

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2024.0429000

5G-MobiCare: A Secure 5G Assisted Remote Mobile Health Monitoring Platform

HEMANGI GOSWAMI¹ (Member, IEEE), TARUN PANDEY², and HITEN CHOUDHURY³

¹Manipal Institute of Technology, Bengaluru, Manipal Academy of Higher Education, Manipal, 576104, Karnataka, India (e-mail: hemangi.goswami@manipal.edu)

²Ministry of Electronics and Information Technology, New Delhi, 110003, Delhi, India (e-mail: tarun.p@meity.gov.in)

³Department of Computer Science and Information Technology, Cotton University, Guwahati, 781001, Assam, India (e-mail: hiten.choudhury@cottonuniversity.ac.in)

Corresponding author: Hemangi Goswami (e-mail: hemangi.goswami@manipal.edu).

ABSTRACT E-Healthcare utilizes IoT-enabled medical devices equipped with sensors to gather and transmit patient health data to a centralized electronic health record (EHR) system via mobile networks, enabling remote health management. This setup generates vast amounts of real-time data, making secure device authentication essential to ensure data privacy and security. In critical scenarios like ambulance care, quick and reliable authentication becomes crucial as devices remain in motion. To address this, a remote registration and group authentication scheme is proposed for eSIM-enabled medical devices using the 5G mobile network for transmitting sensitive health data. eSIM-enabled sensors provide a flexible, secure means of connecting to healthcare networks, while group authentication further enhances efficient and reliable communication. Lightweight cryptographic techniques, including Elliptic Curve Cryptography (ECC), one-way hash functions, and XOR operations, address the resource constraints of medical sensors. A group secret key enables collective device authentication, reducing computational and communication overhead. The scheme's security is validated using BAN logic and the Automated Validation of Internet Security Protocols and Applications (AVISPA). The proposed scheme enhances security and efficiency for e-healthcare systems. The group secret key reduces resource usage, making the approach suitable for constrained devices. Lightweight cryptographic functions ensure data security without overburdening sensors. Security validations confirm robustness against threats. The proposed framework for eSIM-enabled medical devices leverages the 5G network and lightweight cryptographic techniques to provide secure, efficient communication of health data. This approach enhances patient management, particularly in critical scenarios like ambulance care, where reliable authentication is vital. Future work can explore scalability and broader IoT applications.

INDEX TERMS ECC, e-Healthcare, Group Authentication, Group Secret Key, IoT, 5G Mobile Network.

I. INTRODUCTION: IOT IN HEALTHCARE APPLICATION

e-healthcare is a real-time use-case of an IoT application that involves the transmission of a substantial amount of sensitive data or information over the public Internet [1]. With advancements in healthcare technologies, the healthcare system has evolved from Healthcare 1.0 to Healthcare 4.0, significantly enhancing patient monitoring [2]. Healthcare 1.0 relied on manual patient records, while Healthcare 4.0 leverages IoT, cloud computing, fog computing, and telehealthcare technologies. This transformation offers benefits such as reduced in-person visits, cost-effectiveness, timely interventions, lower risks of hospital-acquired infections, and increased flexibility. In Healthcare 4.0, medical devices

equipped with sensors are attached to patients to monitor various health parameters like heart rate, body temperature, blood glucose, blood pressure, and pulse [3] [4]. This data is then transmitted via a mobile network to a centralized electronic health record (EHR) system located in a remote server known as telehealthcare. Authorized third parties or doctors can remotely access, monitor, analyze, and manage a patient's health condition. Additionally, eSIM-enabled medical sensors play a pivotal role in e-healthcare systems, offering flexible and secure real-time connections with healthcare networks. The integration of eSIM with IoT is a growing trend in the IoT industry [5] [6]. eSIM-enabled medical sensors provide advantages like remote patient monitoring, emergency

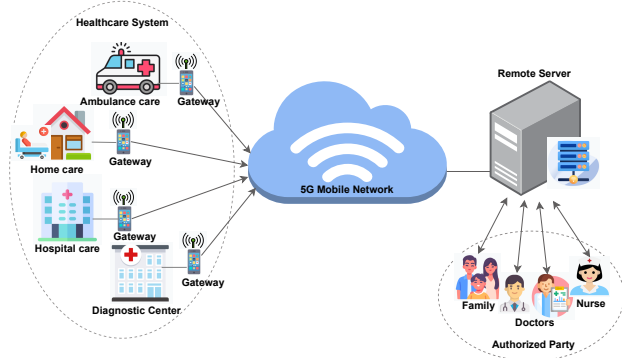


FIGURE 1: Architecture of e-Healthcare System.

alerts, video consultations, and ambulance and emergency services.

Figure 1 illustrates the architecture of an e-healthcare system supported by 5G mobile networks. In the healthcare system domain, various types of healthcare services are integrated, including ambulance care, home care, hospital care, and diagnostic centers. Each of these service points is equipped with IoT-enabled medical devices that use sensors placed in the patient's body to collect real-time patient health data such as vital signs, ECG readings, glucose levels, and more. These sensors transmit the data through gateways that act as communication bridges between medical devices and the mobile network infrastructure. The gateways forward this data securely through the 5G mobile network, enabling high-speed, low-latency communication. This ensures reliable and uninterrupted transmission of sensitive medical information, even in dynamic and mobile environments such as ambulance care. The transmitted data is received by a remote server, where it is processed and stored in an Electronic Health Record (EHR) system. Authorized users—including doctors, nurses, family members, and other approved parties can remotely access and analyze the patient's health information. This enables continuous monitoring, emergency interventions, and efficient medical decision-making, regardless of the patient's physical location.

A. MOTIVATION AND PROBLEM STATEMENT

A healthcare system may generate a massive amount of real-time data at regular or scheduled intervals using the medical devices attached to the patient's body. Effectively handling real-time data is essential for the success of e-healthcare systems, as it enables timely interventions, informed decision-making, and improved patient outcomes. Therefore, prioritizing device authentication is a key aspect for providing the necessary security and privacy safeguards while transmitting the collected data as well as remote monitoring of the stored data in a healthcare IoT environment [7] [8] [9]. Moreover, in some critical medical scenarios like in ambulance care, when a patient's health deteriorates or when immediate medical intervention is required, a patient may need to be transferred from home care to a nearby hospital using an ambulance. In

such cases, the devices with sensors that are attached to the patient's body are constantly on the move. Therefore, for reliable and secure use of these types of essential services where some devices are constantly mobile, device authentication must be rapid. In a large-scale e-healthcare environment, individually authenticating devices becomes a challenging task due to resource constraints and latency concerns. Therefore, group authentication serves as a valuable tool for managing the authentication process, offering the potential to improve efficiency without sacrificing security.

Within the existing literature, various group authentication schemes have been proposed to ensure efficiency and security in an e-healthcare system. However, many of these schemes do not meet all security requirements, such as confidentiality, anonymity, integrity, forward secrecy, and may not withstand common attacks like replay attacks, eavesdropping attacks, denial of service attacks, and man-in-the-middle attacks. In addition, many existing works do not consider the remote registration and credential provisioning of eSIM-enabled medical sensors before authentication starts. Remote provisioning is especially important because it allows doctors and authorized users to access patient data and monitor their health from different locations, which is a key feature in modern e-healthcare systems. They also fail to use lightweight cryptographic methods, which are important to reduce the processing load on medical sensors that have limited resources. These gaps make it difficult to apply such schemes effectively in real-world, large-scale healthcare systems. The motivations of the paper explained above are listed below.

- (a) To prioritize device authentication for providing the necessary security and privacy safeguards while transmitting the collected data, as well as remote monitoring of the stored data.
- (b) For reliable and secure use of essential services like ambulance care, where devices are constantly on the move, the authentication of the devices must be quick.
- (c) In a large-scale e-healthcare environment, authenticating the devices on an individual basis is going to be a challenging task due to resource constraints and latency concerns.
- (d) Most of the schemes present in the existing literature are not able to meet security requirements like confidentiality, anonymity, integrity, forward secrecy, etc., and are not resistant to some common attacks like replay attack, eavesdropping attack, denial of service attack, man-in-the-middle attack, etc.
- (e) Remote credential provisioning to the eSIM-enabled medical sensors before the authentication begins, is also not considered by the existing proposals.
- (f) To address the limitations of individual authentication and reduce communication/computational overhead, a group authentication scheme is necessary for improving scalability, performance, security, and ease of adoption and implementation in dynamic e-healthcare environments.

B. RESEARCH CONTRIBUTION

By considering the motivations discussed in the previous section, such as the need for efficient, secure, and scalable authentication in e-healthcare systems, this paper proposes a group-based authentication scheme for eSIM-enabled medical devices using the 5G mobile network as its communication backbone. The main contributions of the paper are listed below.

- (a) A novel group authentication mechanism is introduced, where all medical sensors associated with a USIM-enabled gateway form a group, with the gateway acting as the group leader to manage group-level authentication tasks.
- (b) Medical sensors are registered remotely through a trusted USIM-enabled gateway, eliminating the need to go to the home network for registration. It supports the flexible addition and integration of new sensors into the network remotely through the already registered gateway, enabling seamless scalability.
- (c) The protocol employs resource-efficient cryptographic techniques, including Elliptic Curve Cryptography (ECC), one-way hash functions, and XOR operations, suitable for low-power medical sensors.
- (d) A group secret key is generated to facilitate simultaneous group-based authentication of devices, significantly reducing communication and computational overhead.
- (e) After successful authentication, sensitive patient data is securely transmitted to a remote server over a 5G network, ensuring confidentiality and real-time accessibility for authorized users.
- (f) Unlike many existing approaches, the proposed scheme includes a deregistration mechanism that detaches sensors from the network if abnormal behavior is detected, such as prolonged inactivity or missed authentication, maintaining the integrity and efficiency of the system.
- (g) The scheme achieves low computational overhead, minimal communication cost, and reduced authentication latency, making it highly suitable for real-time e-healthcare scenarios.
- (h) The protocol's security is formally verified using BAN logic and the AVISPA tool, demonstrating resistance against various security threats.

C. PAPER ORGANIZATION

This remaining paper is organized as follows. Some of the existing works present in the literature are discussed in Section II. The proposed protocol is explained in detail in Section III. Section IV performs the security validation of the proposed scheme. Performance analysis of the proposed scheme is presented in Section V. Finally, Section VI concludes the paper.

