IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 June 2024, accepted 27 June 2024, date of publication 2 July 2024, date of current version 15 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3422038

RESEARCH ARTICLE

RLKS-TMS: A Robust and Lightweight Key Agreement Scheme for Telemedicine System

ABULRAHMAN ALZAHRANI
Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
e-mail: aasalzahrani1@uj.edu.sa

This work was supported by the University of Jeddah, Jeddah, Saudi Arabia, under Grant UJ-23-DR-102.

ABSTRACT It is challenging in the e-healthcare system to monitor patients using wearables or embedded sensors that can gather real-time physiological data, analyze lab test results, conduct medical examinations, and recommend treatments because all the associated sensitive information transmission is through a hostile environment; it is always possible for an unauthorized person to access them. To improve the security of the telemedicine system in such a situation, it is imperative to develop a real-time data transmission system that can effectively handle the tasks carried out by devices in the telemedicine system. This allows administrators to assess the correctness of the various users' work and remotely monitor the real-time data gathered by the smart sensing devices. However, as stated, the real-time data is shared across a public channel—and is private and sensitive; an attacker accesses the sensitive information about the telemedicine system and makes it public to disturb user privacy and violate its security. A robust and lightweight key agreement scheme must be designed for the telemedicine system to create a secret session key between a chosen wearable or smart sensing device and the telemedicine server—a trustworthy entity installed in the telehealthcare environment. Otherwise, security for such sensitive information cannot be guaranteed. Therefore, this article presents the design of a robust and lightweight authentication protocol named RLKAS-TMS that can effectively alleviate the security and privacy concerns of sensitive medical information over a public network channel.

INDEX TERMS Verifiability, unlinkability, reachability, indistinguishability, confidentiality, vulnerability.

I. INTRODUCTION

It is essential to recognize the condition of using their conceivable for intelligent psychological data gathering in the healthcare system. Wearables can be useful devices for gathering, evaluating, and sharing psychological data at a time when data-driven decision-making is becoming more and more important in medical procedures [1]. This extends beyond the conventional domains of medical records and provides opportunities for a finer understanding of individuals' mental health. Technology may give medical practitioners a thorough and up-to-date perspective by gathering psychological data in an intelligent manner, which facilitates better decision-making. When we consider how this sophisticated data collection helps healthcare providers, the importance of it all becomes clear [2]. Technologies have the potential to significantly improve and expedite patient treatment by providing a multitude of psychological data-derived insights. This data-driven strategy makes it possible to comprehend each patient's demands more precisely and individually [3]. It helps medical practitioners to customize treatment regimens and diagnostics based on a comprehensive understanding of the patient's health. It ushers in a new era of accuracy, effectiveness, and better healthcare provision. The promise of computers to improve healthcare continues to be a symbol of advancement and recognition of the life-changing potential for the field of healthcare in the future as technology advances [4], [5].

In addition, the tremendous influence of technology and the emergence of telemedicine constitute an amazing

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

resource that greatly enhances the worldwide convenience of both individuals and institutions [6]. By utilizing the transformational potential of the Internet, telemedicine makes it possible to access a shared pool of resources on-demand, transforming how data is processed, stored, and made accessible. With the help of this cutting-edge technology, geographical barriers are broken down, resulting in a seamlessly connected world where services and information are easily available from almost anywhere [7]. A new era of more effective and widely accessible data management and cooperation is ushered in by the telemedicine system, which represents a paradigm change. The telemedicine server's shared resources enable people and organizations to save infrastructure costs, improve cooperation across many units, and streamline operations [8]. This revolution in computing represents a major turning point in the history of technology, allowing for a more effective and linked global society in which knowledge can be shared and cooperative projects may work across many skilled individuals [9], [10].

Moreover, there is a lack of qualified healthcare professionals—vital to every human being—and residents in rural and isolated places in the modern world do not have access to high-quality healthcare facilities. Patients in rural regions can now benefit from telemedicine-based systems, which gather patient data through wearables, laboratory diagnosis, and semi-skilled medical professionals. Experienced medical professionals can then access this data from any place and recommend medication to the patients [11]. In short, the sensors, wearable technology, labs, and semi-skilled healthcare practitioners have utilized a wireless channel to accumulate health-related data from various patients. The patient data is disseminated via open channels under this system, which poses numerous threats. Therefore, an appropriate security framework must be implemented on both the sender and the recipient sides to ensure the security of the exchanged sensitive information. Such a system will then benefit the patient by enhancing their quality of life, easily monitoring remotely, reducing labor work in the hospitals, saving time, minimizing costs, decreasing accountability, providing online support, and increasing the degree of trust and reliance on data by the doctors [12].

Researchers have proposed security mechanisms using different cryptographic methods to protect telemedicine platforms in the past decade. However, these schemes have many drawbacks; for example, [13] suffer from brute force and ESL (Ephemeral Secret Leakage) attacks and cannot deliver forward secrecy, [14] have DoS and insider threats, [15] are vulnerable to insider and side-channel attacks, in [16] the physician identity can easily pick by an attacker for impersonating a legitimate doctor, [17], [18], [19] and [20] are suffering from privacy issue, the patient is easily traceable, and cannot resist impersonation attack, [21] is susceptible to brute force and offline password guessing attacks, and [22] is suffering from high computation costs due to modular exponentiation. Therefore, this research aims to secure the telemedicine system to make it worthwhile for patients and healthcare professionals. The major contributions of this research work are as follows:

- To design a protocol by utilizing Elliptic Curve Cryptography (ECC), this is a lightweight, robust, and remotely authenticates the telemedicine system to avail the healthcare facility securely.
- To design a "no-password " based scheme by using secret numbers, keys, random numbers, identities, and hash codes to validate out-of-band and resist brute force and dictionary attacks.
- To check the correctness and mutual authentication of the RLKAS-TMS through the Real-Or-Random Model.
- To scrutinize the secrecy, confidentiality, verifiability, unlinkability, reachability, and indistinguishability of the session secret key through a programming verification toolkit, ProVerif.
- To analyze the RLKAS-TMS informally in confirming that it resists all known attacks.
- To measure the performance metrics by considering storage, communication, and computation costs.
- To comparatively analyze the RLKAS-TMS for security functionalities and performance metrics for lightweightness and robustness.

The rest of the paper is organized as in section II explains the preliminaries and definitions of necessary ideas, section III surveys the literature and defines the problems in the existing work, section IV demonstrates the system architecture, section V designs the RLKAS-TMS, section VI scrutinizes the security of the RLKAS-TMS both formally and informally, section VII measures the performance metrics and comparison of security and performance and in section VIII concludes the research work.

