# DESIGN OF BLOCKCHAIN-BASED SECURE AND PRIVACY-PRESERVING MUTUAL AUTHENTICATION PROTOCOLS

**Thesis**

***Submitted in partial fulfillment of the requirements for the degree of***

**DOCTOR OF PHILOSOPHY**

by

**INDUSHREE M**

(Enrollment No. E20SOE815)

Under the Supervision of

**Dr. MANISH RAJ**


SCHOOL OF COMPUTER SCIENCE ENGINEERING & TECHNOLOGY

BENNETT UNIVERSITY

GREATER NOIDA, U.P - 201310

June 7, 2024

*Dedicated to*
*My family & friends*

# DECLARATION

*By the Ph.D. Research Scholar*

I hereby *declare* that the Research Thesis entitled **Design of Blockchain-based Secure and Privacy-preserving Mutual Authentication Protocols** which is being submitted to the **Bennett University** in partial fulfillment of the requirements for the award of the Degree of **Doctor of Philosophy** in **School of Computer Science Engineering & Technology** is a *bonafide report of the research work carried out by me*. The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.

**Indushree M**

Reg. No.: E20SOE815

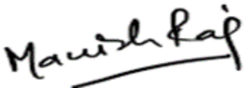
School of Computer Science Engineering & Technology

Place: Bennett University, Greater Noida.

Date: June 7, 2024

# SUPERVISOR'S CERTIFICATE

This is to *certify* that the Research Thesis entitled **DESIGN OF BLOCKCHAIN-BASED SECURE AND PRIVACY-PRESERVING MUTUAL AUTHENTICATION PROTOCOLS** submitted by **INDUSHREE M**, (Reg. No.: E20SOE815) as the record of the research work carried out by her, is *accepted as the Research Thesis submission* in partial fulfillment of the requirements for the award of degree of **Doctor of Philosophy**.



**Dr. Manish Raj**
Research Supervisor
School of Computer Science Engineering & Technology
Bennett University, Greater Noida, India
Date: June 7, 2024

# ACKNOWLEDGMENT

I would like to acknowledge the moral and intellectual supports given to me by my supervisor **Dr. Manish Raj** during my PhD program. Thanks to my supervisor's constant guidance and approaches through which this long and difficult journey becomes smooth and interesting. His way to do research as well as his attitude towards study and analysis of any particular subject influenced me immensely, and I still feel there is a lot to learn from him. Among other things, I have always admired his ability to discuss research problems from scratch to formalize rigorously, his scientific bravery in supporting ideas that sounded completely mental at first glance. Most important of all was probably his calm and constant belief in my ability to get a PhD.

I would like to take this opportunity to thank **Prof. Abhay Bansal**, Dean, School of Computer Science Engineering & Technology, for his support and cooperation during my PhD program.

I am thankful to and fortunate enough to get constant encouragement, support and guidance from all the Teaching staff of School of Computer Science Engineering & Technology which helped me in successfully completing my thesis work. Also, I would like to extend my sincere regards to all the non-teaching staff of Bennett University for their timely support.

I would like to express my sincere gratitude to **Dr. Shashidhara R** for his guidance and valuable suggestions in Blockchain.

I would like to thank my parents, my brothers and friends for their moral support and patience during the course of my research work. Finally, I would like to thank all of them whose names are not mentioned here but have helped me in any way to accomplish the work.

Indushree. M.

Place: Bennett University, Greater Noida Indushree M

Date: June 7, 2024

# ABSTRACT

Mobile devices have seamlessly integrated into our everyday routines, offering access to an extensive range of applications and services encompassing communication, e-commerce, social networking, and location-based services. However, with this convenience comes the risk of privacy and security threats. Mobile devices are susceptible to security threats as they depend on open channels for transmitting data through radio waves. Adversaries can exploit this vulnerability to launch attacks such as eavesdropping, masquerading, and tampering, leading to financial losses and information leakage. Therefore, safeguarding the processes of authentication, maintaining data confidentiality, and the preservation of data integrity becomes crucial.

Furthermore, authentication is the procedure for verifying a claimed identity and is critical in the context of global mobile networks. This is especially crucial as users necessitate uninterrupted and secure roaming services across various foreign agents. Developing a reliable and anonymous authentication protocol that safeguards user privacy poses a considerable challenge. Mutual authentication, which verifies the identity of all communication entities, is essential to mitigate network threats when mobile users are unaware of attackers or third parties.

This thesis proposes novel blockchain-based mutual authentication protocols for both global mobility networks and Telecare Medical Information Systems (TMIS). These protocols address critical security and privacy challenges inherent in each domain. Centralized authentication models in mobility networks leave them vulnerable to unauthorized access and identity theft. Similarly, TMIS struggle with data breaches, unauthorized access to patient information, and potential manipulation of medical records. This thesis explores how blockchain technology, with its tamper-proof ledger and decentralized structure, can enhance security in both areas. By enabling secure identity verification, data storage, and fine-grained access control, these protocols have the potential to revolutionize security and privacy practices in mobility networks and TMIS.

We proposed Blockchain based secure and privacy-preserving authentication protocols utilize a combination of cryptographic primitives for secure communication and user verification. This includes secure hash functions for data integrity, symmetric ciphers like AES for secure channels, and asymmetric cryptography like ECC for key exchange and digital signatures. Furthermore, we leverage blockchain technology for a decentralized approach. Crucial authentication parameters are stored on the blockchain's tamper-proof ledger, while Solidity smart contracts manage user authorization on the blockchain. To ensure the protocol's robustness, the proposed approach employs the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool for formal security verification. In addition, the proposed authentication protocols were rigorously evaluated for computational and communication overhead, confirming the practical implementation of the decentralized authentication framework in global mobility networks and telecare medical information systems.

**Keywords: Authentication, Blockchain, Smart Contracts, Session Key, Global Mobility Network, Telecare Medical Information System (TIMS), Security, Privacy, AVISPA, Smart-card.**

# Contents

# List of Figures

# Abbreviations and Acronyms

| | |
|---|---|
| GPS | : GlobaL positioninG systeM |
| GLOMONET | : GlobaL mobilitY networK |
| ECC | : Elliptic-Curve-Cryptography |
| DLP | : Discrete Logarithm Problem |
| SBT | : Soulbound Token |
| ProVerif | : Protocol Verification |
| OFMC | : On the Fly-Model Checker |
| ATSE | : Attack-searcher |
| AVISPA | : Automated Validation of Internet Security Protocols and Applications |
| HLPSL | : High Level Protocol Specification language |
| NIST | : National Institute of Standards and Technology |

# Chapter 1

# INTRODUCTION

In this chapter, Mobile technology's rapid advancement demands mobile devices with low power consumption and secure communication capabilities.This has brought about a significant concern regarding privacy issues between mobile device users and service providers. If the network is not secure, there is an increased risk of alteration, theft, unauthorized access,or physical damage to sensitive information stored within the network. Hence, it is essential to implement security measures capable of safeguarding against a spectrum of network vulnerabilities and threats.

To maintain the trustworthy and safe operation of computer networks in our increasingly connected world, protecting network security is of the paramount importance. While no network can ever be completely impervious to attacks, having a robust security system in place is essential for securing user information. A reliable network security mechanism plays a crucial role in protecting against various threats, such as data theft and damage resulting from cyberattacks or other malicious activities. By implementing a comprehensive network security strategy, businesses can significantly reduce their exposure to risks and minimize the effect of any possible security breaches. In accordance with the guidelines set by the NIST, security encompasses the adoption of measures to secure a networked environment, with the ultimate goal of fulfilling specific objectives that pertain to preserving the confidentiality, availability, and resources of integrity in the information system. It means ensuring that sensitive data within network is secure from unauthorized access, remains accessible to authorized users, and is kept confidential from potential intruders. Overall, implementing strong network security measures is critical for ensuring the safe and secure operation of computer networks,

protecting sensitive data, and safeguarding against the risks of cyberattacks and other security threats. To ensure the design of a secure network infrastructure, the following factors should be taken into consideration. (Shashidhara et al., 2021):

1. *Authentication*: Authentication is a crucial service Madhusudhan and Mittal (2012) that allows for user identification. It permits a system to confirm the authenticity of the person trying to gain access by verifying their identity through attributes, knowledge, and possessions. This multi-factor authentication approach ensures that the system remains secure and intact while granting user access.

2. *Authorization*: The process of verifying if an authenticated user possesses the requisite permissions to access a resources in network referred as authorization. During this process, the system checks the user's access rules to determine whether they are allowed to perform the requested action on the resource. Based on these rules, the system either grants or denies the user's request for resource access. Effective authorization mechanisms are essential for network security, as they help prevent unauthorized access to sensitive data or resources.

3. *Confidentiality*: Data confidentiality entails safeguarding sensitive information transmitted through a network to prevent unauthorized access. It guarantees that solely authorized recipients can retrieve the data by converting it into an unreadable format using encryption, which can only be decoded with the appropriate decryption key. Data confidentiality is a critical element of networks security, as it serves to safeguard sensitive information.

4. *Data Integrity*: Integrity service is a vital component of network security, designed to thwart unauthorized data modification or alteration during transmission. The integrity service is engineered to identify any efforts to tamper with the data and guarantee that the received data matches precisely with what was originally transmitted by the authorized user. By providing an assurance of data accuracy and authenticity, the integrity service enables users to trust the data they receive over the networks. This helps prevent active threats that may compromise the validity and reliability of the data, ensuring that the data remains intact and unal-

tered throughout the transmission.

5. *Non-repudiation*: Digital non-repudiation is a security service that guarantees the sender's inability to disavow sending a message and the recipient's inability to deny receiving it at a later time. It provides proof of the origin and delivery of a message or service, making it an essential aspect of secure communication.

A network security infrastructure is essential to offer multiple layers of protection against different types of attacks. This is accomplished by dividing information into various components, encrypting each of them, and then routing them through separate paths. This approach is designed to thwart eavesdropping and other security breaches effectively. To create an effective security plan, it is crucial to have a comprehensive knowledge of security concerns such as potential attackers, required security levels, and network vulnerabilities. Understanding these concepts aids in precisely determining the necessary range of security to safeguard the information stored within the network and the context in which it operates.

## 1.1 Authentication Demystified: A Comprehensive Overview

Confirming the identity of a user by verifying their claimed identity through various methods like identification documents, digital signatures, and certificates is referred to as the authentication process. User authentication is crucial for any security infrastructure, as it serves as a foundation for other security measures. Authorization involves granting access privileges based on a user's identity, while audit trails require authentication to ensure accountability for actions taken. When authentication is lacking, it becomes difficult to differentiate between authorized and unauthorized entities, which can compromise both confidentiality and integrity measures, posing a security risk.
In a distributed environment, ensuring authentication becomes more complex because of the constant risk posed by malicious users or programs. They attempt to access sensitive information, disrupt services, or impersonate legitimate entities by tampering with data. Therefore, it is essential to establish secure and trustworthy authentication methods among the communicating parties within the networks.

Authentication mechanisms can be divided into three broad categories, which are determined by the factors they rely on.

1. *Knowledge*: Single-factor authentication involves confirming a user's identity using just one recognized factor, which can include a security question, personal identification number or password.

2. *Ownership*: Two-factor authentication involves the authentication of identity through something that a user own, like Smart-cards, authentication Tokens, mobile Devices, or any other physical object in addition to Something familiar, like Password, Security question, a personal identification number etc

3. *Inherence*:Three-factor authentication entails verifying a user's identity through personal traits like signatures,fingerprints,voice prints and iris.

Single-factor authentication methods that rely solely on passwords are simple to implement and use, but they have limitations.Low-entropy passwords are susceptible to guessing attacks and provide weak identity verification. Smart-card-based authentication requires users to own both a valid password and a smart-card for successful login, strengthening security measures.Three-factor authentication shares similarities with smart-card-based systems but includes an extra authentication factor,such as biometric characteristics, required for further verification. While three-factor authentication with biometric characteristics provides a high level of security, it has some limitations. For example, accidents or health conditions may cause damage to a person's eyes, vocal cords, or hands, which can prevent them from using the biometric authentication factor. Additionally, the cost of implementing and maintaining a three-factor authentication system offers higher security compared to single or Two factor authentication systems. Because of these benefits, using a Password based authentication system in combination with smart-cards is considered a straightforward and convenient method for safeguarding data confidentiality. Shamshad et al. (2020).

## 1.2 User authentication process scenario for Global Mobility Networks

In this scenario a Global mobile networks, users can access services provided by their Home Agent (HA) even while connected to Foreign Networks (FNs). Robust authentication methods are employed to secure roaming services between a user's home network and the foreign networks they visit. Wheneve a MU transitions to a FN under the management of a FA, an authentication process occurs, with support from the user's home agent in their home network. This ensures the security of roaming services, this authentication process grants the Mobile User (MU) access to services in Foreign Networks, even Figure 1.1 shows that when they travel beyond the originally assigned coverage area.

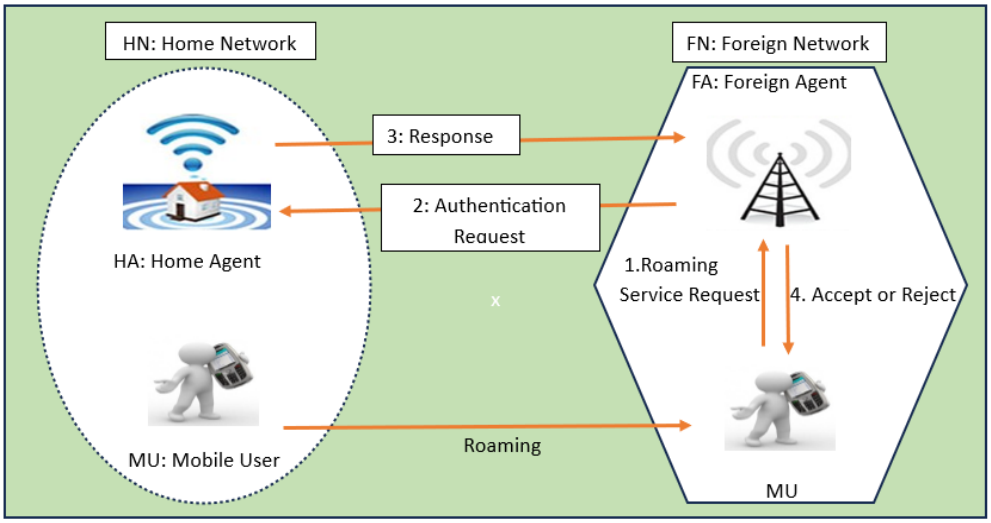



Figure 1.1 User authentication for roaming services in GLOMONET

Enhancing mobile user authentication for improved security is vital for preserving privacy in mobile environments. Today's communication technologies face significant security vulnerabilities, especially in wireless networks due to their open nature. These networks lack inherent security measures, making them more susceptible to network security attacks. Consequently, developing and designing a strong protocol for secure mobile roaming service remains a constant challenge.

In global mobility networks, two-factor authentication, which utilizes smart cards and

passwords, is widely adopted due to its high portability and user-friendliness. In this setup, users only required to recall a valid password and own a smart card issued by the home agent during their mobile user registration.

## 1.3 Authentication in Telecare Medical Information System(TMIS)

In healthcare, there's an immense amount of data, including billing records, medical research, and patient histories. This data can be challenging to manage in an organized manner. Secure data sharing is an approach that allows healthcare providers and related entities to confirm the accuracy of this information, which is essential for maintaining the security of medical services.

Paper-based patient medical records are challenging to transfer between locations,

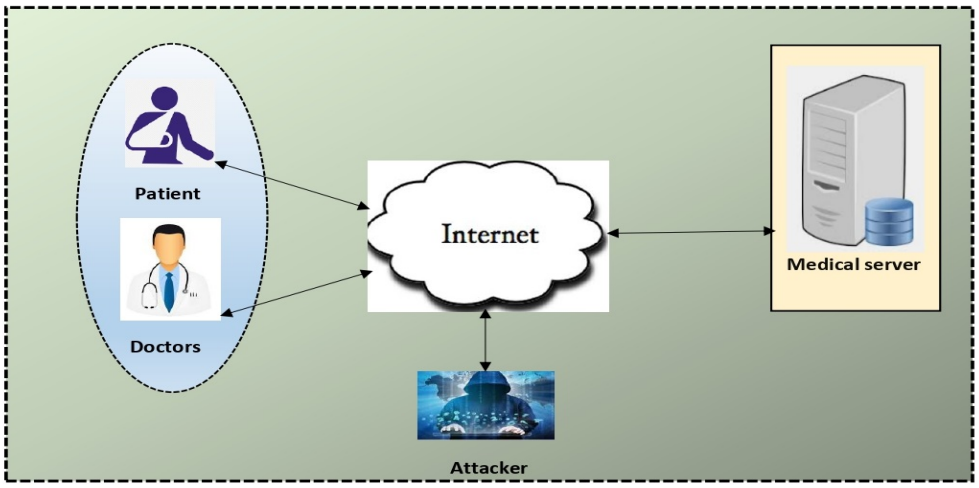



Figure 1.2 User authentication in TMIS

making it difficult to access medical services. Nowadays, Electronic Medical Records (EHRs) store most health-related information, but these digital repositories are susceptible to various security threats, putting health data at risk.

The complex task of sharing health information securely and promptly has a significant impact on patient healthcare. Figure 1.2 illustrates a privacy-preserving user authentication scheme for TMIS. Certainly, numerous patients have concerns regarding safeguarding the privacy of their personal health data. To achieve widespread adoption,

trustworthiness, and security of the TMIS, it is imperative to address the challenge of securely disseminating health information among insurance companies, patients, and healthcare organizations. Furthermore, addressing piracy and the misuse of drugs is crucial, as forged or unauthorized medications can lead to fatal effect for patients. Consequently, the issues of prescription and drug misuse represent another significant challenge in the healthcare sector.

Robust authentication techniques guarantee that unauthorized users cannot access the server's services. Initially, many authentication methods primarily depended on passwords, which, despite their widespread use, are vulnerable to various attacks. To mitigate these vulnerabilities and enhance system security, smart card-based password authentication schemes were introduced, ultimately becoming one of the most commonly employed authentication mechanisms.

### 1.3.1 Applications

Primary applications of authentication within the global mobility network encompass the following:

- *Cellular systems*: The infrastructure of cellular-networks is extensive and intricate, involving multiple entities working in coordination, including the core network and IP. Consequently, a robust authentication service is essential to ensure security across all potential communication pathways within the network.

- *Banking industry*: Authentication systems play a pivotal role in safeguarding privacy and secrecy in banking related applications such as Mobile banking, UPI (Unified Payment Interface), Wallet transactions, and Internet banking.

- *Telemedicine*: Telemedicine system necessitate robust authentication services to guarantee privacy and data confidentiality, meeting the requirements of both patients and healthcare professionals.

- *Industrial Internet*: An authentication system allows organizations to enhance network security by granting access to safeguarded resources, foe example databases,

websites, computer systems and other network-based applications or services, exclusively to authenticated users.

- *Internet of Things (IoT)*: IoT devices enhance the daily lives of individuals, yet their heterogeneous and dynamic nature poses significant security and privacy risks. Authentication protocols are employed in IoT environments to mitigate these security threats.

### 1.3.2 Attacks in mobile environments

Security breaches within the GLOMONET environment manifest in two ways: passive attackers can compromise message confidentiality by eavesdropping on communications between Mobile Units (MU) and Foreign Agents (FA) via intercepted channels, while active attackers may impersonate MUs to gain unauthorized access to FA services through HA. The following is a list of the potential security risks in global mobility networks:

**A:1** *"Insider Attack"* - In such a scenario, If a trusted insider with access to a server obtains a mobile user's password, they could impersonate the legitimate user to gain access to other servers where the user is registered.

**A:2** *"DoS-Attack"* - Unauthorized users attempt to disrupt login sessions by entering incorrect passwords. Only the home agent, not the mobile user, can detect this activity. These unauthorized users may repeatedly engage in this activity to flood the system with requests, obstructing legitimate users' access and potentially causing the authentication system to become overwhelmed.

**A:3** *"Forgery Attack"* - An intrusion attempts to mislead either the FA or HA by intercepting information being broadcast over the open communication channel and posing as the authorized Mobile user.

**A:4** *"PassWord-Guessing-Attack"* - Many passwords, they are vulnerable to attacks using guessed passwords because of weak entropy. In these cases, a potential intruder captures authentication messages being transmitted over a Public channel,

locally stores them, and subsequently attempts to verify guessed passwords by comparing them to the intercepted messages.

**A:5** *"Replay Attack"* - In order to deceive the MU, HA, or FA, this involves transmitting replay messages or information that has been intercepted from a public network.

**A:6** *"Stolen-Verifier Attack"* - Using a stolen password verifier, a malevolent user might pretend to be a trusted user and access the system without authorization.

**A:7** *"Smart-card loss Attack"* - A tamper-resistant smart card is required for the password authentication protocol to be secure. Without tamper resistance, an attacker can steal a user's smart card and extract the password by analyzing power consumption. Subsequently, An attacker might easily change or guess a user's password and pretend to be them.

### 1.3.3 Requirements for Security

According to user authentication protocols in mobility environment should adhere to the following security criteria, as outlined by Karuppiah and Saravanan (2015)

**SR:1** *Mutual authentication* - In order to stop forgery attacks, a strong authentication process is established among the Home Agent, Foreign Agent, and Mobile User. Each of these entities must mutually authenticate one another.

**SR:2** *Untraceability and User anonymity* - Mobile user's identity must remain confidential, even from third parties like the foreign agent. Untraceability implies that it should be impossible for an adversary to connect two conversations that originate from the same user.

**SR:3** *Forward secrecy* - In spite of the system's secret key being compromised, it assures that past session keys are never disclosed because to the principle of complete forward secrecy. Once the session key has been obtained, the entire session is no longer secure.

**SR:4** *Robustness against attacks* - In this case, a protocol should possess the capability to withstand various attacks, including insider attacks, replay attacks, stolen-verifier attacks, password guessing attacks, and impersonation attacks, even in scenarios where an adversary possesses full knowledge of the information stored in the smart card.

**SR:5** *Session key and fairness* - In this scenario, mutual authentication between the Mobile User (MU) and the Foreign Agent (FA) alone is insufficient to ensure data confidentiality. It is also crucial to negotiate a session key to establish a secure channel between them. Furthermore, the mutual authentication and key agreement protocol concludes with both the MU and FA agreeing on a session key derived from equal contributions from all involved entities.

**SR:6** *Local password verification* - Prior to interacting with other entities such as the HA or FA, the user's smart card must authenticate the user's identity and password for validity. If the user enters an incorrect password during the login phase, the system should promptly inform the user with an error message.

**SR:7** *User Friendliness* - The user should have the freedom to choose their own password and identity, and their device should allow password changes without needing assistance from the Home Agent.

**SR:8** *No time-synchronization* - The authentication procedure shouldn't rely on time stamp techniques to counteract Replay attack. Even when remote user authentication protocols use timestamps to ensure message freshness, they can remain susceptible to replay attacks due to unpredictable transmission delays in current networks. Furthermore, in the context of current network systems, clock synchronization is a difficult and expensive process.

**SR:9** *Free-From-Verification table* - In this risk, the system or server does not store passwords or verification tables, and there should be no presence of verification tables, even in hashed form, on the remote system.

## 1.4 Secure user authentication for mobile roaming service using Blockchain

GLOMONET is becoming one of the most important developing network environments for providing flawless roaming services in foreign networks. In the GLOMONet, mobile gadgets have become an integral aspect of our daily routines, with applications such as commerce, social networking, communication, and information exchange, among others.In a mobility network, the mobile user is allowed to pair their devices with alternative widgets utilising Bluetooth, GPS, and WiFi in order to receive broad internet services and other region-based services systematically.

