application in various public networks.	AI, Garlic Routing	Robust Privacy Network, Integration to existing networks.	Security Mechanism
Li Jiatao, et. al. [25]	2023	To develop a data sharing for IoT based on Blockchain Technology and Onion Routing.	Blockchain Technology, IoT, Onion Routing	Ensuring data privacy and security, Integration	Efficient Data sharing mechanisms
Mohd Anwar, et. al. [26]	2023	Designed a mutual authentication method using deep learning - hybrid cryptography techniques for securing data in cloud computing.	Deep Learning, Cloud Computing, hybrid cryptography techniques	Secure Authentication	Robustness authentication methods
Jadav Nilesh, et. al. [27]	2023	Proposed a privacy preserving architecture for secure data transmission between Internet of Mobile Vehicles (IoMVs) using Garlic Routing with 5G networks.	Garlic Routing, 5G, Internet of Mobile Vehicles (IoMVs)	Privacy in data exchange	Efficiency and Scalability

Vehicle-to-Everything i.e. V2X communications helps vehicle to communicate with various entities like other vehicles that is (Vehicle-to-Vehicle (V2V)), to other people (Vehicle-to-Person (V2P)), to infrastructure (Vehicle-to-Infrastructure (V2I)) and to networks (Vehicle-to-Networks (V2N)). So the authors of [31], address the security challenges that can come in Vehicle-to-Everything (v2X) communication networks. The author has proposed an advance and intelligent garlic routing approaches in enhancing data trans-

Table 3.3: Litrrature Review - Integration of Blockchain and Routing Techniques in security

Author	Year	**Objectives**	**Techniques**	**Future Scope**
Gupta et. al. [28]	2022	Secure message exchange	Blockchain, Onion routing, LSTM, AI	Testbed for additional security attacks
Samuel et. al. [21]	2022	Blockchain based anonymity	Blockchain, garlic routing, PoA and PoEoI consensus	Cost analysis, scalability, collaboration
Gupta et. al. [29]	2022	Secure data dissemination	Blockchain, onion routing, AI	Scalability, privacy, effeicency security
Gupta et. al. [30]	2022	Secure D2D communication	Blockchain-based onion routing	Blockchain based onion routing protocol for IoMV
Samuel et. al. [22]	2022	Privacy and anonymity	Garlic routing, blockchain, onion routing, differential privacy	Transaction reversibility scalability, efficency

mission in V2X communication networks.

Enhancing data privacy and integrity in healthcare systems through the integration of blockchain technology and routing algorithms like onion routing and garlic routing is a novel approach to the security of the IoMT. It can guarantee the security, integrity, and accessibility of sensitive medical data by utilizing the tamper-evident ledger of blockchain technology in conjunction with the secure data transmission capabilities of routing approaches. This combination also allows data to be safely transmitted between devices, providers, and databases and creates permanent records of medical transactions. The integration of blockchain technology with routing approaches has great promise for revolutionizing IoMT security, enhancing patient trust, and more effective and secure healthcare services through collaborative research and innovative solutions.

Dilawar et. al. [6] proposes the use blockchain technology to assure the confidentiality of IoMT data transmission. It proposes an IoMT-based architecture for security that uses blockchain technology to enable secure data transmission over connected nodes and talks about the underlying technology of blockchain. The paper's primary contribution is its use of blockchain technology to deal with the requirements for secrecy, authenticity, and integrity in the IoMT system.

Sharma et. al. [9] proposes a framework called EMRI that utilizes Blockchain technology to enhance scalability, privacy, and security in healthcare data transactions. IoMT platform's centralised architecture frequently raises issues with scalability, privacy, and security. EMRI offers a decentralised, unchangeable environment for safe communication and patient data privacy protection through the integration of Blockchain technology. To guarantee the compliance of privacy policies and the authenticity of blocks, the framework integrates smart contracts and PoW. EMRI reduces requirement for patient mobility and depends less on third parties by providing a scalable and secure system for healthcare data transactions.

Jolfaei et. al. [32] presents a study of blockchain-based IoMT systems with a focus on scalability. It examines previous work, points out a scalability gap, and suggests ways to close it. The study also covers the privacy and security features of IoMT systems and highlights how blockchain technology may offer robust security.

Pratima et. al. [33] proposes Using the Identity-Based Encryption (IBE) algorithm, a blockchain-based IoT architecture that fortifies the security of healthcare systems. The architecture seeks to enhance data exchange procedures while protecting patient privacy and security. It makes effective use of smart contracts to outline the fundamental functions of the healthcare system and permits EHR sharing. Through testing, the suggested scheme is assessed and determined to be more effective than well-known schemes currently in use. Overall, the study offers a viable strategy for leveraging blockchain and IoT technologies to improve the efficiency and security of healthcare data sharing.

Ali et. al. [34] proposes a new architecture based on software-defined networking (SDN) for heterogeneous and complex IoMT networks. The primary innovation is the implementation of a multiprotocol controller that can support various wireless communication protocols and machine learning algorithms for prioritising tasks based on time constraints and load balancing. In order to promote multiprotocol concord in IoMT environments, the paper attempts to address the difficulties in managing and sustaining communication in heterogeneous networks and offer an adaptive and programmable networking strategy.

Nameem et. al. [35] proposes a comprehensive analysis of the architecture, protocols, and applications of the IoMT in the healthcare industry. It examines the application of blockchain, edge/fog computing, and machine learning in IoMT systems and talks about the possibilities as well as the obstacles in the field. The objective of this paper is to furnish a comprehensive synopsis of IoMT and its prospective advantages within the domain of medicine.

Sadek et. al. [36] discusses the privacy and security challenges of IoT healthcare systems and proposes a robust solution for real-life deployment. It discusses possible hostile assaults on IoT medical devices and offers particular defences and strategies against them. In addition, the paper presents the AMbient Intelligence (AMI) Lab architecture as a case study centred around the Internet of Things and evaluates its efficacy against existing IoT solutions. The paper's overall goal is to offer guidance and practical solutions for guaranteeing the privacy and security of IoT healthcare systems.

Sharma et. al. [11] presents Blockchain-Fog-IoMT architecture for medical care, integrating blockchain, fog computing, and IoMT. It aims to enhance security, privacy, and scalability while reducing processing overhead. The framework enables faster data processing, remote patient tracking, and monitoring, creating a decentralized platform for healthcare services.

Filippos et. al. [37] presents PBFT is a robust consensus technique for IoMT blockchains. Among resource-constrained IoMT devices, the approach seeks to improve scalability, lower communication overhead, improve security, enable decentralised accountability, as well as remove single points of failure.

Ramzan et. al. [38] discusses security and resource effects related to the incorporation of multi-ledger blockchain technologies into IoMT are analysed. It emphasises the drawbacks of using centralised data storage in IoMT applications and the advantages of implementing blockchain technology. According to the findings, switching to a decentralised Blockchain-based Internet of things (BIoT) enhances security, independence from external parties and the elimination of a singular point of failure. With resource-constrained IoMT devices, the suggested multi-ledger blockchain architecture exhibits scalability and flexibility.