II. RELATED WORK

Authentication in e-healthcare systems is crucial for ensuring the security and privacy of sensitive health-related data and the reliability of medical device communications. In the last

decade, some notable authentication protocols proposed by different researchers in the field of e-healthcare to preserve security and privacy are explained below.

A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks was proposed by Wu et al. in 2017 [10]. The scheme is divided into four phases: initialization, registration, authentication, and password change. Authors claimed that the proposed scheme is resistant to various attack like insider attack, off-line guessing attack, user forgery attack, sensor capture attack, gateway forgery attack, de-synchronization attack, user tracking attack, and session key disclosure attack. However, group authentication and remote registration of the devices are not considered in the proposal. In 2018, Wu et al. also proposed a novel mutual authentication scheme for smart Healthcare systems under the global mobility networks notion [11]. The scheme included four phases: initialization, registration, mutual authentication, and key agreement and password renewal phase. According to the authors, the scheme was resistant to insider attack, off-line guessing attack, user forgery attack, agent spoofing attack, de-synchronization attack, replay attack, known-key attack, tracking attack and gives Strong forward security, Password changeability, and mutual authentication. However, the scheme did not consider some requirements like group authentication of the devices. Additionally no communication medium is mentioned by the authors for the authentication mechanism. In 2019, Amintoosi et al. devised a lightweight authentication scheme 'Slight' for smart healthcare services [12]. Slight consisted of the registration phase, login and authentication phase, ownership transfer phase, and password update phase. They justified the scheme's strength in terms of resistance to various known security attacks like replay attack, Insider Attack, Known-session-specific Temporary Information Attack, Known-key Secrecy, Sensor Impersonation Attack, user Impersonation Attack, Server Impersonation Attack, Denial of Service Attack, Password Guessing Attack, Stolen Verifier Attack, Man-in-the-middle Attack, Key Compromise Impersonation (KCI) attack and the provision of perfect forward secrecy and known-key secrecy. Tanveer et al. proposed a resource-efficient authentication and key exchange scheme 'REAS-TMIS' for telecare medical information systems in 2022 [3]. The scheme was based on authenticated encryption with associative data, one-way hash function, elliptic curve point multiplication, chaotic map, etc. Hamed et al. devised a secure patient authentication scheme in the healthcare system in 2022 [13]. The authors used symmetric encryption techniques, crypto hash functions, and a one-time pad in the proposed scheme to provide good security as well as maintain adequate performance. The scheme was based on five phases: setup, registration, login and authentication, healthcare, and key management. Authors claimed that the scheme is resistant to various harmful attacks like MITM, insider, replay, spoofing, and impersonation and provides mutual authentication, anomalies, and key management. In 2025, Saleem et al. the proposed a secure authenticated key-management protocol

for e-healthcare environments using CBC-AES encryption and Physical Unclonable Functions (PUF) [14]. According to the authors, the scheme is designed to protect against a wide range of attacks, including impersonation, session key leakage, and device cloning. Both formal and informal security analyses are conducted to demonstrate its robustness, with the ROR model validating resistance to various threats. Performance evaluation shows that the proposed protocol reduces communication and computation overheads compared to several existing schemes. In 2023, Lee et al. proposed two lightweight RFID authentication and key agreement protocols for e-healthcare systems using Physical Unclonable Functions (PUFs) and cloud computing [15]. These protocols are designed for both secure and public communication channels, addressing the limitations of traditional cryptosystems in resource-constrained environments. Authors claimed that by leveraging the uniqueness of PUFs and avoiding key storage on cloud servers, the proposed schemes enhance security, efficiency, and scalability. They also provide strong protection against replay, stolen verifier, and key compromise attacks, while ensuring session key security, fairness, and perfect forward/backward secrecy. Renuka et al. designed a three-factor authentication scheme for a smart healthcare system in 2019, [16]. The proposed mechanism was based on two entities, a user and an authentication server. According to the authors, the scheme gave forward and backward secrecy, session-specific temporary information, user anonymity, and mutual authentication, as well as was resistant to impersonation attack, DoS attack, stolen verifier attack, password guessing attack, and replay attack. An RSA-based authentication scheme was developed for authorized access to healthcare services by Dharminder et al. [17]. The scheme was developed for telecare medicine information systems. The technique used two message exchanges between the user and the server to provide a shared session key and to establish mutual authentication. A secure three-factor authentication scheme was devised by Sahoo et al. for healthcare systems using IoT-enabled devices [18]. The authors used elliptic curve cryptography to provide a high level of security with a smaller key size. Authors claimed that the scheme provided session key security, secured password update, mutual authentication, user anonymity, perfect forward secrecy, and also was resistant to attacks like key compromise impersonation attack, stolen smart card attack, insider attack, replay attack, offline password guessing attack, forgery attack, server spoofing attack. Several other authentication schemes like [19], [20], [21] etc. are proposed by different authors to enhance the efficiency of e-healthcare applications. However, a notable limitation in many of these schemes is the absence of group authentication for patients or medical devices.

Even though many authentication schemes have been developed for e-healthcare systems, most of them do not support group authentication, which is important for managing multiple medical devices or patients at the same time, especially in fast-moving situations like ambulance care. Also, many existing methods don't allow remote registration of devices,

Protocol	Author	Technology used	Gaps identified
Two-Factor Auth Scheme	Wu et al. (2017) [10]	ECC, Hash, XOR, Four-PhaAuthenticated Encryption, ECC, Hash, Chaotic Mapse Protocol	No group authentication, No remote registration
Mutual Auth Scheme	Wu et al. (2018) [11]	ECC, Hash, Key Agreement	No group authentication, No remote registration
SLIGHT	Amintoosi et al. (2019) [12]	Multi-phase (Login, Ownership Transfer, Update), Secure Hashing	No group authentication, No mention of remote registration
REAS-TMIS	Tanveer et al. (2022) [3]	Authenticated Encryption, ECC, Hash, Chaotic Map Symmetric Encryption, One-Time Pad, Hash	No group authentication, No remote registration
Secure Patient Auth Scheme	Hamed et al. (2022) [13]	Password, Biometrics, Authentication Server	No device-level focus, No remote registration
Three-Factor Scheme	Renuka et al. (2019) [16]	RSA, Mutual Auth with Session Key Exchange	not lightweight, No group authentication, no remote registration
RSA-Based Scheme	Dharminder et al. (2020) [17]	Physical Unclonable Functions (PUFs), cloud computing	No group authentication, no remote registration
Cloud Computing-Based RFID Authentication Protocols Using PUF Authenticated Key-Management Mechanism	Saleem et al. (2025) [14]	CBC-AES encryption, Remote Management, Physical Unclonable Functions (PUF)	No group authentication, no eSIM involved
ECC-Based Scheme	Sahoo et al. (2021) [18]	ECC, Three-Factor, Smart Card	No remote registration, No group authentication
Others	Karthigaiveni et al. [19], Rajasekar et al. [20], Khemissa et al. [21]	ECC, Hashing, Biometrics, Smart Cards	Mostly lack group auth and remote registration
Proposed Scheme		ECC, Hashing, XOR	Remote registration, Group Authentication, eSIM-based

TABLE 1: Comparison of Existing Authentication Schemes in E-Healthcare Systems

which is necessary for real-time use in different locations. These missing features show that current methods are not fully suitable for modern healthcare needs. That's why there is a need for a new method that is lightweight, secure, and efficient, especially for eSIM-enabled medical devices using 5G mobile networks. The proposed scheme aims to bridge these gaps by ensuring remote registration, group authentication, minimizing communication overhead, and fulfilling essential security requirements while addressing the resource limitations of medical sensors. The detailed explanation of the proposed scheme is discussed in the following Section.

III. THE PROPOSED SCHEME FOR E-HEALTHCARE SYSTEM

In this section, the proposed system model and the proposed scheme are discussed in detail.

A. PROPOSED SYSTEM MODEL

This section presents the architecture of the proposed system in which various medical sensors are planted in or on the patient's body for collecting health-related information. First of all, the medical devices/sensors are registered with the core 5G mobile network through a registered USIM-enabled gateway (GW). GW has already established a connection successfully with the core 5G network infrastructure to access the services and therefore it is considered a trusted entity of the 5G mobile network. During the registration process, all the security credentials required for the authentication process are provisioned by the home network remotely through the corresponding USIM-enabled device and by communicating with the subscription manager and certificate authority. Before every data session, authentication of all the medical sensors is performed. For the authentication process, some groups are formed and the devices present in a group are authenticated simultaneously. The devices that are connected with a particular USIM-enabled device are considered to belong to a group and that particular GW is considered as a group leader and acts as a gateway between the devices and the core 5G mobile network. A group secret key is also generated among the group members and using that key the devices are authenticated in a group by the home network. After successful authentication, data collected by the medical sensors are transmitted to the USIM-enabled group leader or the gateway. The group leader aggregates all the data received from the medical sensors and transmits it to a remote server using a core 5G network. Any authorized doctor, nurse, or family member can access and monitor those stored data remotely. Whenever a new sensor is added to the existing group of the system, it needs to be registered with the network's core infrastructure and the registration process is performed remotely through the corresponding registered gateway. In addition, if some sensors do not participate in the authentication process for a particular period of time then, a deregistration process is initiated to discard the sensor from the existing network. Figure 2 shows the architecture of the proposed system model.

B. PRELIMINARIES AND BASIC NOTATIONS

To devise the proposed scheme, an elliptic curve with equation $y^2 = (x^3 + ax + b) \bmod p$ is used. Here, p is a prime number and $(4a^3 + 27b^2) \bmod p \neq 0$. USIM-enabled GW is considered a trusted entity of the 5G network since it has already successfully established a connection with the core infrastructure of the 5G mobile network. The notations used in the proposed scheme and their descriptions are shown in Table 2. The proposed scheme is divided into four phases.