Network contexts raise fundamental security and privacy challenges, such as mutual authentication, secrecy, and user anonymity. As a result, in network environments, user anonymity becomes a vital component. The current situation required the development of reliable network architecture for global mobile environments. Furthermore, GLOMONet provides roaming services to mobile subscribers. These services enable a user to utilize the offerings provided by their HN while being in a FN. The well-built secure authentication techniques will be used to secure roaming services in GLOMONet between users HN and FN being overtaken. Whenever a MU roams from present location to another one in a mobility network, roaming service is used to ensure the continuity of the mobile network service. Constructing a user model in a mobility network, the HA, FA, and MU are all involved in authentication. The security of this environment is compromised if an attacker is able to eavesdrop messages delivered over the open channel between the mobile user and foreign agent. Therefore, it is necessary for the home agent, mobile user, and foreign agent to exchange data securely.

### 1.4.1 Blockchain importance in GLOMONET

In general, designing a secure architecture for providing roaming services requires proper organization, collaborations that can significantly benefit from the design of a decentralized network, and consideration of any use cases that necessarily require an accurate combination of network services provided by the network environment. In particular, Blockchain is being utilized to address a variety of challenging tasks across

the entire network, and it is providing support in the continuous rapid growth of a number of wired devices, such as data services and data traffic. A blockchain is a decentralized, immutable record that ensures network confidentiality, integrity, privacy, and authentication. Blockchain is a P2P network that runs on the IP protocol. It is transparent, decentralized and provides the security to the users. Using cryptographic hash the previous blocks are interconnected to each other once the new blocks is added in to a blockchain network, it make sure that the chain is never broken since all the blocks are subsequently connected and each activities stored permanently in the network. The capacity of Blockchain plays a vital role in acquiring noticeable attention in telecom industries. With the advancement of Soulbound Tokens (SBT), the user could then share this digital identity with other parties, such as employers or educational institutions, as proof of their identity and qualifications. Because the Soulbound tokens cannot be copied or transferred, so digital identities created using them are secure and easily verifiable without the need for a centralized authority.

## 1.5 Motivation of the work

Cryptographers worldwide have been working diligently to develop robust authentication and key establishment protocols based on computational mathematics to address the various security threats that exist in wireless and GLOMONET. In this case, when constructing a efficient and secure robust mutual authentication protocols, researchers primarily employed computationally rigorous security mechanisms. However,these authentication methods may not be the best approach for mobility contexts with limited resources. Therefore, developing a reliable authentication protocol using lightweight crypto-primitives for wireless and mobile contexts is crucial.

A comprehensive examination of current Mobile user authentication protocols in the mobility networks uncovers security vulnerabilities present in numerous privacy-preserving protocols documented in the literature. Consequently, the development of a robust and enhanced security protocol in this context is of paramount importance. Furthermore, this authentication protocol must meet all security prerequisites within the mobility network while also maintaining low computational overhead.

## 1.6 Research Objectives

1. Analyzing a security robustness of different authentication and key agreement protocols in the existing literature to enhance security, maintain confidentiality, ensure data integrity, and preserve privacy in healthcare and Global Mobility Networks.

2. Designing a new and secure and secure authentication framework based on Blockchain for TMIS and GLOMONET through the utilization of smart contracts. This framework aims to safeguard user privacy and anonymity while also withstanding various network attacks.

3. Comprehensive security analysis using a strong adversary model and formal verification will be conducted to validate the robustness of the proposed protocols.

4. Ultimately, we will carry out a performance analysis of the proposed security protocols to assess communication and computational overhead.

## 1.7 Contributions

This thesis makes the following contributions. It involves the analysis of existing protocols and the proposal of various authentication protocols for roaming service in global mobility networks and telecare medical information system, which are as follows:

1. After conducting rigorous cryptanalysis, we have pinpointed various security vulnerabilities in existing authentication protocols. Our goal is to address these vulnerabilities by introducing an efficient and secure light-weight authentication protocols using decentralized Blockchain.

2. Proposed a novel and secure authentication protocols using Blockchain for TMIS and GLOMONET through the utilization of smart contracts. The proposed framework aims to safeguard user privacy and anonymity while also withstanding various network attacks.

3. The proposed authentication protocols has been rigorously evaluated for security using Dolev-Yao attacker model. In addition, both informal security analysis and formal security verification has been performed by utilizing High-Level Protocol Specification Language (HLPSL) to prove the security strength of the proposed protocols.

4. A novel approach blockchain based user authentication mechanism using a non-transferable Soulbound Token (SBT) for mobility networks has been proposed.

5. The proposed protocols are practically demonstrated and evaluated using the SPAN simulator, considering several network performance parameters into account, the outcomes of analysing the performance and simulations validate the system robustness, computational efficiency, and practical feasibility of the proposed authentication protocol for resource limited global mobility Networks and TMIS.

## 1.8 Thesis Structure and Outline

The thesis is structured as outlined below.

**Chapter : 1**, Offers a comprehensive perspective on authentication within global mobility networks and telecare medical information systems. It delves into key aspects, including prominent authentication applications, security threats, and prerequisites for global roaming services in mobile environments. Additionally, the research's motivation and objectives are outlined.

In **Chapter : 2**, Introduces fundamental cryptographic concepts and primitives, including operations like XOR or Exclusive-OR, one way hash functions, and both the algorithms called public and private keys are used. Furthermore, it incorporates the mathematical foundations required for designing and analysis of Authentication Schemes for roaming services in Glomonet. These mathematical concepts includes Diffie-Hellman key exchange, the ECC, DLP, Zero Knowledge Proofs, and Homomorphic encryption to ensure secure communication.

**Chapter : 3**, A review of prior research on user authentication for roaming services in mobile networks, as well as Telecare Medical Information Systems, has been presented.

The analysis reveals that many authentication schemes are susceptible to commonly recognized attacks and demand significant resources communication and computational and overheads.

**Chapter : 4**, Examines the threat and network models associated with authentication in Glomonet. Introduces an innovative blockchain-based mutual authentication system tailored for mobility networks, featuring immutability, peer-to-peer communication, decentralization, and distribution. This system prioritizes user anonymity and provides strong defense against numerous types of attacks. Additionally, the proposed authentication framework includes a some of the blockchain consensus computer protocols to ensure security, reliability & fault tolerance in the mobile environments.

In **Chapter : 5**, Represents a decentralized authentication secure framework for the Telecare Medical Information System implemented with Blockchain technology. The protocol consists of 4 phases: initialization, registration, decentralized authentication, and password change. An informal security requirement analysis confirms that the newly designed security framework effectively stands up to various types of attacks and successfully meets all design objectives within the healthcare system. Additionally, the results of performance analysis and simulations provide confirmation regarding the computational efficiency of the proposed authentication protocol.

**Chapter : 6**, Introduces a blockchain-based authentication protocol specifically designed for roaming in mobile environments. Performance analysis confirms that this protocol, employing SBT (Secure Blockchain Technology), offers both security and practical feasibility within resource-constrained wireless and mobile environments.

**Chapter : 7**, Summarizes the thesis by emphasizing its contributions and delves into potential avenues for future research.

# Chapter 2

# CRYPTOGRAPHIC PRIMITIVES

In this chapter, it introduces fundamental crypto-primitives and mathematical foundations necessary for the protocol design and security analysis of authentication protocols in global mobility networks, specifically for roaming services. Initially this section outlines the characteristics of One way Hash function and XOR properties. Subsequently, it provides concise discussions on the Computational Diffie-Hellman Problem, DLP-Discrete Logarithmic Problem, Diffie-Hellman key exchange, ECC- Elliptic Curve Cryptosystem, Zero Knowledge Proofs, and Homomorphic encryption.

## 2.1 Foundational Concepts

- **Cryptographic**: A Process of applying guidelines and strategies to transform a understandable message into an unintelligible one and later reversing this process to return the message to its original form.

- **E: Encryption**: A process of transforming plain text into ciphertext using a key is referred to as the encryption process.

- **D: Decryption**: The decryption process is the method of transforming ciphertext into plaintext with the help of a key.

- **Cryptanalysis**: Cryptanalysis, also known as codebreaking, is the study and practice of decrypting messages without knowing the key.

## 2.2 Essential Crypto-Primitives

Cryptographers often choose lightweight crypto-primitives, such as hash functions, symmetric encryption, and XOR operations, to ensure the efficiency and confidentiality of authentication systems.

### 2.2.1 Hash Function:

A secure one-way hash function takes a variable-length input and produces a fixed-length output, called a hash value. It has the following properties:

- As a result of the output is deterministic, ensuring that a particular message will consistently generate the same hash value.
- It is very efficient to compute H(P) for a given input message P, but it is computationally impossible to reverse the process and recover P from the given H(P), is often referred to as the one-way property.
- Finding two inputs, X and Y, such that H(X) = H(Y) is a difficult task, which pair is named a hash collision.
- Making even minor modifications to the input message leads to a significant alteration in the hash or message digest.

Hash functions are employed to produce the MACs (Message Authentication Codes) to ensure message integrity. The SHA (Secure Hash Algorithm) comprises a collection of standardized algorithms, each capable of producing digests of varying lengths. Among these, SHA-1 with a length of 160 bits, has found extensive use in various cryptographic applications.

### 2.2.2 XOR or EXCLUSIVE-OR cipher

The XOR algorithm in cryptography applies successive addition's principles:

$$p \oplus p = 0,\ p \oplus 0 = p$$

$$(q \oplus p) \oplus p = q \oplus 0 = q$$

Associative:

$$p \oplus (q \oplus r) = (p \oplus q) \oplus r$$

## 2.3 Public/Private Key Cryptography Algorithms

Public key mechanisms use a two keys for enciphering and deciphering. The private is private, while the public key is available to all. Examples of popular public key algorithms include RSA and ECC.

Private key algorithms use the same key for all crypto operations, and this key is shared between transmitter and receiver. Examples of private key protocols include AES, DES, and Blowfish.

## 2.4 Key Exchange using Diffie-Hellman algorithm

The D-H key exchange method allows two parties to establish a shared secret key over an insecure communication channel, even if they have no prior knowledge of each other. D-H key exchange procedure as shown below:

1. Sender generate two prime numbers, $p$ and $q$, and compute $n = pq$. Then, she selects an element $g \in G$.

2. Afterward, sender proceeds to choose a secret key $S_{HA} = a(< q)$ and finds the public-key $P_{HA} = g^a \ mod \ p$, then transmits to Receiver.

3. Likewise, receiver selects the secret key $S_{FA} = b(< q)$ and determines the corresponding public-key component $P_{FA} = g^b \ mod \ p$ to share with sender.

4. Afterward, sender finds a shared secret key $K_{FH} = P_{FA}^a \ mod \ p$ using Bob's public key. Similarly, Bob computes $K_{FH} = P_{HA}^b \ mod \ p$ using Alice's public key.

### 2.4.1 Computational Diffie-Hellman problem

Let's consider a group $G$ with order $q$, the computational Diffie-Hellman problem states that, given $g$, $g^x$, $g^y$, where $g$ is a generator and $x$, $y$ $\varepsilon$ $\{1, 2, ..., q-1\}$ are nonce, it is computationally infeasible to compute the value $g^{xy}$.

## 2.5 Zero Knowledge Proofs (ZKPs)

Zero-knowledge proofs (ZKPs) improves the privacy, security, and scalability of blockchains. The significance of ZKPs in Blockchain technology becomes evident through the following aspects. First, ZKPs empower the validation of a statement without disclosing the underlying information or data. This makes them an ideal tool for enhancing the privacy of blockchain transactions, ensuring that sensitive transaction data remains private while still allowing for verification and validation. Second, ZKPs offer a robust security by allowing the confirmation of a statement without exposing any information related to it. This makes them an effective tool for preventing fraud and ensuring the integrity of blockchain transactions.

By using ZKPs, Blockchain can achieve an enhanced level of security, making it a more reliable platform for storing and transferring data. In addition, ZKPs can help address the scalability challenge facing blockchain technology. With the growing number of users and transactions on a blockchain, the system becomes more complex, and the transaction processing time increases. ZKPs can reduce the computational burden of validating transactions, facilitating blockchain to efficiently manage a large number of transactions and users while preserving its security and privacy.

### 2.5.1 Prerequisites of a ZKPs protocol

Certain prerequisites must be satisfied for a protocol to consider as a zero-knowledge proof (ZKPs) protocol:

1. **Completeness**: The protocol must be complete, meaning that if a statement is true, the prover can convince a verifier with high probability.

2. **Soundness**:The protocol must be sound, meaning that it is computationally impossible for the prover to convince the verifier that a false statement is true.

3. **Zero knowledge**: Furthermore, the protocol should adhere to the zero-knowledge principle, ensuring that the verifier acquires no supplementary knowledge apart from the confirmation of the statement's truth.

4. **Computational Efficiency**: The protocol must be computationally efficient, meaning that it must be feasible to generate and verify the proof using reasonable computational resources

### 2.5.2 Homomorphic Encryption

Homomorphic encryption performs computations on encrypted information without decryption. In the context of ZKPs, homomorphic encryption can enhance the efficiency of ZKP verification. It allows verifiers to perform computations on encoded data without requiring decryption, thus maintaining data confidentiality. This can greatly reduce the computational overhead associated with ZKP verification, which is particularly important in applications that require frequent ZKP verification, such as blockchain systems. By using homomorphic encryption in ZKPs, it is possible to significantly increase the scalability and efficiency of ZKP-based systems while maintaining their high level of security and privacy.

## 2.6 Summary

This chapter provides an overview of cryptographic primitives, including EXCLUSIVE-OR or (XOR) operations, hash functions, public and private-key algorithms. Additionally, the chapter discusses the mathematical foundations necessary for designing and analyzing the roaming service in authentication protocols. These foundations include D-H key exchange, ECC cryptosystems, DLP, Zero knowledge proofs and Homomorphic Encryption.

# Chapter 3

# REVIEW OF RELATED WORKS

## 3.1 Analysis of Authentication Schemes in Global Mobility Networks

The goal of Researchers, Cryptographers, and Wireless organizations have been striving to design secure protocols and frameworks that employ robust cryptographic techniques to defend against a variety of attacks in mobile environments. Yet, the majority of traditional authentication protocols, including two-factor authentication protocols, found in wireless and mobility network literature, are susceptible to common attacks like impersonation attacks, insider attacks, replay attacks, SQL injections etc.

In 2011, He et al. (2011) presented a secure user authentication protocol utilizing smart cards for wireless environments. The authors were confident that their protocol provided User-anonymity and effective protection in resistance to Replay-attack and Impersonation-attacks. The authors in Yoon et al. (2011) introduced a simple authentication system designed for battery-powered mobile devices operating in wireless and mobile communication networks. This authentication technique is not only effective but also enhances security while preserving user anonymity. However, Li and Lee (2012) examined He et al. (2011) authentication scheme and concluded that their protocol is not user-friendly and is unable to guarantee fairness in the key agreement and user anonymity. Consequently, Li and Lee (2012) suggested a novel authentication protocol for wireless and mobile networks that ensures user anonymity.

In 2013, Jiang et al. (2013) presented an improved authentication mechanism. to support the security of global mobility networks. However, Wen et al. (2013) subsequently identified vulnerabilities in Jiang et al. (2013)'s scheme, including susceptibility to

stolen verifier, replay, and denial of service attacks. Wen et al. (2013) proposed a new technique to address these security weaknesses in previous authentication protocols. Later, Li et al. (2013) also put out a new authentication technique, claiming that it met all security requirements for the mobility network. In 2014, Zhao et al. (2014) identified that the technique proposed by Mun et al. (2012) was found to be vulnerable to password guessing attacks, forgery attacks and insider attacks. Additionally, it lacked the ability to offer user friendliness, or mutual authentication, and user anonymity. Subsequently, they introduced a novel authentication protocol aimed at addressing the security flaws present in the existing authentication protocols.

In 2015, Karuppiah and Saravanan (2015) proposed a secure authentication system emphasizing user anonymity for roaming service within global mobility networks. This protocol is designed to provide various advantages, including resilience against several types of attacks, untraceability and user anonymity. However, Madhusudhan et al. (2016) identified security flaws in their authentication scheme and subsequently introduced a secure and lightweight authentication mechanism for roaming service in mobile networks. Later on,Several authentication protocols have been proposed to provide roaming services in global mobile networks Madhusudhan et al. (2018); Gope and Hwang (2016a); Lee et al. (2017); Xu et al. (2018); Ahmadi and Nikooghadam (2019). However, the current authentication procedures are more computationally complex and do not meet all security needs in the mobility network Shashidhara et al. (2020).

Madhusudhan et al. (2018); Shashidhara et al. (2020) conducted security analyses of the recently proposed mutual authentication systems outlined in Karuppiah and Saravanan (2015); Xu et al. (2018). The existing protocols were found to be vulnerable to Replay, Injection, and Dictionary attacks.

Blockchain-based protocols in wireless and mobility networks offer enhanced user-friendliness by ensuring a tamper-proof operations, robust user authentication mechanism, and decentralized services. Some of the blockchain-based authentication protocols are as follows: In Nguyen et al. (2021), the authors introduced an innovative blockchain-based roaming management protocol featuring a comprehensive analysis of the Proof-of-Stake (PoS) consensus mechanism and a Smart-contract enabled roam-

ing management platform to address the problem of roaming fraud for mobile service providers. Due to its reliance on a single-factor authentication technique, Blockchain networks cannot mutually authenticate home agents, foreign agents, and mobile subscribers. The authors also fail to provide smart contracts for user authentication and blockchain implementation.

The authors in Al-Qerem (2022) used a RAFT as consensus algorithm for blockchain application of roaming services for mobile network. The raft consensus validate transactions and commits a blocks on to the ledger. It can lead to significant storage savings, particularly if the transaction load is low. However, the proposed approach is to improve the system performance during roaming process and the RAFT consensus protocol fails to address mutual authentication, user anonymity requirements.

To make the roaming service in 5G networks easier, Weerasinghe et al. (2021) the authors suggested a novel blockchain based architecture. For seamless connectivity regardless of MNOs connected with each 5G local operators, the suggested approach provides roaming tenants with a universal account. To address the issue of mistrust amongst MNOs (Mobile Network Operators), the authors Mafakheri et al. (2021) proposed a blockchain network that is permissioned and built on smart contracts.The suggested architecture use smart contracts to automatically handle billing settlement without relying on trusted third-party. Additionally, there are a several number of blockchain based protocols that have been implemented in the literature. These protocols focused on authentication in Smart-City applications Esposito et al. (2021), the smart grid Hao et al. (2021), decentralized identification Ferreira et al. (2021), and improving privacy preservation in fog computing environments Baniata and Kertesz (2020); Baniata et al. (2021); Baniata and Kertesz (2022).

## 3.2 Analysis of Authentication Schemes in TMIS

Electronic Health Records (EHR) serve as repositories for various information, including patient particulars, clinical notes, laboratory findings, medical images, financial

records, medical history, and insurance information. Therefore, the patient's anonymity is crucial, and a breach of their privacy might result in major security concerns in Telecare Medical Information Systems (TMIS). As a result, numerous security protocols based on diverse aspects helped to secure data privacy and patient anonymity. Nonetheless, a solution was provided to circumvent certain flaws seen in some Two-Factor authentication schemes Chen et al. (2019); Lu and Zhao (2021); Lo et al. (2020); Giri et al. (2015). Current authentication protocols, on the other hand, are open to modification, denial-of-service attacks, and guessing attacks.

Tan (2014) suggested an Elliptic Curve Cryptography-based safe authentication technique for TMIS, and Yoon and Yoo (2013) proposed a mutual authentication mechanism to protect user privacy. Their authentication procedures, on the other hand, were entirely ineffective in maintaining user anonymity and untraceability. Fan and Lin (2009) later developed a privacy-preserving protocol for TMIS as a cure for the protocols, although their approach was similarly susceptible to password guessing attacks.

Renuka et al. (2019) introduced a Two-Factor authentication method to enhance security in smart healthcare. Mishra et al. (2014) also developed a solid three-factor security architecture based on the bio-hashing technique. Nevertheless, many of these mutual authentication techniques are insecure or lack certain useful security requirements, demonstrating that building a viable mutual authentication scheme for healthcare is always challenging. The increasing demand for blockchain privacy and security in healthcare has been noticed in recent years because of the built-in anonymity, autonomy, encryption, and immutability aspects of blockchain. Addressing a range of challenges in response to the significant merits of blockchain within the context of TMIS, researchers have proposed solutions Lin et al. (2018).

Yue et al. (2016) have published a blockchain based secure architecture that allows a third-party user to calculate stored data without invading the patient's privacy. Xia et al. (2017) proposed a blockchain based data sharing platform to tackle authentication concerns. As a result, their authentication methodology incorporates a private blockchain network concept, allowing only known entities to access patient information after verifying their identity related information.

The health of blockchain-based applications was then examined by Kuo et al. (2017) examined many obstacles to blockchain technology adoption in the health sectors and provided solutions as well. In addition, Zhang and Lin (2018) have presented a secure Blockchain-based authentication methodology for safeguarding the privacy of a patient's health data. Their system is made up of federated and permissioned blockchain networks, which ensures that patient data is kept private and secure. Very recently, Fan et al. (2018) presented a complex system for processing patient data based on Blockchain. Medblock has increased the security of health records by integrating authentication and symmetric encryption methodologies into their protocol.

In contrast to the previous mentioned blockchain based medical electronic records, patients privacy can be violated if a third-party individual or organisation other than the hospital attempts to access patients' vital data via Telecare Information Systems (TMIS) Chen et al. (2019). We have not discovered any scholarly articles or related information on blockchain-based mutual authentication protocols for the TMIS environment at this time. Thus, we proposed a security and privacy preserving framework for TMIS utilizing a private blockchain. On the one hand, each hospital has its own private blockchain, on the other side, multiple hospitals collaborate to form a federated blockchain. Patients' electronic medical records are encrypted before being stored in the hospital's private blockchain.

## 3.3 Blockchain-Based Authentication Protocol for Mobile Network Roaming Services

As a result of the rapid advancements in communication technology, mobile users can now move throughout the world and utilize the mobile network's ubiquitous services. GLOMONet has recently emerged as one of the most promising venues for providing flawless roaming service in foreign networks. But the wireless and mobility environments, on the other hand, are well-known for being more vulnerable to attacks. The attacker has the ability to eavesdrop, manipulate, or prevent sensitive data sent via the radio channel. As a result, in the mobility environment, the mutual authentication procedure between communication entities is critical.

In 2015, Karuppiah and Saravanan (2015) examined the Rhee et al. method, observing that it is susceptible to impersonation, password guessing, as well as the point that Rhee et al.technique does not notice incorrect passwords immediately. After that Karuppiah and Saravanan (2015) also presented a new and secure authentication methods with user anonymity for GLOMONET roaming services. However, Wu et al. (2017) Shows that Gope and Hwang (2016b) authentication mechanism is insecure for GLOMONet. Thus, Wu et al. (2017) introduced a novel mutual authentication system employing a two factor scheme to rectify the shortcomings observed in recent schemes from 2016. Recently, in 2021 Shashidhara et al. (2020) demonstrated Xu et al. (2018) authentication's and key agreement technique had some security weaknesses and Shashidhara et al. (2020) stated that Xu et al. (2018) protocols is exposed to some common known attacks. Further, Shashidhara et al. (2020) established a secure and robust mutual authentication scheme for mobility environments as a solution. Furthermore, they implemented security scheme is light-weight, secure, and computationally efficient, according to the performance evaluation. In 2020, Nikooghadam et al. (2020) reviewed and illustrate the flaws in the work of Ghahramani. Subsequently, Nikooghadam et al. (2020) proposed a more secure and efficient authentication system for roaming users in GLOMONET and key agreement technique and also verified the proposed scheme's security in both a descriptive and formal manner using Scyther, a formal verification tool.

To design proper Authentication protocols using Blockchain in GLOMOnet, very little research work has been done to date, and it is becoming a popular and well-supported technology. Most of the work in this field is currently taking place in the Blockchain space, and some of the existing work that is published for authentication protocol using Blockchain is highlighted as follows.

In 2022, Taylor et al. (2020) published a paper titled "A systematic literature review of Blockchain cyber security" in which they presented a comprehensive analysis of Blockchain's role in enhancing cybersecurity and the author's development of innovative Blockchain applications for network security, certification schemes, web applications, public key cryptography, and machine visualization.

In 2022, Li et al. (2022) propose a dynamic group key agreement protocol and authentication protocol built on Blockchain. This protocol streamlines the authentication process for each user within a group, where users only need to authenticate their immediate neighbor once. This improvement enhances efficiency while simultaneously reducing computation and communication costs.