Kumar et. al. [39] has proposes a framework that combines fog computing, blockchain technology, and AI for secure home monitoring of COVID-19 patients. It involves wearable smart devices, secure communication, and a private blockchain. Experimental results show improved machine learning performance and reduced data poisoning attacks.

Panasenko et. al. [40] has proposed a lightweight blockchain scheme for IoMT that focuses on ensuring data integrity and authenticity. The scheme utilizes hash-based message authentication codes (HMAC) and a simplified consensus algorithm suitable for low-resourced sensor devices. By leveraging HMAC based on common cryptographic standards, the scheme provides a high level of security and prevents fraudulent falsification of data. While acknowledging its limitations, the paper highlights the scheme's advantages and considers it reasonably common for IoMT applications. Future work includes developing a protocol for transferring patients between intermediate computers to address one of the main limitations of the scheme. All things considered, the suggested plan provides a workable way to handle IoMT data processing that ensures authenticity and integrity.

Mecline et. al. [41] suggests a framework for the secure exchange of data over IoMT using blockchain technology along with Bald Eagle Search Optimisation. The framework attempts to solve the problem of safely exchanging patient health data across IoMT devices. The suggested framework comprises the following six stages: information sharing, data preservation, authentication, registration, as well as key issuance. The article assesses the effectiveness of the suggested method using results from experiments and comparative analysis.

Mallick et. al. [42] has Intelligent healthcare systems have been integrated with Blockchain technology and IoMT via a proposed framework. This framework aims to provide decentralised, secure, and transparent healthcare services. It includes fog computing and mist computing to improve performance and reduce latency. By utilising a drop-off standing mechanism, utility and patient delay periods are reduced when connecting to the Mist system. An analytical model and numerical findings are provided in the paper to illustrate the efficacy of the proposed system. In general, the article highlights the benefits of implementing Blockchain-based IoMT in the medical field and proposes avenues for additional study.

Sandi et. al. [43] has A privacy-preserving architecture was suggested for the purpose of securely detecting misbehaviour in lightweight IoMT devices, with a specific focus on the APS. In order to enhance confidentiality and safety, the architecture integrates Bi-LSTM via blockchain technology. The suggested model uses a corresponding incentive structure and achieves sustainable privacy preservation. Empirical benchmarking of the model's efficacy demonstrates a high recall rate for identifying malicious events. Along with these topics, the paper covers related work, the essential system models as well as components, and the suggested system's architectural design. All things considered, the paper offers a thorough strategy to handle privacy and security issues in lightweight IoMT devices.

Lakhan et. al. [44] presents A blockchain-based federated learning solution designed for healthcare within the IoMT.The system's objectives are to protect patient privacy and eliminate fraud in medical applications. It introduces the FL-BETS framework, which schedules workloads on distributed fog and cloud nodes to ensure privacy preservation and fraud prevention while minimising latency and the use of energy. The current blockchain and machine learning techniques are surpassed in terms of fraud detection, validation of information, power consumption, and delay limits by the design. The study concludes by discussing future work on mobility fraud detection and anomaly detection in the blockchain-enabled fog-cloud network.

Ishita et. al. [45] describes a secure blockchain technology architecture for IoMT-device-based medical application development. It concentrates on integrating biometric authentication and bio-keys to improve security and privacy within the healthcare ecosystem. The upsides, drawbacks, and difficulties of combining blockchain technology with IoT are covered in the paper, along with how blockchain can help guarantee data security and privacy in the medical field.

Kumar et. al. [31] proposes an architecture for enhancing the security of V2X communication in the IoT ecosystem. It utilizes AI-based classifiers, garlic routing, and blockchain integration to secure data exchange. The proposed architecture achieves high accuracy in classifying data and reduces the likelihood of data compromise. The paper focuses on securing V2X communication and does not explicitly mention its limitations.

Kumar et. al. [3] introduces GRADE, a secure data sharing framework for IIoT. It utilizes deep learning and garlic routing techniques to address security challenges in IIoT environments. The framework predicts non-malicious and malicious data requests using LSTM-based Nadam optimizer and forwards non-malicious requests through the GR network. Session tags are encrypted and stored in an IPFS-based blockchain for scalability. GRADE aims to enhance data security in IIoT by combining these technologies.

Kumar et. al. [27] proposes a garlic routing-based framework for secure data exchange between Internet of military vehicles (IoMVs) using 5G technology. Several encryption layers are used by the framework to guarantee security and privacy. When compared to other schemes, it provides low bit error rates as well as a high anonymity rate. In border regions, the suggested framework improves IoMV security and privacy.

Kumar et. al. [46] proposes a secure framework for sharing EHRs in healthcare 4.0. It utilizes an unmanned aerial vehicle (UAV)-assisted system that incorporates onion routing (OR) network and artificial intelligence (AI)-based techniques. The OR network protects patient data from numerous threats by guaranteeing its security and anonymity. AI algorithms are used to identify whether EHR data is malicious or not, enabling the forwarding of only non-malicious data. The model achieves high rates of anonymity and accuracy when evaluated based on performance metrics. The study emphasises the need of security in EHR systems and offers an OR and AI-based solution for safe EHR sharing in the context of healthcare 4.0.

Gupta et. al. [29] proposes a framework for secure and anonymous data dissemination in IoT environments using blockchain and AI-based secure onion routing. The framework attempts to solve security, privacy, scalability, and efficiency concerns with the distribution of IoT data. It makes use of blockchain and onion routing with private and secure communication, and machine learning algorithms for data classification. The suggested framework attains low latency, low cost of storage of data, and high accuracy. Future work will be focused on enhancing security, efficiency, privacy, and scalability.

Gupta et. al. [30] proposes a blockchain-based onion routing protocol called B-IoMV for secure and anonymous D2D communication in an IoMV environment. The necessity of security, privacy, anonymity, and trust are all addressed in relation to military missions involving intelligent and networked military vehicles. Blockchain technology is used by the protocol to guarantee data sharing, accurate documentation, and transparency amongst IoMVs. Additionally, it uses the IPFS protocol to increase scalability and efficiency. Data storage costs, network bandwidth usage, and communication latency are used to assess the suggested solution.

Gupta et. al. [22] proposes a blockchain system called GarliChain to address privacy and anonymity issues in energy trading within smart grids. GarliChain protects prosumers' privacy and anonymity by fusing consortium blockchain technology with garlic routing. It presents a reputation management system, a stochastic path selection algorithm, and an enhanced encryption mechanism. The efficient operation of the suggested system is confirmed by simulation results, which also demonstrate that it is secure against both active and passive attacks. The efficiency of GarliChain for prosumers in smart grids is highlighted in the paper along with a comparison with other current systems.