- *Sensor Registration*, where all the medical sensors/devices are registered with the home network through a

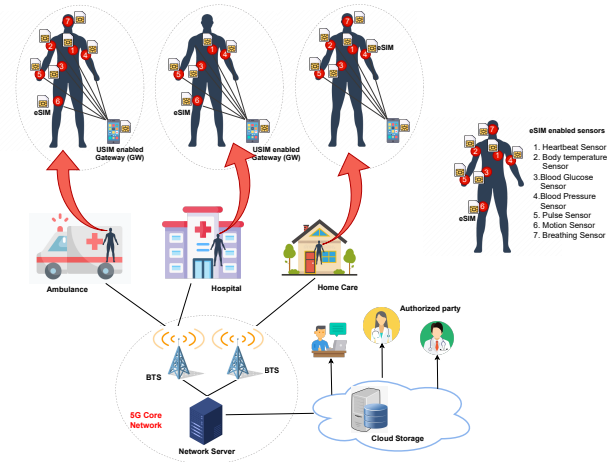


FIGURE 2: Architecture of the Proposed System Model.

TABLE 2: Notations and their descriptions used in the proposed protocol.

Notations	Descriptions
MD_i	Medical device with sensor
GW	USIM enabled Gateway
IMSI	International mobile subscriber identity
SUPI	Subscription permanent identifier
SUCI	Subscription concealed identifier
CRT	Certificate of the device
CRTF	Certificate generated by HN for GW
K	Shared secret key between GW and HN
SSK_i	Shared secret key between GW and MD_i
MDPub	Public key of the IoT device
MDPri	Private key of the IoT device
HNPub	Public key of the HN
SMPri	Private key of the subscription manager
SMPub	Public key of the subscription manager
GWPri	Private key of the gateway
GWPub	Public key of the gateway
SID_i	Permanent identity of the medical sensor 'i'
$TSID_i$	Temporary identity of the medical sensor 'i'
K_{EC}	Shared secret key generated using ECIES
GK	Group key
PK_i	Partial group key
SP_i, S_i, M_i	Security parameter for device 'i'
RAND, RN, R, N, NC	Random nonce
MAC	Message authentication code
CK	Cipher key
IK	Integrity key
AUTN	Authentication token
RES	Response value
XRES	Expected response

trusted entity of the home network.

- *Group Key Establishment*, where a group of IoT devices is formed to perform group authentication of the medical devices.
- *Group Authentication*, where a group of IoT devices is authenticated simultaneously to reduce resource consumption by individual device authentication in large IoT deployments.
- *Sensor Deregistration*, where a device is removed from the IoT network when the device is no longer in use, has been replaced, or poses a security risk.

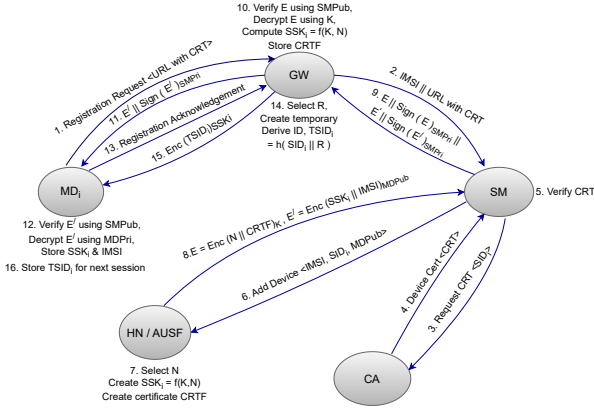


FIGURE 3: Proposed sensor registration phase.

C. SENSOR REGISTRATION

In this phase, the medical sensors are added/enrolled into the e-healthcare system to enable the 5G mobile network to recognize and communicate with the medical sensors. This process is done remotely by one of the trusted entities of the home network, i.e., USIM-enabled user equipment by communicating with the subscription manager and the certificate authority. After the successful addition of the medical devices, some security credentials are provided to the sensors by the home network remotely for authentication purposes. Figure 3 shows the mechanism involved in the sensor registration process.

The steps involved in this phase are explained below.

- 1) Medical device ' MD_i ' sends a registration request to the GW by sending the URL that contains the certificate ' CRT '.

MSG 1: $MD_i \rightarrow GW$: URL with CRT

- 2) GW forwards the request to the SM by sending ' $(IMSI || URL \text{ with } CRT)$ '.

MSG 2: $GW \rightarrow SM$: $IMSI || URL \text{ with } CRT$

- 3) SM then requests CA for the device certificate by sending the medical device's identity ' SID_i '.

MSG 3: $SM \rightarrow CA$: SID_i

- 4) CA transmits the certificate to the SM.

MSG 4: $CA \rightarrow SM$: CRT

- 5) SM verifies the certificate ' CRT '.

- 6) If verification is successful, SM requests HN to add the medical device by transmitting ' $(IMSI || SID_i || MDPub)$ '.

MSG 5: $SM \rightarrow HN$: $IMSI || SID_i || MDPub$

- 7) HN extracts the shared secret key ' K ' stored against the received ' $IMSI$ ', selects a nonce ' N ', and generates the shared secret key ' SSK_i ' for the ' MD_i ' and the GW as follows.

$$SSK_i = f(K, N) \quad (1)$$

It also creates a certificate ' $CRTF$ ' for the GW and medical devices containing the identity of the HN, the identity of the GW, and all the identities of the medical devices.

- 8) HN transmits two security parameters ' E ' and ' E' ' to the

SM. ' E ' contains ' N ' and ' $CRTF$ ' and is encrypted by ' K '. ' E' ' contains ' SSK_i ' and ' $IMSI$ ' and is encrypted by the medical device's public key ' $MDPub$ '.

MSG 6: $HN \rightarrow SM$: $E = Enc(N || CRTF)_K$, $E' = Enc(SSK_i || IMSI)_{MDPub}$

- 9) SM forwards ' E ' and ' E' ' by signing with its private key ' $SMPri$ ' along with the plaintext ' E ' and ' E' '.

MSG 7: $SM \rightarrow GW$: $E || Sign(E)_{SMPri}$, $E' || Sign(E')_{SMPri}$

- 10) GW decrypts ' E ' with the SM's public key ' $SMPub$ ' and compares the received ' E ' with the decrypted one. If both the values are the same, GW decrypts ' E ' with the shared secret key ' K ' to get the nonce ' N '. After that, it also calculates the shared secret key ' SSK_i ' as follows. $SSK_i = f(K, N)$ It then stores the ' $CRTF$ '.

- 11) GW forwards the signed ' E' ' with the original ' E' ' to the MD_i .

MSG 8: $GW \rightarrow MD_i$: $E' || Sign(E')_{SMPri}$

- 12) MD_i decrypts ' E' ' with the SM's public key ' $SMPub$ ' and compares the received ' E' ' with the decrypted one. If both the values are the same, MD_i decrypts ' E' ' with the device private key ' $MDPri$ '. Then it stores the ' SSK_i ' and ' $IMSI$ ' in its local repository.

- 13) ' MD_i ' sends a registration acknowledgment message to the GW.

MSG 9: $MD_i \rightarrow GW$: Registration Acknowledgement

- 14) After receiving the registration success message, GW generates a temporary identity ' $TSID_i$ ' for the ' MD_i ' using a nonce ' R ', device's original identity ' SID_i ', and a one-way hash function as follows. The ' $TSID_i$ ' will be used in the next authentication process.

$$TSID_i = h(SID_i || R) \quad (2)$$

- 15) GW transmits the temporary identity ' $TSID_i$ ' to the ' MD_i ' by encrypting with ' SSK_i '.

MSG 10: $GW \rightarrow MD_i$: $Enc(TSID_i)_{SSK_i}$

- 16) ' MD_i ' stores ' $TSID_i$ ' for the next authentication.

D. GROUP KEY ESTABLISHMENT PHASE

The steps involved in the proposed group secret generation phase 4 are as follows.

- 1) GW transmits a *Group Generation Request* to all the medical devices present in the network $\langle MD_1, MD_2, \dots, MD_i, \dots, MD_n \rangle$ by sending the hashed value of the ' $IMSI$ ' and a random number ' $RAND$ ' and by encrypting with the shared secret key ' SSK_i ' between the GW and ' MD_i '.

MSG 1: $GW \rightarrow MD_i$: $Enc(h(IMSI) \oplus RAND)_{SSK_i}$

- 2) Medical device ' MD_i ' then calculates the hashed value of the ' $IMSI$ ' with which it is registered with. If the calculated hash value is equal to the received hash value, then it creates a security parameter ' SP_i ' as follows.

$$SP_i = h(SSK_i \oplus RAND) \quad (3)$$

- 3) ' MD_i ' transmits its temporary identity ' $TSID_i$ ' by performing the XOR operation with the shared secret key

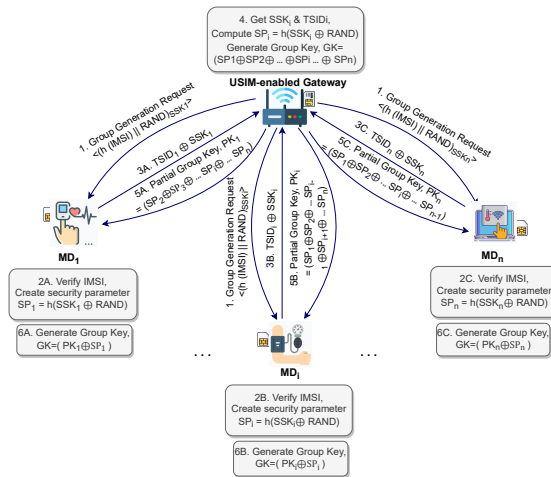


FIGURE 4: Proposed group key establishment phase.

‘ SSK_i ’ to the corresponding GW.

$$\text{MSG 2: } MD_i \rightarrow GW : TSID_i \oplus SSK_i$$

- 4) GW extracts the stored ' SSK_i ' against the received value and also computes the security parameter ' SP_i ' as follows. $SP_i = h(SSK_i \oplus RAND)$ This process is performed for all the devices, from which temporary identities are received. After that, GW generates the group key ' GK ' using all the calculated security parameters.

$$GK = SP_1 \oplus SP_2 \oplus SP_i \oplus \dots \oplus SP_n \quad (4)$$

- 5) GW then sends a partial group key ' PK_i ' to the ' MD_i 's by XORing all the received security parameters from the other medical devices present in that network.