## 3.4 Summary

This chapter reviews existing user authentication protocols for roaming services in wireless and mobile environments, including the Telecare Medical Information System. Our analysis shows that many of these protocols are insecure and have high computational and communication overhead.

# Chapter 4

# BLOCKCHAIN BASED DECENTRALIZED AUTHENTICATION PROTOCOL FOR MOBILITY ENVIRONMENTS

Traditional, centralized authentication models have inherent vulnerabilities. These vulnerabilities can lead to unauthorized access, roaming fraud, identity theft, and data breaches. A centralized system creates a single point of failure, and if compromised, could expose a vast amount of user data. Decentralized authentication protocols, using blockchain technology, offer a significant improvement in security and privacy. By storing crucial authentication parameters on a distributed ledger, these protocols eliminate the central point of attack. The tamper-proof nature of blockchain ensures data integrity and prevents unauthorized modifications. Additionally, decentralized authentication empowers users with greater control over their data. Solidity smart contracts manage user authorization on the blockchain, fostering a transparent and secure access control system.

In this chapter, we present Mobile-Chain, an innovative blockchain-based authentication system tailored for mobility environments. Our system prioritizes safeguarding user privacy and ensures robust security, including mobile user authentication, privacy, confidentiality, and integrity of the data. The proposed security framework is executed on Ethereum blockchain, utilizing the solidity smart contract. Extensive analysis demonstrates the proposed system resilience to various attacks common in mobile networks. Moreover, we subject the authentication framework to formal verification

through AVISPA. Notably, performance evaluations confirm the protocol's efficiency, computational efficacy, and feasibility for implementation in resource-limited wireless and mobility environments.

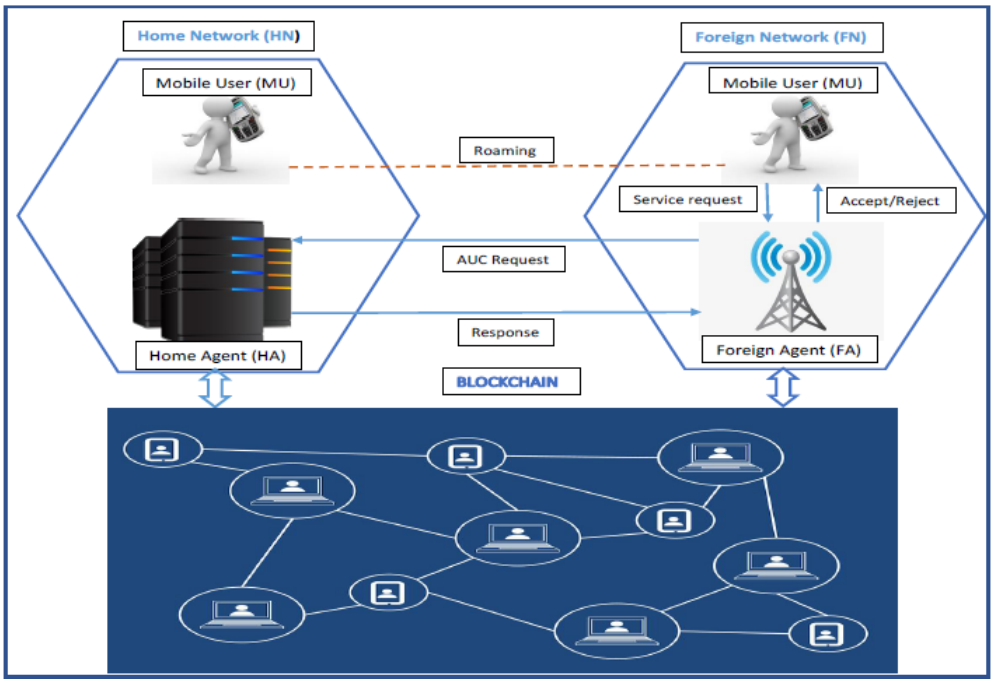



Figure 4.1 Blockchain based mutual authentication for roaming service.

In the roaming scenario, MU, HA, and FA make up the common authentication mechanism. After successfully registering with the Home Network, an MU can utilise the HA's services (HN). Foreign network administered by FA is visited by the registered user Gope and Hwang (2016b). Mutual authentication between the entities is essential in this case to prevent adversaries from gaining unauthorised access. Additionally, the current authentication protocols expose highly sensitive user privacy, such as anonymity and location information.

Figure 4.1 shows a mobility environment with roaming service that uses a blockchain-based authentication architecture. During registration, the mobile user sends a request to their Home Agent (HA). The HA processes this request and stores the user's registration information on a tamper-proof blockchain ledger. When a registered user roams onto a Foreign Network, the Foreign Agent can then securely authenticate the user by

verifying their information on the shared blockchain. This eliminates the need for a central server and reduces the risk of unauthorized access to user data.

## 4.1 Motivation

Blockchain is gaining recognition from academia and research organizations, where it is used to build secure frameworks. Its primary purpose is to ensure security, transparency, and decentralization across a multitude of applications. The cryptographers and the Industry have identified some critical issues associated with authentication and authorization in the existing roaming scenarios, which include:

- In global mobility networks, the majority of the authentication protocols now in use are susceptible to well-known attacks Karuppiah et al. (2017). To thwart Replay-attacks, the authentication methods also make use of a timestamp mechanism. However, the network's unpredictable delays cause the timestamp system to fail Madhusudhan et al. (2018).

- Two factor authentication is used by the current mutual authentication protocols. Passwords and smart cards are used for mobile user authentication. Password guessing and stolen-verifier attacks can be used against these protocols Zhao et al. (2014).

- The unaddressed unauthorized access to content related to mobile users is considered a significant breach of user security.

- All mobile users must authenticate with foreign agents through the home network before they may access the required services Xu et al. (2018).

- Additionally, a centralised infrastructures of the current authentication systems for mobile networks create significant problems during system failures or network breakdowns.

As a result, the roaming service within the framework of mobility networks requires a strong security architecture based on blockchain is established to ensure protection against a variety of attacks.

### 4.1.1 Security Requirements & Design Goals

Key factors in Design & Security Requirements for Mobile Roaming Service

- *User-anonymity:* For mobile nodes, traditional smart-card-based authentication algorithms don't provide privacy, since a malicious or compromised attacker can disclose the user's identity during the authentication phase. Therefore, the mobile user's identifying information should be kept private He et al. (2011).

- *Untraceability and Unlinkability:* The intercepted messages exchanged during the authentication phase shouldn't be linked, allowing the attacker to trace the origin or location of the mobile user Li et al. (2013). Blockchain is pseudonymous in nature, therefore for the majority of its architecture, an intruder cannot determine the identities of mobile nodes by examining transactions.

- *Single registration:* A single registration with the HA would be necessary for the authentication process before the mobile users could log in. Mobile user registration just needs to be done once to make it practical Madhusudhan and Shashidhara (2019).

- *Session key fairness:* The authentication protocol should provide secure session key establishment, where all communication entities, such as MU, FA, and HA, participate in the session key negotiation in order to achieve secure communication Madhusudhan et al. (2016).

- *Security infrastructure:* Technology like blockchain is required because, unlike centralised systems, it prevents all information from being kept in one location. The central server failure or single point of failure is therefore nonexistent. Additionally, blockchain maintains data in distributed ledgers that guarantee data integrity, secrecy, and transparency.

- *Computational gain:* An authentication system could be effective and lightweight to address the mobile terminals' resource limitations.By including important cryptographic operations in the protocol architecture, computational efficiency can be gained.

### 4.1.2 Research contributions

The research contributions are as follows:

1) In this chapter, a novel Mobile-Chain that is a reliable user authentication protocol for global mobility networks has been presented. This decentralised security architecture guarantees mutual authentication, anonymity, and resilience to diverse threats.

2) In this protocol, blockchain enhances the mutual authentication between the user and service provider, guarding it against various network attacks such as stolen verifier and dictionary attacks etc.

3) In the proposed approach, the mobile user is connected to a secure crypto wallet to keep the authentication information provided by the HA. Because of lost or stolen smart cards, the blockchain-based protocol protects users from password-guessing attacks.

4) To demonstrate the reliability of the proposed blockchain-based authentication system's security, a thorough functional requirements analysis and comparison have been conducted. The protocol specification language has also been used to do a formal security validation.

5) The proposed framework is implemented on Ethereum blockchain using solidity smart contracts. This implementation enhances safety, tamper-proof & decentralization in the blockchain based mobility environment.

6) Significantly, a performance assessment of the proposed approach demonstrates that the mobile chain protocol exhibits reduced computational burden when contrasted with existing authentication frameworks.

### 4.1.3 System models

We follow the Dolev-Yao threat model to describe the potentiality of the intruder and common privacy issues encountered during mutual authentication in mobility environments. The Dolev-Yao model is a very powerful adversarial model that is generally

Table 4.1 Advantages and Disadvantages of Current Authentication Protocols in Mobility Environments.

| Authors | Research article | Published Year | Merits | Demerits |
|---|---|---|---|---|
| He et al. He et al. (2011) | The user authentication protocol using smart-card for mobile communication | 2010 | User anonymity, single registration and computational efficiencies. | Susceptible to replay attacks and clock synchronization problem. |
| Yoon et al. Yoon et al. (2011) | A secure mutual-authentication for roaming in mobile communications | 2011 | Preserve privacy, anonymity and provides reliable roaming services | Prone to insider attacks, unfairness in session-key computation. |
| Li et al. Li and Lee (2012) | A novel privacy-preserving authentication using smart-card for wireless communication | 2012 | Fairness in key agreement, forward secrecy and resistance to impersonation attacks | No local password verification, inefficient due to computational complexity. |
| Niu and Li Li et al. (2013) | An enhanced remote user authentication protocol for roaming service | 2013 | Local password verification and provides perfect forward secrecy | Susceptible to insider attacks and DoS attacks. |
| Zhao et al. Zhao et al. (2014) | An anonymous authentication protocol for the mobile networks | 2014 | Anonymity, local password verification and no password tables | Susceptible to replay attacks and DoS attacks. |
| Sarvanan and Muttu Karuppiah and Saravanan (2015) | A secure authentication protocol with anonymity in global mobile networks | 2015 | Provides privacy, anonymity and untraceability. | Prone to password guessing, stolen verifier attack and forgery attack. |
| Gope and Hwang Gope and Hwang (2016a) | Energy efficient and light weight authentication protocol for secure communications in mobility networks | 2016 | Provides energy efficiency and computational gain | Vulnerable to DOS attacks and suffers from clock synchronization problems. |
| Lee et al. Lee et al. (2017) | A novel mutual authentication protocol for roaming service in the mobile network | 2017 | Prevents impersonation attacks and smart-card loss attack | Prone to replay attacks and insider attack. |
| Xu et al. Xu et al. (2018) | An efficient mutual authentication protocol for global mobility networks | 2018 | Secure against clock synchronization problem, improves performance gain. | Vulnerable to Bit-flipping and Denial of Service attacks. |
| Madhusudhan et al. Madhusudhan and Shashidhara (2020) | A secure user authentication with privacy for mobile networks. | 2019 | Secure against various attacks and computational efficient | Susceptible to SQL injection and dictionary attacks. |
| ahmadi et al. Ahmadi and Nikooghadam (2019) | A secure session key agreement authentication in mobility network preserving anonymity. | 2019 | Attains anonymity, untraceability and mutual authentication | Vulnerable to impersonation and replay attacks. |
| Shashidhara et al. Madhusudhan and Shashidhara (2019) | Anonymous mutual authentication scheme for roaming in Resource-Constrained mobile devices. | 2019 | Resistance to DoS attacks, replay attacks and provides local password verification | Prone to Bit flipping and dictionary attacks. |



considered as the benchmark for assessing cryptographic algorithms. The adversary is capable of obtaining any message that is transmitted via the network. In order to send messages to any entity, the attacker can pose as another entity or act as a normal network user so, the Dolev-Yao model is an easy-to-use framework for examining security protocols that are frequently used in distributed systems and networks.

In addition, we also follow the honest-but-curious (HBC) adversary model. Among all the adversarial models, this model is the least robust.

Table 4.1 outlines the advantages and disadvantages of security protocols designed for mobile user authentication in global mobility environments for roaming services.

**Network model**

The authentication framework aims to establish a secure communication platform for MU, HA, and FA over unsecured public channels in a distributed mobility network with ubiquitous services. Within this context, all mobility entities engage in the exchange of authentication messages across an unreliable public network, such as the Internet. Certainly, trust cannot be assumed across all communication participants within the global mobile environments. With the proliferation of mobile subscribers in cellular and mobile networks, the security risks and system complexity are notably heightened. Moreover, while the mobility network manages packet transmission and reception, it does not inherently offer security services like authentication. Consequently, unauthorized mobile users can potentially eavesdrop on,or manipulate sensitive information transmitted over the network.

**Attacker model**

Let's consider a scenario where an adversary, denoted as $\mathscr{A}$, has full control over a public network. In this role, $\mathscr{A}$ has the capability to selectively manipulate sensitive information exchanged between MU, HA, and FA. These actions include dropping, replaying, intercepting, delaying, and eavesdropping on data, all with minimal delays as described in. Moreover, in situations involving verifier or password tables stored in a database, intruder $\mathscr{A}$ can potentially gain access to this information via SQL injection type techniques such as CSS. Further, $\mathscr{A}$ could track the user identity & location details of MU when the mutual authentication framework employs consistent parameters across various sessions.

Further, the adversary $\mathscr{A}$ will attain to extract the sensitive information from the lost/stolen smart-cards Li and Lee (2012); Mun et al. (2012).

## 4.2 Blockchain-based security framework

The security framework uses PBKDF (Parallel Blockchain Key Derivation Function) as the key derivation protocol which simplifies and improves the performance of the roaming process in the mobility networks Lee and Ma (2020). The proposed authentication protocol will be implemented using the Ethereum blockchain. Currently, the Ethereum network uses Proof-of-Stake (PoS) as a consensus algorithm. In this network model, base stations will acts as validators to verify the transactions. The mobile user terminal associated with an Ethereum wallet (Similar to MetaMask), which generates a public-private key-pair for the mobile user.

Before the authentication system starts, FA and HA establishes a common Secret-key using a dynamic Diffie-Hellman key exchange mechanism. In the initial phase, HA will act as an authentication server and distribute the genesis block to all base stations. In addition, HA collects the public keys and acts as a key distribution center. Further,

Table 4.2 Crypto notations used in this chapter

| Notation | Description |
|---|---|
| $MU, HA, FA$ | Mobile User, Home Agent, & Foreign Agent |
| $ID_M, ID_H, ID_F$ | Identity of MU, FA, HA |
| $PW_M$ | User Password |
| $S_{FA}$ | FA's shared secret-key |
| $S_{HA}$ | HA's private-key |
| $(E/D)_K$ | Encryption/decryption using $K$ |
| $C_M$ | Counter variable |
| $h(.)$ | Hash algorithm |
| $SK$ | Session-key |
| $\|\|$ | Concatenation |
| $\mathscr{A}$ | Attacker |
| $\oplus$ | Exclusive-OR |

the mobile user attaches to the base station and receives its genesis block. In return, the mobile user provides the timestamp, random string, and it's public key to the base

station. Eventually, the source base station broadcast MU's information to all other base stations in the network for possible authentication during the roaming process. Regarding mutual authentication, the proposed protocol encompasses three key phases: 1) Registration 2) Mutual Authentication and finally 3) Password Change Phase. Table 4.2 provides a list of the system's mathematical and cryptographic notations.

### 4.2.1 Proposed Registration Phase

Table 4.3 Registration phase of the proposed protocol

| **Mobile User** | **Home Agent** |
|---|---|
| Choose $ID_M, PW_M, N_M$<br>Computes:$R_1 = h(ID_M \|\| N_M)$ | |
| $R_1 = \{h(ID_M \|\| N_M)\} \rightarrow$ | |
| | $H_M = h(R_1 \|\| S_{HA})$<br>Initialize $C_M = 0$<br>HA stores $\{R_1, C_M\}$<br>on Blockchain |
| $\leftarrow R_2 = \{H_M, C_M, h(.)\}$ | |
| MU selects a password $PW_M$<br>Computes: $M_P = h(ID_M \|\| PW_M \|\| N_M)$<br>MU stores $\{H_M, M_P, C_M, N_M\}$ on wallet | |

Table 4.3 shows the registration phase of the mobile user to get registration parameters from the home agent.

### 4.2.2 Proposed Login and Authentication Phase

In this scenario, an MU moves into other networks to access the services they require. Here, mutual authentication occurs involving an MU, FA, and HA. Furthermore, the protocol employs a dynamic DH mechanism to establish the shared secret key between

Foreign Agent & Home Agent. Login and mutual authentication procedure is summarized in Table 4.4.

Table 4.4 Proposed mutual authentication and session-key negotiation phase

| Mobile User | Foreign Agent | Home Agent |
|---|---|---|
| Generate $R_M$<br>$M_A = h(ID_M \| N_M) \oplus R_M$<br>$M_B = h(H_M \| C_M) \oplus R_M$<br><br>$M_1 = \{M_A, ID_H, M_B\} \longrightarrow$ | | |
| | Generate $R_F$<br>$F_A = h(M_A \| S_{FA}) \oplus R_F$<br>$F_B = h(F_A \| S_{FA})$<br><br>$M_2 = \{ID_F, F_A, F_B, M_B\} \longrightarrow$ | |
| | | $S_{FA} = h(ID_F \| S_{HA})$<br>$F_B^* = h(F_A \| S_{FA})$; $F_B^* \stackrel{?}{=} F_B$<br>$H_M^* = h(R_1 \| S_{HA})$<br>$R_M^* = h(H_M^* \| C_M) \oplus M_B$<br>$M_A^* = h(R_1) \oplus R_M^*$<br>$M_B^* = h(H_M^* \| C_M) \oplus R_M^*$; $M_B^* \stackrel{?}{=} M_B$<br>$R_F = h(M_A^* \| S_{FA}) \oplus F_A$<br>$H_A = h(ID_H \| M_B^* \| S_{FA})$<br>$H_B = h(H_M^* \| ID_F \| C_M)$<br>$H_C = h(ID_H \| R_M^*) \oplus R_F$<br>Update $C_M = C_M + 1$<br><br>$M_3 = \{H_A, H_B, H_C\} \longleftarrow$ |
| | $H_A^* = h(ID_H \| M_B \| S_{FA})$; $H_A^* \stackrel{?}{=} H_A$<br>$SK = h(M_A \| R_F \| ID_H)$<br><br>$M_4 = \{H_B, H_C\} \longleftarrow$ | |
| $H_B^* = h(H_M \| ID_F \| C_M)$; $H_B^* \stackrel{?}{=} H_B$<br>$R_F = h(ID_H \| R_M) \oplus H_C$<br>$SK = h(M_A \| R_F \| ID_H)$; Update $C_M = C_M + 1$ | | |

### 4.2.3 Mobile User Password change phase

In this process, a registered mobile user with authorized access can locally update their default password. The password renewal phase consists of the following steps:

S1: An enrolled mobile user inputs their identity, denoted as $ID_M$, and their corresponding password, indicated as $PW_M$, via the user interface.

S2: The device performs a computation, producing the value $M_P$ by combining the elements $ID_M$, $PW_M$, and $N_M$ as follows: $M_P = h(ID_M||PW_M||N_M)$. It then proceeds to compare $M_P^*$ with $M_P$. If the comparison yields a mismatch, the password renewal phase is immediately terminated. Conversely, if the two values match, the local password verification is deemed successful, ensuring the legitimacy of the mobile user.

S3: Subsequently, the mobile user enters their new password denoted as $PW^NM$, and the device performs a computation to determine a new value, $MP^N$, using the formula: $M_P^N = h(ID_M||PW^NM||NM)$.

Finally, the device updates the value of $M_P$ with the newly computed $M_P^N$. In conclusion, the mobile user retains the following parameters: $H_M, M_P^N, C_M, N_M$.

## 4.3 Security analysis

A comprehensive security analysis has been outlined. An attacker denoted as $\mathscr{A}$ endeavors to compromise the security protocol by exploiting the information exposed during communication between HA, FA & MU. However,$\mathscr{A}$ remains unsuccessful in accessing and taking control of the proposed security framework. Ultimately, the blockchain protocol prevents various network attacks and fulfills all criteria in mobile networks.

### 4.3.1 Withstand replay attacks

Within the Mobile-Chain system, an efficient counter-based strategy is utilized to effectively counteract replay attacks. In the event of an intrusion where an unauthorized party attempts to replay a previous message, the Home Agent (HA) detects this security breach by accessing the blockchain and analyzing the original counter value $C_M$ linked to the mobile user. Consequently, this system ensures a robust defense against replay attacks.

### 4.3.2 Prevention of DoS attack

To guard against Denial of Service (DoS) attacks, the implemented system features local password verification. In this process, the Mobile User (MU) device calculates $M_P^* = h(ID_M||PW_M||N_M)$ and checks if it matches $M_P^* \stackrel{?}{=} M_P$ locally at the client side. If the verification fails, the protocol immediately denies access to the system and terminates the authentication procedure. This design ensures swift detection of incorrect credentials, effectively minimizing additional communication and computational overhead.

### 4.3.3 Clock Synchronization Problem

The Mobile-Chain system, as put forward, employs counters denoted as $C_M$ in place of timestamps as a defense mechanism against replay attacks. This approach necessitates the presence of additional clocks at the Home Agent (HA), Foreign Agent (FA), and Mobile User (MU). Timestamp-based authentication protocols are susceptible to replay attacks due to the unpredictable transmission delays inherent in global mobility networks, which can result from node failures or network partitions.

In the proposed protocol, the counter value is systematically incremented based on the mobile user's interactions with the home agent.

## 4.4 Implementation of the proposed authentication protocol

The proposed protocol (Mobile-chain) is implemented using the Ethereum blockchain. One of the most widely used blockchain platforms for developing decentralised applications and smart contract solutions is Ethereum. It supports Layer 2 solutions which are crucial because they support scalability and higher throughput without compromising the Ethereum blockchain's integrity, enabling total decentralisation, transparency, and security. In addition, the ethereum is open-source with huge community support and supports for interoperability. Besides, this platform ensures privacy using zero-knowledge proofs.

The smart contracts for registration and authentication phases are written in solidity, compiled using Remix, and deployed to the Ethereum making use of Ganache.

The core components of the proposed system primarily comprises two key phases: registration and user authentication. In the registration phase, a mobile network administrator registers the system on a decentralized blockchain by assigning it a system identification number *SID*. Subsequently, the blockchain system undertakes the verification of the uniqueness of the Service Identifier (*SID*) and proceeds to create a new block using a smart contract. Following a successful registration, the blockchain system generates a certificate for the mobility network. This is achieved through the use of its private key denoted as $E_{PR}(SID)$.

After the certificate is encrypted using the network administrator's public key ($C_S = E_{PU}(E_{PR}(SID))$), the system proceeds to transmit it to the network administrator. The network administrator, in turn, decrypts the certificate ($C_S$) using the corresponding private key and subsequently disseminates it to all other mobility entities, including the Mobile User (MU), Home Agent (HA), and Foreign Agent (FA).

Algorithm 1 provides an outline of the smart contract utilized for the registration of mobility systems within the blockchain.

**Algorithm 1** Smart contract for the mobility system registration

*SID* registered with blockchain Global parameters: *sys*: Object *BC*: Blockchain //check for SID on blockchain $(SID - exists(sys.id, BC) = true)$ *SID* already exists on blockchain return error() $register - SID(BC, sys.id)$

Upon receiving the certificate ($C_S$) from the network administrator, mobile devices such as the Mobile User (MU), Foreign Agent (FA), and Home Agent (HA) each generate a unique certificate known as an access token. These access tokens incorporate essential information, including the network identifier (*SID*) provided by the administrator, as well as device identifiers ($ID_M$, $ID_H$, and $ID_F$).