The smooth amalgamation of blockchain technology with privacy-maintaining routing methodologies, like Onion and Garlic Routing, offers an all-encompassing security structure for IoMT applications. A thorough analysis of how these technologies work together to improve the overall security posture for medical data transmission is given in this section. Also the techniques, objectives and future scope are there mentioned in the table **??**.

Gupta et. al. [28] proposes a secure message exchange system for the IIoT that combines blockchain and onion routing technologies. It uses an AI-based algorithm to classify non-malicious and malicious message requests, and enhances the security of the onion routing network with additional fields. The system is evaluated using various performance metrics and shows improved throughput and security compared to traditional methods. The paper suggests future work on testing additional security attacks in IIoT applications.

Samuel et. al. [21] proposes a blockchain-based system called GarliMediChain for anonymous and private sharing of COVID-19 information in IoT-based e-health monitoring. The system makes use of consensus protocols, blockchain technology, and garlic routing. It guards against security-related threats and is resilient, effective, and flexible. Future analyses of overall expenses, scalability, and cooperation with other institutions are suggested in the paper.

Chapter 4

Proposed Framework

In view of the increasing electronic health record (EHR) integration in health care systems, there is need for tough security measures such as those that will safeguard sensitive patient data. Due to their centralized storage system, data breaches or unauthorized access could easily occur. This paper proposes employing blockchain technology and anonymous communication channels when building a safe smart healthcare structure.

4.1 System Model

The proposed system model compares several key components working together to secure patient data showed in figure 4.1.

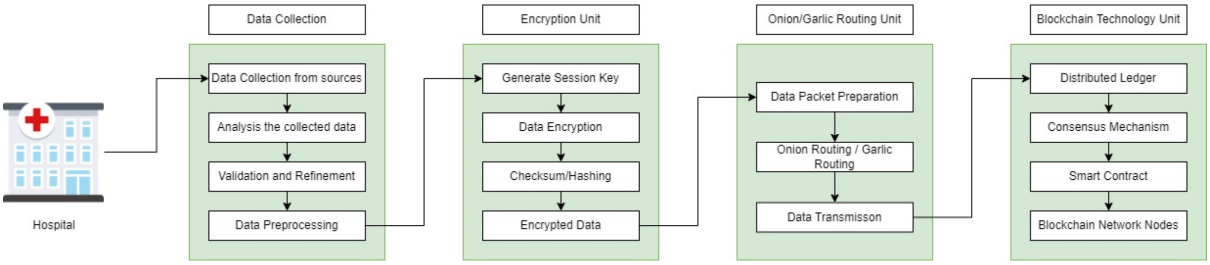

Figure 4.1: System Model

- Data Collection: Sensor data from medical devices attached to patients is collected for real-time monitoring or historical analysis.
- Data Preprocessing: The collected data undergoes preprocessing steps to remove noise, standardize formats, and ensure data quality for further processing.
- Data Encryption Unit: Robust cryptographic algorithms encrypt the preprocessed data to render it unreadable by unauthorized parties in case of interception.

- Checksum/Hashing: A cryptographic hash function generates a unique mathematical fingerprint (hash) of the data. This hash serves as a tamper-evident seal, allowing verification of data integrity during transmission and storage.

- Smart Contract: Smart contracts are self-executing programs deployed on the blockchain network. In this context, the smart contract can govern data access permissions, defining who can access specific data and under what conditions.

- Blockchain Technology Unit: Blockchain technology acts as a distributed ledger that securely stores the encrypted data and the associated hashes. The distributed nature of the blockchain ensures data immutability, as any modification attempt would be reflected across all nodes on the network.

- Data Transmission: Encrypted data packets are transmitted over a secure communication channel to the blockchain network.

- Blockchain Network Nodes: These nodes maintain copies of the blockchain ledger and participate in the consensus mechanism to validate transactions and ensure data integrity on the network.

- Onion/Garlic Routing Unit: The framework can be further enhanced by incorporating an anonymized communication channel such as onion or garlic routing. This layer encrypts data in multiple layers, with each layer revealing the address of the next node in the path, not the actual data itself. This anonymous the communication path, making it more difficult for attackers to track data flow.

- Data Decryption: Authorized recipients with the necessary decryption keys can decrypt the data upon receiving it from the blockchain network.

- Analysis: Decrypted data can be analyzed by healthcare professionals or used for various medical purposes, such as disease diagnosis, treatment planning, or research.

4.2 Proposed framework

Smart healthcare on the other hand is the use of smart systems and technologies in improving the care that patients receive as well as in the delivery of health services, with e-HIS and EHR at their core. Health IT also cook and organize patient health data in