II. FOUNDATION

This section gives a comprehensive explanation of the study's major ideas their concept, and reasoning for performing the completion of this research work. These are briefly explained one by one as under:

A. ROR MODEL

Real-Or-Random (RoR) model originated from [23], sometimes known as a theoretical black box. It is an oracle used in cryptography that uniformly selects a (really) random response from its output domain for each unique query. When a question is asked again, a mathematical function chosen uniformly at random or a function that maps every potential inquiry to a (fixed) random response from its output domain is what is meant to be understood as a random oracle (RoR) model.

B. PROVERIF

This is an automated software verification toolkit [24] used for verifying session key secrecy, integrity, reachability, and authenticity. This widely used toolkit consists of channels, constants, variables, constraints, queries, and functions. This language is based on pi-Calculus and originated from

applied system engineering. A classical formal verification tool for verifying the cryptographic-based security protocol in enabling and discovering attacks, proving security for unbounded messages and sessions.

C. THREAT MODEL

This research adopted the well-known threat model presented by Dolev and Yao [25] and thus named it DY-Model. According to this model, Ạ can learn the identity, extract information from the message exchanged over an open channel, get the key previously computed by the security protocol, and know the long-term secret keys a, and b. Ạ has the power to update, insert, delete, and copy messages communicated over the wireless channel. With the session state and session keys, Ạ discloses the secret credentials in the sessions. Therefore, a user authentication scheme designed for a telemedicine system should ensure that even if Ạ learns about some type of private credential, like session keys or ephemeral secrets; it won't significantly impact the confidentiality of the other credentials. Lastly, it is supposed that the telemedicine server in the medical setting may be secured with a locking mechanism to prevent physical capture by Ạ. As a result, the telemedicine server is regarded as one of the most reliable wireless network technologies.

D. HASH CRYPTOGRAPHIC FUNCTION

This research uses a secure, collision-free, one-way hash cryptographic function [26]. It performs a mathematical operation by transforming an input numerical value into an output numerical value that has been compressed (image of the input numerical values). The cryptographic hash function generates the hash that accepts arbitrary-length inputs, but its result remains fixed. The cryptographic hash function has the following key features:

- The hash image is computationally hard to reverse, thus called a one-way function.
- Finding any input value x that hashes to z should be challenging if a hash function (h) yielded a hash value (z).
- It isn't easy to produce an identical hash of the two distinct inputs, and thus, the hash function named is a collision-free one-way hash cryptographic function.

E. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

This is a type of asymmetric key cryptography based on the curve over the x-axis and y-axis [27] that is defined over a finite field, E/F_q be a curve over F_p and a group of prime number q and a sub-group of E/F_q whereas p and q are two large primes, which satisfy the equation $y^2 = x^3 + ax + b$. Additionally, ECC utilizes an elliptic curve's points, given a 160-bit key size, offers more security than conventional cryptosystems, lower the key length while maintaining the same level of security, and boosts performance.

III. LITERATURE REVIEW

Mir and Nikooghadam [13] used Telemedicine information systems (TMIS) for home healthcare by saying that patient privacy is protected through secure authentication and encryption, while the existing user authentication schemes in TMIS have security vulnerabilities. After that, they presented an improved biometrics-based authentication and key agreement scheme, proven secure and efficient for TMIS. The security of the RLKAS-TMS is verified using the Random Oracles Model (ROM) and BAN logic, while the AVISPA tool is used for formal security analysis of the scheme. The resistance of the RLKAS-TMS against well-known attacks has also been investigated through discussions. However, their scheme doesn't resist brute-force and ESL attacks and cannot deliver perfect forward secrecy. Shufang et al. [28] is focused on analyzing and improving a privacy-preserving authentication scheme for TMIS. They cryptanalyzed the scheme proposed by Yu and Park [29] by saying that their scheme is vulnerable to impersonation, replay, and tracking attacks. It also demonstrated that the Yu and Park [29] scheme is computationally inefficient and does not provide mutual authentication. After that, they [28] proposed a symmetric cryptographic-based authentication scheme using a one-way hash function and XOR operations to design their scheme. However, they failed to analyze their scheme formally and could not simulate it for attack checking.

Zheng et al. [14] said that Telemedicine is rapidly growing due to the increasing demand for medical services. The existing authentication protocols in telemedicine systems have security vulnerabilities. After that, they proposed an improved authentication protocol based on asymmetric cryptography using the MD5 technique to address these vulnerabilities, which offers indistinguishability, forward secrecy, and resists various attacks. Their security and performance analysis sections show that their protocol is efficient and secure. Also, their scheme effectively resists attacks such as retransmission, tracking, eavesdropping, man-in-the-middle, and denial of service. However, they filed to analyze the security of their improved scheme and do not resist DoS and insider attacks.

Li et al. [15] argued that using telecare medical information systems (TMIS) in hospitals is a dire need of the era, while secure authentication can preserve patients' privacy because there are many security weaknesses in the previous authentication protocols—an enhanced version of mutual authentication and privacy preservation protocol is required to mitigate all the known weaknesses. The improved protocol must have the capability to ensure message authentication, patient anonymity, unlinkability, and report confidentiality. Basically, [15] cryptanalyzed the scheme of Mohit et al.'s [30] by saying that their scheme is vulnerable to forgery attacks and patient anonymity and unlinkability are not ensured. However, [15] does not analyze the security of their enhanced protocol, and their scheme is vulnerable to insider and

side-channel attacks, as they do not use time stamps during the verification process.

Amin et al. [16] reviewed and analyzed Das et al. [31] scheme by demonstrating that their claim is baseless and invalid and identifying a design flaw. After that, they proposed a hash cryptographic function-based authentication scheme for telemedicine systems by analyzing their security through AVISPA and Scyther tools and compared the performance. They further discussed the importance of secure electronic health systems by criticizing previous authentication protocols for numerous security weaknesses and their effect on human lives. However, the authentication phase of the protocol consisted of $\{K_p, M_1, ID_k, TID_p, T_1\}$ message having physician identity, which the attacker can eavesdrop on and use for launching impersonation and masquerade attacks.

Dwi et al. [17] demonstrated that telemedicine efficiently distributes health services; it is the future of the health service model, and its implementation requires rigorous security—the available security system is posed to MITM and ESL attacks. So, they have proposed a protocol based on JavaScript Object Notation Remote Procedure Call (JSON-RPC) for communication in the multi-tier system that shows a high service resistance to communication load. However, the privacy of patient-sensitive information is not preserved, and it can easily be traceable.