In this context, the smart contract undertakes the validation of the system identifier (*SID*). If the comparison process proves successful, it assures the system's legitimacy. Subsequently, the smart contract permits the devices to complete their registration with the blockchain. Ultimately, a block is created to map the relationship between the system ID (*SID*) and the device ID (*EID*). A new certificate, referred to as an "Auth-

```
pragma solidity ^0.6.8;
/*Creating a Smart Contract for Mobility-Chain*/
contract Mobile_chain{
struct Home_agent
{
int ID_HA;
string S_HA;
string R1;
int CM;
string HM;
}
Home_agent [] HA;
/*insert MU registration details on Blockchain*/
function insert_Home_agent( int ID_HA, string memory
S_HA, string memory R1, string memory HM, int CM) public
{
Home_agent memory Block=Home_agent(ID_HA, S_HA, R1, CM, HM);
HA.push(Block);
}
/*retrieve authentication parameters*/
function retrieve_Home_agent(int ID_HA) public view
returns(string memory, string memory, string memory)
{
uint i;
for(i=0;i<HA.length;i++)
{
Home_agent memory Block=HA[i];
// Searching for HA's details in Blockchain
if(Block.ID_HA==ID_HA)
{
return(Block.S_HA, Block.R1, Block.HM);
}
}
/*If details not exists in the Blockchain*/
return("Not Found");
}
}
```

Figure 4.2 Smart Contracts in Solidity: Secure Storage and Retrieval of Authentication Data on the blockchain.

pass," is then distributed to the devices for future authentication purposes.

Devices such as the Home Agent (HA), Foreign Agent (FA), and Mobile User (MU) have the capability to securely store and retrieve their authentication parameters on the blockchain utilizing the "Auth-Pass" issued during the device registration phase. A smart contract embedded within the blockchain initiates transactions and assesses the legitimacy of devices based on the presence of $SID, EID$ in the "Auth-Pass". When the validation process is successful, the device gains permission to execute storage, retrieval, and update operations within the decentralized network. In the event that the validation fails, the authentication protocol with the blockchain is promptly terminated. During registration, the mobile user sends a request to their Home Agent (HA). The HA processes this and stores the user's registration information on a tamper-proof blockchain ledger. A secure smart contract, programmed in Solidity as shown in 4.2,

facilitates the storage and retrieval of these authentication parameters on the blockchain. When a registered user roams onto a Foreign Network, the Foreign Agent can then securely authenticate the user by verifying their information through this shared blockchain, eliminating the need for a central server and mitigating the risk of unauthorized access to user data. The smart contract, responsible for the storage and retrieval of authentication parameters from the blockchain using Solidity programming, is depicted in Figure.

The proposed smart contract, authored in Solidity, is compiled using Remix to obtain the Ethereum Virtual Machine (EVM) bytecode. Subsequently, the contract is deployed onto the Ethereum blockchain network with the assistance of MetaMask. This interaction between Remix and MetaMask is facilitated through web injection. Additionally, the proposed protocol features a user interface designed to verify the transactions recorded during the mobile user authentication process. This verification is performed within a personal blockchain network referred to as "Ganache."

## 4.5 Formal security analysis: simulation study

The system undergoes a formal verification process using the AVISPA tool. This tool is designed with the aim of creating an extensive language for the specification of threat models. In addition, AVISPA serves as a valuable resource for security organizations by enabling the detection of vulnerabilities within authentication protocols.

To commence the process, the Mobile User (MU) first acquires a start signal during the transition phase, resulting in a change in the state of MU from 0 to 1. The variable "State" serves as a crucial element in the High-Level Protocol Specification Language (HLPSL) for preserving the current state value.

The mobile user initiates a request denoted as $R1$ to the Home Agent (HA) for registration, signaling this request using the $SND()$ method. As a response, the mobile user receives a set of authentication parameters, including $Hm, C_M, H(.)$, from the Home

**%MU specification in HLPSL:**

role Mobile_user (MU, HA, FA: Agent,
Snd, Rcv: channel(dy))
PK: private key, SK: session key
H: hash_operation; played-by MU
local State: nat,
IDh, IDf, IDm, Nm, Rf', Mp, Cm,
PWm, Hm, R1, Sha: text,
Ma, Mb, Hb, Rm', Hc: text,
const fa_ha_rf', mu_fa_rm',
init State := 0
p1, p2, p3, p4 : protocol id
transition

**% MU registration with HA**

State: = 0 /\ Rcv(start) =|>

**% Send registration request to HA**

State': = 1 /\ Nm':= new() /\ R1':= H(IDm.Nm')
/\ Snd({R1'}_PK)/\ secret(IDm, p1, {MU, HA})
/\ secret(Nm', p2, MU)

**% Receive registration response from HA**

State: = 1 /\ Rcv({H(R1.Sha).Cm.H}_PK)
=|> State': = 2 /\ secret(Sha, p3, HA)

**% Login and authentication phase**

/\ Rm': = new() /\ Ma': = {H(IDm'.Nm')}.xor Rm'
/\ Mb': = H(Hm'.Cm').xor Rm'

**% Send authentication request to FA**

/\ Snd(Ma'.Mb'.IDh)
/\ witness (MU, FA, mu_fa_rm, Rm')

**% Authentication response from FA**

State:= 2 /\ Rcv((H(Hm'.IDf.Cm')).
H(Idh.Rm').xor Rf')=|>

**% Compute session-key**

State':= 6 /\ SK':= H(Ma'.Rf'..IDh)
/\secret(SK', p3, {MU, FA})

end role

**% Home Agent Specification in HLPSL**

role Home_agent (MU, HA, FA: agent,
Sha: HA's secret-key, Sfa: FA's secret key
Snd, Rcv: channel(dy)), H: hash_operation,
played_by HA
local State : nat,
R1, Cm, Hm, IDh, IDf, Nm',Rf,
Rm', Ma, Mb, Fa, Fb, Ha, Hb, Hc: text,
const fa_ha_rf, mu_fa_rm , ha_fa_rf,
init State: = 0; p1, p2, p3, p4, p5 : protocol-id

**% HA receives registration request from MU.**

transition
State = 0 /\ Rcv({H(IDm.Nm')}_SK) =|>
State' := 3 /\ secret(IDm, p1, {HA, MU})
/\ secret(Hm', Cm p2, {MU, HA})

**% Send registration response**

/\ Hm':= H((IDm.Nm').Sha)
/\ Snd({Hm'.Cm'}_Sha)/\ secret(Sha, p3, HA)

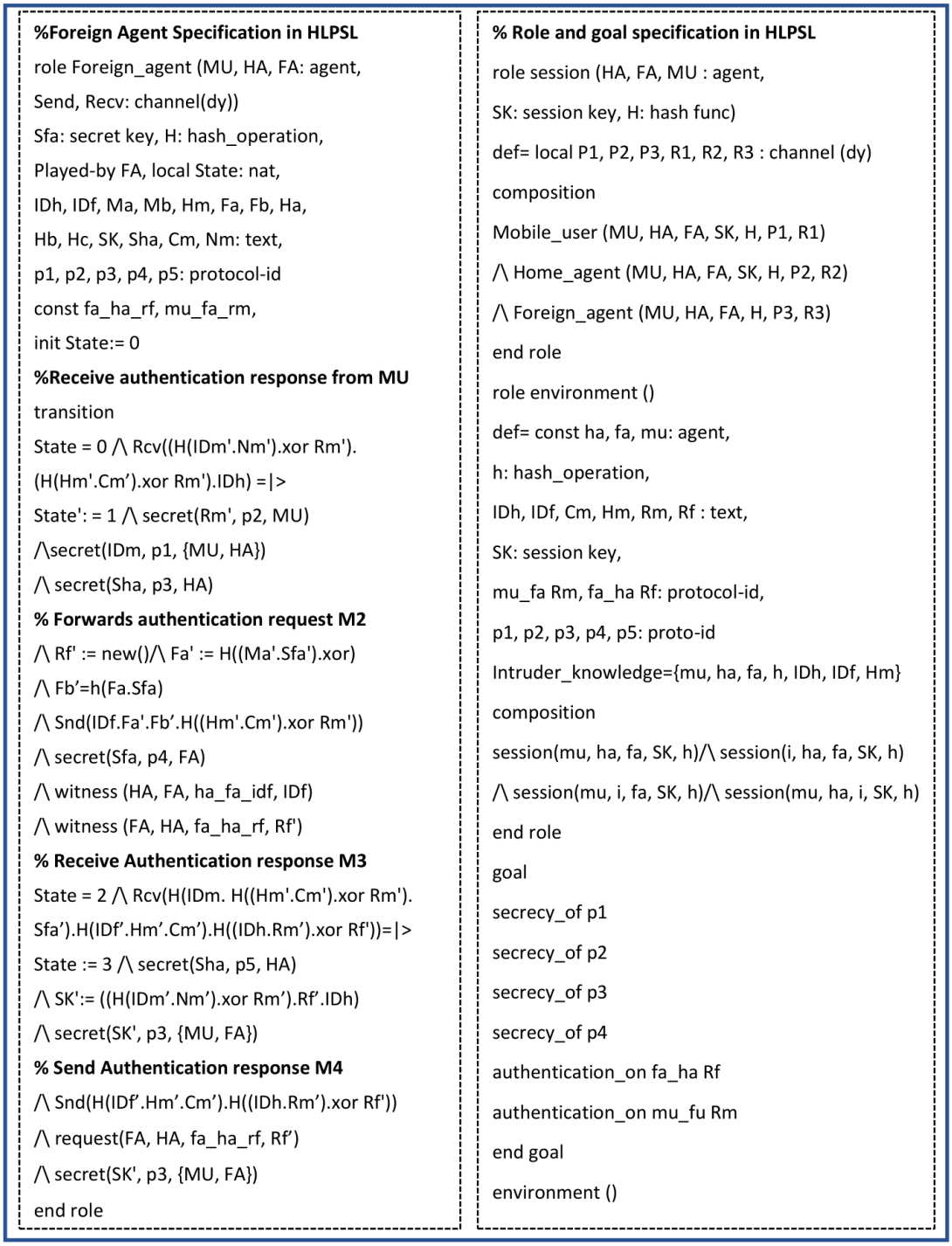
**% Receive authentication request M2**

State = 3 /\ Rcv(IDf.(H(Ma.Sfa). xor Rf'.
h(Fa.Sfa).H((Hm'.Cm'). xor Rm'))=|>
State' := 5 /\ secret(Sfa, p4, FA)

**% Send authentication response M3**

/\ Rm' := H(Hm'.Cm').xor Mb'
/\ Rf' =H(Ma'.Sfa). xor Fa
/\ Ha'=H(IDh.Mb'.Sfa)/\Hb'=H(Hm'.IDf.Cm')
/\Hc'=(H(IDh.Rm'). xor Rf')
/\ Snd(Ha'.Hb'.Hc')/\ secret(Sha, p5, HA)
/\ secret(Rm', Cm, {MU, HA})
/\ secret(Rf', Sfa, {FA, HA})
/\ request(MU, HA, mu_ha_idm, IDM)
/\ request(FA, HA, fa_ha_idf, IDF)
/\ witness (MU, HA, mu_ha_rm, RM')
/\ witness (FA, HA, fa_ha_rf, RF')
end role

Figure 4.3 Mobile user and home agent HLPSL specification.



**%Foreign Agent Specification in HLPSL**

role Foreign_agent (MU, HA, FA: agent,
Send, Recv: channel(dy))
Sfa: secret key, H: hash_operation,
Played-by FA, local State: nat,
IDh, IDf, Ma, Mb, Hm, Fa, Fb, Ha,
Hb, Hc, SK, Sha, Cm, Nm: text,
p1, p2, p3, p4, p5: protocol-id
const fa_ha_rf, mu_fa_rm,
init State:= 0

**%Receive authentication response from MU**

transition
State = 0 /\ Rcv((H(IDm'.Nm').xor Rm').
(H(Hm'.Cm').xor Rm').IDh) =|>
State': = 1 /\ secret(Rm', p2, MU)
/\secret(IDm, p1, {MU, HA})
/\ secret(Sha, p3, HA)

**% Forwards authentication request M2**

/\ Rf' := new()/\ Fa' := H((Ma'.Sfa').xor)
/\ Fb'=h(Fa.Sfa)
/\ Snd(IDf.Fa'.Fb'.H((Hm'.Cm').xor Rm'))
/\ secret(Sfa, p4, FA)
/\ witness (HA, FA, ha_fa_idf, IDf)
/\ witness (FA, HA, fa_ha_rf, Rf')

**% Receive Authentication response M3**

State = 2 /\ Rcv(H(IDm. H((Hm'.Cm').xor Rm').
Sfa').H(IDf'.Hm'.Cm').H((IDh.Rm').xor Rf'))=|>
State := 3 /\ secret(Sha, p5, HA)
/\ SK':= ((H(IDm'.Nm').xor Rm').Rf'.IDh)
/\ secret(SK', p3, {MU, FA})

**% Send Authentication response M4**

/\ Snd(H(IDf'.Hm'.Cm').H((IDh.Rm').xor Rf'))
/\ request(FA, HA, fa_ha_rf, Rf')
/\ secret(SK', p3, {MU, FA})
end role

**% Role and goal specification in HLPSL**

role session (HA, FA, MU : agent,
SK: session key, H: hash func)
def= local P1, P2, P3, R1, R2, R3 : channel (dy)
composition
Mobile_user (MU, HA, FA, SK, H, P1, R1)
/\ Home_agent (MU, HA, FA, SK, H, P2, R2)
/\ Foreign_agent (MU, HA, FA, H, P3, R3)
end role
role environment ()
def= const ha, fa, mu: agent,
h: hash_operation,
IDh, IDf, Cm, Hm, Rm, Rf : text,
SK: session key,
mu_fa Rm, fa_ha Rf: protocol-id,
p1, p2, p3, p4, p5: proto-id
Intruder_knowledge={mu, ha, fa, h, IDh, IDf, Hm}
composition
session(mu, ha, fa, SK, h)/\ session(i, ha, fa, SK, h)
/\ session(mu, i, fa, SK, h)/\ session(mu, ha, i, SK, h)
end role
goal
secrecy_of p1
secrecy_of p2
secrecy_of p3
secrecy_of p4
authentication_on fa_ha Rf
authentication_on mu_fu Rm
end goal
environment ()

Figure 4.4 Formal HLPSL Specification: Foreign Agent, Sessions, Environment, & Goals.

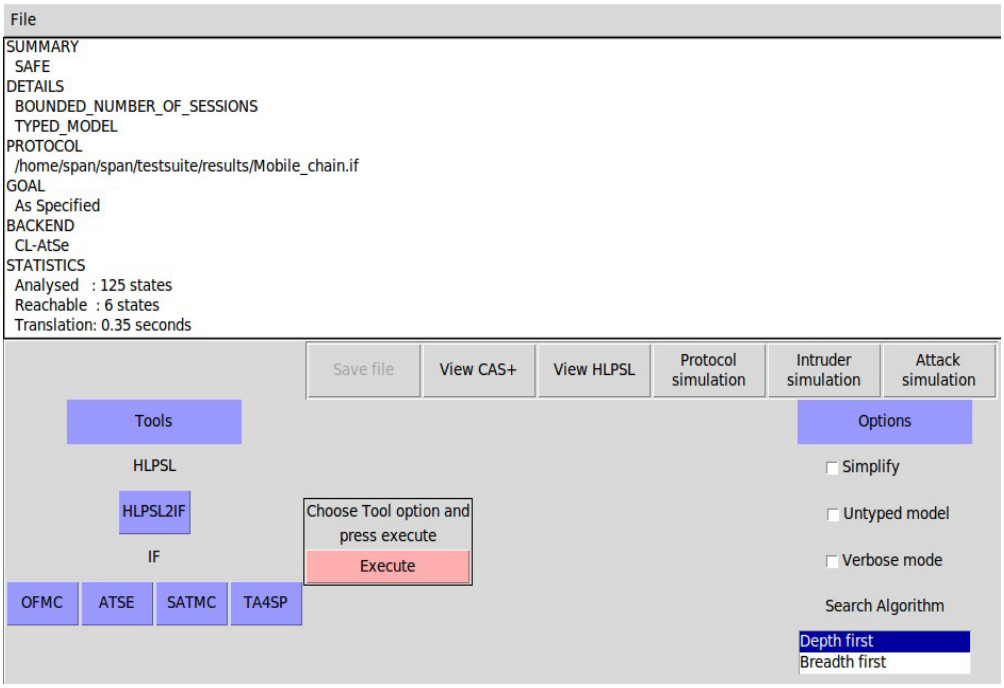



Figure 4.5 Proposed system Result analysis using AVISPA & ATSE back-end.

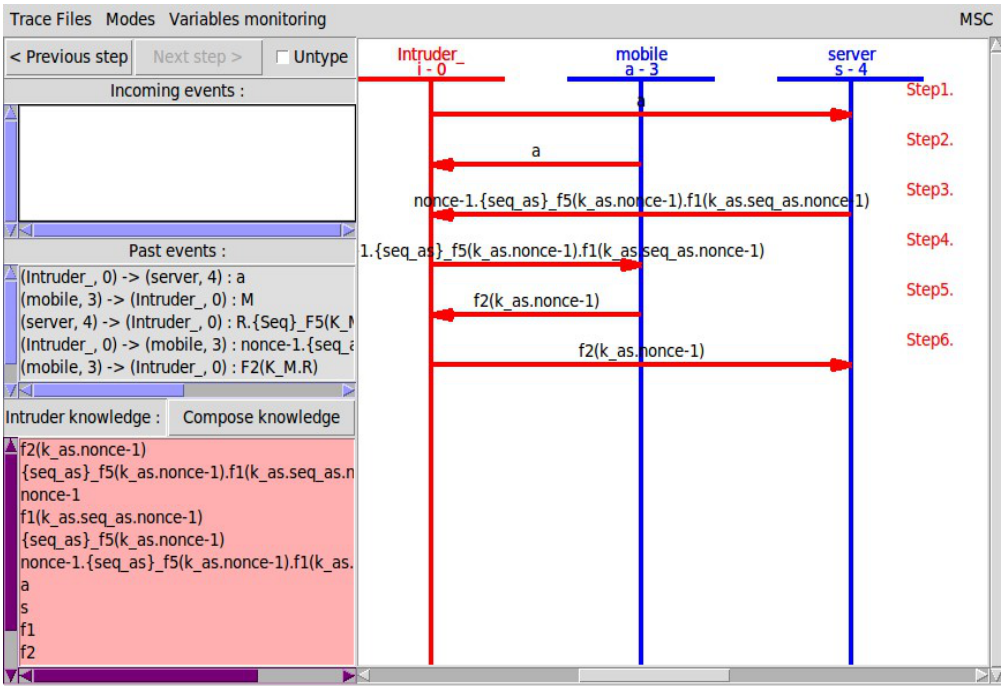



Figure 4.6 Message flow for an MU & HA communication utilising SPAN.

Agent through the use of the $RCV()$ method. Simultaneously, the mobile device generates a random nonce called $R_M$ to ensure the freshness of the message. Subsequently, it

composes and sends an authentication request $M_1 = ID_H, M_A, M_B$ to the Foreign Agent (FA) via the public network.
The Foreign Agent (FA) then returns the authentication response $M_4 = H_B, H_C$ to the mobile user. Finally, the Mobile User computes the session key, which represents the shared secret between the Home Agent and the Mobile User.

The HLPSL role specification for the Mobile User is visually depicted in Figure 4.3. In the HLPSL language, a role system defines the fundamental roles, principals, and the finite number of sessions involved in authentication protocols. Key data types utilized in HLPSL include: *const, text,* $symmetric_key, agent, public_key, nat$. These basic types facilitate the establishment of communication between the involved parties.

The communication entities within the proposed system are described in High-Level Protocol Specification Language (HLPSL) as: $Mobile\_user$, $Home\_Agent$, and $Foreign\_Agent$. Each of these entities plays distinct roles within a session, environment, and is guided by specific security goals. The declaration statement, as exemplified by $played\_by\ MU$, signifies the role of the Mobile User in the HLPSL process.

Transitions are denoted in the form of $X = | > Y$, where event $X$ is emitted, and activity $Y$ is executed according to the composition rules. The property $authentication\_on$ outlines the prerequisites for the authentication process. Additionally, the goal property $secrecy\_of\ SK$ specifies the requirement that the variable $SK$ remains confidential throughout communication, with a particular focus on assessing the extent of knowledge accessible to potential intruders.

The HLPSL specification encompasses both registration and authentication scenarios within the security system. For instance, the statement $(IDM, p1, \{MU, HA\})$ denotes that the variable $ID_M$ is exclusively known to the Mobile User (MU) and Home Agent (HA), identified by the protocol identifier $p1$. The Home Agent validates the Mobile User based on the parameters $\{H_M, C_M\}$, while simultaneously, the Mobile User assesses the legitimacy of the Home Agent using a freshly generated random nonce represented by $M_B$.

Furthermore, the property $witness(MU, FA, mu\_ha\_rm, RM')$ serves as a means to provide evidence to the Foreign Agent (FA) through the presentation of a newly generated random nonce, denoted as $R_M$, during each authentication session initiated by the Mobile User.

HLPSL role specifications for the Home Agent (HA) and the Foreign Agent (FA) are presented in Figures 4.3 and 4.4, respectively. These role specifications facilitate mutual authentication between the Foreign Agent (FA) and Home Agent (HA) through the utilization of variables $ID_F, R_F$. Similarly, mutual authentication between the Home Agent (HA) and Foreign Agent (FA) is achieved via the variables $R_F, H_A$.

Furthermore, within this security system, confidentiality of services encompassing $ID_M, N_M, N_F, SK$ is ensured through secret properties that are linked with different protocol entities.

The HLPSL role specification for sessions, environment, and security goals, as demonstrated in Figure 4.4, highlights the composition of sessions consisting of MU, HA, and FA roles. The environment in which the security framework is assessed is defined with consideration for the intruder's knowledge ($intruder_knowledge$), while security goals and requirements are detailed within the goal specification.

The proposed system is represented as a composition of four distinct sessions, involving various players, including communication entities and the intruder, $i, MU, FA, HA$. Similarly, the player configurations in the second, third, and fourth sessions are $MU, i, FA, HA$, $MU, FA, i, HA$, and $MU, HA, FA, i$, respectively.

The HLPSL roles assigned to MU, HA, and FA are executed within the AVISPA tool, utilizing the ATtack SEarcher (ATSE) backend. The security protocol's outcome, as revealed in Figure 4.5, confirms that the proposed authentication system is resilient against attacks and aligns with all the specified security requirements in wireless environments.

The summary includes essential details such as test vectors, criteria for determining the security framework's safety or vulnerability, the number of visited nodes, the depth

of attack search, and the time taken, all of which are illustrated in Figure 4.5. Additionally, the AVISPA Output Format (OF) displays the protocol's name, the goals it aims to achieve, and back-end implementation details.