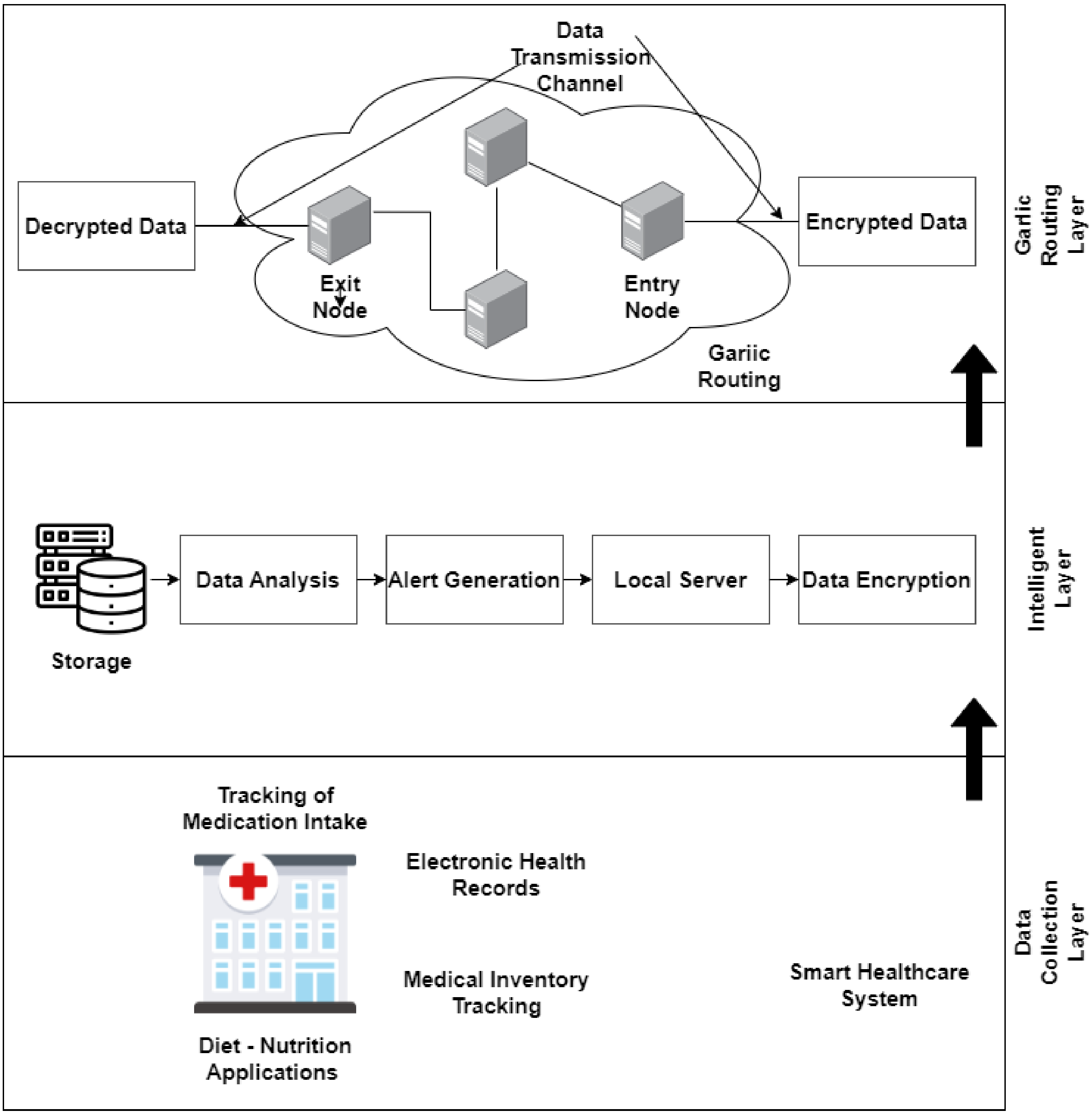

Figure 4.2: Proposed Framework

one place and provide a full picture of patient's history, laboratory tests or treatment plans than other care providers. This integration helps dovetail the medication since the patient is administered the correct doses as well as avoiding the complications resulting from drug interactions. In addition, diet and nutrition applications can be integrated with EHRs to track patients' diet and nutrients while offering dietary instructions and prescriptions as per the patients' diet and nutritional requirements. The integration of these applications provides effective support by promoting the monitoring of individuals' overall health in cooperation with a variety of physicians, which results in the optimization of health through the usage of data and the facilitation of physicians' collaboration.

Data cleaning is the first step in preparing raw data for analysis, in the context of healthcare data, specifically, data preprocessing is the process of making pre-processed datasets ready for analysis. The pre-processing stage includes data cleansing, data scaling, and data reduction, as well as the removal of large fields of no use. Other aspects of preprocessing are also important in healthcare such as data anonymization to enhance privacy and to address any remaining regulations like HIPAA. In this case, once the data is preprocessed, the cognitive and analytical techniques like the machine learning algorithms can be employed so as to gain more insight about the data. It assists in the process of constructing patterns and prognosis for the changes that would be valuable for evaluating patient care and for decision-analysis.

Hence, what analyzed from such a data setup is sophisticated alert formation systems to discern between a real and synthesized threat. For instance, irregularities in ACLs for patient health information may signify a breach of security, thus triggering notification to the IT security department. On the other hand, clinical alerts can be for non-threatening information for example notifying physicians that a specific patient is worsening or observing wrong medications given, this will make the clinical service provider intervene appropriately. The processed and analyzed data is then saved in the hospitals local servers and retain sovereignty of the data while at the same time keeping the patients data more secure from third parties while at the same time allowing the doctors to continuously monitor the patient and tweak the care plans for the betterment of the patient.

Garlic routing is an advanced method that is used in the anonymization networks for the improvement of privacy and security of the messages where a number of messages are bundled and encrypted. Each ‘clove’ of garlic, if you will, is an encrypted message, that is encapsulated within the ‘bulb,’ which itself is encrypted as well. Garlic routing involves transmitting data by enveloping several messages in one compound and routing them through different intermediate points in the network. Every node only partially deciphers a layer of the encryption just to know which other node the message should be forwarded to and does not actually read the top-secret message below the encryption layers. Sol: This greatly hinders the ability to track the source, destination, or contents of the data packets, making it highly secure against the threats posed by eavesdropping and traffic analysis.

First of all, it is crucial since garlic routing is a critical issue in the context of Internet of Medical Things (IoMT) applications. Firstly, IoMT devices frequently process patient data, which is considered to be the most valuable information – PHIs and real-time data. Preserving the confidentiality and integrity of this data is equally important as the protection of the patients’ information and adherence to the healthcare laws and policies. Secondly, IoMT networks may experience several cyber attacks such as data interception and unauthorised access. These risks are addressed by Garlic routing as it provides anonymity to the communication channels and encrypts the data at various layers of communication, which are largely inaccessible to any intrusion. This level of security is sufficient for establishing the confidence of the healthcare providers in the IoMT systems to harness these technologies and advance the quality of healthcare without the intrusion of the security loopholes.

Chapter 5

Result Analysis

5.1 Dataset

Faisal et. al. [47], created framework to detect malicious activity in IoT healthcare. They created new dataset using IoT-Flock tool which is a IoT traffic generator. This tool will allow them to create traffic patterns tailored to IoT use cases. In the virtual environment, they created two beds, each with nine patient monitoring devices and a control unit. By using IoT-Flock tool, researchers generated malicious traffic within this simulated intensive care unit setting. In dataset, traffic is generated by two widely used IoT application-layer protocols - CoAP and MQTT. They used a python script to extract features from the captured traffic and convert the pcap records into CSV files, forming a structured dataset. Also, they divided this dataset into a testing set and a training set, enhancing its usability for evaluating and training intrusion detection systems.

5.2 Experimental Setup

For experimental setup, we did following steps like dataset preprocessing, feature selection and machine learning model testing and training. Also mentioned the experimental setup in the tabel 5.1.

5.2.1 Data Preprocessing

The data is collected by capturing network traffic. Initially, this data was in a format called Pcap files and transformed these Pcap files into CSV files using python to make our analysis more practical. This step was essential to prepare and study the dataset effectively. Label Encoder was also used to replace the dataset's categorical features,

Table 5.1: Experimental Setup

Component	Description
Dataset	Synthetic IoT traffic dataset simulating healthcare environment
Data Size	10,000 normal traffic instances, 2,000 malicious traffic instances
Data Features	Timestamp, Source IP, Destination IP, Protocol, Packet Size, Flags, Payload, etc.
Preprocessing Steps	Data normalization, Feature selection using Chi-Square test, Data splitting (70% training, 30% testing)
Models Evaluated	Naive Bayes (NB), k-Nearest Neighbors (kNN), Random Forest (RF), Logistic Regression (LR)
Performance Metrics	Accuracy, Precision, Recall, F1 Score
Tools and Libraries	Python 3.8, Scikit-learn 0.24, NumPy 1.19, Pandas 1.2, Matplotlib 3.3
Software Environment	Google colab
Results Visualization	Bar charts for metric comparison

such as protocol type (e.g., CoAP and MQTT), with numerical values to facilitate further processing. Dataset was authenticated at the end to verify missing values. After verifying those missing values, it was then replaced by 0. Then dataset was divided into two groups-training and testing at random using a split ratio of 70:30 which means 30% dataset was chosen randomly for testing and rest 70% for training.