MSG 3: $GW \rightarrow MD_i$: Partial Group key(PK) = $SP_1 \oplus SP_2 \oplus SP_{i-1} \oplus SP_{i+1} \dots \oplus SP_n$

- 6) ' MD_i ' finally generates the group key ' GK ' by XORing the received ' PK_i ' with its own security parameter ' SP_i ' as follows.

$$GK = PK_i \oplus SPi \quad (5)$$

E. AUTHENTICATION PHASE

After the group is generated by the gateway node, all the nodes present in the group are authenticated by the gateway and the HN. A mutual authentication between the medical devices and the gateway is performed using the group key generated in the group key establishment phase. All the medical devices that are connected with a particular gateway are authenticated by the HN in a group. In this phase, the functions that have been already used by 3GPP's 5G-AKA are also used with some additional functions for group authentication [22] [23]. After every successful authentication, medical data are transmitted to the remote server in a secure way. Figure 5 shows the proposed authentication scheme and the detailed steps involved in the process are explained below.

- 1) Medical device ' MD_i ' sends a request for authentication to the gateway node by sending the temporary identity ' $TSID_i$ ' encrypted with ' GK '.

$$\text{MSG 1: } MD_i \rightarrow GW : Enc(TSID_i)_{GK}.$$

- 2) The gateway aggregates all the requests received from the medical devices present in that group.
- 3) The gateway transmits the request to the Authentication Server Function (AUSF) by sending ' $SUCI/5G - GUTI, Enc(\sum(TSID_i))_K$ '.

$$SUCI = Enc(SUPI)_{K_{ECIES}} \quad (6)$$

$$\mathbf{MSG2: GW} \rightarrow \mathbf{AUSF: SUCI/5G-GUTI, Enc(\sum(TSID_i))_K}$$

- 4) AUSF transmits the '*SUCI*' to the UDM as an authentication vector request.

MSG 3: $AUSF \rightarrow UDM : SUCI$

- 5) UDM extracts the 'SUPI' from the 'SUCI' to get the shared secret key 'K' between the gateway and the HN. It then selects a random number 'RN'. By using the key 'K' and a set of one-way hash functions, UDM generates the authentication vector 'AV', which consists of ('RN', 'AUTN', 'XRES' and 'K_{AUSF}').

$$MAC = f1(RN)K \quad (7)$$

$$AUTN = f'(MAC) \quad (8)$$

$$XRES = f2(RN)_K \quad (9)$$

$$CK = f3(RN)_K \quad (10)$$

$$IK = f4(RN)_K \quad (11)$$

$$K_{AUSF} = KDF(CK, IK) \quad (12)$$

- 6) UDM then forwards the calculated 'AV' to the AUSF.
MSG4: $UDM \rightarrow AUSF : AV(RN, AUTN, XRES, K_{AUSF})$
 7) AUSF sends the 'RN' and 'AUTN' to the gateway.

MSG 5: $AUSF \rightarrow GW : RN, AUTN$

- 8) After that, the gateway calculates the 'AUTN' and compares the calculated 'AUTN' with the received one to validate the HN. It also calculates the 'RES'. It then selects a random nonce 'NC' to calculate the security parameter ' S_i '.

$$S_i = h(NC)GK \quad (13)$$

- 9) The gateway transmits ' S_i ' along with the nonce ' NC ' by signing with its private key ' $GWPr_i$ '.

MSG 6: $GW \rightarrow MD_i : Enc(S_i || NC)_{GWPri}$

- 10) ' MD_i ' decrypts the received value with the public key of the gateway ' GWP_{pub} '. It then calculates the ' S_i ' and compares the calculated value with the received one to authenticate the gateway. It also computes another security parameter ' M_i '.

$$M_i = h(NC)SSK_i \quad (14)$$

- 11) ' MD_i ' transmits ' M_i ' and temporary identity of the medical device ' $TSID_i$ ' by encrypting with the group key ' GK ' to the gateway.

$$\mathbf{MSG\ 7: } MD_i \rightarrow GW : Enc(M_i || TSID_i)_{GK}$$

- 12) The gateway calculates the ' M_i ' for the medical device with temporary identity ' $TSID_i$ '. It then compares the

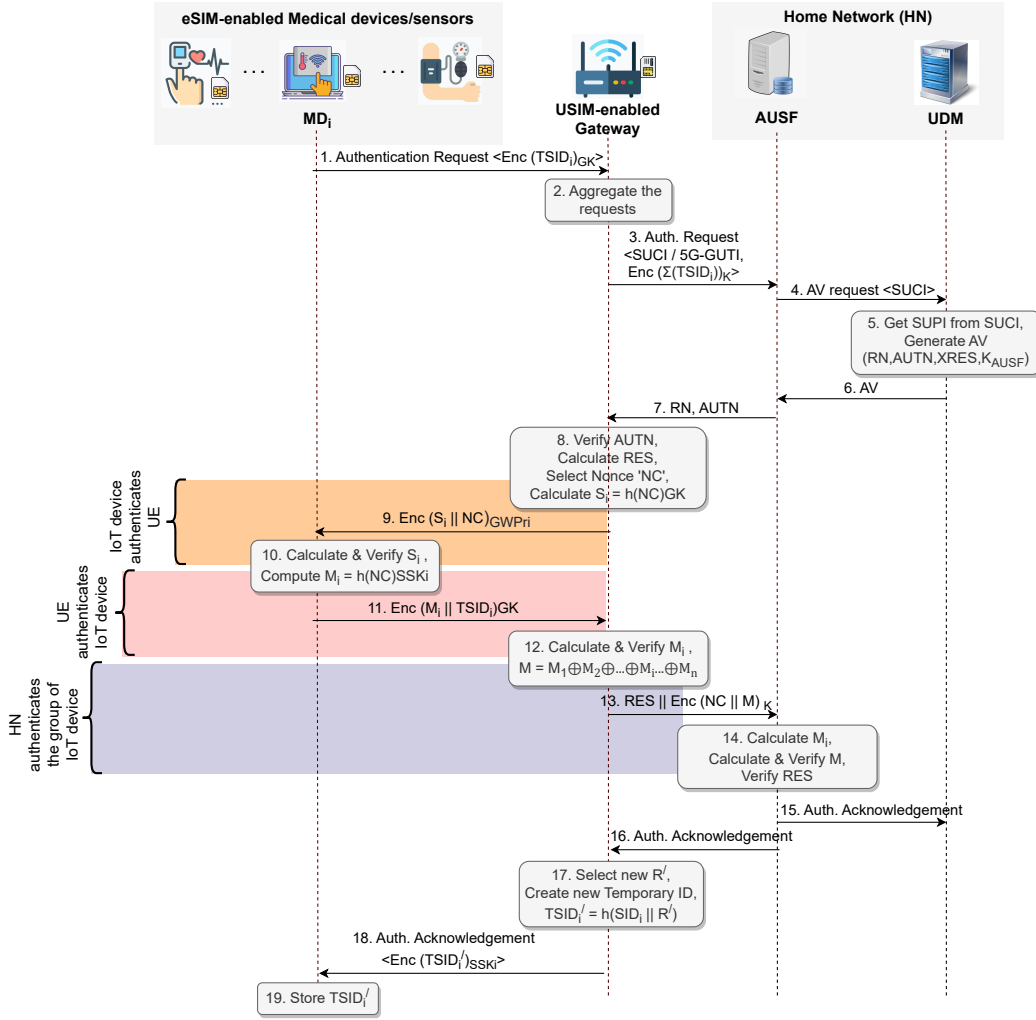


FIGURE 5: Proposed group authentication phase.

calculated value with the received one to authenticate the medical device ' MD_i '. The gateway also generates a security parameter ' M ' using all the ' M_i 's received from the medical devices present in that group.

$$M = M_1 \oplus M_2 \oplus \dots \oplus M_i \oplus \dots \oplus M_n \quad (15)$$

- 13) The gateway sends the ' NC ' and ' M ' by encrypting with the key ' K ' along with the ' RES ' to the AUSF.

MSG 8: $GW \rightarrow AUSF : RES || Enc(NC || M)$

- 14) AUSF computes ' M_i 's for all the medical devices, that are participating in that particular authentication process. By using all the calculated ' M_i 's, it also calculates ' M '. It then compares the calculated ' M ' with the received one to authenticate the gateway and the medical devices in a group. It also verifies the ' RES ' by comparing the calculated value with the received one.

- 15) AUSF responds with an *authentication acknowledgement* message to the UDM.

MSG 9: $AUSF \rightarrow UDM : \text{Authentication Acknowledgement}$

- 16) AUSF also transmits an *authentication acknowledgement* message to the gateway.

MSG 10: $AUSF \rightarrow GW : \text{Authentication Acknowledgement}$

- 17) The gateway then creates a new temporary identity ' $TSID'_i$ ' for the medical device using a new random number ' R' ', the original identity of the medical device, and a one-way hash function. The new ' $TSID'_i$ ' will be used in the next session for authentication.

$$TSID'_i = h(SID_i || R') \quad (16)$$

- 18) The gateway then transmits the *authentication acknowledgement* to the MD_i by sending ' $TSID'_i$ ' encrypted by the shared secret key ' SSK_i '.

MSG 11: $GW \rightarrow MD_i : Enc(TSID'_i)_{SSK_i}$

- 19) After decrypting the message, ' MD_i ' stores ' $TSID'_i$ ' in its local database for the next session.

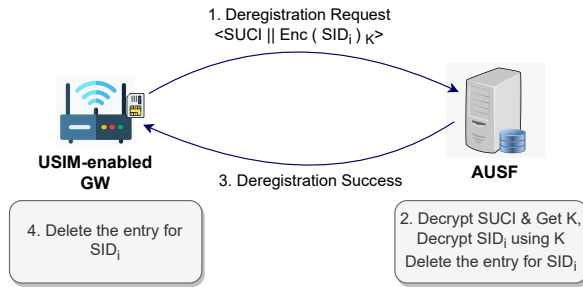


FIGURE 6: Proposed deregistration phase.

F. SENSOR DEREGISTRATION

If a medical device is inactive for a period of time, then a deregistration process is initiated by the gateway. The mechanism involved in the process is shown in Figure 6 and the steps are explained below.