Table 4.5 Comparison of the security requirements and functionalities.

| Functional & security requirements | Protocol Karuppiah and Saravanan (2015) | Protocol Reddy et al. (2016) | Protocol Xu et al. (2018) | Protocol Shashidhara et al. (2020) | Proposed |
|---|---|---|---|---|---|
| Mutual authentication | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mobile user privacy | ✓ | × | ✓ | ✓ | ✓ |
| Prevents insider attack | × | × | ✓ | ✓ | ✓ |
| Withstand SQL Injection | × | × | × | × | ✓ |
| Withstand impersonation attacks | × | × | × | ✓ | ✓ |
| Resilience to bit-flipping attack | × | × | × | × | ✓ |
| Withstand stolen-verifier attack | × | × | ✓ | ✓ | ✓ |
| prevent password-guessing attacks | × | ✓ | ✓ | ✓ | ✓ |
| Prevent replay attacks | ✓ | ✓ | ✓ | × | ✓ |
| Consensus mechanisms | × | × | × | × | ✓ |
| Perfect-forward secrecy | ✓ | × | × | ✓ | ✓ |
| Anonymity and untraceability | × | × | ✓ | ✓ | ✓ |
| Fair session-key negotiation | ✓ | ✓ | × | ✓ | ✓ |
| Security against DoS attacks | × | ✓ | ✓ | ✓ | ✓ |
| Clock-synchronization problem | × | × | × | ✓ | ✓ |
| Decentralization | × | × | × | × | ✓ |
| Local password verification | ✓ | ✓ | ✓ | ✓ | ✓ |

Table 4.6 Comparison of the security requirements and functionalities.

| Notation | Primitive used | Algorithm | Execution-time (S) |
|---|---|---|---|
| $T_H$ | Hash function | Secure Hash Algorithm-256 | 0.0005 |
| $T_{Asym}$ | Asymmetric system | Elliptic Curve Integrated Encryption | 0.0172 |
| $T_M$ | Modular exponentiation | Diffie-Hellman key exchange | 0.522 |
| $T_{Sym}$ | Symmetric cryptosystem | Advanced Encryption Algorithm | 0.0087 |
| $T_P$ | Point multiplication | Elliptic-curve cryptosystem | 0.763 |

The proposed security protocol is brought to life through the use of a tool known as Security Protocol Animator (SPAN). SPAN operates interactively to construct Message Sequence Charts (MSC) for the specified protocol, enabling users to visualize the trace of activities involving the Mobile User (MU), Foreign Agent (FA), and Home Agent (HA) as defined in HLPSL. Within SPAN, there is an "intruder mode" that enables the interactive creation of attacks and provides users with a visual representation of these attacks. Moreover, SPAN maintains an execution trace corresponding to the protocol's operation, permitting simulations of attacks when any vulnerabilities are encountered in the authentication protocol. A message sequence chart for interactions between mobile users and servers, considering the intruder's knowledge of the system, is presented in Figure 4.6. This chart confirms that the protocol successfully safeguards secret keys

Table 4.7 Performance analysis

| Computation | Protocol Xu et al. (2018) | Protocol Karuppiah and Saravanan (2015) | Protocol Shashidhara et al. (2020) | Protocol Reddy et al. (2016) | Proposed |
|---|---|---|---|---|---|
| *MU* | $7T_H$ | $8T_H + 3T_M$ | $6T_H$ | $10T_H + 3T_P$ | $5T_H$ |
| *FA* | $4T_H$ | $3T_H$ | $4T_H$ | $5T_H + 2T_P$ | $4T_H$ |
| *HA* | $9T_H + 2T_{Sym}$ | $8T_H + T_M + 3T_{Sym}$ | $10T_H + T_{Sym}$ | $7T_H + 2T_P$ | $10T_H$ |
| **Total** | $20T_H + 2T_{Sym}$ | $19T_H + 4T_M + 3T_{Sym}$ | $20T_H + T_{Sym}$ | $22T_H + 7T_P$ | $19T_H$ |
| **Time (sec)** | **0.0274** | **2.524** | **0.0187** | **5.353** | **0.0095** |

Table 4.8 Analysis of cryptographic operations

| Protocol / Phase | Protocol Xu et al. (2018) | | Protocol Karuppiah and Saravanan (2015) | | | | Protocol Shashidhara et al. (2020) | | Protocol Reddy et al. (2016) | | Proposed | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | H | E/D | H | E/D | E | M | H | E/D | H | P | H | E/D |
| **Registration** | 3 | 1 | 5 | 1 | 0 | 0 | 4 | 1 | 5 | 1 | 3 | 1 |
| **Login & Auc** | 20 | 2 | 24 | 3 | 3 | 1 | 20 | 1 | 22 | 7 | 19 | 1 |
| **Password change** | 4 | 0 | 10 | 0 | 0 | 0 | 4 | 0 | 6 | 0 | 2 | 0 |
| **No of operations** | **27** | **3** | **39** | **4** | **3** | **1** | **28** | **2** | **33** | **8** | **24** | **2** |

and prevents their disclosure.

M: Modular operation; E/D: Encryption and Decryption; H: Hash function; P: Point multiplication; E: Exponentiation.

## 4.6 Performance Analysis

The Blockchain-based authentication protocol put forth in this study is subjected to a comparative analysis against well-established, as well as recently introduced, authentication systems found in existing literature. This evaluation is aimed at assessing the protocol's efficacy in enabling roaming services within mobile environments. Subsequently, A variety of approaches have been used to assess the communication and computing complexity of the proposed protocol.

### 4.6.1 Security properties comparison

Here, functionalities and security requirements of the proposed security framework are compared with the relevant authentication schemes Karuppiah and Saravanan (2015); Xu et al. (2018); Shashidhara et al. (2020); Reddy et al. (2016). A newly proposed protocol is developed to meet all the requirements in mobile environments with robust resistance to attacks. Table 6.1 illustrates the functional and properties of security

that the proposed system enhances. Clearly, the protocol is constructed on a decentralized network architecture, ensuring security among MU, HA, and FA. Furthermore, the blockchain-based protocol safeguards against a variety of attacks in global mobile environments.

Table 4.9 Analysis of the communication cost (bits)

| Phase | Protocol Xu et al. (2018) | Protocol Karuppiah and Saravanan (2015) | Protocol Shashidhara et al. (2020) | Protocol Reddy et al. (2016) | Proposed |
|---|---|---|---|---|---|
| Registration | 640 | 1120 | 640 | 960 | 640 |
| Login | 800 | 800 | 480 | 800 | 480 |
| Authentication | 2560 | 2400 | 1440 | 1760 | 1440 |
| **Total (bits)** | **4000** | **4320** | **2560** | **3520** | **2560** |

### 4.6.2 Performance evaluation

Indeed, it is an established reality that devices operating within mobile and wireless environments typically possess limited computational resources. Indeed, the devices are constrained by minimal computing capabilities, including low power, bandwidth, memory, and processing capacity. Therefore, it becomes imperative to create a lightweight and energy-efficient mutual authentication system that upholds user privacy and security in both mobile and wireless environments.

A mobile network security protocol's performance and efficiency depend on its communication cost, which is the number of messages exchanged between an MU, HA, and FA. Moreover, secure authentication system design considers both communication and computational costs, which are affected by the choice of cryptographic algorithms.

The parallel blockchain key derivation function enables base station transceivers to precompute the handover key in anticipation of the handover mechanism activation by the trigger. In the roaming process, the mobile user derives a handover key and then validates it against a matching key with a destination station. Thus, the roaming process with the blockchain improves the performance of the handover process in the mobility network as compared to the current LTE system Lee and Ma (2020). However, the blockchain system performance in the mobility network depends on the probability of adding the block to the chain, and the number of blocks exchanged during the

roaming process. The average block time is approximately 10 seconds in the Ethereum blockchain network Kim (2019). A large number of blocks in the network incurs competition for the communication channel, which results in a lower packet delivery ratio. Eventually, it decreases the probability of a successful block exchange between MU, FA, and HA. Nevertheless, this issue could be addressed using the PB-KDF mechanism in the system-initialization phase Lee and Ma (2020).

Significantly, numerous cryptographic algorithms were simulated on a smartphone to assess the protocol performance within the constraints of limited resource in mobile environments. A Smartphone operating on the Android system features an advanced RISC machines Cortex-A8 processor. The simulation is conducted at a frequency level of 0.72 GHz. Various cryptographic systems were implemented through an object-oriented programming language utilizing Multiprecision Integer and Rational Arithmetic C++ Library (MIRACL), a library primarily designed for securing mobile devices and other embedded devices with smart capabilities. The hash computation is notably carried out using SHA-256, which is recognized for its security compared to other hash functions. A summary of various cryptographic algorithms is presented in Table 5.6. The execution time of various authentication protocols are shown in Table 4.7. The authentication and SK negotiation protocol is executed more frequently than other phases because it provides a single registration for the MU.

Table 4.7 shows that the mutual authentication framework completes the entire authentication and session key establishment process in 0.0095 seconds. Whereas, other protocols in the literature Xu et al. (2018); Karuppiah and Saravanan (2015); Shashidhara et al. (2020); Reddy et al. (2016) takes more computation time than the proposed protocol. Table 4.8 compares the computation overhead of cryptographic functions used in registration, authentication, and password changes. The proposed protocol uses lightweight ciphers like hash functions and private key cryptosystems, making it lightweight, efficient, and implementable in resource-limited mobile networks.

The communication cost (bits) of this security protocol and the relevant security protocols Xu et al. (2018); Karuppiah and Saravanan (2015); Shashidhara et al. (2020);

Reddy et al. (2016) for the mobility networks are outlined in Table 5.8.

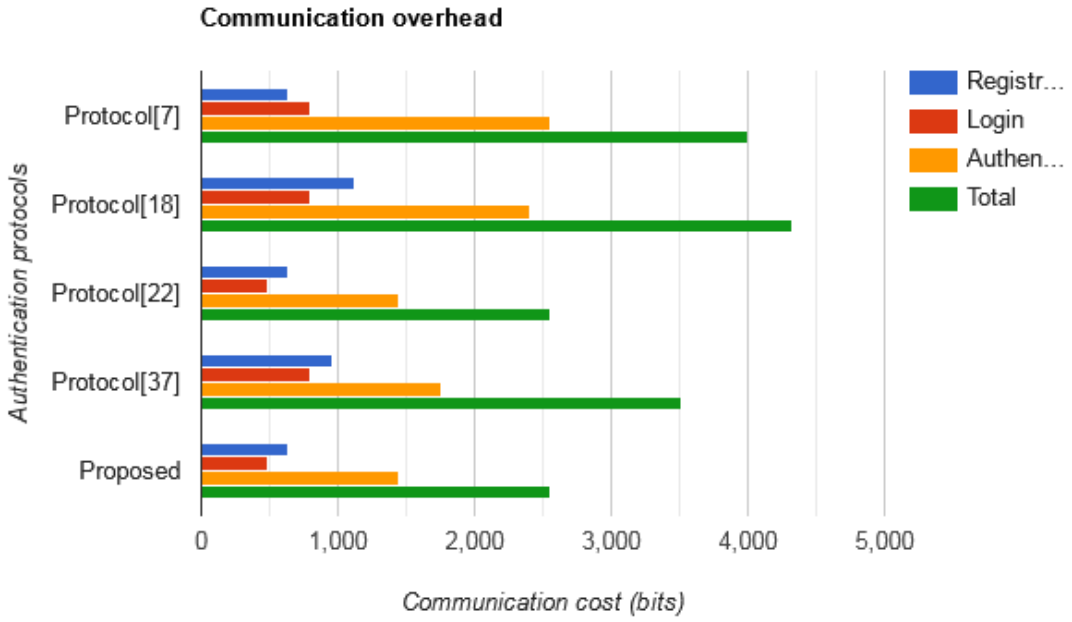



Figure 4.7 Comparison of the communication overhead

To assess the communication cost of the authentication protocols, a secure hash algorithm with a 160-bit length was utilized. Various components within the system, such as the counter value $C_M$, timestamps, user data, and random numbers $R_M, R_F, N_M$, all had a fixed length of 160 bits. Moreover, the length of modular exponentiation and elliptic curve point multiplication operations were assumed to be 320 bits each. Specifically, the registration request $R_1 = h(ID||N_M$ and the response $R_2 = H_M, C_M, h(.)$ in the proposed security protocol collectively required (160+160+160+160)=640 bits. Similarly, a login message $M_1 = M_A, ID_H, M_B$ was composed of (160+160+160)=480 bits, while the authentication request $M_2 = ID_F, F_A, F_B, M_B$ from the Foreign Agent necessitated (160+160+160+160)=640 bits. Consequently, the authentication response $M_3 = H_A, H_B, H_C$ from the Home Agent and the session key (SK) negotiation message $M_4 = H_A, H_B$ from the Foreign Agent jointly comprised (480+320)=800 bits. In summary, the proposed system framework was designed to function with a total data size of (640+480+640+800)=2560 bits. The communication complexity of this security system

and the relevant mutual authentication protocols Xu et al. (2018); Karuppiah and Saravanan (2015); Shashidhara et al. (2020); Reddy et al. (2016) are compared and depicted in Figure 4.7. Clearly, the Mobile-Chain mutual authentication framework exhibits minimal communication overhead. This is reflected in its reduced in number of messages exchange & communication bits. Consequently, the mutual authentication framework in blockchain significantly improves both communication and computational efficiencies.

## 4.7 Summary

In the conclusion, An innovative blockchain-based mutual authentication system framework is introduced for mobility environments, characterized by attributes such as immutability, decentralization, peer-to-peer network architecture, and distribution. This security solution ensures user anonymity and robust protection against various attacks. Furthermore, formal security verification and validation are carried out using AVISPA with the HLPSL language. Subsequently, the proposed blockchain-based framework is implemented through platform known as Ethereum , employing smart-contract developed using the program language called Solidity. As a result, the performance analysis shows that the framework meets all functional and security requirements for mobility environments.

Further, the protocol is lightweight, efficient, possesses less communication and computational overhead as compare to the recent mutual authentication systems in Xu et al. (2018); Karuppiah and Saravanan (2015); Shashidhara et al. (2020); Reddy et al. (2016) to provide a roaming service in the mobility environments.

# Chapter 5

# A SECURE BLOCKCHAIN-BASED AUTHENTICATION FOR TMIS USING SMART CONTRACTS

Data interoperability in health-care is a problem that has yet to be solved. The key question is how to accomplish data confidentiality, data integrity, user anonymity, drug traceability, and data misuse in the health-care industry, including detecting fake drugs. Blockchain technology combined with smart contracts (Chain code) provides a novel technique to securely store patient medical records. Patients will have more control over their information thanks to Blockchain, and health providers, such as hospitals, will have access to patient medical records held by others. Furthermore, Blockchain in healthcare allows users to check the accuracy of patient health information, drug traceability, conduct immutable medical audits, and maintain data security. In this article, we design a secure decentralized authentication framework for Telecare Medical Information System (TIMS) using Blockchain (TMIS-Chain). Smart contracts written in the Solidity programming language are used to create the proposed decentralised system. Consequently, the healthcare contracts are compiled using Remix and deployed to the personal Blockchain network Indushree and Raj (2023).

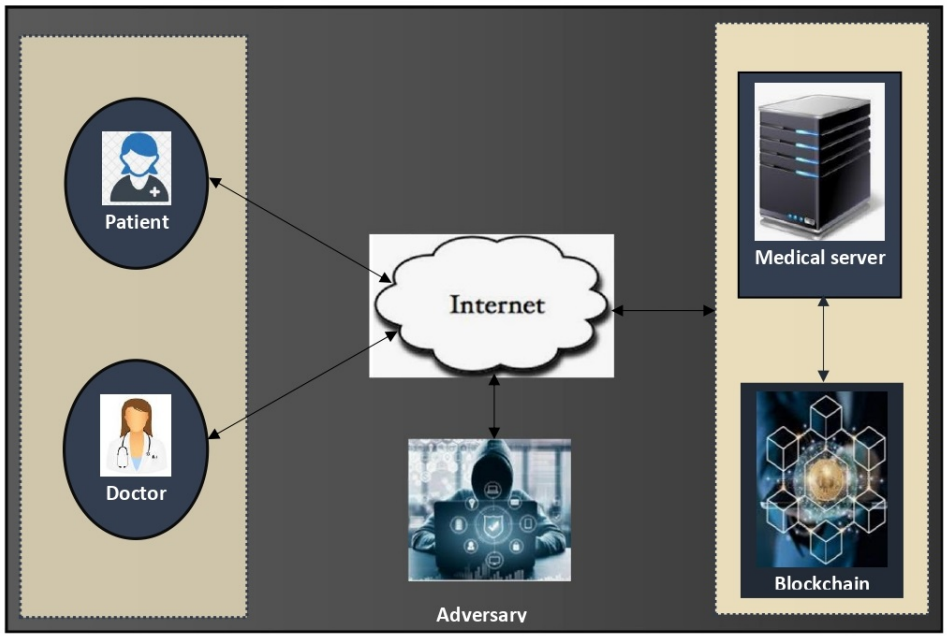



Figure 5.1 Blockchain-based authentication for TMIS

## 5.1 Motivation

The conventional patient record sharing systems have several drawbacks like data interoperability, availability of essential data to physicians, restricted patients' access to their medical information, and ultimately, user privacy, data integrity, and drug traceability are major issues. In addition, health information stored and accessed through conventional TMIS can easily be modified with fraudulent intent Amin et al. (2018). Nevertheless, health related information can be lost due to natural disasters or tampering. Placing patient health information in the medical Blockchain system could fix these flaws.

- The information kept on the distributed ledger could be read by anyone. In view of the fact that the transactions on the Blockchain network can never be modified or deleted.

- Blockchain is implemented in a decentralised network, which means that no single party has control over or ownership over Blockchain This makes the system

robust against failures.

- The information present in the transaction is public to everybody on the blockchain network, but it does not mean that the information present in the ledger is readable. This technology replaces names with identifiers known as pseudo anonymity. Blockchain employs Public Key Infrastructure (PKI) to encrypt the contents of the ledger in a secure manner.

### 5.1.1 Security requirements in TIMS

In the TMIS environment, the authentication framework should satisfy:

*R1* *Integrity*: Healthcare systems require a high level of integrity. Messages exchanged over the network must not be modified, and the consistency and reliability of data in cloud services must be maintained throughout their existence. As a result, only authorised people should be permitted access to such applications.

*R2* *User Privacy*: The adversary $\mathscr{A}$ does not identify the patient or doctor from authentication sessions, nor does it link authentication sessions that are associated with the same party Indushree et al. (2022).

*R3* *Mutual Authentication*: Mutual authentication entails both parties submitting certification requirements for the other. This criterion is critical in avoiding spoofing entities from attacking systems.

*R4* *Scalability*: In healthcare, it refers to the ability to ensure that the size of a system has no bearing on its efficiency. For example, if the user base's resource usage skyrockets, the time needed for the successful service operations like authentication must remain unaffected.

*R5* *Robustness against threats*: Even if the adversary has access to all of the information contained on the smart-card, the Blockchain-based authentication architecture should withstand several attacks.

*R6* *Availability*: The term "availability" refers to the capacity for lawful users to access resources as needed. To guarantee strong authentication, a healthcare system must be able to withstand denial-of-service (DoS) attacks.

## 5.2 Research contributions

The following are the contributions to this article:

- We designed a secure, decentralised authentication framework for the TIMS using Blockchain. Patients, doctors and medical servers can securely authenticate and access health records using the proposed decentralised application using Blockchain.
- Smart contracts written in the Solidity programming language are used to create the proposed decentralised system. In addition, the solidity contracts are compiled using Remix and deployed to the personal Ethereum Blockchain network.
- Through informal security analysis, we proved that the proposed security framework resists various attacks and satisfies all design goals in the healthcare system.
- Finally, a rigorous performance evaluation is carried out to measure the computational and communication overhead of the proposed system and other relevant authentication protocols. The results show that the proposed decentralized authentication framework is secure, efficient, and practically implementable in the healthcare system.

## 5.3 Threat model

We will use the Dolev-Yao (DY) threat model to describe the intruder's potential and typical privacy concerns in Telecare Medical Information Systems (TMIS). The health

Table 5.1 Crypto symbols used in this chapter.

| Symbol | Description |
|---|---|
| $PW$ | Password of the user |
| $ID$ | User's identity |
| $S_B$ | Server's secret key |
| $P_B$ | Server's public key |
| $SK$ | Session key |
| $T_X$ | Transaction number |
| $C_r$ | Counter value |
| $R_N$ | Random number |
| $N_M$ | Nonce |
| $H(.)$ | Hash operation |
| $\|\|$ | Concatenation operation |
| $\oplus$ | Bitwise XOR operation |

data kept on the server is vulnerable to a variety of threats and privacy risks, which result in information theft and loss Madhusudhan et al. (2018). The attacker's capabilities are listed below:

1. An intruder $\mathscr{A}$ has full control of the channel used to transmit data between a patient or doctor and a medical server connected to the Blockchain.

2. Messages sent across a public-channel like the Internet can be sniffed, discarded, reordered, replayed, injected, deferred, and tampered with at will by the adversary Shashidhara et al. (2020).

3. If an adversary sends a large number of queries to the medical blockchain, the node may be unable to complete routine data transactions, exposing the medical servers to Denial-of-Service attacks.

4. In polynomial time, the adversary textbf$\mathscr{A}$ may guess the user's passwords. However, guessing the associated private keys, pseudo random, and hash values in a given polynomial time is impossible.

5. The initial branch of the chain can be replaced by an adversary that controls 51

percent of the resources of the whole Blockchain network. An adversary might use this approach to introduce blocks to the medical blockchain network with faked transaction data (51% attack).

6. The adversary $\mathscr{A}$ can discover a user's lost or stolen device and extract device parameters by analyzing power consumption.

## 5.4 Proposed decentralized authentication protocol for TMIS

In this section, a novel blockchain-based authentication protocol has been proposed for the Telecare Medical Information System Indushree and Raj (2024). The mathematical symbols used in this research paper are outlined in Table 5.1.

### 5.4.1 Initialization phase

Before the authentication system can begin, a few basic parameters are transferred between Network Hospitals (NH) and the medical server connected to the Blockchain Network (BN) in order to create a shared secret key utilising the public-key distribution mechanism. The initialization procedure is as follows:

1. The network hospital and the Blockchain server agree on some initial parameters and choose large prime integers $p$, $q$, and a generator polynomial $g$ from group $G$.

2. The Blockchain Network (BN) selects a secret-key $S_B = a$; where $(a < q)$. Eventually, Blockchain computes its public-key $P_B = g^a \pmod{p}$.

3. After that, the Blockchain Network sends its public-key $P_B = g^a \pmod{p}$ to the Network hospital.

4. The network hospital, on the other hand, chooses its secret-key $S_H = b$ where $(b < q)$ and computes the public-key $P_H = g^b \pmod{p}$.

5. Later, the network hospital transfers its public-key $P_H = g^b \pmod{p}$ to the Blockchain server.

6. Upon receiving the public key from the hospital, the Blockchain computes the shared secret key $K_{BH} = g^{ab} \pmod{p}$; Similarly, hospital network also computes $K_{BH} = g^{ba} \pmod{p}$. Further, the shared secret $K_{BH}$ encrypts communication between the Blockchain server and network hospitals.

### 5.4.2 User registration

If a patient or doctor wishes to register with a medical server connected to the Blockchain Network (BN), they must do so using a secure communication channel. The following are the steps in the user registration process.

R1 : The user device computes and sends the registration request $R_1 = h(ID||R_N$ to the Blockchan server using a secure communication channel.

R2 : The Blockchain medical server computes $B_S = h(R_1||S_B)$ and initializes the counter $C_r = 0$ to prevent replay attacks during user authentication process. In addition, the server stores the registration details $\{R_1, C_r\}$ on Blockchain and gets the transaction number $T_X$ for the same.

R3 : After that, the medical server sends the registration response message $R_2 = \{B_S, C_r, T_X\}$ .

R4 : The user device computes: $R_U = h(ID||PW||R_N)$

$R_V = B_S \oplus h(PW||R_N)$

$R'_N = R_N \oplus h(PW||ID)$

Finally, the user device maintains information $\{R_U, R_V, C_r, T_X, R'_N\}$ for accessing desired services from the medical server. The user registration process is summarized in Table 5.2.

Table 5.2 The user registration.

| **User** | | **Blockchain** |
|---|---|---|
| Selects $\{ID, PW, R_N\}$<br>$R_1 = h(ID\|\|R_N)$ | | |
| | $R_1 = \{h(ID\|\|R_N)\} \longrightarrow$ | |
| | | $B_S = h(R_1\|\|S_B)$<br>Stores $\{R_1, C_r\}$ on Blockchain. |
| | $\longleftarrow \{B_S, C_r, T_X\} = R_2$ | |
| $R_U = h(ID\|\|PW\|\|R_N)$<br>$R_V = B_S \oplus h(PW\|\|R_N)$<br>$R'_N = R_N \oplus h(PW\|\|ID)$<br>Stores$\{R_U, R_V, C_r, T_X, R'_N\}$ in the user device | | |

### 5.4.3 Decentralized authentication phase

Following successful mutual authentication over the Blockchain, the registered patient or doctor can access the requested health services from the medical server. The following stages are used to define the authentication:

**A1:** $User \rightarrow Server : \{B_1, C'_r, N_M, T_X\}$

Then, computes the following:

$$R_N = R'_N \oplus h(ID||PW)$$

$$R'_U = h(ID||PW||R_N)\ R'_U \stackrel{?}{=} R_U$$

$$B_S = R_V \oplus h(PW||R_N)$$

$$A_1 = h(B_S \oplus N_M)$$

$$B_1 = h(T_X||A_1||C'_r)$$

Finally, the user device records $N_M$ and sends the authentication request $M_1 = \{B_1, C_r', N_M, T_X\}$ to the medical Blockchain server.