Son et al. [18] said that in the Telecare medical information system (TMIS) implemented in a wireless body area network (WBAN), a secure authentication process between patient and server is essential, and the limited storage power of wearable devices can be resolved with the cloud computing. Accessing patient data in a controlled manner is critical for quality healthcare. So, they have proposed a protocol that uses a bi-linear paring, blockchain, and CP-ABE (Ciphertext-policy attribute-based encryption) for data integrity and access control. However, in the authentication phase, $\{PK_i, D_i, PID_i, T_1\}$ message consisted of pseudo-identity $PID_i{=}SID_i$ x L_{i1} and the pseudo-identity consisted of patient secret identity SID_i, which the adversary can easily pick the message form the open channel, find out the actual identity and trace out the legitimate patient. Therefore, Son et al. [18] don't resist traceability attacks. The privacy of patients' sensitive information is not preserved.

Lei and Chuang [19] discussed the issue of privacy protection in telecare medicine information systems and the importance of robust authentication and key agreement (AKA) schemes. They argued that the previous schemes did not achieve user anonymity and untraceability and consisted of password tables in which attackers could quickly launch forgery and password update attacks. They have proposed a three-factor authenticated key agreement scheme based on ECC with a biometric fuzzy extractor in providing user anonymity and untraceability, an Online update phase to avoid the involvement of the registration center, and preventing the registration center in the mutual authentication phase. However, in the authentication phase, the first message exchanged between the user and the telemedicine server consisted of DI_D, which is equal to $ID_U + Q_U$ user identity in raw format, in which an attacker can capture from the open channel and launches impersonation and traceability attacks. Also, they have not simulated their scheme for possible attacks using any software toolkit.

Dharminder et al. [20] proposed a Chebyshev chaotic map-based authentication protocol for healthcare telemedicine services using the fuzzy extractor technique. They demonstrated that the existing protocols in the field have vulnerabilities such as password-guess and identity-guess attacks and do not ensure security and anonymity; their communication and computation costs are inefficient. However, the patient's identity in the first message is transmitted openly, which attackers can easily capture from the public channel and violate the privacy of the patient's sensitive information. Therefore, [20] is suffering from privacy and traceability issues.

Ryu et al. [21] expressed their view regarding the importance of TMIS in the recent COVID-19 pandemic; as the sensitive patient data is communicated via an open channel in TMIS, patient privacy is a big challenge; no one guarantees its protection and preserves the privacy of patient sensitive information and shown resistance all known threats. Yupapin et al. [32] proposed a scheme based on the Chebyshev chaotic map method by arguing that a secure authentication protocol for telecare medicine information systems (TMIS) is mandatory, allowing remote access to medical services and a secure exchange of electronic medical records. They have utilized the fractional chaotic maps for secure authentication and never used public server keys and additional messages and rounds for key validation. However, they failed to analyze the security of their Chebyshev chaotic map-based authentication scheme. Also, communication costs have not been measured. Actually [21] revisited the authentication scheme Sahoo et al. [33] proposed and identified vulnerabilities in their scheme, which does not have lower communication costs and better security features. After that, they proposed a scheme based on biometrics using the ECC technique for the telemedicine system consisting of initialization, registration, authentication, and password change phases. However, their scheme does not resist brute force and offline password-guessing attacks.

Ramadan and Raza [22] argued that during the COVID-19 pandemic and other crises, the Telemedicine system efficiently delivers services to the healthcare system through WBANs, WSNs, or IoT. But security and privacy are the major concerns for remote healthcare systems. WBANs consist of wearable sensors for monitoring health conditions and onward transmission to telemedicine servers via an open channel, posing numerous attacks. After that, they proposed a secure framework named WBAN-19 for telemedicine systems during COVID-19. Their scheme can efficiently deliver services to doctors while investigating the

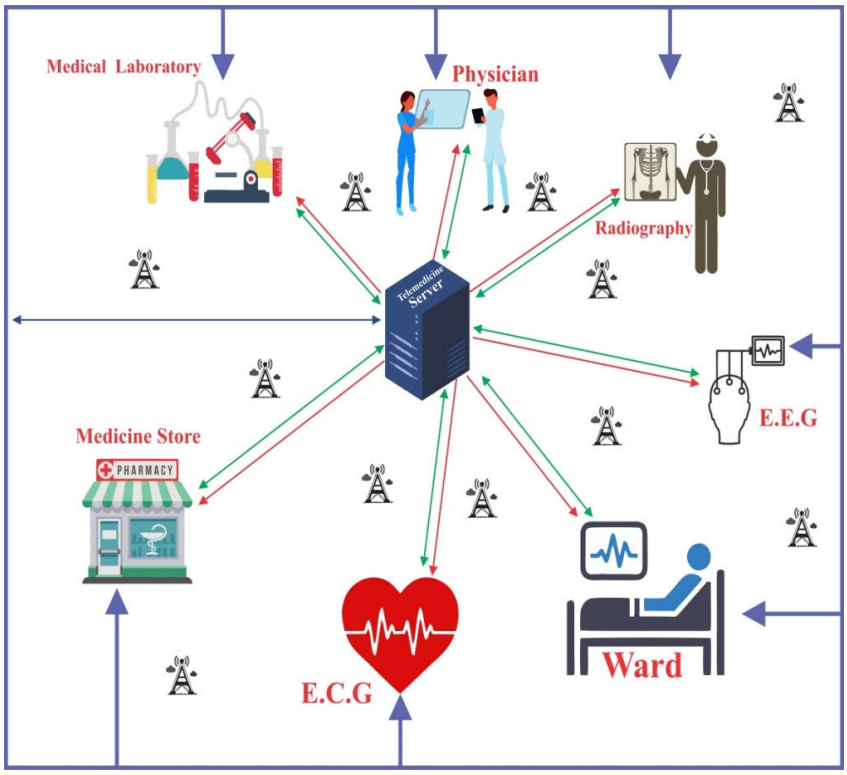

FIGURE 1. System architecture of the proposed security mechanism.

symptoms of COVID-19. They used paring cryptography to design identity-based encryption, equality tests, aggregation, encryption techniques, and the KeyGen method for generating public and private keys. However, they did not analyze the security of their proposed protocol. Also, their proposed security framework suffers from high computation costs due to modular exponentiation.

IV. SYSTEM ARCHITECTURE

The system model mainly consisted of a telemedicine server, and users (Paramedic Staff, Radiology machine, mobile devices used by doctors, Electrocardiogram (ECG), Electroencephalogram (EEG), patient, laboratory, medicine store, etc.) and a telemedicine server as shown in Figure 1. This article demonstrates all the associated entities as sensors, wearable, or simply a user specified in the proposed system model.