- 1) The GW transmits a deregistration request to the AUSF by sending the temporary identity ' SID_i ' of the device ' MD_i ', which is encrypted by the shared secret key ' K ' along with its SUCI.
- 2) AUSF extracts the key ' K ' against that SUCI, decrypts the message using the key ' K ', and deletes the entry from its local repository for that medical device with identity ' SID_i '.
- 3) AUSF then transmits a deregistration success message to the GW.
- 4) After receiving the deregistration success message from AUSF, the GW also deletes the entry for that particular device ' MD_i ' with identity ' SID_i ' from its local database.

IV. SECURITY ANALYSIS

In an e-healthcare system, security and privacy are essential to protect patients' sensitive health-related data. In this section, we have done the analysis of various common security properties by using three methods: informal security analysis, formal security analysis using BAN logic, and formal security analysis using an automated tool AVISPA.

A. ADVERSARY MODEL

In the proposed scheme, we adopt the Dolev–Yao model as our chosen adversary model [24] [25]. This selection is primarily driven by the significant security vulnerabilities identified within the communication channel between medical devices and the gateway. Within the Dolev–Yao model, an intruder is endowed with complete control over the communication channel. This control encompasses the ability to insert, delete, analyze, manipulate, or eavesdrop on messages exchanged between the entities involved. If the intruder successfully persuades other parties within the environment that they are a legitimate part of the network, it opens the door to various potential attacks.

B. INFORMAL SECURITY ANALYSIS

Some of the key security properties of e-healthcare systems are considered in this section.

- 1) **Mutual Authentication:** In the proposed group authentication phase, the ' MD_i ' authenticates the GW by comparing the received ' S_i ' (Equation 13) with the calculated one (Steps 8,9, and 10 in Figure 5). In addition, the GW authenticates the ' MD_i ' (Equation 14) by comparing the received ' M_i ' with the calculated one (Steps 10,11 and 12 in Figure 5). Therefore, the proposed scheme could provide mutual authentication between the medical device and the gateway.
- 2) **Forward and Backward Secrecy:** The group key ' GK ' is generated freshly in every data session as discussed in Equation 3 and 4 in Section III-D, which is not related to past or future group keys. In addition, a fresh nonce is used for authenticating the ' MD_i 's and the GW in every data session. Therefore, by compromising the current ' GK ' and nonce, any adversary cannot guess the past and future ' GK 's and cannot compromise the past or future communications. Thus, the proposed protocol guarantees forward and backward secrecy.
- 3) **Anonymity:** In the proposed scheme, real identities of the ' MD_i 's and the ' GW ' are not used during the message transmissions among the entities. Instead of using the real identity ' SID_i ' of the ' MD_i ', a temporary identity ' $TSID_i$ ' is used in every data session to prevent the disclosure of the real identity of the device to any unauthorized party. In addition, the permanent identity of the gateway (SUPI) is also transmitted in an encrypted form, i.e., SUCI. Moreover, one-way hash functions are used to generate the temporary identities from the real identities of the medical devices from the temporary identities. Therefore, the proposed protocol ensures user anonymity.
- 4) **Integrity:** In the proposed scheme, one of the outcomes of a successful mutual authentication process is the establishment of an integrity key from the established key ' K_{SEAF} ' like in 5G-AKA for securing the communications between the user equipment/gateway and the serving network. In addition, if any authorized third party wants to access the stored data from the remote server, the digital certificate ' $CRTF$ ', which is generated by the trusted authority HN, is used for validating the source of data acquired from the medical devices.
- 5) **Confidentiality:** After successful mutual authentication between the gateway and the HN, a cipher key is generated from the established key ' K_{SEAF} ' like in 5G-AKA for securing the communications between the user equipment/gateway and the serving network. In addition, data transmitted among the authorized entities are always in an encrypted form, which can't be accessed by any unauthorized party.
- 6) **Untraceability:** In every data session, freshly generated

nonce is used for the authentication process. As a result, no attacker can be able to trace any medical device's identity. Moreover, for the authentication mechanism, one-way hash functions are used because of their non-invertible property. Therefore, the adversary can't trace the messages exchanged among the authorized entities.

- 7) **Session key secrecy:** The session key ' SSK_i ' is transmitted to the medical device by encrypting with the device's public key ' $MDPub$ '. Therefore, without the device's private key ' $MDPri$ ', no attacker can be able to access the key ' SSK_i '. In addition, the group key ' GK ' is not transmitted over the communication channel. Instead of the ' GK ', a partial key ' PK_i ' is transmitted to every ' MD_i ' and every device generates the ' GK ' in its own by using the ' PK_i ' and its own security parameter ' SP_i ' as shown in Equation 4, 5, and MSG 3 in Section III-D.
- 8) **Resistance against various common attacks:**

- **Man-in-the-middle attack:** Our security protocol provides robust protection against Man-in-The-Middle (MiTM) Attacks. This is achieved through the utilization of two crucial keys: the group key ' GK ', shared among all group members, and the unique shared secret key ' SSK_i ' between the medical device and the GW. Every transmitted message is securely encrypted using either the ' GK ' or ' SSK_i ', rendering it inaccessible and unmodifiable by any unauthorized third party.
- **Replay attack:** In our proposed scheme, we employ a sequence number ' SQN ' during the authentication phase, which effectively guards against replay attacks, ensuring the security of the system.
- **Eavesdropping attack:** In our proposed scheme, the confidentiality of transmitted information is upheld, as all sensitive data is securely transmitted in an encrypted format. This robust encryption mechanism ensures protection against eavesdropping attacks, making it highly resistant to unauthorized interception of sensitive information.

C. FORMAL SECURITY ANALYSIS

This section provides formal security analysis of the proposed scheme using BAN logic and an automated tool AVISPA.

1) Using BAN Logic

The Burrows–Abadi–Needham (BAN) logic serves as a formal tool for verifying security, employing a set of rules and underlying assumptions to scrutinize security protocols [26]. It is instrumental in determining the trustworthiness of transmitted data and information. The notations and rules integral to BAN logic are elaborated in Table 3.

The analysis is based on the following security assumptions, as presented below.

- A1: $AUSF \models GW \xrightarrow{K} AUSF$
A2: $GW \models GW \xrightarrow{K} AUSF$
A3: $AUSF \models GW \xrightarrow{SUP} AUSF$

TABLE 3: Notations and Rules of BAN logic.

Notation	Description
$A \models B$	A believes B.
$A \Rightarrow X$	A has jurisdiction over X.
$A \triangleleft X$	A sees X.
$A \sim X$	A once said X.
$\#(X)$	X is fresh.
$A \xleftrightarrow{K} B$	A and B share a key K.
$\xrightarrow{pubkey^{-1}} A$	$pubkey^{-1}$ is the private key of A.
$\xrightarrow{pubkey} A$	$pubkey$ is the public key of A.
$\{X\}_K$	X is encrypted with key K.
$\langle X \rangle_Y$	X is combined with Y.
Rule1 : $\frac{A \models A \xleftrightarrow{K} B, A \triangleleft \{X\}_K}{A \models B \mid \sim X}$	Message meaning rule.
Rule2 : $\frac{A \models B \mid \Rightarrow X, A \models B \mid \Rightarrow X}{A \models X}$	Jurisdiction rule.
Rule3 : $\frac{A \models \#(X), A \models B \mid \sim X}{A \models \#(X)}$	Nonce verification rule.
Rule4 : $\frac{A \models \#(X)}{A \models \#(X, Y)}$	Freshness conjunction rule.

- A4: $GW \models GW \xleftrightarrow{SSK_i} MD_i$
A5: $MD_i \models GW \xleftrightarrow{SSK_i} MD_i$
A6: $AUSF \models GW \xleftrightarrow{K} AUSF$
A7: $AUSF \models GW \xleftrightarrow{SSK_i} MD_i$
A8: $AUSF \models GW \xleftrightarrow{KECC} AUSF$
A9: $GW \models GW \xleftrightarrow{KECC} AUSF$
A10: $MD_i \models \xrightarrow{GWPub} GW$
A11: $MD_i \models GW \xleftrightarrow{GK} MD_i$
A12: $GW \models GW \xleftrightarrow{GK} MD_i$
A13: $AUSF \models \xrightarrow{MDPub_i} MD_i$
A14: $GW \models \xrightarrow{MDPub_i} MD_i$

The security goals, we have considered for the proposed scheme, are as follows.

- G1.** Mutual authentication must be enabled between the medical device and the GW, i.e.,
 $MD_i \models GW \sim S_i$ and $GW \models MD_i \sim M_i$
G2. Medical devices must be authenticated by the HN/AUSF in a group through the GW, i.e.,
 $AUSF \models GW \sim M$ and $AUSF \models M$
G3. Medical device and GW believe in the session key, generated by HN/AUSF, i.e.,
 $GW \models SSK_i$ and $MD_i \models SSK_i$
G4. AUSF authenticates the identity of the GW, i.e.,
 $AUSF \models GW \sim SUCI$

Proof:

From Assumptions A10, A11, Equation 13, and MSG 6 of Section III-E, it may be derived using message meaning rule as,

$$\frac{MD_i \models MD_i \xleftrightarrow{GK} GW, MD_i \models \xrightarrow{GWPub} GW, MD_i \triangleleft (S_i)_{GWPri}, S_i = h(NC)GK}{MD_i \models GW \sim S_i} \quad (17)$$

i.e., ' MD_i ' believes the group key ' GK ' and public key ' $GWPub$ ' of the GW. Since ' MD_i ' receives ' S_i ' by encrypting with ' $GWPri$ ' and ' S_i ' is a function of the ' GK ', therefore ' MD_i ' believes that ' GW ' once said ' S_i '.

From Step Number 10 in Figure 5, it may be derived as

$$MD_i \models MD_i \Rightarrow S_i \quad (18)$$

Using the Equation 18, it may be stated that

$$MD_i \models S_i \quad (19)$$

i.e., ' MD_i ' believes that it has the power to create ' S_i ' and therefore it believes ' S_i '. From Equation 17 and 19, if the received ' S_i ' as well as the calculated ' S_i ' are same, ' MD_i ' authenticates the ' GW '. From Assumptions A4, A12, Equation 14, and MSG 7 of Section III-E, using message meaning rule it may be derived as,

$$\frac{GW \models MD_i \xleftrightarrow{GK} GW, GW \models MD_i \xleftrightarrow{SSK_i} GW, GW \triangleleft (M_i)_{GK}, M_i = h(NC)SSK_i}{GW \models MD_i \sim M_i} \quad (20)$$

i.e., The ' GW ' believes the group key ' GK ' and shared secret key ' SSK_i ' between ' MD_i ' and ' GW '. In addition, ' GW ' receives ' M_i ' by encrypting with ' GK ', where ' M_i ' is a function of a nonce and ' SSK_i '. Therefore ' GW ' believes that ' MD_i ' once said ' M_i '.