**A2:** $Server \rightarrow User : \{C_1\}$

Upon receiving the request, the medical server retrieves the user details $\{R_1, C_r\}$ using transaction number $T_X$ and compares the stored counter value $C_r$ with the received one. In addition, the server computes the following:

$$B_S' = h(R_1||S_B)$$

$$A_1' = h(B_S' \oplus N_M)$$

$$B_1' = h(T_X||A_1'||C_r)$$

After that, the server checks $B_1' \stackrel{?}{=} B_1$. Then, computes the following:
Update the counter on the Blockchain $C_r^* = C_r + 1$

$$SK = h(B_S'||N_M||C_r^*)$$

$$C_1 = h(SK||C_r^*)$$

Finally, the medical blockchain server returns the authentication response $M_2 = \{C_1\}$ to the user.
The user device updates its counter value $C_r^* = C_r + 1$ and computes SK as follows:

$$SK' = h(B_S||N_M||C_r^*)$$

$$C_1' = h(SK'||C_r^*)$$

Then examines $C_1' \stackrel{?}{=} C_1$. The protocol will be stopped if the verification fails. Otherwise, the user and medical server exchange authentication information and agree on the session-key $SK$ to encrypt further conversations. The decentralized authentication and

session-key negotiation process is summarized in Table 5.3.

Table 5.3 Decentralized authentication phase.

| **User** | **Blockchain** |
|---|---|
| Input $ID, PW$ | |
| Generate a Random nonce $N_M$ | |
| $R_N = R'_N \oplus h(ID\|\|PW)$ | |
| $R'_U = h(ID\|\|PW\|\|R_N)$ $R'_U \stackrel{?}{=} R_U$ | |
| $B_S = R_V \oplus h(PW\|\|R_N)$ | |
| $A_1 = h(B_S \oplus N_M)$ | |
| $B_1 = h(T_X\|\|A_1\|\|C'_r)$ | |
| $\xrightarrow{M_1 = \{B_1, C'_r, N_M, T_X\}}$ | |
| | Derive $\{R_1, C_r\}$ from Blockchain |
| | Verify $C'_r \stackrel{?}{=} C_r$ |
| | $B'_S = h(R_1\|\|S_B)$ |
| | $A'_1 = h(B'_S \oplus N_M)$ |
| | $B'_1 = h(T_X\|\|A'_1\|\|C_r)$ |
| | $B'_1 \stackrel{?}{=} B_1$ |
| | Update $C^*_r = C_r + 1$ on Blockchain |
| | $SK = h(B'_S\|\|N_M\|\|C^*_r)$ |
| | $C_1 = h(SK\|\|C^*_r)$ |
| $\xleftarrow{M_2 = \{C_1\}}$ | |
| Update $C^*_r = C_r + 1$ on the device | |
| $SK' = h(B_S\|\|N_M\|\|C^*_r)$ | |
| $C'_1 = h(SK'\|\|C^*_r)$ | |
| $C'_1 \stackrel{?}{=} C_1$. | |

### 5.4.4 User password change phase

Without accessing the medical server, the patient or the doctor can change the password.

The following are the processes for changing the user password:

P1: If a patient or Doctor wishes to change his/her default password, they must sub-

mit the identity $ID$ and password $PW$ through the terminal. Then, the device computes the following:

$$R_N = R'_N \oplus h(ID||PW)$$

$$R'_U = h(ID||PW||R_N)$$

$$R'_U \stackrel{?}{=} R_U$$

P2: The user device checks whether $R'_U \stackrel{?}{=} R_U$. If the verification succeeds, the legality of a patient or doctor is ensured. Otherwise, the request for a password change is rejected.

P3: Upon successful verification, the user freely selects a new password $PW*$ and computes the following:

$$R^*_U = h(ID||PW^*||R_N)$$

$$R^*_V = B_S \oplus h(PW^*||R_N)$$

$$R^*_N = R_N \oplus h(PW^*||ID)$$

P4: Finally, the user device replaces the old values $\{R_U, R_V, C_r, T_X, R'_N\}$ with new values $\{R^*_U, R^*_V, C_r, T_X, R^*_N\}$ in the smart-card.

## 5.5 Security analysis

We examine and demonstrate that, in the context of the Telecare Medical Information System, the suggested decentralised authentication architecture based on Blockchain is resistant to various attacks.

### 5.5.1 User privacy-protection

During user registration, the user sends $R_1 = h(ID||R_N)$ to the medical server, which is composed of a hashed identity and a random number. Even if the attacker captures message $\{R_1, R_2\}$ from the public channel, he or she will be unable to determine the patient's or doctor's identity. In addition, the identity of users is not included in the authentication messages $M_1 = \{B_1, C_r', N_M, T_X\}, M_2 = \{C_1\}$ sent between the user and the medical server.

Consequently, the authentication messages $M_1, M_2$ are dynamic in nature due to the usage of the unique random number $N_M$ in each session, it is impossible for an attacker to track the user's location by correlating past conversations derived from the public channel. As a result, the suggested decentralized authentication mechanism safeguards the privacy of users.

### 5.5.2 Protection of DoS attacks

In this attack scenario, the infected nodes could transmit malicious traffic to the medical server, preventing other legitimate users from accessing the network's services. The attackers may even be able to take down the entire server. The proposed solution, on the other hand, uses a decentralised network such as Blockchain to store patient health records.

The proposed Blockchain authentication protocol employs Delegated Proof-Of-Stake (DPOS) as a consensus algorithm, ensuring that no double-spend transactions are forwarded, as well as no forwarding of the same block or transactions. Limit the block size to 1MB and disconnect a peer that sends too many messages. As a result, distributed denial-of-service attacks are prevented by the proposed system.

### 5.5.3 Resistance to insider attack

The user sends $R_1 = h(ID||R_N)$ to the medical server through a secure channel. As a result, an attacker cannot get user credentials such as identity $ID$ and password $PW$. After that, the medical server also sets up the counter and stores $\{R_1, C_r\}$ on the tamper-proof Blockchain.

An insider attack to mimic the medical server is impossible due to the Diffie-Hellman problem's difficulty. The server's secret key $S_B$ is extremely difficult to deduce. Therefore, the proposed framework can guard against insider threats in the context of TMIS.

### 5.5.4 Resistance to replay attack

Due to network latency considerations, the suggested framework abstains from employing timestamps to mitigate the risk of replay attacks in transmitted messages. This approach is unsuitable for real-time implementation. The authorized authentication requests would be rejected even if there was a tiny time gap between the clocks.

The suggested technique uses the counter $C_r$ at the medical server and user side, which is updated in every authentication session, to prevent replay attacks. When inspecting the counter value $C_r' \stackrel{?}{=} C_r$ of a patient or doctor, the medical server would notice the attack if an attacker replayed the previous message.

If the authentication request $M_1$ is a replay message, the comparison $C_r' \stackrel{?}{=} C_r$ will fail. As a result,the authentication request was denied by the medical server. Therefore, the suggested approach uses a counter $C_r$ to prevent replay attacks.

### 5.5.5 Mutual authentication

The authentication between the user and the server is achieved through exchanging and validating the authentication messages $M_1, M_2$. The medical server authenticates a

patient or Doctor, upon receiving $M_1 = \{B_1, N_M, C_r\}$. The server computes:

$$B'_S = h(R_1||S_B)$$

$$A'_1 = h(B'_S \oplus N_M)$$

$$B'_1 = h(T_X||A'_1||C_r)$$

$$B'_1 \stackrel{?}{=} B_1$$

If the verification succeeds, the medical server successfully authenticates the user and computes SK. Otherwise, the request for authentication is declined.
Similarly, the patient or doctor can authenticate the medical Blockchain server by receiving $M_2 = \{C_1\}$. The user computes:

$$SK' = h(B_S||N_M||C^*_r)$$

$$C'_1 = h(SK'||C^*_r)$$

$$C'_1 \stackrel{?}{=} C_1$$

If the verification succeeds, the user successfully authenticates the medical server and agrees with the session key for encrypting further conversations.

### 5.5.6 Prevents impersonation attacks

Consider this: an attacker $\mathscr{A}$ intercepts certain publicly disclosed information and attempts to impersonate a legitimate medical server to defraud the user or masquerades as an authorized user to gain access to the server's services. The intruder $\mathscr{A}$ would confront a variety of challenges in this scenario, which are detailed below:

**Resistance to user impersonation**

An attacker would need both the identity $ID$ and password $PW$ to impersonate a patient or doctor. However, the user's login credentials are not communicated across a public channel in the proposed protocol's login and authentication messages. As a result, the proposed protocol is resistant to user impersonation attacks.

**Resistance to server impersonation**

An adversary can't forge the msg $M_2 = \{SK, C_1\}$ to defraud the patient or doctor without knowing the server key $S_B$ and shared-key $K_{BH}$. In addition, the intruder is unable to extract $B_S$ in order to compute the session key. As a result, the proposed method is resistant to impersonation attacks on servers.

### 5.5.7 Prevention of sybil attacks

Sybil attacks on the network relate to a rogue node controlling numerous blockchain nodes, weakening or eliminating the redundant backup mechanism. Multiple data backups might be stored on Sybil nodes in this attack scenario, putting them at risk. The attacker uses this approach to try to fill the network with clients under its control while refusing to transmit genuine blocks. Furthermore, it relay only attacked blocks, resulting in double spending.

The proposed decentralized authentication framework makes use of the delegated proof-of-stake protocol to address the sybil attack. This mechanism, diversifies the connections and permits outbound connections to one IP per/16 IP address. Hence, the proposed authentication framework prevents sybil attacks.

## 5.6 Formal security verification

The authentication framework is implemented in the HLPSL, which is a role based system, which means that we define the activities of each type of module participants. We

then "glue" various roles together into a composite role and explain how the resultant actors communicate with each other. Every role provides the information (parameters) that the participants can use first, as well as the participant's initial state and transitions Shashidhara et al. (2021).

The RCV and SND signals are of the form of channels, suggesting that they are channels through which the role-playing agent (a patient or doctor) will connect with the medical server. HLPSL is a typed language, in which all identifiers start with capital letters, while all constants start with a lowercase. State is a **nat** (natural number) in HLPSL, and the local section specifies the local variables of the users in the communication. In addition, HLPSL has state transitions that represent receiving a msg and sending a reply. A transition is made up of a trigger when an event occurs.

The Dolev-Yao (DY) intruder model is represented by the communication channel (dy) in HLPSL. In this threat scenario, the intruder has complete network control, meaning that all information transmitted by the user or medical server will be intercepted by the attacker. He has the ability to attack, examine, and/or change conversations, as well as send whatever message he constructs to anybody he wants while pretending to be another agent.

All channels used by the basic roles, such as user and medical server, are declared by the session role. It is also used to describe a single protocol execution in HLPSL. Parallel sessions are described by the environment role, which is the top-level role. In addition, HLPSL specifies security goals via enhancing basic role transitions. The security objectives aid in the achievement of security requirements such as mutual authentication, confidentiality, and so on.

The proposed authentication architecture is validated using AVISPA, a prominent formal verification tool. AVISPA is a technology that is used to formalise and test the robustness of security protocols in wireless and mobility environments.

```
% ------------------------------------------------------------------------
% Patient or Doctor role specified in HLPSL
% ------------------------------------------------------------------------
role user (
A, B : agent, % A is a patient or Doctor and B is medical server
SK : symmetric_key,
% S is the symmetric key between the user and the medical server
H : hash_func, % H is a hash function
SND, RCV : channel (dy) % Dolev-Yao channel
)
played_by A
def=
local
State : nat, % Transition state
RN,ID,PB ,TX: text
CR,NM : nat
PW ,BS ,RU ,RV ,RM' SC, A1 ,B1 ,R1,R2,M1,C1 ,M2 : text
 init
State := 0
transition
 % The patient or Doctor registration
0.    State = 0 /\ RCV(start) =|>
        State' := 2 /\ RN' := new() /\ ID' := new() /\ SND(H{ID'.RN'}_SK)
        /\ witness(B, A, rna, RN')
% User receives registration response

2.   State = 2 /\ RCV({BS'.CR'.TX'}_SK) =|>
   State' := 4 /\ RU' := H(ID'.PW'.RN')/\ RV':= BS' xor(PW'.RN')
   /\ RM'' := RM' xor (H(PW'.ID'))

   % User input identity, password, and waits for verification from the device

   4.   State = 4 /\ RCV(start) =|>
    State' := 6 /\ RM' := xor(RM''(H(ID'.PW')) /\ RU' := (H(ID'.PW''.RM''))

   % User sends the authentication message to the medical server

   6. State = 6 /\ NM' := new() /\ BS' := RV' xor(H(PW.RM))
   /\ A1' := xor(H(BS'.NM')) /\ B1 := H(TX'.A1'.CR')
   /\ SND(H(TX'.xor(H(BS'.NM')).CR'), CR', NM', TX')
   /\ witness(A, B, user_server_tx, TX')
   /\ witness(A, B, user_server_cr, CR')
   % User receives authentication response from the medical server

   10. State = 8 /\ RCV(C1') =|>
         State' := 10 /\ SK' := H(BS'.NM'.CR') /\ C1''=H(SK'.CR'

   end role
   % ------------------------------------------------------------------------
```

Figure 5.2 HLPSL role specification for the patient/doctor.

HLPSL role specification of the user, medical server, session, and the environment roles have shown in Figures 5.2, 5.3 and 5.4, respectively. During the registration process , the patient or doctor sends $R_1$ using **Send()** channel to the medical server. Consequently, the user receives $SC = \{B_S, C_r, T_X\}$ from server using **Recv()** channel.

In decentralized authentication process, the user MU sends $M_1 = \{B_1, T_X, C_r, N_M\}$ to the Blockchain network. Eventually, the medical server successfully authenticates the user and returns $M_2 = \{C_1\}$ to the user through a public channel.

Under the ATSE and OFMC backends, the protocol is simulated in AVISPA with the SPAN tool.

```
% ------------------------------------------------------------------------
% Blockchain Medical Server role specified in HLPSL
% ------------------------------------------------------------------------
role server (
A, B : agent, % A is a patient or Doctor and B is medical server
SK : symmetric_key,
% S is the symmetric key between the user and the medical server
H : hash_func, % H is a hash function
SND, RCV : channel (dy) % Dolev-Yao channel
)
played_by B
def=
local
State : nat, % Transition state
RN : text, % Random number
ID : text, % Identity of the patient or Doctor
PB : text, % Public key of the medical blockchain
SB : text % Secret key of the medical blockchain
TX : text, % Transaction ID
CR : nat, % Counter number
NM : nat, % Random nonce
BS : text, % Server computation
A1 : text, % User computation during login
B1 : text, % User computation during login
R1 : text, % Registration request
M1 : text, % User message
C1 : text, % Server computation
M2 : text % Server Message

init
State := 1
transition
% Medical server receives R1 from user
% and if the user does not exist in the database

1. State = 1 /\ RCV(H(ID'.RN')_SK) =|>
State' := 3 /\ CR' := new() /\ BS' := H(H(ID'.RN').SB')
/\ SND({BS', CR', TX'})
/\ witness(B, A, server_user_bs, BS')

% Medical server receives the authentication message M1 and verifies
7. State = 3 /\ RCV(H(TX'.xor(H(BS'.NM')).CR'), CR', NM', TX') =|>
State' := 5 /\ BS' := H(H(ID'.RN').SB')
 /\ A1' := H(xor(BS', NM')) /\ B1' := H(TX'.A1'.CR') /\
SK' := H(BS'.NM'.CR') /\ C1' := H(SK'.CR') /\ SND(C1')
/\ request(B, A, server_user_cr, CR')

end role
% ------------------------------------------------------------------------
```

Figure 5.3 HLPSL role specification for the patient/doctor.

## 5.7 TMIS implementation using blockchain

The proposed decentralised authentication framework is built on the Blockchain (TMIS-Chain) and uses smart contracts to implement it. Patients and doctors can register with the medical server in this scenario by providing identity information. Users can also upload medical records to the Blockchain network via a decentralised Web. The InterPlanetary File System (IPFS) is a peer-to-peer networking protocol for storing and sharing health records in a distributed file system that employs content addressing to uniquely identify each patient medical record in a global name-space.

TMIS-Chain is a proposed secure framework for medical health records that keeps a digital copy of a patient's medical history, including diagnoses, medications, and bills. A doctor, hospital, or pharmacy uploads these details, which are then fed into the decentralised Blockchain to ensure security, privacy, and data integrity. This information

```
% ------------------------------------------------------------------------
% Session role
% ------------------------------------------------------------------------
role session (
A, B : agent, % A is the user and B is the medical server
SK : symmetric_key,
% S is the symmetric key between the user
% and the medical server
H : hash_func % H is a hash function
)
def=
local
SAB, RAB, SBA, RBA : channel(dy)
composition
user(A, B, S, H, SAB, RAB)
 /\ server(A, B, S, H, SBA, RBA)
end role
% ------------------------------------------------------------------------
```

```
role environment()
def=
const
rna, user_server_bs, user_server_cr, server_user_tx: protocol_id
a, b : agent,
sab, sai, sib : symmetric_key,
h : hash_func
intruder_knowledge = {a, b, sai, sib, h}
composition
session(a, b, sab, h)
/\ session(a, b, sab, h)/\ session(a, i, sai, h)/\ session( i, b, sib, h)
end role
goal
authentication_on rna %  Weak auth
secrecy_of cr  % Smart card must remain secret to user
weak_authentication_on user_server_tx
weak_authentication_on user_server_bs
end goal
environment()
```

Figure 5.4 HLPSL role specification for the session, goal and environment.


Figure 5.5 Simulation results analysis using OFMC and ATSE backends.

can only be viewed, not edited by the individual. Accountability is maintained while patient medical records are kept secure.

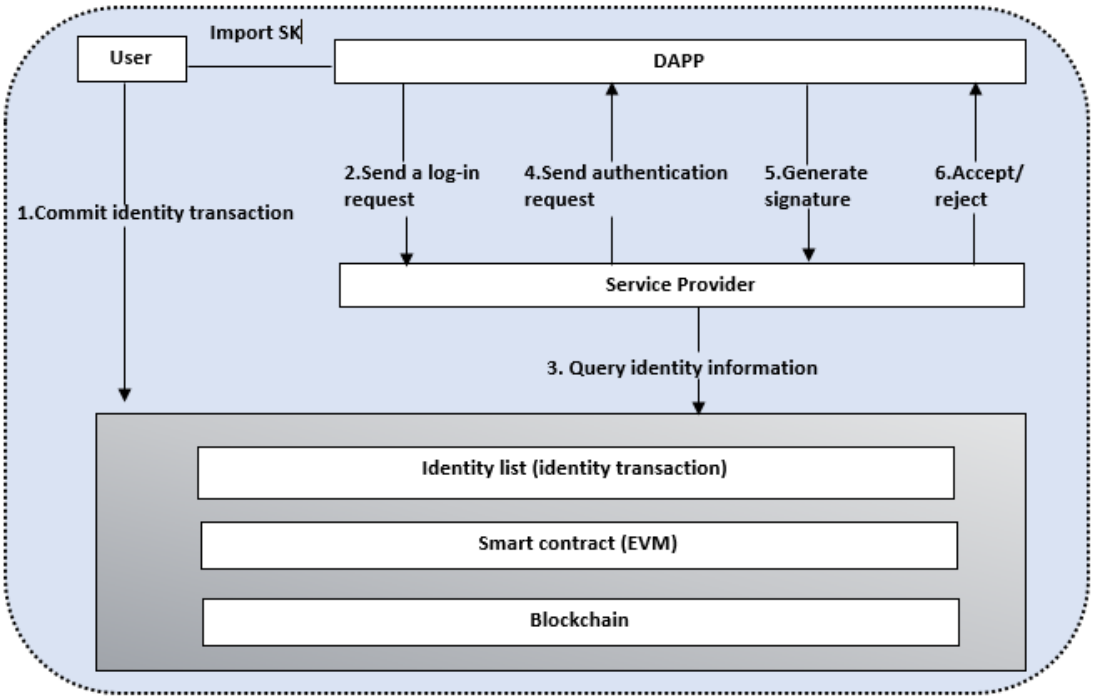



Figure 5.6 The Blockchain-based architecture for healthcare

Smart contracts using the Solidity programming language were used to implement the user and medical server roles. The contracts were compiled in the Remix IDE and then deployed to Ganache, an Ethereum personal blockchain network. The front-end for the Decentralized Application (DAPP) is built using ReactJS, HTML, and CSS, and it uses MetaMask to execute wallet transactions. As a middle-ware, Web3 and npm are utilised. The Blockchain-based TMIS architecture, as shown in Figure 5.6.