5.2.2 Feature Section

Feature selection is crucial for a ML model's performance. After the pre-processing of data, it was observed that one would use a LR algorithm since studies carried out earlier show that this method works well. In order to train and test machine learning models, LR algorithm was used so as to identify top ten features namely: ['frame.time_delta', 'tcp.flags.ack', 'tcp.flags.push', 'tcp.time_delta', 'tcp.flags.reset', 'mqtt.hdrflags', 'mqtt.msgtype', 'mqtt.qos', 'mqtt.retain', 'mqtt.ver']. These features' specifics are provided in [48].

5.2.3 Machine Learning Models Testing and Training

Once sorted and selected traits, the ML model needs to be trained from that point on. Prior to training ML models, the data was split into test and train data sets. The dataset was divided between two exclusive sets by 70% for training and 30% for testing using a split ratio of 70:30. In the training dataset, six commonly used ML classifiers were trained for detecting evil IoT traffic in healthcare. This gives us the six most common ML classifires - Logistic Regression (LogR), Random Forest (RF), K-Nearest Neighbours (KNN) and Naive Bayes (NB).

5.3 Result and Analysis

The machine learning methods are evaluated using four performance metrics: accuracy, precision, recall and F1-score. These methods are used to detect malicious and non malicious data and what are the possibilities of malicious attacks on data while being transmitted. These machine learning methods helps to identify which algorithm can predict near to exact attack.

Precision - When a security violation occurs, precision refers to the capability of the system to accurately identify the attack. The metric denotes the ratio of precisely predicted attacks (TP) to actual attacks (FP), or TP + FP). From a mathematical perspective, Equation 5.1 describes it:

$$PrecisionScore = TP/(FP + TP) * 100 \tag{5.1}$$

Recall - It describes the system's capacity to promptly identify a botnet attack when one takes place within the network. It can be stated mathematically as Equation 5.2:

$$Recall = TN/(TN + FN) * 100 \tag{5.2}$$

Accuracy - The overall system's precision is evaluated based on its ability to accurately distinguish between healthy and malicious packets, labelling the former "normal packet" and the latter "attack packet." It represents the proportion of precise forecasts for each individual sample. Its mathematical expression is given by Equation 5.3:

$$Accuracy = (TP + TN)/(TP + FN + TN + FP) * 100 \tag{5.3}$$

F1-score - The harmonic mean for recall and precision is expressed by the F1-score. The ratio of accurate predictions for both attack and normal traffic in the test set is described. Its mathematical expression is given by Equation 5.4.

$$F1 - score = (2 * Precision * Recall)/(Precision + Recall) \tag{5.4}$$

Table 5.2 shows the accuracy, precision, recall, F1-Score of various Machine Learning Algorithms like Naive Bayes, k-Nearest Neighbors, Random Forest and Logistic Regres-

Table 5.2: Result of various Machine Learning Algorithms

Methods	Accuracy	Precision	Recall	F1-Score
Naive Bayes (NB)	79.671077	97.705297	52.18225	68.509194
k-Nearest Neighbors (KNN)	98.646699	97.703314	96.462254	98.582638
Random Forest (RF)	98.70676	99.785159	96.512276	98.653517
Logistic Regression (LR)	93.286969	90.351641	98.503939	94.707189

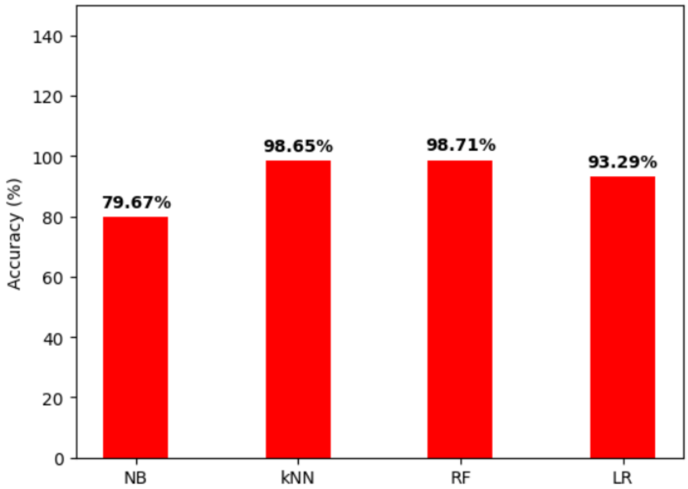

Figure 5.1: Accuracy

sion.

In figure 5.1, the k-Nearest Neighbors (kNN) and Random Forest (RF) models have the highest accuracy values, approximately 98.65% and 98.71%, respectively. Logistic Regression (LR) follows with an accuracy of about 93.29%. Naive Bayes (NB) has the lowest accuracy at approximately 79.67%. This indicates that kNN and RF are the best-performing models in terms of accuracy, while NB lags behind.

In figure 5.2, random Forest (RF) achieves the highest precision at about 99.80%. Naive Bayes (NB) and k-Nearest Neighbors (kNN) have similar precision values, around 97.70%. Logistic Regression (LR) has the lowest precision at approximately 90.35%. This suggests that RF is the best model for correctly predicting positive instances, while LR has the highest rate of false positives.

In figure 5.3, Logistic Regression (LR) has the highest recall at approximately 98.50%.