A. TELEMEDICINE SYSTEM (TMS)

A few decades back, radios and telephones were the primary forms of communication doctors used while practicing telemedicine. Telemedicine facilities, as known today, did not exist. Usually, telemedicine entailed a physician consulting with a patient over the phone while possibly taking some notes. Telemedicine was a less formal procedure typically reserved for urgent medical situations. These days, telemedicine platforms offer doctors a well-organized, safe way to practice remotely. They can monitor patient health information, share medical information with other doctors for consultation, record all remote patient visits, bill patients, receive payment from outside payers, and much more. The definition and capabilities of telehealth have been greatly enlarged by modern technology, and platforms for telemedicine have undergone major improvements. The telemedicine server provides the following facilities to the healthcare system:

- Remote real-time interactive session with experts for timely and emergency care.
- The communication of health data, laboratory test records, X-rays, MRI, etc., between a patient and doctor securely.
- The embedded sensor collects the physiological information of a patient, stored in a telemedicine server for diagnosis by doctors. Typically, remote monitoring is only for those patients who suffer from some chronic diseases like cardiovascular diseases, asthma, etc.
- Storing medical records of citizens
- Providing telehealth facilities
- mobile health applications
- personalize medicine information
- Wearables facility description

B. TRUSTED AUTHORITY

TA is a crucial component of telemedicine service providers; it oversees organizations that shield patients from health threats, provides a secure work environment for medical staff, and ensures that health initiatives serve public health and welfare. TA creates norms and functions at all levels, ensures

that healthcare organizations and facilities adhere to public health regulations, and offers safe treatment to all patients and system visitors. Thus, TA keeps an eye on private and public healthcare providers and facilities, alerts the government to changes in the healthcare sector's operations, upholds more rigid safety measures, and works to enhance healthcare delivery while adhering to rules.

C. USER (U)

The user is either a patient admitted in the medical ward, a sensor embedded for physiological data collection, or a medical store, physician, radiographer, medical laboratory, or some other paramedical staff member. Anyone who desires to avail of the services of a telemedicine server should be a user. In the proposed system model, a user and telemedicine server are first registered with the trusted authority center, a company, organization, or industry that provides remote telehealth care services. It is worth mentioning that telemedicine and telehealth are the same and are used interchangeably. It will then be operationalized for citizens to provide telehealth care facilities. As stated, the security of patients/labs/doctors, etc., and sensitive information is challenging and needs careful consideration. This article has proposed a security framework for protecting such sensitive data on both the user and telemedicine server sides.

V. PROPOSED KEY AGREEMENT SCHEME

This article section presents the proposed lightweight protocol for telemedicine information systems. The protocol consisted of registration and authentication phases. These phases are described one by one, while the notation used for designing the protocol is shown in Table 1.

TABLE 1. Notations and their descriptions.

Symbols	Meaning
U	User
TMS	Telemedicine Server
$E_q(x, y)$	Elliptic Curve
UK_U	User private Key
a, b	Secret Keys
UK_{TMS}	Session Key (Telemedicine Server)
h(.)	Hash Function
$\oplus$	Bitwise XOR
P	Point on $E_q(x, y)$
ID_U	User Identity
ID_{TMS}	Telemedicine Server Identity
PK_{pub}	Public Key
TS	Timestamp
ΔT	Transmission Delay
$\|$	Concatenation Function
TA	Trusted Authority

A. TELEMEDICINE SYSTEM REGISTRATION

Upon registering the telemedicine system with the trusted authority, the following steps are performed:

Step: 01: The server connected to the trusted authority (TA) chooses a random number $L_{TMS} \in Z_P^*$ and ID_{TMS}, compute: $PK_{Pub1}=L_{TMS}.P$ and sends $\{ID_{TMS}, PK_{Pub1}\}$ message towards the TA, over a secure channel.

Step 2: On receiving $\{ID_{TMS}, PK_{Pub1}\}$ message, the TA chooses $M_{TA}\} Z_P^*$, ID_{TA}, computes $PK_{TA}=M_{TA}.P$, $PK_{Pub2}=PK_{Pub1}+PK_{TA}$ stores $\{ID_{TMS}, PK_{Pub2}\}$ and sends $\{ID_{TA}, PK_{Pub2}, M_{TA}, PK_{TA}\}$ message back towards the telemedicine server.

Step 3: The telemedicine server upon receiving $\{ID_{TA}, PK_{Pub2}, M_{TA}, PK_{TA}\}$ message, computes $UK_{TMS}=(L_{TMS}+M_{TA})$ mod P, $PK_{Pub2}=UK_{TMS}$, $PK_{Pub3}=UK_{TMS}.PK_{TA}$, and stores $\{ID_{TMS}, UK_{TMS}, PK_{TA}, ID_{TA}, PK_{Pub3}\}$ in its memory as shown in module I.

TMS	TA
Choose $L_{TMS} \in Z_P^*$ and ID_{TMS}	
Compute: $PK_{Pub1}=L_{TMS}.P$	
$\{ID_{TMS}, PK_{Pub1}\}$ →	
	Choose $M_{TA} \in Z_P^*$ and ID_{TA}
	Compute: $PK_{TA}=M_{TA}.P$
	$PK_{Pub2}=PK_{Pub1}+PK_{TA}$
	Store: $\{ID_{TMS}, PK_{Pub2}\}$
← $\{ID_{TA}, PK_{Pub2}, M_{TA}, PK_{TA}\}$	
$UK_{TMS}=(L_{TMS}+M_{TA})$ mod P	
$PK_{Pub2}?=UK_{TMS}$	
$PK_{Pub3}=UK_{TMS}.PK_{TA}$	
Stores $\{ID_{TMS}, UK_{TMS}, PK_{TA}, ID_{TA}, PK_{Pub3}\}$	

MODULE 1. Telemedicine registration phase.

B. USER REGISTRATION

This phase is taking the following steps:

Step 1: The user chooses a large random number $L_U \in Z_P^*$ identity ID_U, computes $PK_{Pub1}=L_U.P$ and sends $\{ID_U, PK_{Pub1}\}$ message towards TA over a secure channel.

Step 2: Upon receiving $\{ID_U, PK_{Pub1}\}$ message the TA also chooses $M_{TA} \in Z_P^*$ identity ID_{TA}, computes $PK_{TA}=M_{TA}.P$, $PK_{Pub2}=PK_{Pub1}+PK_{TA}$, stores $\{ID_U, PK_{Pub2}\}$ and sends $\{ID_{TA}, PK_{Pub2}, M_{TA}, PK_{TA}\}$ message back to the user.

Step 3: When receiving $\{ID_{TA}, PK_{Pub2}, M_{TA}, PK_{TA}\}$ message, the user computes $UK_U=(L_U+M_{TA})$ mod P, confirms $PK_{Pub2}?=UK_U$ calculates $PK_{Pub3}=UK_U.PK_{TA}$ and stores Stores $\{ID_U, UK_U, PK_{TA}, ID_{TA}, PK_{Pub3}\}$ as shown in Module II.