Only registered patients can upload their medical records to the Blockchain-based Decentralized Application (DAPP). IPFS adds the health records as a node that returns a hash. Following that, the hash is saved on the blockchain. Patients who have registered can use Blockchain to examine their medical records. A patient might also grant access to his records to a doctor.Permission can be revoked at any time if the doctor no longer requires access. The registration process of the patient and doctor using smart contracts is shown in Figure 5.9. Only when the patient grants access to the doctor may they view the patient's medical records. Eventually, network hospitals/doctors will be able

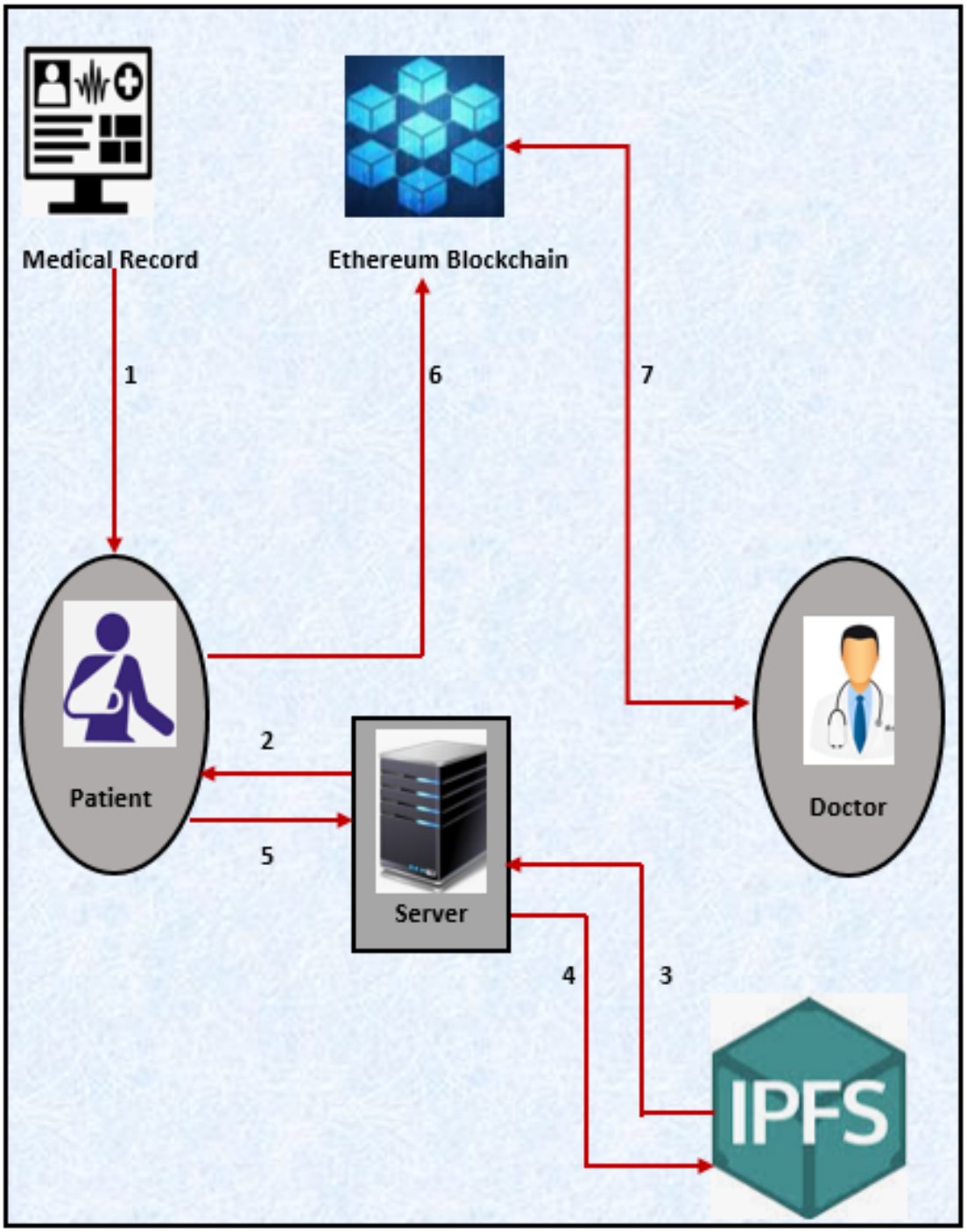



Figure 5.7 The major steps in TMIS-Chain application

to upload each patient's diagnosis, prescriptions, and bills to the Blockchain using IPFS. The TMIS-Chain operational process is as shown in Figure 5.7:

1. The decentralised application allows registered users to upload medical records.

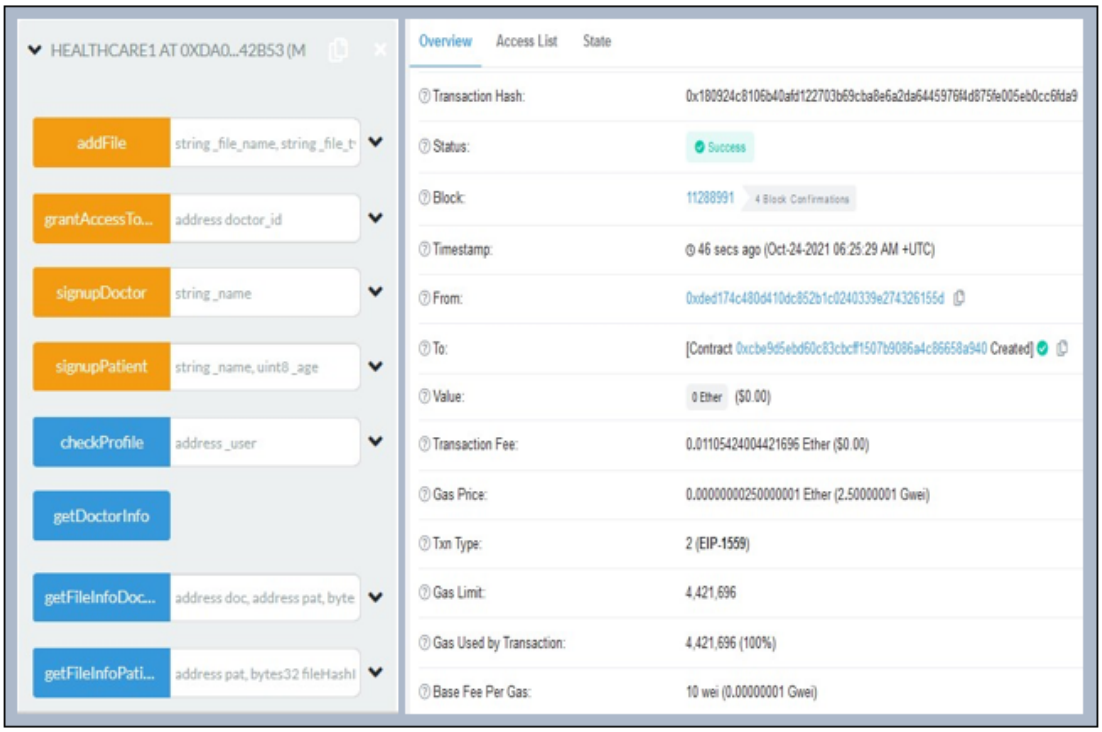



Figure 5.8 Healthcare smart contract deployment and block details.

2. The client-side record is subsequently encrypted and transferred to the medical server.

3. This encrypted file is sent from the medical server to the IPFS network for decentralised storage.

4. IPFS network returns a file hash after being stored.

5. The file hash is then returned to the user application by the medical server.

6. The hash is then kept on the decentralized Blockchain network, which is secure and immutable.

7. Only the doctor has access to his or her patient's medical records.

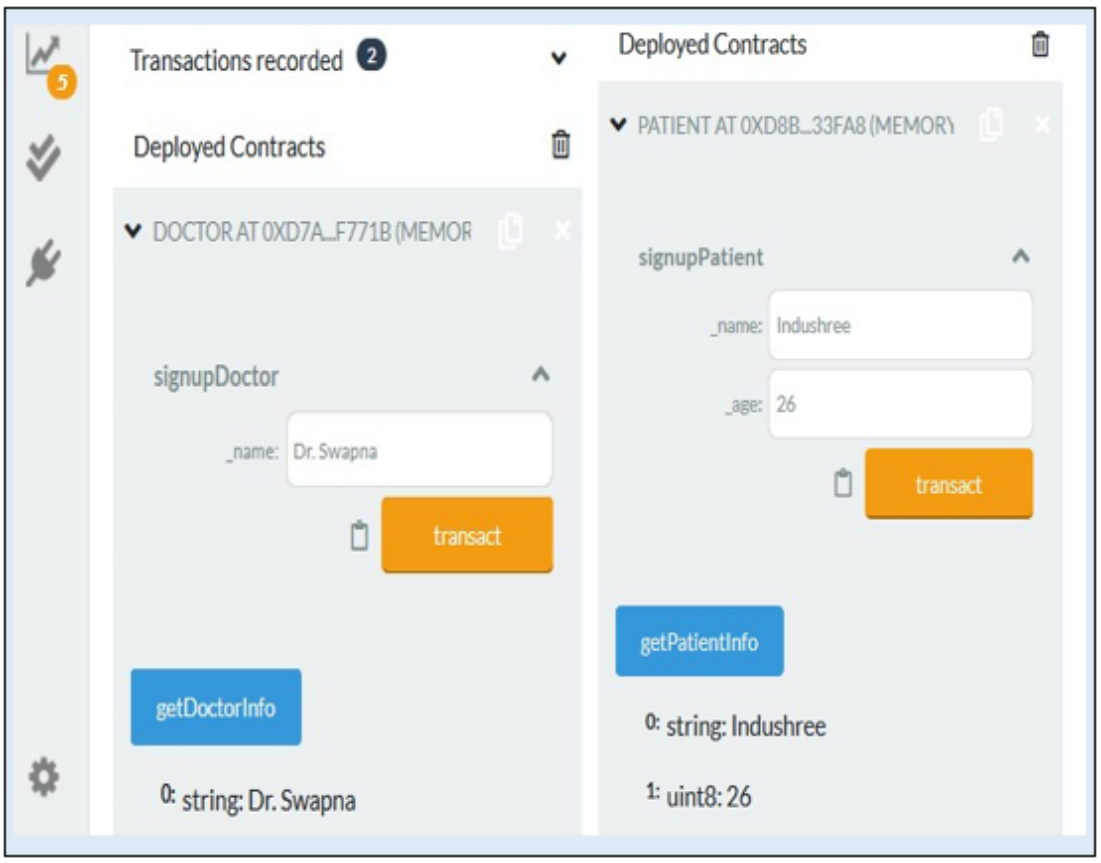



Figure 5.9 Registration process of the patient and doctor using smart contracts

## 5.8 Performance evaluation

The proposed decentralized authentication framework is implemented through the Ethereum personal blockchain network known as Ganache. The patient, doctor, and medical server smart contracts are first developed in the Solidity programming language. Remix IDE is used to compile the smart contracts, which generate byte code using the Ethereum Virtual Machine (EVM). As a result, smart contracts that have been compiled are deployed into the personal blockchain network. The healthcare smart contract deployment and block details are shown in Figure 5.8.

We used blockchain to examine the performance and features of the proposed TMIS-Chain. The major goal is to create a framework for secure, efficient, and low-cost authentication. In addition, we discuss how blockchain differs from typical centralised

authentication solutions in terms of functionality. The suggested system has the following features:

- **Cost**: On the Ethereum test network, we developed and deployed the model. The cost of smart contract creation and execution of its functions was calculated. On the day of the evaluation, the gas price was 2.50000001 Gwei (0.0000000025 Ether) and 1 Ether was 4234.22 USD. The average gas price was around 18,000,000,000 Wei at the time of analysis. The cost of deploying smart contract creation and execution functionalities is summarised in the table below. We noted that the largest cost is incurred at the moment of contract creation in Table 5.4. All other smart contract features, on the other hand, were less expensive.

- **Security**: Authentication, data integrity, secrecy, and non-repudiation are among the security challenges addressed by the proposed Blockchain framework for the healthcare system. To begin, distinct modifiers are available in the solidity language that can validate the user's identity. The blockchain is an immutable ledger because the information recorded on chain is not modifiable. The functionality of smart contracts and transaction information are tamper-proof. Furthermore, the suggested security architecture confirms a user's validity using information stored on the blockchain.

- **Verification**: The verification feature of a blockchain-based authentication system is effectively achieved, and user anonymity is checked using public key and digital signature. Each user's public and private keys are generated via the Ethereum wallet. The user signs a message as a digital signature with their private key to establish ownership of the public key, and then the digital signatures are confirmed with their public key.

The authentication system is evaluated and compared to recently proposed authentication protocols in Telecare Medical Information Systems. Table 5.5 compares the

Table 5.4 Smart contact deployment and interaction costs.

| **Functionality** | **Transaction cost (Ether)** | **Gas Fee** |
|---|---|---|
| Patient contract creation | 0.01105424 | 4,421,696 |
| signupPatient | 0.00018291 | 73,167 |
| Doctor contract creation | 0.00116262 | 465,0501 |
| signupDoctor | 0.00017486 | 69,947 |
| Healthcare contract creation | 0.00157671 | 1,576,710 |
| addFile | 0.00018575 | 70,125 |
| grant-Access-To-Doctor | 0.00016166 | 160,575 |
| getPatient-Info-For-Doctor | 0.00012117 | 142,437 |
| getFile-Info-Patient | 0.00017486 | 68947 |
| get-File-Info-Doctor | 0.00017568 | 56784 |

proposed framework's security requirements to those of other security protocols used to provide authentication in TMIS. Table 5.5 shows that the proposed Blockchain-based healthcare system meets all design goals and is resistant to all attacks.

Table 5.5 Security requirements

| **Security requirements** | **Proposed** | **Protocol Lu and Zhao (2021)** | **Protocol Lo et al. (2020)** | **Protocol Giri et al. (2015)** | **Protocol Zhang and Lin (2018)** | **Protocol Das (2015)** |
|---|---|---|---|---|---|---|
| User privacy | ✓ | × | × | ✓ | × | ✓ |
| Mutual authentication | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Prevent impersonation attacks | ✓ | ✓ | ✓ | × | ✓ | × |
| Prevent replay Attacks | ✓ | ✓ | ✓ | ✓ | × | × |
| Prevent sybil attacks | ✓ | × | ✓ | × | × | × |
| Prevent DoS attacks | ✓ | ✓ | ✓ | × | × | ✓ |
| Prevent modification attacks | ✓ | ✓ | ✓ | × | × | × |
| No time synchronization | ✓ | × | × | × | × | ✓ |
| Local password verification | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| User friendliness | ✓ | ✓ | × | ✓ | ✓ | ✓ |

Several crypto operations were simulated on a Crypto library in order to examine the computation complexity of the authentication system. MIRACL, a Crypto++ library, is used to implement the cryptographic algorithms. Furthermore, the SHA-256, AES, and Elliptic Curve Integrated Encryption Scheme are the hash function, private key, and public-key cryptosystems, respectively. The execution time of several cryptographic algorithms is listed in Table5.6. based on experimental data.

Table 5.6 Execution time of cryptographic algorithms.

| Symbol | Description | Execution-time (S) |
|---|---|---|
| $T_{SM}$ | symmetric key algorithm | 0.0087 |
| $T_H$ | hash function | 0.0005 |
| $T_{ASM}$ | symmetric key algorithm | 0.01725 |
| $T_P$ | point multiplication on Elliptic curve | 0.763 |
| $T_M$ | modular exponentiation | 0.522 |

We measured the user and medical server's computing overhead in the login and authentication stages, as these are performed more frequently than the initialization and password change phases.The user registration process in the proposed authentication framework employs five hash functions as well as a symmetric key computation. During the login and authentication procedure, there are 12 hash operations and one symmetric operation. In the proposed protocol, there are a total of $\{17T_H + 2T_{SM}\}$ cryptographic computations. Table 5.7 shows that the proposed Telecare Medical Information System authentication framework is more efficient than existing protocols.

Table 5.7 Comparison of the computational overhead

| Phase | Scheme Lu and Zhao (2021) | Scheme Lo et al. (2020) | Scheme Giri et al. (2015) | Scheme Zhang and Lin (2018) | Scheme Das (2015) | Proposed |
|---|---|---|---|---|---|---|
| Registration | $2T_H + T_{SM}$ | $3T_H$ | $5T_H$ | $2T_H + 2T_{ASM}$ | $5T_H$ | $5T_H + T_{SM}$ |
| Login | $2T_H + T_M + T_{SM}$ | $3T_H + T_P$ | $6T_H + T_M$ | $3T_H$ | $5T_H$ | $5T_H$ |
| Authentication | $9T_H + T_M + 5T_{SM}$ | $5T_H + 3T_P + 2T_{SM}$ | $9T_H + T_M$ | $8T_h + 4T_{ASM}$ | $11T_H + 2T_{ASM}$ | $7T_H + T_{SM}$ |
| **Total** | $13T_H + 2T_M + 7T_{SM}$ | $11T_H + 4T_P + 2T_{SM}$ | $20T_H + 2T_M$ | $13T_H + 6T_{ASM}$ | $20T_H + 2T_{ASM}$ | $17T_h + 2T_{SM}$ |
| **Execution time (s)** | **1.114** | **3.075** | **1.054** | **1.038** | **0.044** | **0.025** |

Table 5.8 Communication overhead (bits)

| Phase | Proposed | Scheme Lu and Zhao (2021) | Scheme Lo et al. (2020) | Scheme Giri et al. (2015) | Scheme Zhang and Lin (2018) | Scheme Das (2015) |
|---|---|---|---|---|---|---|
| Registration | 640 | 640 | 960 | 1280 | 640 | 640 |
| Login and authentication | 800 | 1120 | 1600 | 1600 | 800 | 1120 |
| **Total** | **1440** | **2080** | **2880** | **2560** | **1440** | **1120** |

The communication cost of the proposed methodology and other relevant methods is summarised in Table 5.8. The length of the hash function was assumed to be 160

bits in order to estimate transmission overhead. In addition, the random nonce, timestamp, and user information all have a length of 160 bits. In proposed decentralized framework, the registration requests $RID_1 = \{h(ID||R_N)\}$, and $R_2 = \{B_S, C_r, T_X\}$ are exchanged between the patient/Doctor and medical server. The registration messages require $(160+160+160+160) = 640$ bits. The login message $M_1 = \{B_1, C_r, N_M, T_X\}$ needs $(160+160+160+160) = 640$ bits to send the authentication request from the user to medical server. Furthermore, the authentication response $M_2 = \{C_1\}$ requires 160 bits. As a result, the proposed authentication framework requires a communication overhead of $(640+640+160) = 1440$ bits . In comparison to other protocols, we assure you that the proposed protocol has a low computation and communication overhead. As a result, the suggested authentication framework offers a significant increase in security and is easily implemented in healthcare systems.

## 5.9 Summary

This chapter introduces a secure decentralized authentication framework for the Telecare Medical Information System, demonstrating its ability to resist attacks and meet healthcare system requirements. The framework employs Solidity smart contracts on the Ethereum Blockchain and undergoes rigorous security analysis and performance evaluation, affirming its security, efficiency, and practicality in healthcare.

# Chapter 6

# SECURE USER AUTHENTICATION SYSTEM FOR ROAMING SERVICES IN MOBILITY ENVIRONMENTS USING BLOCKCHAIN

Increase in wireless devices made Mobile communication pervasive. Global Mobile Networks (GLOMONET) provision the roaming service to accomplish this, where Mobile Users must experience secure and seamless roaming services over multiple Foreign Agents. Main objective of Network providers is to have mutual authenticated, secured and light weight service to guard mobile user's data and privacy. Many interesting roaming authentication protocols have been proposed to achieve security and privacy of users in traditional communication networks. But they all suffer from one or another known security attacks with the fact that current mobile networks are prone to attacks. Blockchain technology offers its advantages to establish a secure connection and authentication by safeguarding Mobile User information and privacy with its immutable nature. The study shows that limited work has been done in space protocol design for GLOMONET using Blockchain technology and the main goal of the protocol is to maintain security for transactional data and privacy of the Mobility Users along with anonymity property. In this chapter, Soulbound tokens are used to issue credentials between an MU and HA by serving as a secure and decentralized form of digital identity. The idea behind using soulbound tokens for issuing credentials is to create a tamper-

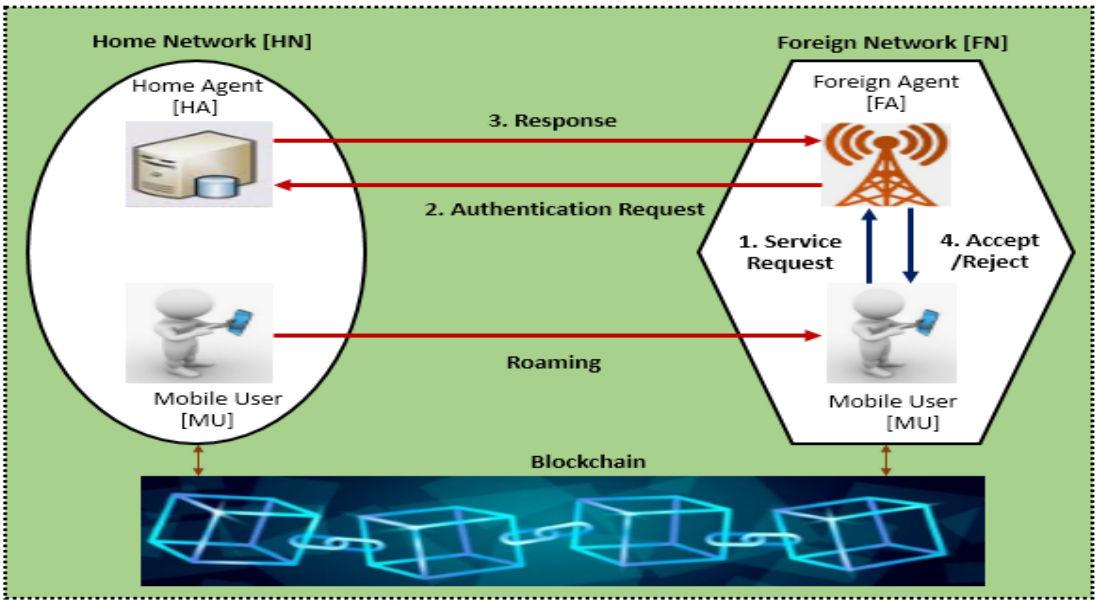



Figure 6.1 Authentication scenario for Mobile Users in GLOMONet

proof and easily verifiable system that reduces the reliance on centralized authorities for identity verification.

## 6.1 Motivations

Several privacy concerns have arisen between network customers using service providers and mobile phones in Glomonet Indushree and Raj (2023). We explored at a various MU authentication approaches that have been established to provide subscribers with roaming services in this section. The following are some of the limitations of the previous authentication techniques.

1. The majority of authentication protocols in global mobility networks are vulnerable to well-known network security flaws.

2. HA, FA, and MU use an unfair key agreement mechanism to distribute secret information amongst user authentication entities. If any entity's static secret val-

ues are exposed over the network, that network's entire security mechanism is compromised.

3. Allocating resources and consumption produced by communication operations and processing is a fundamental challenge in the global mobile network. Mobile devices have minimal resources in terms of processing power, memory, bandwidth, and computational capacity. To implement existing authentication methods, there is a larger communication and computation overhead is expected.

## 6.2 Research Contributions

1. We propose a novel blockchain-based mobile user authentication mechanism using a non-transferable Soulbound Token.

2. Exploiting and testing various security attacks by using security tools and Blockchain technology is used to provide the confidentiality, transparency, privacy, security as well as authentication to the protocols using decentralized network.

3. The proposed system is also verified using a tool called AVISPA.

## 6.3 Security attribute in GLOMONET

The implementation authentication protocol must comply with the following security requirements:

R1 *Mutual-authentication* : Every session, establish secure communication between FA and MU. Firstly MobileUser, ForeignAgent and HomeAgent must be mutually authenticate each other and after the mutual-authentication it generates the SK for further process.

R2 *User untraceability* : An Intruder $\mathscr{A}$ either detects a roaming subscribers during authentication sessions or connects authentication activities that are associated

with the same party.

R3 *Session key (SK) security and fairness*: Because the interactions between MU and FA are encoded by the SK, a SK (session key) negotiation is essential for maintaining a more secure connection. Furthermore, all communication agents contribute to the generation of the session key in certain way.

R4 *Robustness against attack* : Even if an attacker has access to all of the data stored on the SmartCard, the protocol can withstand many threats.

R5 *Computational efficiency* :The authentication technique should be simple in both computation and communication.

R6 *No Time Synchronization* :Because transmission delay is unpredictable in existing networks, remote user authentication systems that use time-Stamps to ensure message freshness may still be vulnerable to replay attacks. Furthermore, in existing network systems, clock synchronization is complex and costly.

## 6.4 Proposed authentication protocol for GLOMONET

The proposed protocol is described below:

1. **Initialization phase** : The system parameters are chosen by the HA.

2. **Registration phase** : Registration phase before providing any health care services to the patients user has to register with the health server so the registration phase is between the user and sever is established. So, once the registration is completed user can access the services from the health server this process is done in Mutual authentication phase.

3. **Mutual authentication phase** : Here the register user should be authenticated first so after that services should be provided that is authentication in this phase the user has to authenticate the server even the server has to authenticate the user

so the mutual authentication will be established. Once the user and health server are agree or authenticated each other so then session key agreement will take place also SK is order to encrypt the information in the secure way.

### 6.4.1 Blockchain-based Soulbound Token (SBT) for Authentication

Soulbound tokens can be used to issue an identity token between a user and a server by serving as a secure and decentralized form of authentication.
Here's how SBT could work in Global Mobility Network:

1. The mobile user would first obtain a soulbound token, which is unique to them and cannot be replicated or transferred.

2. The Home Agent would generate an identity token and send it to the mobile user.

3. The mobile user would use their soulbound token to sign the identity token, which would create a tamper-proof digital signature that proves their identity.

4. The user would then send the signed identity token back to the Home Agent, which would verify the digital signature using the mobile user's soulbound token.

5. If the digital signature is verified, the Home Agent would authenticate the mobile user and grant them access to the requested resources or services.

Overall, using soulbound tokens for issuing identity tokens between users and servers could help to create a more secure and decentralized system of authentication, which could be used in a wide range of applications, such as online banking, e-commerce, and social media.

### 6.4.2 Minting and Issuing the soulbound token

A Home Agent can mint a soulbound token to a mobile user by generating a unique key pair. The private key is securely stored on HA, while the public key is shared with the mobile user.

Steps in SBT Minting and Issuing:

1. The Home agent would generate a key pair consisting of a secret key and the public key.

2. The HA would securely store the private key, which would be used to sign and verify transactions involving the soulbound token.

3. The HA would send the public key to the user, which would be used to create the soulbound token.

4. The mobile user would use the public key to create a new soulbound token, which would be uniquely bound to their identity.

5. The mobile user would store the soulbound token securely on their device, such as a smartphone or a hardware wallet.

6. The mobile user would then use the soulbound token to authenticate themselves to the server, which would verify the digital signature using the private key stored on HA.