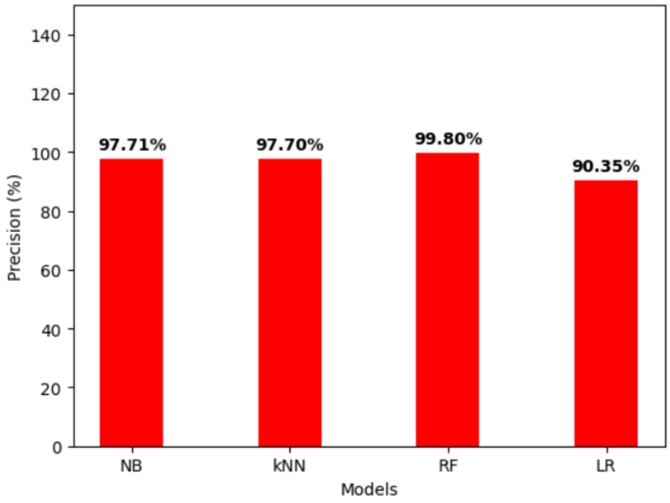

Figure 5.2: Precision

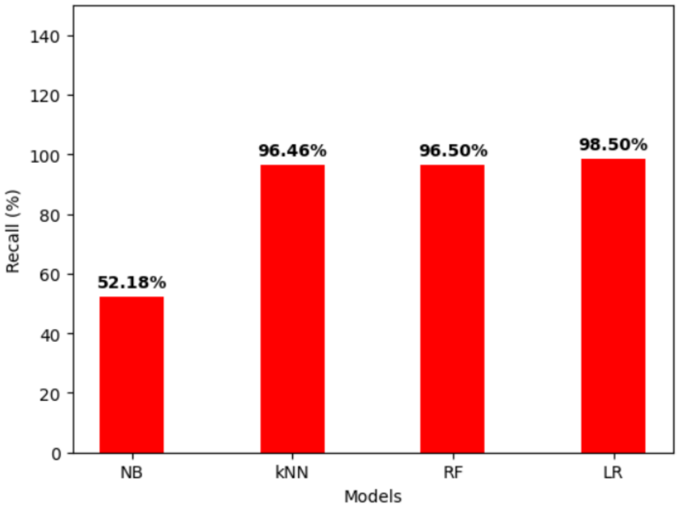

Figure 5.3: Recall

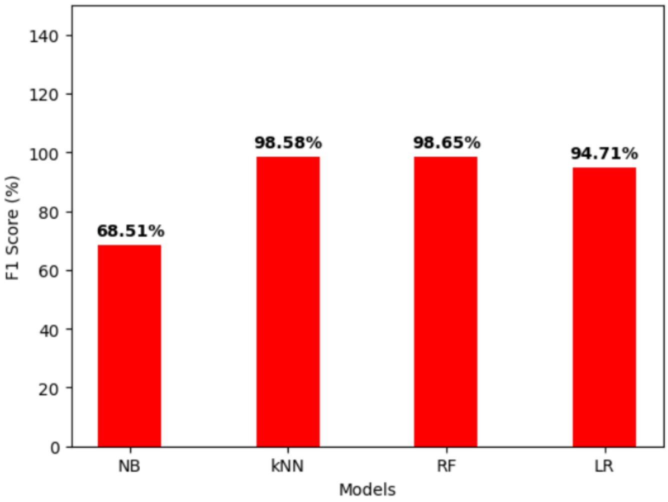

Figure 5.4: F1 Score

Both k-Nearest Neighbors (kNN) and Random Forest (RF) have similar recall values, around 96.50%. Naive Bayes (NB) has the lowest recall at approximately 52.18%. This indicates that LR is the best model for capturing all actual positive instances, while NB misses a significant number of them.

In figure 5.4, Random Forest (RF) has the highest F1 Score at about 98.65%, followed closely by k-Nearest Neighbors (kNN) at approximately 98.58%. Logistic Regression (LR) has a relatively high F1 Score at about 94.71%. Naive Bayes (NB) has the lowest F1 Score at approximately 68.51The F1 Score, which balances precision and recall, suggests that RF and kNN provide the best overall performance, while NB performs poorly in balancing precision and recall.

From the figures 5.1, 5.2, 5.3, and 5.4, we cans say that Random Forest (RF) and k-Nearest Neighbors (kNN) consistently show high performance across all metrics. Logistic Regression (LR) performs moderately well, especially in recall, but falls behind RF and kNN in precision and F1 Score. And Naive Bayes (NB) has the lowest performance across all metrics, indicating it is the least effective model among the four evaluated. Overall, the results suggest that for this particular dataset, RF and kNN are the most effective models, providing high accuracy, precision, recall, and F1 scores. Logistic Regression is a good alternative but not as effective as RF and kNN, while Naive Bayes performs significantly worse compared to the other models.

Chapter 6

Research Challenges and Future Directions

While blockchain-based security frameworks integrated with routing techniques offer substantial advantages for securing IoMT applications, several challenges persist. This section provides a detailed examination of the challenges faced by current implementations and explores potential future directions for advancing the security landscape in healthcare. Figure 6.1 depicts the various challenges in securing the IoMT applications.

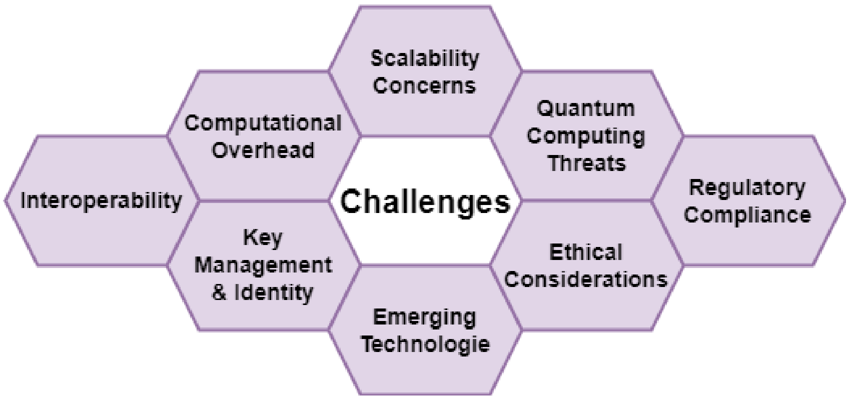

Figure 6.1: Research Challenges and Future Directions

- **Scalability Concerns:** The scalability of blockchain-based solutions in IoMT applications remains a significant challenge. As the number of connected medical devices increases, the transaction volume on the blockchain grows, potentially leading to performance bottlenecks. Solutions are needed to address scalability issues without compromising the decentralization and security attributes of blockchain.

- **Computational Overhead:** The integration of privacy-preserving routing techniques, such as Onion and Garlic Routing, introduces computational overhead. This overhead can impact the efficiency and responsiveness of IoMT applications, particularly those requiring real-time processing. Research efforts should focus on optimizing these techniques to strike a balance between privacy and performance.

- **Interoperability:** Achieving interoperability between diverse healthcare systems and blockchain platforms remains a challenge. Seamless integration with existing healthcare infrastructures requires standardized protocols and communication interfaces. Future research should prioritize the development of interoperable solutions to ensure the widespread adoption of blockchain-based security frameworks.

- **Key Management and Identity:** The management of cryptographic keys and identity verification in healthcare blockchain networks is a critical concern. Ensuring secure and user-friendly methods for key management is essential, especially considering the diverse user roles within the healthcare ecosystem. Research efforts should explore innovative approaches for robust key management and identity verification.

- **Emerging Technologies:** The rapid evolution of technology introduces both opportunities and challenges. Future research directions should explore the integration of emerging technologies, such as artificial intelligence (AI) and edge computing, to enhance the capabilities of blockchain-based security frameworks. These technologies can contribute to more efficient data processing and real-time decision-making in IoMT applications.

- **Quantum Computing Threats:** The advent of quantum computing poses potential threats to traditional cryptographic algorithms used in blockchain and routing techniques. Future research should focus on developing quantum-resistant cryptographic solutions to safeguard the security of healthcare data in the post-quantum era.