U	TA
Choose $L_U \in Z_P^*$ and ID_U	
Compute: $PK_{Pub1}=L_U.P$	
$\{ID_U, PK_{Pub1}\}$ →	
	Choose $M_{TA} \in Z_P^*$ and ID_{TA}
	Compute: $PK_{TA}=M_{TA}.P$
	$PK_{Pub2}=PK_{Pub1}+PK_{TA}$
	Store: $\{ID_U, PK_{Pub2}\}$
← $\{ID_{TA}, PK_{Pub2}, M_{TA}, PK_{TA}\}$	
$UK_U=(L_U+M_{TA})$ mod P	
$PK_{Pub2}?=UK_U$	
$PK_{Pub3}=UK_U.PK_{TA}$	
Stores $\{ID_U, UK_U, PK_{TA}, ID_{TA}, PK_{Pub3}\}$	

MODULE 2. User registration phase.

U	TMS
Choose $a \in Z_P^*$, record T_U	
Compute: $Q_1=a.PK_{Pub2}$	
$Q_2=E_{UKu}(ID_U \oplus Q_1)$	
$Q_3=h(PK_{Pub3}\|\|T_U\|\|ID_U\|\|Q_1)$	
$\{Q_1, Q_2, Q_3, T_U\}$ →	
	Get ID_U by decrypting $D_{PKpub3}(ID_U)=UK_{TMS}.Q_1$
	Compute: $Q_4=UK_{TMS}.Q_1$
	$Q_3^*=h(PK_{Pub3}\|\|T_U\|\|ID_U\|\|Q_1)$
	Confirm: $Q_3^*?=Q_3$
	Choose: $b \in Z_P^*$, record T_{TMS}
	Compute: $Q_5=b.PK_{Pub1}$
	$Q_6=b.Q_4$
	$SK_{TMS}=h(ID_{TMS}\|\|ID_U\|\|Q_5\|\|Q_6)$
	$Q_7=h(PK_{Pub3}\|\|T_{TMS}\|\|ID_{TMS}\|\|SK_{TMS})$
← $\{Q_4, Q_6, Q_7, T_{TMS}\}$	
Compute: $Q_6^*=(a.PK_{Pub3} \bmod P).\ Q_5$	
Confirm: $Q_6^*?=Q_6$	
$SK_U=h(ID_U\|\|ID_{TMS}\|\|Q_5\|\|Q_6^*)$	
$Q_7^*=h(PK_{Pub3}\|\|T_{TMS}\|\|ID_{TMS}\|\|SK_U)$	
Confirm: $Q_7^*?=Q_7$	
Keep SK_{TMS}, SK_U as session secret key	

MODULE 3. **Key agreement phase.**

C. KEY AGREEMENT PHASE

This is the most important phase of the protocol in which a user which is either a physician, radiography, sensors, wearables, medial stores, laboratory or any other facility provided by the owner of telemedicine system. This phase is accomplished in the following steps:

Step 1: The user chooses a random number $a \in Z_P^*$, record T_U, computes $Q_1=a.PK_{Pub2}$, encrypts $Q_2=E_{UKu}(ID_U \oplus Q_1)$, $Q_3=h(PK_{Pub3}||T_U||ID_U||Q_1)$ and sends $\{Q_1, Q_2, Q_3, T_U\}$ message towards the telemedicine server over an insecure channel.

Step 2: When the telemedicine server received $\{Q_1, Q_2, Q_3, T_U\}$ message, confirm identity by descripting Q_2 using PK_{pub3} $D_{PKpub3}(ID_U)=Q_1 \oplus Q_2$, computes $Q_4=UK_{TMS}.Q_1$, $Q_3^*=h(PK_{Pub3}||T_U||ID_U||Q_1)$, confirms $Q_3^*?=Q_3$, if couldn't validated, the process is terminated, and deny message displayed to the user. While for a successful confirmation, the telemedicine server also chooses a random number $b \in Z_P^*$, record T_{TMS}, computes $Q_5=b.PK_{Pub1}$, $Q_6=b.Q_4$, $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$, $Q_7=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS})$ and sends $\{Q_4, Q_6, Q_7, T_{TMS}\}$ message back to the user over a public channel.

Step 3: The user when receiving $\{Q_4, Q_6, Q_7, T_{TMS}\}$ message, computes $Q_6^*=(a.PK_{Pub3} \bmod P).\ Q_5$, confirms $Q_6^*?=Q_6$, if couldn't validated, the process is terminated and deny message displayed to the user, otherwise, computes $SK_U=h(ID_U||ID_{TMS}||Q_5||Q_6^*)$, $Q_7^*=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_U)$ and again confirms $Q_7^*?=Q_7$, if doesn't confirmed, the process termination take place, otherwise, keeps SK_{TMS}, SK_U as session secret key as shown in module III, and diagrammatically is shown in Figure 2.

VI. SECURITY ANALYSIS

The security analysis of the proposed ECC-based security mechanism can be tested through worldwide techniques of the Real-Or-Random (RoR) model [23], ProVerif [24] simulation, and attacks discussion. These are explained one by one as follows:

A. ROR ANALYSIS

The nomenclature of RoR is shown in Table 2.

Proof: The protocol P consisted of two main entities, U and TMS which were actively involved in the authentication phase. The adversary Ą action is explained as follows:

- ***Execute***$(\prod_i^t, \prod_i^j)$ **:** In this query, the adversary Ą launches an eavesdropping attack on the exchanged message between two legitimate entities.
- ***Send***$(\prod_i^t, m)$**:** Ą sent m to P and receives a response.
- ***Corrupt***$(\prod_i^U)$**:** Ą launches this attack on U to get something beneficial, and the output should be recorded.
- ***Test***$(\prod_i^t)$**:** This query can simulate the session key SK between U and TMS by following the indistinguishability feature via the RoR model in which the adversary Ą can flip a coin if got 1-win (compute SK), 0-lose (not compute SK) and $\perp$ (null).

Let's suppose $\prod_i^U$ and $\prod_j^{TMS}$ are the i^{th} and j^{th} participants of U and TMS and $\prod^t$ is said to be the accepted state of P, then, Ą runs the following queries for fabricating P.

TABLE 2. ROR nomenclature.