From Step Number 12 in Figure 5, it may be derived as

$$GW \models GW \Rightarrow M_i \quad (21)$$

Using the Equation 21, it may be stated that

$$GW \models M_i \quad (22)$$

i.e., ' GW ' believes that it has the power to create ' M_i ' and therefore it believes ' M_i '. From Equation 20 and 22, if the received ' M_i ' is same as the calculated ' M_i ', ' GW ' authenticates the ' MD_i '. Hence, **G1 is achieved**.

$$\frac{AUSF \models AUSF \xleftrightarrow{K} GW, AUSF \triangleleft (M)_K, M = M1 \oplus M2 \oplus M_i}{AUSF \models GW \sim M} \quad (23)$$

i.e., The ' $AUSF$ ' believes the shared secret key ' K ' between ' $AUSF$ ' and ' GW '. In addition, ' $AUSF$ ' receives ' M ' by encrypting with ' K ' and therefore ' $AUSF$ ' believes that ' GW ' once said ' M '.

From Equation 14, 15 and Step Number 14 in Figure 5, it may be derived as

$$AUSF \models AUSF \Rightarrow M \quad (24)$$

From Equation 24, it may be stated as

$$AUSF \models M \quad (25)$$

i.e., ' $AUSF$ ' believes that it has the power to create ' M ', where $M = M1 \oplus M2 \oplus \dots \oplus M_i$ and therefore it believes ' M '. From Equation 23 and 25, if the received ' M ' is same as the calculated ' M ', ' $AUSF$ ' authenticates the group of ' MD_i 's. Hence, **G2 is achieved**.

$$\frac{MD_i \models AUSF \Rightarrow SSK_i, MD_i \models AUSF \models SSK_i}{MD_i \models SSK_i} \quad (26)$$

$$\frac{GW \models AUSF \Rightarrow SSK_i, GW \models AUSF \models SSK_i}{GW \models SSK_i} \quad (27)$$

i.e., ' GW and ' MD_i ' believes that ' $AUSF$ ' has the power to control ' SSK_i '. In addition, both ' GW and ' MD_i ' believe ' $AUSF$ ' and ' $AUSF$ ' believes ' SSK_i '. Hence, it can be concluded as ' GW and ' MD_i ' believe ' SSK_i '. From Equation 26 and 27, **G3 is achieved**.

$$\frac{AUSF \models GW \xleftrightarrow{K_{ECIES}} AUSF, AUSF \triangleleft SUCI, SUCI = Enc(SUPI)_{K_{ECIES}}}{AUSF \models GW \sim SUCI} \quad (28)$$

i.e., ' $AUSF$ ' believes the key ' K_{ECIES} ' between ' $AUSF$ ' and ' GW ' as well as it receives the identity ' $SUPI$ ' by encrypting with the key ' K_{ECIES} '. Therefore, ' $AUSF$ ' believes that the ' GW ' once said ' $SUCI$ '.

From Equation 28, **G4 is achieved**.

2) Using AVISPA

This section presents the formal analysis of the proposed scheme using a formal verification tool Automated Validation of Internet Security Protocols and Applications (AVISPA) to validate the security properties of the protocols and uncover security vulnerabilities or potential attacks. If there are vulnerabilities, AVISPA may generate an attack simulation to demonstrate how the protocol can be exploited. Here, we have utilized the High-Level Protocol Specification Language (HLPSL) to describe a protocol model, depicting the message exchanges during the authentication process (7). It offers several analysis tools like OFMC, CL-ATSE, SATMC, and TA4SP, each suited for different types of security properties. For the analysis, we have employed OFMC and CL-AtSe as backend tools. Our primary objective for this analysis is to establish mutual authentication between the IoT device and the user equipment (UE) and to resist the authentication against various common attacks. The results of this analysis are illustrated in Figure 8, where both OFMC and CL-AtSe indicate that the analysis results are "safe". This outcome strongly suggests that mutual authentication has been successfully achieved between the IoT device and the UE within our proposed scheme. The protocol simulation, as visualized in Figure 9, confirms the secure functioning of the protocol. Furthermore, we have accounted for the capabilities of an intruder who possesses knowledge of all involved parties and the hash functions employed within the protocol. Following protocol and intruder simulations, the acquired knowledge by the intruder is detailed in the lower left corner of Figure 10. This assessment demonstrates that the intruder's gained knowledge at the conclusion of the entire authentication cycle is insufficient to facilitate attacks like Man-in-the-Middle (MiTM), Replay attacks, eavesdropping, etc., between the messages exchanged by authorized parties. Consequently, we can confidently assert that our proposed scheme exhibits no identified vulnerabilities or susceptibilities to attacks.



FIGURE 7: Program written for formal verification using AVISPA

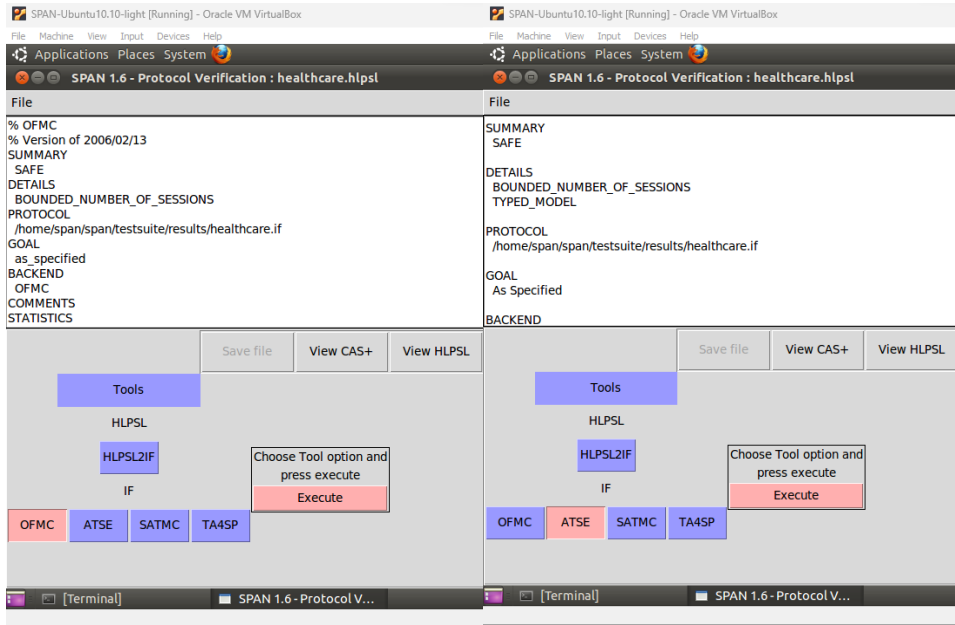


FIGURE 8: Results obtained using AVISPA

V. PERFORMANCE ANALYSIS

Within this section, we first analyze the performance of our scheme, specifically focusing on aspects like computational overhead and communication overhead, and then compare our scheme with other authentication schemes present in the existing literature.

A. COMPUTATIONAL OVERHEAD

To determine the computational overhead, we measured the duration of key cryptographic operations employed within the protocols. These operations were executed on both an Arduino Uno Rev3 microcontroller board and a computer system featuring an Intel(R) Pentium(R) 1.90 GHz Processor, 6.00 GB RAM, and a 1TB HDD for terminal and network components, respectively. The resulting execution times, derived from our analysis, are detailed in Table 4.

To simplify the calculation process, we assume that there are 20 IoT devices in a group (denoted as n). In the proposed protocol, the terminal side employs two hash functions, one elliptic curve decryption algorithm, two symmetric encryptions, and one symmetric decryption. As a result, we can calculate the total computational overhead of the proposed scheme at the terminal side as follows.

$$T_{ter} = 2 * T_h + T_{ec.dc} + 2 * T_{sc.en} + T_{sc.dc} = 1144.36ms. \quad (29)$$

In the proposed protocol, the network side employs $(6+n)$ hash functions, one random number generation function, one elliptic curve decryption algorithm, and $n-1$ XOR operations. As a result, we can calculate the total computational overhead of the proposed scheme at the network side as follows.

$$T_{net} = (6+n) * T_h + T_r + T_{ec.dc} + (n-1) * T_x = 10.34ms. \quad (30)$$

We have also included a table (Table 5) that presents a comparison between the overall computational requirements of our proposed protocol and several existing protocols. However, most of the schemes consider the authentication of patients with the medical server. Additionally, no communication medium is also mentioned in the papers. Therefore, to compare the schemes with our proposed scheme in terms of computational overhead, we have considered the communication medium as 5G mobile network. Therefore, it can be considered that with the existing operations the operations present in the mechanism for 5G-AKA also included for overall computational cost.