- **Ethical Considerations:** The integration of blockchain and routing techniques raises ethical considerations regarding the balance between data security and patient privacy. Striking the right balance and addressing ethical concerns, such as consent management and data ownership, is crucial. Future research should explore frameworks that not only meet technical requirements but also adhere to ethical principles in healthcare.

- **Regulatory Compliance:** The evolving landscape of healthcare regulations and privacy standards poses challenges for implementing blockchain-based security frameworks. Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) is crucial but complex. Future research should focus on developing solutions that seamlessly align with regulatory requirements while maintaining the security and privacy of healthcare data.

As blockchain-based security frameworks continue to evolve in the context of IoMT applications, addressing these challenges and exploring future directions becomes imperative. The dynamic nature of healthcare, coupled with technological advancements, necessitates ongoing research to ensure that these frameworks remain resilient, adaptable, and capable of meeting the diverse and evolving needs of the healthcare ecosystem. The subsequent sections delve into the advantages and disadvantages of these frameworks, providing a nuanced understanding of their implications for the security landscape in IoMT applications.

Chapter 7

Conclusion

The combination of blockchain-based security and standard routing approaches in IoMT platforms is a major step toward tackling current issues. The proposed work is dedicated to the Onion Routing, and Garlic Routing. The proposed framework shows how we can apply garlic routing for secure communication in IoMT healthcare. It describe the improvements, such transparency or routing is applied to privacy, making patients' identities invisible and strengthened. The relevant examples of its use are identified. It is expected that the future cases of usage will lead to more transactions between patients and medical institutions. Also from the result we can say that KNN and RF shows high accuracy scores indicating strong prediction. NB has highest accuracy but has low recall, that indicate a bias towards the positive predictions. LR shows low accuracy and F1-Score, but also shows a trade off between recall and precision. However, certain barriers must be evaluated to identify the most effective solutions. As these technologies undergo various evolution's and revolutionize IoMT applications, the need to strike a balance between robust security and user-friendly experiences remains paramount. The research presents the potential routing techniques in healthcare. It is a significant step toward a secure and patient-centric future landscape. Interdisciplinary teamwork and continued research will inform the development of blockchain-based security in healthcare.

Bibliography

[1] M. Attaran, “Blockchain technology in healthcare: Challenges and opportunities,” *International Journal of Healthcare Management*, vol. 15, no. 1, pp. 70–83, 2022.

[2] S. Mehandiratta and R. Agarwal, “Increasing trust and privacy by using blockchain technology in the onion router network,” in *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pp. 1–5, IEEE, 2024.

[3] N. K. Jadav, R. Kakkar, H. Mankodiya, R. Gupta, S. Tanwar, S. Agrawal, and R. Sharma, “Grade: Deep learning and garlic routing-based secure data sharing framework for iiot beyond 5g,” *Digital Communications and Networks*, vol. 9, no. 2, pp. 422–435, 2023.

[4] R. Dwivedi, D. Mehrotra, and S. Chandra, “Potential of internet of medical things (iomt) applications in building a smart healthcare system: A systematic review,” *Journal of oral biology and craniofacial research*, vol. 12, no. 2, pp. 302–318, 2022.

[5] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, “Blockchain-assisted secured data management framework for health information analysis based on internet of medical things,” *Personal and ubiquitous computing*, vol. 28, no. 1, pp. 59–72, 2024.

[6] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, “Blockchain: securing internet of medical things (iomt),” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, 2019.

[7] R. Kumar and R. Tripathi, “Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain

and ipfs technology," *the Journal of Supercomputing*, vol. 77, no. 8, pp. 7916–7955, 2021.

[8] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717–11731, 2021.

[9] S. R. Mallick and S. Sharma, "Emri: A scalable and secure blockchain-based iomt framework for healthcare data transaction," in *2021 19th OITS International Conference on Information Technology (OCIT)*, pp. 261–266, IEEE, 2021.

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

[11] S. R. Mallick, S. Sharma, P. K. Tripathy, and N. K. Ray, "Adoption of blockchain-fog-iomt framework in healthcare 4.0 digital revolution," in *2022 OITS International Conference on Information Technology (OCIT)*, pp. 603–608, IEEE, 2022.

[12] W. Rafique, M. Khan, S. Khan, J. S. Ally, *et al.*, "Securemed: A blockchain-based privacy-preserving framework for internet of medical things," *Wireless Communications and Mobile Computing*, vol. 2023, 2023.

[13] B. M. Alshammari, "Aibpsf-iomt: Artificial intelligence and blockchain-based predictive security framework for iomt technologies," *Electronics*, vol. 12, no. 23, p. 4806, 2023.

[14] R. A. Alsemmeari, M. Y. Dahab, A. A. Alsulami, B. Alturki, and S. Algarni, "Resilient security framework using tnn and blockchain for iomt," *Electronics*, vol. 12, no. 10, p. 2252, 2023.

[15] M. Wazid and P. Gope, "Backm-eha: A novel blockchain-enabled security solution for iomt-based e-healthcare applications," *ACM Transactions on Internet Technology*, vol. 23, no. 3, pp. 1–28, 2023.

[16] Q. Lin, X. Li, K. Cai, M. Prakash, and D. Paulraj, "Secure internet of medical things (iomt) based on ecmqv-mac authentication protocol and ekmc-scp blockchain networking," *Information Sciences*, vol. 654, p. 119783, 2024.

[17] N. Singh and A. K. Das, "Tfas: two factor authentication scheme for blockchain enabled iomt using puf and fuzzy extractor," *The Journal of Supercomputing*, vol. 80, no. 1, pp. 865–914, 2024.

[18] M. Li, H. Tang, A. R. Hussein, and X. Wang, "A sidechain-based decentralized authentication scheme via optimized two-way peg protocol for smart community," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 282–292, 2020.

[19] X. Cheng, Y. Chen, J. Zou, Y. Zhang, and N. Hu, "An anonymous communication system based on software defined architecture," in *International Symposium on Mobile Internet Security*, pp. 396–407, Springer, 2021.

[20] S. P. Sankar, T. Subash, N. Vishwanath, and D. E. Geroge, "Security improvement in block chain technique enabled peer to peer network for beyond 5g and internet of things," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 392–402, 2021.

[21] O. Samuel, A. B. Omojo, S. M. Mohsin, P. Tiwari, D. Gupta, and S. S. Band, "An anonymous iot-based e-health monitoring system using blockchain technology," *IEEE Systems Journal*, 2022.

[22] O. Samuel and N. Javaid, "Garlichain: A privacy preserving system for smart grid consumers using blockchain," *International Journal of Energy Research*, vol. 46, no. 15, pp. 21643–21659, 2022.