Participants	n-participants denoted by G={G_1, G_2, ……., G_n}
Protocol	P
Adversary	Ą
Hash Queries	q_E, q_S, and q_H
Oracles of each participant	i-instances
Polynomial numbers	n, i
$\prod_i^t j$	t^{th} protocol running on entity j
$SK_i^t j$	Accept state
Length for a hash function	L_H
Length of hash for another transcript in Ƥ	$n = 2^{lh}$
Advantage with Ą in breaking P	$Adv_{Ą}^{P}$
Success Rate with A in entering P with polynomial attempts i	$Sus_{Ą}^{i}$
L_i	Outgoing information from G_i
M_j	Outgoing information from G_2
$ES - Reveal \prod_i^t j$	Ą obtains ephemeral secret of G_1
$PK_{Pub1} - Replace \prod_i^t j$	Ą replaces public key of G_1
$PK_{Pub2} - Reveal \prod_i^t j$	Ą available for the public key of G_2
$PK_{Pub3} - Reveal \prod_i^t j$	Ą available for the public key of G_3
$UK_{SN} - Reveal \prod_i^t j$	Ą get the secret key of G_1
$UK_{TMS} - Reveal \prod_i^t j$	Ą get the secret key of G_2
$UK_{SN} - Reveal \prod_i^t j$	Ą get nothing (⊥)
$Send(\prod_i^t j, M)$	Ą-sending M to G_1 in session $\prod_i^t j$
$Test(\prod_i^t j)$	Ą-flipping a coin 1-succeeded, 0-lose
$\prod_i^t j$ and $\prod_j^t i$=Identifier	Session matching occur
$\prod_i^t j$ = Accepted	Ą SK

- ✓ ***Execute***$(\prod_i^U, \prod_j^{TMS})$Ą launches snooping/eavesdropping attack by implementing Execute (·) query on {Q_1, Q_2, Q_3, T_U} and {Q_5, Q_6, Q_7, T_{TMS}} messages transmitted among U and TMS.
- ✓ ***Enc/Dec*** $(\prod_i^U$***, M, CT):***Ą uses Enc function to encrypt M form CT and uses Dec function to decrypt CT into regional M.
- ✓ ***Reveal*** $(\prod^t)$***:***Ą while running this query gets SK computed by P on instance t.
- ✓ **Send** $(\prod^t$**, M):**Ą applies this query on {Q_1, Q_2, Q_3, T_U} message or {Q_5, Q_6, Q_7, T_{TMS}} message in acting as man-in-the-middle attack. Suppose the message denies Ą role as an active attacker. In that case, it means the transmission over an open network channel is not revealed to anyone; otherwise, the reply of Ą should be acknowledged to the simulator.
- ✓ **Corrupt** $(\prod^t)$**:**Ą inserting something new in the stored credentials for checking the forward secrecy, if all the corresponding credentials become changed, then forward secrecy is successful, else, Ą successfully disturbed/corrupt the stored parameters of U and TMS. Ą uses power analysis [34], statistical measurement of consumed power [35], and reverse engineering [36] techniques to reveal the real identity, which later on he/she will use for impersonation, masquerading, and eavesdropping attacks.
- ✓ ***Test*** $(\prod^t)$***:***Ą uses this query for establishing session with P and the output get either be correct session key or not, Ą flips a coin, if got 1-Win, 0-Lose, ⊥-Null.
- ✓ ***Partnering:*** $\prod_i^U$ and $\prod_j^{TMS}$ are said to be partners of each other if they are in an accepted state and mutually authenticate each other.
- ✓ ***Freshness:*** If the share session secret key between $\prod_i^U$ and $\prod_j^{TMS}$ is not compromised by Ą, then it means the $\prod^t$ is treated as fresh, else, outdated SK can easily be identified and Ą reaches many secret credentials via reverse engineering technique [36]. This also means that if the backward secrecy is not preserved, then Ą can easily find any secret credentials from the previous session key.
- ✓ ***Semantic Security:*** Let Ą runs ***Test*** $(\prod^t)$ interferes P by n (polynomial) attempts, Ą has the following advantage in breaking P:

$$Adv_{Ą}^{\mathcal{P}} \leq \frac{(q_S + q_E)^2}{n} + \frac{q_H^2}{2^{l_h}} + 2Adv_{Ą}^{\text{ECC}} \tag{1}$$

For Real Attack:

$$Adv_{Ą}^{\mathcal{P}} = \left|2\Pr\left[Sus_{Ą}^{0}\right] - 1\right| \tag{2}$$

For Execute(·) ***and Test***(·) ***Queries***

$$\Pr\left[Sus_{Ą}^{1}\right] = \Pr\left[Sus_{Ą}^{0}\right] \tag{3}$$

For Session Key:

$$\Pr\left[Sus_{\text{A}}^{2}\right] - \Pr\left[Sus_{\text{A}}^{1}\right] = Adv_{\text{A}}^{\text{ECC}} \tag{4}$$

For Hash Collision: As per birthday paradox [37], the chances of collision are $\frac{q_H^2}{2^{l_h+1}}$. The hash collision probability for another tuple is $\frac{(q_S+q_E)^2}{2n}$.

$$\Pr\left[Sus_{\text{A}}^{3}\right] - \Pr\left[Sus_{\text{A}}^{2}\right] \leq \frac{(q_S+q_E)^2}{2n} + \frac{q_H^2}{2^{l_h+1}} \tag{5}$$

For Random number Guessing:

$$\Pr\left[Sus_{\text{A}}^{3}\right] = \frac{1}{2} \tag{6}$$

Eq: (2)-(6), the result obtained as:

$$\frac{1}{2}Adv_{\text{A}}^{\text{P}} \leq \frac{(q_S+q_E)^2}{2n} + \frac{q_H^2}{2^{l_h+1}} + Adv_{\text{A}}^{\text{ECC}} \tag{7}$$

$$Adv_{\text{A}}^{\text{P}} \leq \frac{(q_S+q_E)^2}{n} + \frac{q_H^2}{2^{l_h}} + 2Adv_{\text{A}}^{\text{ECC}} \tag{8}$$

B. PROVERIF SIMULATION

For checking the session's key secrecy, integrity, and reachability, ProVerif is used. Firstly, declare two channels namely private and public, and then all the constants, variables, constraints, queries, and functions were declared. Secondly, the U-side, TA-side, and TMS-side computation steps were coded. Running the code using the process statement, the verification result will be displayed which shows that the attacker cannot reveal any identity, credentials, and session secret key SK is SAFE from the attacker as given below:

Verification summary:
Query inj-event(endTMS(IDTMS)) ==> inj-event(startTMS(IDTMS)) is true.
Query inj-event(endUser(IDU)) ==> inj-event(startUser(IDU)) is true.
Query inj-event(endTA(IDTA)) ==> inj-event(startTA(IDTA)) is true.

Query not attacker(s[]) is true.