The Authentication protocol has been designed using soulbound token smart contracts, which are lines of programming code that are stored on a Blockchain network and are only executed when specific requirements are met. It is referred to as smart since it is capable of independently verifying and executing a contract. The contract, which contains all of the details of a specific agreement, is included in the decentralised Blockchain network. The soulbound token has been implemented using solidity smart

contract and deployed to the Ethereum blockchain network.

Accuracy, openness, independence, security, and uniformity are all intended benefits of smart contracts.On the blockchain, the Ethereum nodes execute smart contracts written in the solidity. Every 10 seconds, at least two additional network nodes must validate each node in the blockchain. Written contract functions may then be triggered and carried out after that.

The soulbound token contract has been compiled through Remix and deployed on Goerli test network. The contract compilation and deployment as shown in Fig. 6.2. In addition, the contract deployment process, minting and issuing an SBT to the mobile user address, and transaction details on the Blockchain as shown in Figs. 6.2, and 6.3, respectively.

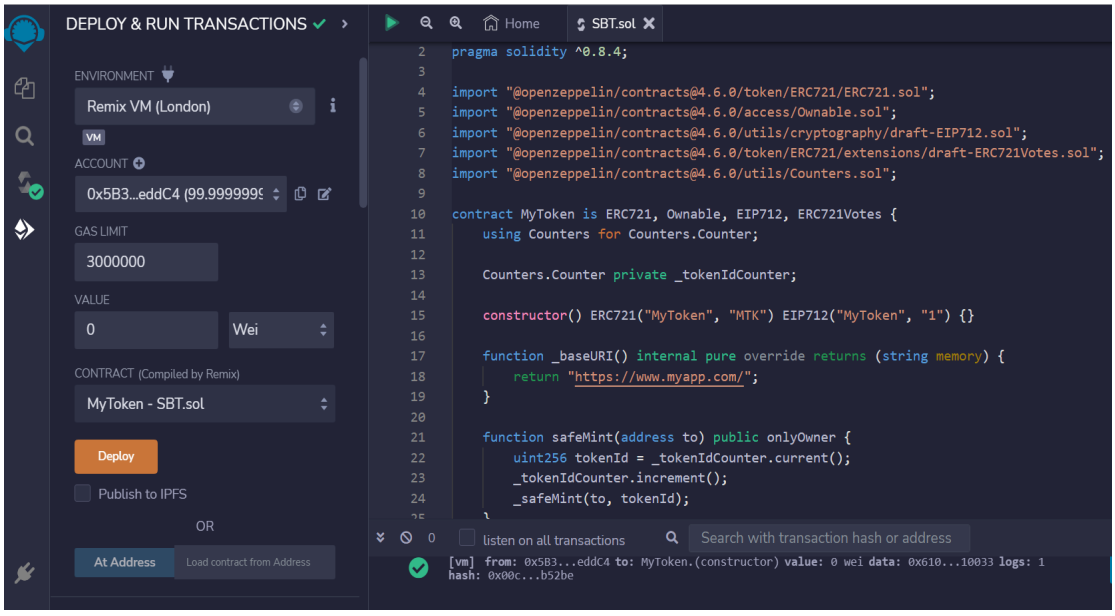



Figure 6.2 Smart contract compilation and deployment process using Remix.

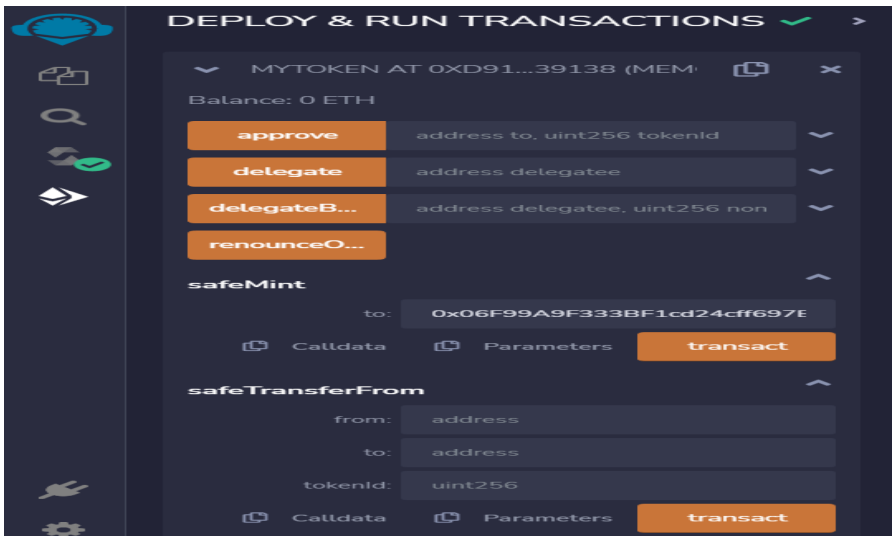



Figure 6.3 Minting and issuing an SBT to the mobile user.

## 6.5 Formal security verification of the proposed protocol

The AVISPA Toolkit is a collection of tools for testing and implementing formal security protocol models. The role-based language HLPSL is frequently used to construct scheme models. AVISPA is a widely used simulation tool for determining if a newly proposed approach authentication technique or protocol is more secure against a numerous of common known security vulnerabilities. HLPSL is used in the AVISPA tool to implement communication. The proposed schemes is used AVISPA tool to validate the informal analysis and automated security. To demonstrate that the recommended protocol scheme is resistant to various common security vulnerabilities, including replay, forgery, smartCard and MITM attacks. Main goal in this scheme is to accomplish the Mutual Authentication, establish the Session- Key, and also implement Desynchronization, resist the common security attacks, finally to reduce the computation and storage burden. Further to check the correctness of the formal security authentication properties it uses tool called AVISPA.

The AVISPA tool usually uses two models for formal verification: CL- AtSe and OFMC If the OFMC and CLAtSe models are SAFE, we can deduce that the newly implemented protocol is secure against a variety of common security attacks. When the protocol is

executed, each user has a specific role to play in AVISPA. Each role is Self-contained, receiving initial input via arguments and communicating with other roles via channels.

The below figure shows the output of proposed protocol AVISPA. The designed protocol is written in HLPSL and we have executed using one of the backend OFMC. Fig 6.4. Shows the result for the proposed protocol is SAFE. If the result is UNSAFE we can use the intruder simulation and attack simulation that show the what information is revealed to the attacker that information is help us to rebuild the protocol.

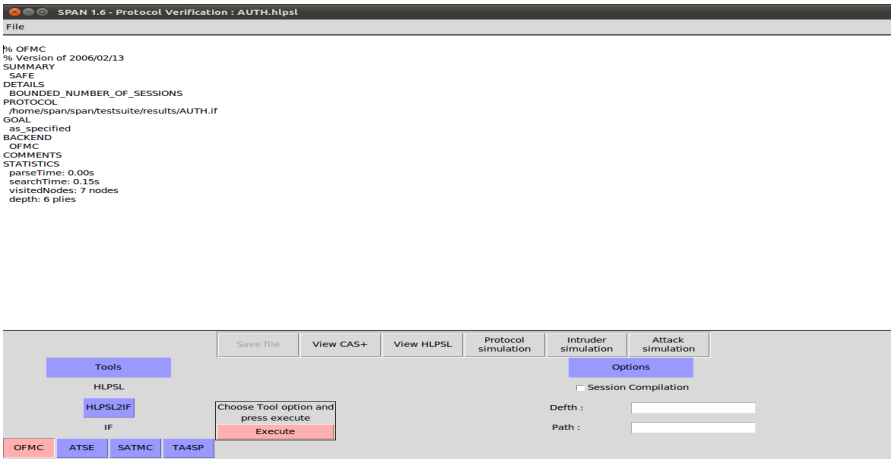



Figure 6.4 Autentication protocol using OFMC.

Table 6.1 Security requirements and Functionality comparison.

| Security requirements & Functionalities | Protocol Karuppiah and Saravanan (2015) | Protocol Reddy et al. (2016) | Protocol Xu et al. (2018) | Protocol Shashidhara et al. (2020) | Proposed |
|---|---|---|---|---|---|
| Mutual authentication | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mobile user privacy | ✓ | × | ✓ | ✓ | ✓ |
| Prevents insider attack | × | × | ✓ | ✓ | ✓ |
| Withstand impersonation attacks | × | × | × | ✓ | ✓ |
| Withstand stolen-verifier attack | × | × | ✓ | ✓ | ✓ |
| prevent password-guessing attacks | × | ✓ | ✓ | ✓ | ✓ |
| Prevent replay attacks | ✓ | ✓ | ✓ | × | ✓ |
| Perfect-forward secrecy | ✓ | × | × | ✓ | ✓ |
| Anonymity and untraceability | × | × | ✓ | ✓ | ✓ |
| Fair session-key negotiation | ✓ | ✓ | × | ✓ | ✓ |
| Security against DoS attacks | × | ✓ | ✓ | ✓ | ✓ |
| Clock-synchronization problem | × | × | × | ✓ | ✓ |
| Decentralization | × | × | × | × | ✓ |
| Local password verification | ✓ | ✓ | ✓ | ✓ | ✓ |

## 6.6 Summary

To communicate between the MU, HA, and FA. The protocol was developed to take advantage of blockchain's features, such as authentication and its preservation of user privacy. Using a formal verification process, we were able to demonstrate the proposed protocol security. The confidentiality of sensitive information and participant authentication have both been successfully validated by this protocol. Overall, using soulbound tokens for identity verification and authentication can help to create a more secure and decentralized system that reduces the reliance on centralized authorities for identity management in Global Mobility Network (GLOMONET).

# Chapter 7

# CONCLUSION AND FUTURE WORK

The present chapter, discusses the thesis' major contributions. The Telecare Medical Information System (TMIS) and future research directions in the domain of authentication for mobile environments are also described.

## 7.1 Contributions

The thesis contributions can be summarized as follows. It involves the analysis of existing protocols and the proposal of various secure and privacy-preserving authentication protocols using Blockchain:

1. Analysed a security robustness of different authentication and key agreement protocols in the existing literature to enhance security, maintain confidentiality, ensure data integrity, and preserve privacy in TMIS and Global Mobility Networks.

2. Proposed a novel and secure authentication protocols using Blockchain for TMIS and GLOMONET through the utilization of smart contracts. The proposed protocols aims to safeguard user privacy and anonymity while also withstanding various network attacks.

3. Comprehensive security analysis using a strong adversary (Dolev-Yao) model and formal verification has been performed using AVISPA to validate the robustness

of the proposed authentication protocols.

4. Ultimately, performance analysis of the proposed authentication protocols have been conducted to assess communication and computational overhead. Considering several network performance parameters into account, the outcomes of analysing the performance and simulations validate the system robustness, computational efficiency, and practical feasibility of the proposed authentication protocol for resource limited global mobility Networks and TMIS.

**Chapter 4**, presents a blockchain-based mutual authentication system has been introduced for mobility networks. This system possesses decentralized, peer-to-peer, immutable, and distributed characteristics. This security system ensures anonymity and provides resistance against various types of attacks. We have performed a thorough analysis comparing security and functional requirements to demonstrate the strength of the authentication system. Furthermore, we have implemented the proposed blockchain-based framework on the Ethereum using smart-contracts created in the Solidity. This implementation enhances security and decentralization within the mobile network. In conclusion, A performance analysis validates that the mobile-chain authentication framework satisfies all functional and requirements for security in the domain of mobile networks. Moreover, the protocol is efficient, lightweight, and entails minimal communication and computational overhead compared to recent protocols designed for roaming services in mobile environments.

In the contribution of **Chapter 5**, we proposed a secure and decentralized authentication framework for the TMIS, making use of Blockchain technology. We have demonstrated that the proposed security framework effectively withstands various attacks and aligns with all the design objectives within the healthcare system. The proposed decentralized system utilizes smart contracts developed in the Solidity. The proposed decentralized system utilizes smart contracts written in the Solidity. Patients,

Doctors, and medical servers can securely authenticate and access health records using the proposed decentralised application. The authentication framework is defined using HLPSL, and its security is validated through the AVISPA formal security verification tool. Furthermore, the proposed protocol was evaluated for its computational and communication overhead, as well as other relevant authentication protocols. The results show that the decentralized authentication framework is secure, making it a practical solution for the healthcare system.

**(Chapter 6)**, A novel blockchain based protocol has been developed for roaming services within GLOMONET, facilitating communication between the MU, HA, and FA. The protocol was developed to take advantage of blockchain's features, such as authentication and its preservation of user privacy. Using a formal verification process, we were able to demonstrate the proposed protocol security. The confidentiality of sensitive information and participant authentication have both been successfully validated by this protocol. Overall, using soulbound tokens for identity verification and authentication can help to create a more secure and decentralized system that reduces the reliance on centralized authorities for identity management in Global Mobility Network (GLOMONET).

## 7.2 Future research directions

Potential areas for future research are discussed in this section. There are several research directions that merit investigation, as outlined below.

- Developing new consensus mechanisms that ensure secure and reliable data exchange to improve the privacy of blockchain-based authentication protocols.
- While blockchain-based user authentication using zero-knowledge proofs is a promising technology, it is still in the experimental stage. The future direction could focus on the practical deployment to make use of this technology and exploring ways to increase its adoption in various industries and use cases.

- Another possible direction is to explore the integration of the blockchain-based user authentication process with other technologies and systems, such as AI or IoT devices, to construct a more robust and comprehensive authentication system.
- Exploring the possibility of using blockchain-based authentication systems to enable secure and efficient data sharing across different healthcare providers, which can facilitate better collaboration and patient outcomes.
- To explore methods for scaling the blockchain-based user authentication process to support a more transactions, nodes, and users in the blockchain networks.

# Bibliography

Ahmadi, F. and Nikooghadam, M. (2019). A secure authentication and session key agreement scheme in global mobile networks preserving user anonymity. *TABRIZ JOURNAL OF ELECTRICAL ENGINEERING*, 49(3), 965–984.

Al-Qerem, A. (2022). Using raft as consensus algorithm for blockchain application of roaming services for mobile network. *International Journal Artificial Intelligent and Informatics*, 3(1), 42–52.

Amin, R., Islam, S. H., Gope, P., Choo, K.-K. R., and Tapas, N. (2018). Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. *IEEE journal of biomedical and health informatics*, 23(4), 1749–1759.

Baniata, H., Anaqreh, A., and Kertesz, A. (2021). Pf-bts: A privacy-aware fog-enhanced blockchain-assisted task scheduling. *Information Processing & Management*, 58(1), 102393.

Baniata, H. and Kertesz, A. (2020). A survey on blockchain-fog integration approaches. *IEEE Access*, 8, 102657–102668.

Baniata, H. and Kertesz, A. (2022). Prifob: a privacy-aware fog-enhanced blockchain-based system for global accreditation and credential verification. *Available at SSRN 4019311*.

Chen, Y., Ding, S., Xu, Z., Zheng, H., and Yang, S. (2019). Blockchain-based medical

records secure storage and medical service framework. *Journal of medical systems*, 43(1), 1–9.

Das, A. K. (2015). A secure and robust password-based remote user authentication scheme using smart cards for the integrated epr information system. *Journal of medical systems*, 39(3), 1–14.

Esposito, C., Ficco, M., and Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, 58(2), 102468.

Fan, C.-I. and Lin, Y.-H. (2009). Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. *IEEE Transactions on Information Forensics and Security*, 4(4), 933–945.

Fan, K., Wang, S., Ren, Y., Li, H., and Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, 42(8), 1–11.

Ferreira, J. C., Ferreira da Silva, C., and Martins, J. P. (2021). Roaming service for electric vehicle charging using blockchain-based digital identity. *Energies*, 14(6), 1686.

Giri, D., Maitra, T., Amin, R., and Srivastava, P. (2015). An efficient and robust rsa-based remote user authentication for telecare medical information systems. *Journal of medical systems*, 39(1), 1–9.

Gope, P. and Hwang, T. (2016a). An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *Journal of Network and Computer Applications*, 62, 1–8.

Gope, P. and Hwang, T. (2016b). Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. *IEEE Systems Journal*, 10(4), 1370–1379.

Hao, X., Ren, W., Choo, K.-K. R., and Xiong, N. N. (2021). A self-trading and authenticated roaming scheme based on blockchain for smart grids. *IEEE Transactions on Industrial Informatics*, 18(6), 4097–4106.

He, D., Ma, M., Zhang, Y., Chen, C., and Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, 34(3), 367–374.

Indushree, M. and Raj, M. (2023). Secure user authentication protocol for roaming services in mobile networks using blockchain. In *International Conference on Data Science and Network Engineering*, 511–523. Springer.

Indushree, M. and Raj, M. (2024). A novel blockchain-based authentication scheme for telecare medical information system. *The Journal of Supercomputing*, 80(1), 1080–1108.

Indushree, M., Raj, M., Mishra, V. K., Shashidhara, R., Das, A. K., and Bhat, V. (2022). Mobile-chain: Secure blockchain based decentralized authentication system for global roaming in mobility networks. *Computer Communications*.

Jiang, Q., Ma, J., Li, G., and Ma, Z. (2013). An improved password-based remote user authentication protocol without smart cards. *Information Technology and Control*, 42(2), 113–123.

Karuppiah, M., Kumari, S., Li, X., Wu, F., Das, A. K., Khan, M. K., Saravanan, R., and Basu, S. (2017). A dynamic id-based generic framework for anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, 93(2), 383–407.

Karuppiah, M. and Saravanan, R. (2015). A secure authentication scheme with user anonymity for roaming service in global mobility networks. *Wireless Personal Communications*, 84(3), 2055–2078.

Kim, S. (2019). Impacts of mobility on performance of blockchain in vanet. *IEEE Access*, 7, 68646–68655.

Kuo, T.-T., Kim, H.-E., and Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211–1220.

Lee, C.-C., Lai, Y., Chen, C., and Chen, S.-D. (2017). Advanced secure anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications: An International Journal*, 94(3), 1281–1296.

Lee, H. and Ma, M. (2020). Blockchain-based mobility management for 5g. *Future Generation Computer Systems*, 110, 638–646.

Li, C. and Lee, C. (2012). A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Mathematical and Computer Modelling*, 55(1), 35–44.

Li, J., Qiao, Z., and Peng, J. (2022). Asymmetric group key agreement protocol based on blockchain and attribute for industrial internet of things. *IEEE Transactions on Industrial Informatics*.

Li, X., Niu, J., Khan, M. K., and Liao, J. (2013). An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications*, 36(5), 1365–1371.

Lin, C., He, D., Huang, X., Choo, K.-K. R., and Vasilakos, A. V. (2018). Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications*, 116, 42–52.

Lo, J.-W., Wu, C.-Y., and Chiou, S.-F. (2020). A lightweight authentication and key agreement scheme for telecare medicine information system. *Journal of Internet Technology*, 21(1), 263–272.

Lu, Y. and Zhao, D. (2021). A chaotic-map-based password-authenticated key exchange protocol for telecare medicine information systems. *Security and Communication Networks*, 2021.

Madhusudhan, R. et al. (2016). An efficient and secure authentication scheme with user anonymity for roaming service in global mobile networks. In *Proceedings of the 6th International Conference on Communication and Network Security*, 119–126. ACM.

Madhusudhan, R. et al. (2018). A secure and lightweight authentication scheme for roaming service in global mobile networks. *Journal of Information Security and Applications*, 38, 96–110.

Madhusudhan, R. and Mittal, R. (2012). Dynamic id-based remote user password authentication schemes using smart cards: A review. *Journal of Network and Computer Applications*, 35(4), 1235–1248.

Madhusudhan, R. and Shashidhara, R. (2019). A secure anonymous authentication protocol for roaming service in resource-constrained mobility environments. *Arabian Journal for Science and Engineering*, 1–22.

Mafakheri, B., Heider-Aviet, A., Riggio, R., and Goratti, L. (2021). Smart contracts in the 5g roaming architecture: The fusion of blockchain with 5g networks. *IEEE Communications Magazine*, 59(3), 77–83.

Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M. K., and Chaturvedi, A. (2014). Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. *Journal of medical systems*, 38(5), 1–11.

Mun, H., Han, K., Lee, Y. S., Yeun, C. Y., and Choi, H. H. (2012). Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modelling*, 55(1), 214–222.

Nguyen, C., Nguyen, D., Dinh, H. T., Pham, A. H., Huynh, N. T., Xiao, Y., and Dutkiewicz, E. (2021). Blockroam: Blockchain-based roaming management system for future mobile networks. *IEEE Transactions on Mobile Computing*.

Nikooghadam, M., Amintoosi, H., and Kumari, S. (2020). A provably secure ecc-based roaming authentication scheme for global mobility networks. *Journal of Information Security and Applications*, 54, 102588.

Reddy, A. G., Das, A. K., Yoon, E.-J., and Yoo, K.-Y. (2016). A secure anonymous authentication protocol for mobile services on elliptic curve cryptography. *IEEE Access*, 4, 4394–4407.

Renuka, K., Kumari, S., and Li, X. (2019). Design of a secure three-factor authentication scheme for smart healthcare. *Journal of medical systems*, 43(5), 1–12.

Shamshad, S., Mahmood, K., Kumari, S., Chen, C.-M., et al. (2020). A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications*, 55, 102590.

Shashidhara, R., Bojjagani, S., Maurya, A. K., Kumari, S., and Xiong, H. (2020). A robust user authentication protocol with privacy-preserving for roaming service in mobility environments. *Peer-to-Peer Networking and Applications*, 1–24.

Shashidhara, R., Lajuvanthi, M., and Akhila, S. (2021). A secure and privacy-preserving mutual authentication system for global roaming in mobile networks. *Arabian Journal for Science and Engineering*, 1–12.

Tan, Z. (2014). A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *Journal of medical systems*, 38(3), 1–9.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., and Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 6(2), 147–156.

Weerasinghe, N., Hewa, T., Dissanayake, M., Ylianttila, M., and Liyanage, M. (2021). Blockchain-based roaming and offload service platform for local 5g operators. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 1–6. IEEE.

Wen, F., Susilo, W., and Yang, G. (2013). A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless personal communications*, 73(3), 993–1004.

Wu, F., Xu, L., Kumari, S., Li, X., Khan, M. K., and Das, A. K. (2017). An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks. *Annals of telecommunications*, 72(3-4), 131–144.

Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., and Zhang, X. (2017). Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2), 44.

Xu, G., Liu, J., Lu, Y., Zeng, X., Zhang, Y., and Li, X. (2018). A novel efficient maka protocol with desynchronization for anonymous roaming service in global mobility networks. *Journal of Network and Computer Applications*, 107, 83–92.

Yoon, E., Yoo, K., Young, and Ha, K. (2011). A user friendly authentication scheme with anonymity for wireless communications. *Computers & Electrical Engineering*, 37(3), 356–364.

Yoon, E.-J. and Yoo, K.-Y. (2013). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. *The Journal of supercomputing*, 63(1), 235–255.

Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40(10), 1–8.

Zhang, A. and Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of medical systems*, 42(8), 1–18.

Zhao, D., Peng, H., Li, L., and Yang, Y. (2014). A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, 78(1), 247–269.

## LIST OF PUBLICATIONS /COMMUNICATIONS BASED ON THESIS:

### Journal papers

**Chapter #4** Indushree M and Manish Raj: Mobile-Chain: Secure blockchain based decentralized authentication system for global roaming in mobility networks. **Computer Communications, Elsevier 200 (2023) 1-16 (SCI Indexed)**.

**Chapter #5** Indushree M and Manish Raj: A Novel Blockchain-based Authentication Scheme for Telecare Medical Information System. **The journal of Supercomputing (Springer) (SCI Indexed)**. Is Accepted for Publication.

- Indushree M and Manish Raj: Cross Channel Scripting and Code Injection Attacks on Web and Cloud-Based Applications: A Comprehensive Review. **Sensors, MDPI (2022), 22, 1959 (SCI indexed)**.

### Conference papers

**Chapter #6** Indushree M and Manish Raj: Secure User Authentication Protocol for Roaming Services in Mobile Networks Using Blockchain. Is Accepted in **International Conference on Data science and network engineering (ICDSNE) Springer, 2023**.

- Indushree M and Shashidhara: Design of a Secure Blockchain Based Privacy Preserving Electronic Voting System. **Proceedings of Emerging Research in Computing, Information, Communication and Applications.(pp. 1-9) Springer 2022(Scopus Indexed)**.