[23] M. Patel, N. K. Jadav, S. Tanwar, and M. S. Obaidat, "Ai and blockchain-enabled onion routing protocol to secure iot communication," in *Intelligent Computing on IoT 2.0, Big Data Analytics, and Block Chain Technology*, pp. 78–94, Chapman and Hall/CRC.

[24] S. Maalavika, G. Thangavel, and S. Basheer, "A review on garlic routing and artificial intelligence applications in public network," in *2023 International Conference on Computer Science and Emerging Technologies (CSET)*, pp. 1–6, IEEE, 2023.

[25] J. Li, D. Han, D. Li, and H. Li, "Blockchain and or based data sharing solution for internet of things," in *International Conference on Blockchain and Trustworthy Systems*, pp. 116–127, Springer, 2023.

[26] A. A. Mohd, S. Kummarikunta, S. K. Thumboor Naga, V. R. Buthukuri, P. Chintamaneni, and R. Vatambeti, "Design of mutual authentication method for deep learning based hybrid cryptography to secure data in cloud computing.," *International Journal of Safety & Security Engineering*, vol. 13, no. 5, 2023.

[27] N. K. Jadav, R. Gupta, and S. Tanwar, "Garlic routing-based privacy preserving framework for secure data exchange between iomvs with 5g," in *2023 International Conference on Network, Multimedia and Information Technology (NMITCON)*, pp. 1–6, IEEE, 2023.

[28] R. Gupta, N. K. Jadav, H. Mankodiya, M. D. Alshehri, S. Tanwar, and R. Sharma, "Blockchain and onion-routing-based secure message exchange system for edge-enabled iiot," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1965–1976, 2022.

[29] R. Gupta, N. K. Jadav, A. Nair, S. Tanwar, and H. Shahinzadeh, "Blockchain and ai-based secure onion routing framework for data dissemination in iot environment underlying 6g networks," in *2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*, pp. 1–6, IEEE, 2022.

[30] R. Gupta, S. Tanwar, and N. Kumar, "B-iomv: Blockchain-based onion routing protocol for d2d communication in an iomv environment beyond 5g," *Vehicular Communications*, vol. 33, p. 100401, 2022.

[31] N. K. Jadav, R. Gupta, S. Tanwar, and P. Bhattacharya, "Intelligent garlic routing for securing data exchange in v2x communication," in *2022 IEEE Globecom Workshops (GC Wkshps)*, pp. 286–291, IEEE, 2022.

[32] A. A. Jolfaei, S. F. Aghili, and D. Singelee, "A survey on blockchain-based iomt systems: Towards scalability," *Ieee Access*, vol. 9, pp. 148948–148975, 2021.

[33] P. Sharma, N. R. Moparthi, S. Namasudra, V. Shanmuganathan, and C.-H. Hsu, "Blockchain-based iot architecture to secure healthcare system using identity-based encryption," *Expert Systems*, vol. 39, no. 10, p. e12915, 2022.

[34] M. Cicioğlu and A. Çalhan, "A multiprotocol controller deployment in sdn-based iomt architecture," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 20833–20840, 2022.

[35] N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Yusupov, and D. Kodirov, "Architecture, protocols, and applications of the internet of medical things (iomt)," *J. Commun*, vol. 17, no. 11, pp. 900–918, 2022.

[36] I. Sadek, J. Codjo, S. U. Rehman, and B. Abdulrazak, "Security and privacy in the internet of things healthcare systems: toward a robust solution in real-life deployment," *Computer Methods and Programs in Biomedicine Update*, vol. 2, p. 100071, 2022.

[37] F. Pelekoudas-Oikonomou, G. Zachos, G. Mantas, J. Ribeiro, J. M. C. Bastos, and J. Rodriguez, "A scalable approach of practical byzantine fault tolerance algorithms for iomt blockchains," in *2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pp. 124–129, IEEE, 2022.

[38] T. Ramzan and S. Zafar, "Blockchain-based security for internet of medical things application," in *2022 International Conference on Cyber Warfare and Security (ICCWS)*, pp. 69–74, IEEE, 2022.

[39] B. Bera, A. Mitra, A. K. Das, D. Puthal, and Y. Park, "Private blockchain-based ai-envisioned home monitoring framework in iomt-enabled covid-19 environment," *IEEE Consumer Electronics Magazine*, 2021.

[40] S. Panasenko, "A lightweight blockchain for the internet of medical things using hash-based message authentication codes," in *2023 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1095–1100, IEEE, 2023.

[41] M. J. FL, S. StewartKirubakaran, G. J. L. Paulraj, I. J. Jebadurai, and J. Jebadurai, "A secure data sharing framework with blockchain in iomt using bald eagle search

optimization," in *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, pp. 198–205, IEEE, 2023.

[42] S. R. Mallick, V. Goswami, R. K. Lenka, T. R. Sahoo, V. Kumar, and R. K. Barik, "Blockchain-based iomt for an intelligent healthcare system using a drop-offs queue," in *2023 First International Conference on Microwave, Antenna and Communication (MAC)*, pp. 1–6, IEEE, 2023.

[43] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight iomt devices," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 710–721, 2022.

[44] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, and W. Wang, "Federated-learning based privacy preservation and fraud-enabled blockchain iomt system for healthcare," *IEEE journal of biomedical and health informatics*, vol. 27, no. 2, pp. 664–672, 2022.

[45] I. Sharma and S. Sharma, "Blockchain enabled biometric security in intemet-of-medical-things (iomt) devices," in *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, pp. 971–979, IEEE, 2022.

[46] N. K. Jadav, R. Gupta, R. Kakkar, and S. Tanwar, "Intelligent onion routing and uav-based electronic health record sharing framework for healthcare 4.0," in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1–6, IEEE, 2023.

[47] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, U. U. Fayyaz, F. Shahzad, N. M. Garcia, and E. Zdravevski, "A framework for malicious traffic detection in iot healthcare environment," *Sensors*, vol. 21, no. 9, p. 3025, 2021.

[48] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, "Mqttset, a new dataset for machine learning techniques on mqtt," *Sensors*, vol. 20, no. 22, p. 6578, 2020.

Shruti Mtech thesis

ORIGINALITY REPORT

8%	4%	5%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	fastercapital.com Internet Source	1%
2	mdpi-res.com Internet Source	1%
3	"Blockchain and Trustworthy Systems", Springer Science and Business Media LLC, 2024 Publication	<1%
4	Nilesh Kumar Jadav, Riya Kakkar, Harsh Mankodiya, Rajesh Gupta, Sudeep Tanwar, Smita Agrawal, Ravi Sharma. "GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G", Digital Communications and Networks, 2022 Publication	<1%
5	Submitted to University of Sheffield Student Paper	<1%
6	Qinyong Lin, Xiaorong Li, Ken Cai, Mohan Prakash, D. Paulraj. "Secure Internet of Medical Things (IoMT) based on ECMQV-MAC	<1%