B. COMMUNICATION OVERHEAD

In this section, we assess the communication overhead of the proposed scheme by measuring its impact on bandwidth consumption. This is determined based on the size of the messages exchanged during the authentication process [29]. To calculate the bandwidth consumption value, we make assumptions regarding the lengths of certain parameters used in the protocol, as given below in Table 6. To facilitate a meaningful comparison between our proposed protocol and different protocols, we have chosen to evaluate the authentication process for ten medical devices simultaneously. When it comes to individually authenticating medical devices, calculating the communication overhead for authenticating ten devices requires the complete protocol to be executed ten times. Consequently, the total communication overhead is ten times that of a single-device authentication round. In contrast, group-based authentication simplifies the process by requiring the repetition of only a few specific steps ten times. We provide a comprehensive comparison of the communication

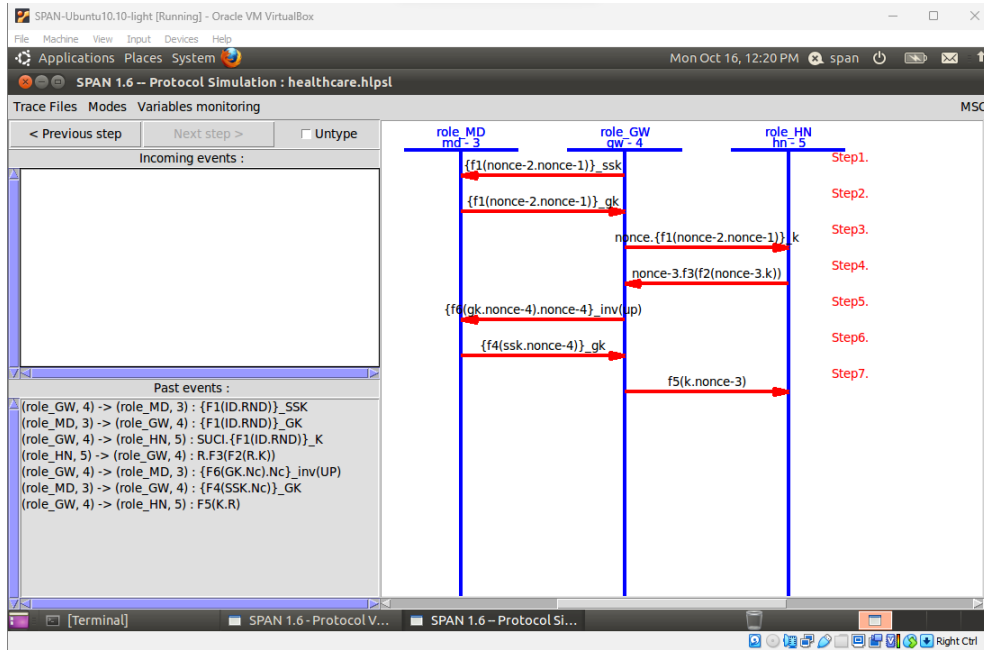


FIGURE 9: Protocol simulation using AVISPA

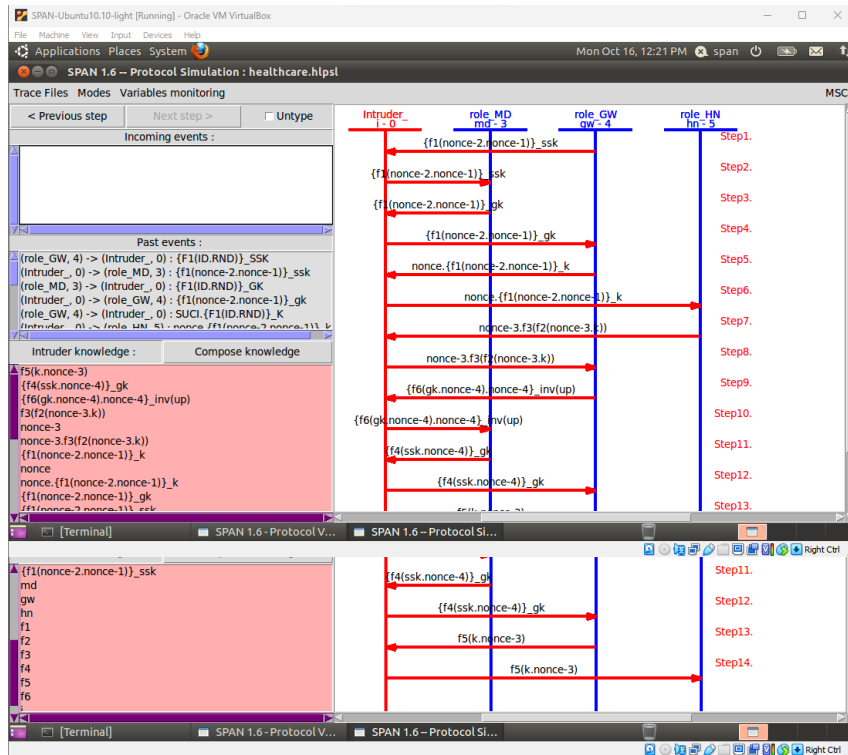


FIGURE 10: Intruder simulation using AVISPA

TABLE 4: Timing analysis of key cryptographic operations.

Cryptographic functions	Symbols	Time at the Terminal Side (ms)	Time at the Network Side (ms)
Time for a random number generation	T_r	0.26	0.46
Time for a hash function	T_h	12.72	0.18
Time for a bio-hash function	T_H	0.398	0.006
Time for a XOR operation	T_x	negligible	negligible
Time for a point multiplication	T_m	1067.24	2.00
Time for a scalar multiplication	T_{sm}	0.44	4.45
Time for a modular exponentiation	T_{ME}	63,486	898.38
Time for a symmetric encryption	$T_{sc.en}$	2.21	1.00
Time for a symmetric decryption	$T_{sc.dc}$	1.89	3.02
Time for a pairing operation	T_p	negligible	negligible
Time for Diffie–Hellman shared key generation	T_{DH}	1098	2.00
Time for elliptic curve encryption	$T_{ec.en}$	$T_{DH} + T_h + T_{sc.en}=1112.93$	$T_{DH} + T_h + T_{sc.en}=3.18$
Time for an elliptic curve decryption	$T_{ec.dc}$	$T_{DH} + T_h + T_{sc.dc}=1112.61$	$T_{DH} + T_h + T_{sc.dc}=5.2$

TABLE 5: Comparison of computational overhead.

Proposals	Computational Overhead (ms)	
	At the Terminal Side	At the Network Side
Li et al. [27]	$8 T_h \approx 101.76$	$7 T_h + 1 T_{ME} \approx 899.64$
Xiang et al. [28]	$9 T_h + 5 T_{SM} \approx 116.68$	$4 T_h + 2 T_{SM} \approx 9.62$
Wu et al. [10]	$6 T_h \approx 76.32$	$11 T_h \approx 1.98$
Renuka et al. [16]	$9 T_h + 2 T_H + 3 T_{ME} \approx 190573.276$	$4 T_h + 4 T_{ME} \approx 3594.24$
Proposed Scheme	1144.36	10.34

TABLE 6: Lengths of certain parameters used in the proposals.

Parameters	Length (bits)
Keyed hash	256
Authentication request/ response	8
Timestamp and Random numbers	32
Cipher generated by symmetric encryption	128
Signed message	256
SUCI	256
Certificate	1024

overheads associated with our proposed protocol and several other existing protocols in Table 7.

1) Discussion

Figure 11(a) depicts a comparison of different protocols in terms of computational overhead at the terminal side. From the figure, it may be concluded that our proposed protocol requires less computational overhead at the terminal side compared to the schemes in references [27], [28], and [10]. Additionally, as shown in the table 5, Renuka et al.'s protocol [16] demands a very high computational overhead for resource-constrained medical devices, which is not feasible in a healthcare environment.

Figure 11(b) displays a graph of computational overhead at the network side in relation to the increase in the number

of terminals/medical devices. It is evident that as the number of terminals participating in the authentication process increases, computational overhead also increases. However, this increase is much less pronounced when compared to other existing schemes, such as [28] and [10]. Therefore, it can be concluded that the proposed protocol yields superior results compared to other schemes.

Figure 11(c) provides a comparison of various protocols in terms of communication overhead, specifically for single-device authentication. Nevertheless, it is worth noting that a healthcare environment typically features hundreds of devices, many of which need to be authenticated simultaneously to achieve efficiency.

Figure 11(d) presents a comparison of communication overhead with respect to the increase in the number of terminals. Xiang et al.'s scheme requires more communication overhead compared to our proposed protocol. Some proposals, such as 5G-AKA and Li et al.'s scheme, demand less communication overhead than our proposed protocol. However, as the number of terminals increases, our scheme gives better result, as shown in Figure 11(d).

VI. CONCLUSION

This paper presents a novel authentication protocol for e-healthcare systems using 5G mobile network to enhance the security and efficiency of authenticating eSIM-enabled medical devices. This system carries particular significance in addressing critical challenges, notably within the realm of ambulance care, where devices and sensors affixed to patients are constantly on the move. Recognizing the resource limitations of medical devices, we have implemented lightweight cryptographic functions that efficiently reduce both computational and communication overheads. Furthermore, we've adopted a group authentication approach, ensuring improved results without compromising the integrity of sensitive data. These contributions collectively provide a robust foundation for e-healthcare environments. The formal and informal security assessments clearly demonstrate the robustness of the proposed scheme against a range of common security threats. Additionally, the performance analysis underscores the effi-

TABLE 7: Comparison of communication overhead.

Proposals	Communication Overhead (bits)
5G-AKA	2672
Xiang et al.	4272
Li et al.	3696
Proposed Scheme	3856

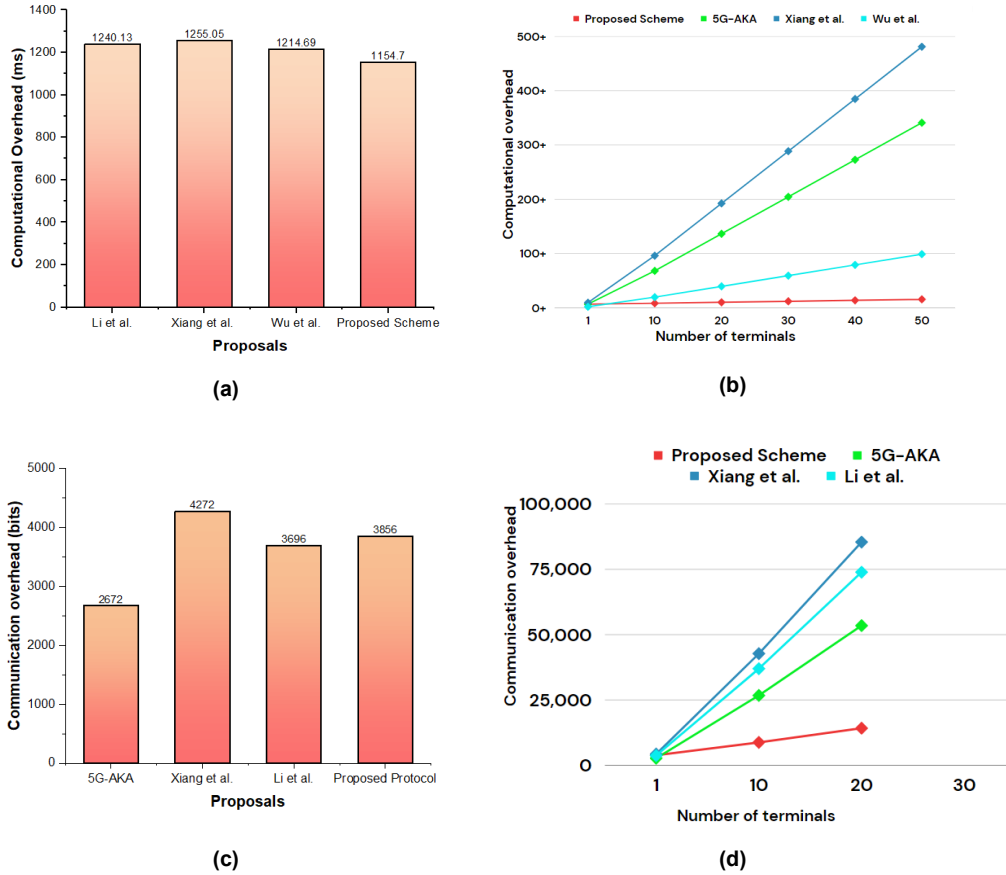


FIGURE 11: (a) Comparison of schemes in terms of computational overhead in the terminal side, (b) Computational overhead at the network side vis-a-vis number of terminals, (c) Comparison of schemes in terms of communication overhead, (d) Communication overhead vis-a-vis number of terminals.

ciency of the scheme. The whole paper may be summarized as follows.