C. INFORMAL SECURITY ANALYSIS

This section discusses different attacks and security functionalities for the proposed authentication scheme informally, as given:

1. Insider threat: The proposed protocol is without a password; the user cannot enter any password in the registration phase. In the registration phase, the user selects a large random number $L_U \in Z_P^*$ identity ID_U, computes $PK_{Pub1}=L_U.P$ and sends $\{ID_U, PK_{Pub1}\}$ message towards the trusted authority over a secure channel. So, the insider threat is invalid for the RLKAS-TMS. Also, the proposed security mechanism is useful for LedgerDB [43] and VeDB [44] strongly which is deployed n a cloud-based e-healthcare system

2. Replay Attack: The first message transmitted between user and server is {Q_1, Q_2, Q_3, T_U}, whereas $Q_1=a.PK_{Pub2}$, $Q_2=E_{UKu}(ID_U+Q_1)$, $Q_3=h(PK_{Pub3}||T_U||ID_U||Q_1)$. So, the attacker could not find anything from the first message. Similarly, the second message between server and user is {Q_5, Q_6, Q_7, T_S} whereas $Q_5=b.PK_{Pub1}$, $Q_6=b.Q_4$, $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$, $Q_7=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS})$, again attacker could not find anything from this message. As these messages contains a large random numbers $a \in Z_P^*$ and $b \in Z_P^*$, timestamps T_U, and T_S and is without a verification table. So, a replay attack is invalid for the RLKAS-TMS.

3. DoS Attack: Due to the confirmation of $Q_3^*?=Q_3$ at the server side and $Q_6^*=Q_6$ at the user side, any illegal attempt of an attacker could be denied because an attacker cannot validate these random checks at both sides. Also, if an attacker desires to launch a DoS attack, he/she has to pass through these computation steps $Q_5=b.PK_{Pub1}$, $Q_6=b.Q_4$, $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$, $Q_7=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS})$ at server side and confirming $Q_7^*=Q_7$ which absolutely impossible for him/her to compute. Therefore, a DoS attack is invalid for the RLKAS-TMS.

4. Impersonation Attack: In the mutual authentication phase, the user takes a large random number $a \in Z_P^*$, records timestamp T_U and computes $Q_1=a.PK_{Pub2}$, $Q_2=E_{UKu}(ID_U+Q_1)$, $Q_3=h(PK_{Pub3}||T_U||ID_U||Q_1)$ and sends {Q_1, Q_2, Q_3, T_U}. The attacker cannot compute such a big message to impersonate the server. Similarly, the server side chooses another large number $b \in Z_P^*$, records T_{TMS}, and computes $Q_5=b.PK_{Pub1}$, $Q_6=b.Q_4$, $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$, $Q_7=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS})$, and sends {$Q_5$, Q_6, Q_7, T_{TMS}} which the attacker cannot compute such a big message for impersonating a legitimate user. Therefore, an impersonation attack is invalid for the RLKAS-TMS.

5. Key Secrecy: Assume the server's private key is compromised; still, the attacker cannot compute the session keys. The adversary must be aware of the user's identity ID_U, server secret key UK_{TMS} and user private key UK_U to compute the session key $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$ or $SK_U=h(ID_{TMS}||ID_U||Q_5||Q_6)$ whereas $Q_5=b.PK_{Pub1}$, $Q_6=b.Q_4$, $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$, $Q_7=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS})$ and $Q_4=UK_{TMS}.Q_1$, $Q_1=a.PK_{Pub2}$. The session key is also not obtained because the attacker requires the private argument of server $b \in Z_P^*$ and user $a \in Z_P^*$. Thus, the suggested approach provides key secrecy.

6. Anonymity: The message transmitted between user and server is {Q_1, Q_2, Q_3, T_U} whereas $Q_1=a.PK_{Pub2}$, encrypts $Q_2=E_{UKu}(ID_U \oplus Q_1)$, $Q_3=h(PK_{Pub3}||T_U||ID_U||Q_1)$, the attacker could not find anything from the publicly transmitted message between user and server. Similarly, the message transmitted between the server and the user is {Q_4, Q_6, Q_7, T_{TMS}} whereas $Q_5=b.PK_{Pub1}$, $Q_6=b.Q_4$, $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$, $Q_7=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS})$ which the attacker again cloud not find anything from the publicly transmitted message between the server and user. An attacker cannot find the identity, so the RLKAS-TMS strongly provides anonymity to the user.