- 1) A registration and authentication scheme for the eSIM-enabled medical devices employed within the e-healthcare framework using the 5G mobile network is proposed.
- 2) The registration and credential provisioning to the medical devices are done remotely to eliminate the need for physical presence of every newly added device to home network for registration. This process is performed with the 5G cellular network through a registered USIM-enabled gateway (GW).
- 3) The authentication of the devices are done in groups based on a group secret key generated during the group secret generation phase to reduce the computational and communication overhead. After successful authentication of the devices present in the group, the patients' sensitive health-related data and information are transmitted to a remote server securely using a 5G mobile network. If some sensors do not participate in the authentication process, then a deregistration process is initiated by the corresponding GW to discard the device from the

network system.

- 4) Considering the resource constraints of the medical sensors, the proposed scheme uses lightweight cryptographic functions like Elliptic Curve Cryptography (ECC), one-way hash function, and XOR operation.
- 5) Formal and informal security analysis of the proposed scheme is performed to show that the proposed protocol is secure. For formal verification BAN logic and an automated tool AVISPA are used.
- 6) The performance analysis of the proposed scheme shows that the scheme requires less computational and communication overhead compared to the schemes present in the literature.

CONFLICT OF INTEREST

The authors declare that they have no competing financial or non-financial interests that could have influenced the work presented in this paper.

REFERENCES

- [1] H. Goswami and H. Choudhury, "A group authentication scheme for iot 5g network enabled e-healthcare system," in *International Conference on*

- Communication, Electronics and Digital Technology*. Springer, 2023, pp. 229–244.
- [2] J. J. Hathaliya and S. Tanwar, “An exhaustive survey on security and privacy issues in healthcare 4.0,” *Computer Communications*, vol. 153, pp. 311–335, 2020.
 - [3] M. Tanveer, A. Alkhayyat, S. A. Chaudhry, Y. B. Zikria, S. W. Kim et al., “Reas-tmis: Resource-efficient authentication scheme for telecare medical information system,” *IEEE Access*, vol. 10, pp. 23 008–23 021, 2022.
 - [4] S. K. Routray and S. Anand, “Narrowband iot for healthcare,” in *2017 International Conference on Information Communication and Embedded Systems (ICICES)*. IEEE, 2017, pp. 1–4.
 - [5] GSMA, “esim whitepaper: The what and how of remote sim provisioning.” Global System for Mobile Communications Association (GSMA), Whitepaper, 2018. [Online]. Available: <https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf>
 - [6] H. Goswami and H. Choudhury, “An esim-based remote credential provisioning and authentication protocol for iot devices in 5g cellular network,” *Internet of Things*, vol. 23, p. 100876, 2023.
 - [7] —, “Security of iot in 5g cellular networks: a review of current status, challenges and future directions,” *International Journal of Communication Networks and Information Security*, vol. 13, no. 2, pp. 278–289, 2021.
 - [8] M. Roy and M. Singh, “Analytical study of blockchain enabled security enhancement methods for healthcare data,” in *IOP Conference Series: Materials Science and Engineering*, vol. 1131. IOP Publishing, 2021, p. 012002.
 - [9] S. Anand and S. K. Routray, “Issues and challenges in healthcare narrow-band iot,” in *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE, 2017, pp. 486–489.
 - [10] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, “A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks,” *Future Generation Computer Systems*, vol. 82, pp. 727–737, 2018.
 - [11] F. Wu, X. Li, L. Xu, S. Kumari, and A. K. Sangaiah, “A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion,” *Computers & Electrical Engineering*, vol. 68, pp. 107–118, 2018.
 - [12] H. Amintoosi, M. Nikooghadam, M. Shojafar, S. Kumari, and M. Alazab, “Slight: A lightweight authentication scheme for smart healthcare services,” *Computers and Electrical Engineering*, vol. 99, p. 107803, 2022.
 - [13] N. M. Hamed and A. A. Yassin, “Secure patient authentication scheme in the healthcare system using symmetric encryption,” *Iraqi Journal for Electrical & Electronic Engineering*, vol. 18, no. 1, 2022.
 - [14] M. A. Saleem, X. Li, K. Mahmood, Z. Ghaffar, Y. Xie, and G. Wang, “Provably secure authenticated key-management mechanism for e-healthcare environment,” *IEEE Internet of Things Journal*, 2025.
 - [15] T.-F. Lee, K.-W. Lin, Y.-P. Hsieh, and K.-C. Lee, “Lightweight cloud computing-based rfid authentication protocols using puf for e-healthcare systems,” *IEEE Sensors Journal*, vol. 23, no. 6, pp. 6338–6349, 2023.
 - [16] K. Renuka, S. Kumari, and X. Li, “Design of a secure three-factor authentication scheme for smart healthcare,” *Journal of medical systems*, vol. 43, pp. 1–12, 2019.
 - [17] D. Dharminder, D. Mishra, and X. Li, “Construction of rsa-based authentication scheme in authorized access to healthcare services: authorized access to healthcare services,” *Journal of medical systems*, vol. 44, pp. 1–9, 2020.
 - [18] S. S. Sahoo, S. Mohanty, and B. Majhi, “A secure three factor based authentication scheme for health care systems using iot enabled devices,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1419–1434, 2021.
 - [19] M. Karthigaiveni and B. Indrani, “An efficient two-factor authentication scheme with key agreement for iot based e-health care application using smart card,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–19, 2019.
 - [20] V. Rajasekar, J. Premalatha, K. Sathya, and M. Saračević, “Secure remote user authentication scheme on health care, iot and cloud applications: a multilayer systematic survey,” *Acta Polytechnica Hungarica*, vol. 18, no. 3, pp. 87–106, 2021.
 - [21] H. Khemissa and D. Tandjaoui, “A lightweight authentication scheme for e-health applications in the context of internet of things,” in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*. IEEE, 2015, pp. 90–95.
 - [22] H. Goswami and H. Choudhury, “Remote registration and group authentication of iot devices in 5g cellular network,” *Computers & Security*, vol. 120, p. 102806, 2022.
 - [23] B. Goswami and H. Choudhury, “A blockchain-based authentication scheme for 5g-enabled iot,” *Journal of Network and Systems Management*, vol. 30, no. 4, p. 61, 2022.
 - [24] I. Cervesato, “The dolev-yao intruder is the most powerful attacker,” in *16th Annual Symposium on Logic in Computer Science—LICS*, vol. 1. Citeseer, 2001, pp. 1–2.
 - [25] Q. Do, B. Martini, and K.-K. R. Choo, “The role of the adversary model in applied security research,” *Computers & Security*, vol. 81, pp. 156–181, 2019.
 - [26] C. Boyd and W. Mao, “On a limitation of ban logic,” in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1993, pp. 240–247.
 - [27] X. Li, J. Niu, M. Karupiah, S. Kumari, and F. Wu, “Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications,” *Journal of medical systems*, vol. 40, pp. 1–12, 2016.
 - [28] X. Xiang, M. Wang, and W. Fan, “A permissioned blockchain-based identity management and user authentication scheme for e-health systems,” *IEEE access*, vol. 8, pp. 171 771–171 783, 2020.
 - [29] P. Borgohain and H. Choudhury, “A lightweight d2d authentication protocol for relay coverage scenario in 5g mobile network,” *Computer Networks*, p. 109679, 2023.

HEMANGI GOSWAMI is working as an Assistant Professor in the School of Computer Engineering in Manipal Institute of Technology (Bengaluru), Manipal Academy of Higher Education, Manipal. She has a Ph.D. degree in Computer Science and Information Technology from Cotton University, India. She has done M.Tech in Information Technology from Gauhati University, India, and has done B.E in Computer Science and Engineering from GIMT, Gauhati University, India. She became a Member (M) of IEEE in 2024. Her area of research interest includes Security and Privacy in IoT and Mobile Communication.



TARUN PANDEY is working as a Scientist E at Ministry of Electronics and Information Technology, South Delhi, Delhi, India. With over a decade of experience in the software industry, Tarun Pandey brings a strong technical foundation and deep domain knowledge to his work. He has served more than 10 years at the Ministry of Electronics and Information Technology (MeitY), where he played a key role in driving critical national initiatives. His work initially focused on cybersecurity projects. Currently, he is leading efforts in language research and development (R & D). Academically, he holds an M.Tech degree from Guru Gobind Singh Indraprastha University (IPU) and is currently pursuing a Ph.D. from the Academy of Scientific and Innovative Research (AcSIR) working as a Scientist E at Ministry of Electronics and Information Technology, South Delhi, Delhi, India.





HITEN CHOUDHURY is working as an Associate Professor in the Department of Computer Science and Information Technology in Cotton University, Assam, India. He has a Ph.D. degree in Computer Science and Engineering from Tezpur University, India. He has done his masters in computer applications from Jorhat Engineering College, India and his graduation in physics from Cotton College, India. His area of research interest includes security issues in mobile communication, IoT, blockchain, D2D communication, etc. He has publications in several national and international conferences and journals.

...