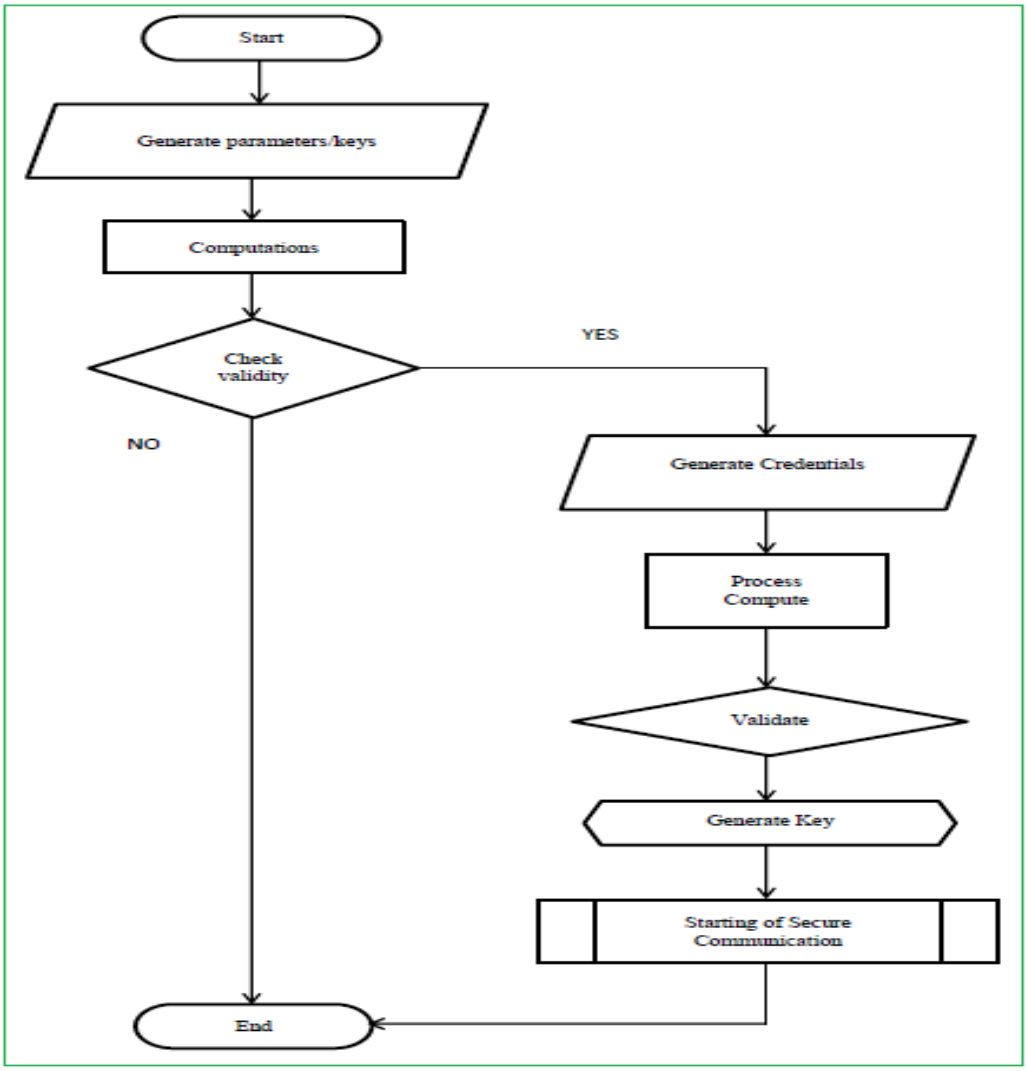

FIGURE 2. Flowchart representation of the proposed security system.

7. Tracking Attack: The identification is not communicated in raw format over a public channel; rather, it is encrypted before being sent to the server, {Q_1, Q_2, Q_3, T_U} whereas Q_1=a.PK_{Pub2}, encrypts Q_2=E_{UKu}($ID_U \oplus Q_1$), Q_3=h($PK_{Pub3}||T_U||ID_U||Q_1$), making it impossible for an attacker to decipher the identity in the initial communication. In a similar vein, the identity in the second message is closely restricted by the public key, secret key, and 160 bits of the ECC key i.e., {Q_4, Q_6, Q_7, T_{TMS}} whereas Q_5=b.PK_{Pub1}, Q_6=b.Q_4, SK_{TMS}=h($ID_{TMS}||ID_U||Q_5||Q_6$), Q_7=h($PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS}$). As a result, the tracking attack does not work with the suggested protocol.

8. Session Key Disclosure Attack: In order to access the session key SK_U or SK_{TMS}, an attacker needs to get hold of the two sets of random numbers a $\in Z_P^*$ and b $\in Z_P^*$. However, the private credentials a$\in Z_P^*$and b$\in Z_P^*$, UK_U and UK_{TMS}, which is SK_{TMS}=h($ID_{TMS}||ID_U||Q_5||Q_6$) as well as the 160-bit public keys PK_{Pub3} and PK_{Pub2} are tightly bound with XOR and hash functions conceal the numbers that are chosen at random. These parameters are not accessible to the attacker. As a result, any illegal attacker's plan to steal the session secret key is safe against harming the key secrecy.

9. Mutual Authentication: After receiving the first {Q_1, Q_2, Q_3, T_U} message, the server calculates Q_4=UK_{TMS}.Q_1, Q_3^*=h($PK_{Pub3}||T_U||ID_U||Q_1$), confirms Q_3^*?=Q_3, if couldn't validated, the process is terminated, and deny message displayed to the user. While for a successful confirmation, the telemedicine server also chooses a random number b$\in Z_P^*$, record T_{TMS}, computes Q_5=b.PK_{Pub1}, Q_6=b.Q_4, SK_{TMS}=h($ID_{TMS}||ID_U||Q_5||Q_6$), Q_7=h($PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS}$) and sends {$Q_4$, Q_6, Q_7, T_{TMS}} message to the user. The user when receiving the second {Q_4, Q_6, Q_7, T_{TMS}} message, calculates Q_6^*=(a.PK_{Pub3} mod P). Q_5, confirms Q_6^*?=Q_6, if couldn't validated, the process is terminated and deny message displayed to the user, otherwise, computes SK_U=h($ID_U||$

$ID_{TMS}||Q_5||Q_6^*$), $Q_7^*=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_U)$ and again confirms $Q_7^*?=Q_7$, if not validated, the process is stopped, otherwise keeps SK_{TMS} and SK_U as session secret key. This means that the participants are mutually authenticated with each other in the RLKAS-TMS.

10. MITM Attack: Although an attacker cannot obtain the large random integers $a\in Z_P^*$ and $b \in Z_P^*$ true identities ID_U and ID_{TMS}, or the secret keys UK_U, UK_{TMS} that is shared between user and server, he/she is unable to produce the authentication messages and session key. Because the attacker cannot access any participant's confidential information, our security framework is shown to be resistant to MITM attempts.

11. Unlinkability: All messages transmitted over the public network channel in the RLKAS-TMS are dynamically renovated and are tightly bound with session keys, secret keys, and random numbers. As a result, there is no fixed information in the messages communicated among participants, so the RLKAS-TMS guarantees the unlinkability of the user.

12. Data Verifiability: A consolidated ledger database with quick verification times and robust external auditability are the leading problems with LedgerDB and VeDB. Yang et al. [42] provided a fantastic solution for mitigating the issue of auditability and strong authentication of centralized storage. As with utilizing a centralized telemedicine server, upon registering with the system, each user stored the hash of data for record, which is tightly bound with random numbers, secret keys, and ECC keys while its copy is already available in the telemedicine server. Suppose an attacker struggles to enter the server and alters or forges the data from the telemedicine server. In that case, each user can use the data hash to determine whether the health records are corrupted. For this reason, data verifiability is enabled by the RLKAS-TMS.

13. Forgery Attack: If an attacker wants to send a message to the server, he/she has to calculate $Q_1=a.PK_{Pub2}$, encrypts $Q_2=E_{UKu}(ID_U\oplus Q_1)$, $Q_3=h(PK_{Pub3}||T_U||ID_U||Q_1)$ and build $\{Q_1, Q_2, Q_3, T_U\}$ message which is not possible, as it contains user secret values UK_U, user identity ID_U and timestamp T_U. So, an attacker cannot know these secret credentials. Similarly, from the server side, if an attacker desires to create $\{Q_4, Q_6, Q_7, T_{TMS}\}$ message, he/she has to calculate $Q_4=UK_{TMS}.Q_1$, $Q_3^*=h(PK_{Pub3}||T_U||ID_U||Q_1)$, confirms $Q_3^*?=Q_3$, if couldn't validated, the process is terminated, and deny message displayed to the user. While for a successful confirmation, the telemedicine server also chooses a random number $b\in Z_P^*$, record T_{TMS}, computes $Q_5=b.PK_{Pub1}$, $Q_6=b.Q_4$, $SK_{TMS}=h(ID_{TMS}||ID_U||Q_5||Q_6)$, $Q_7=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS})$, which is not possible, suppose he/she is succeeded and validated $Q_3^*?=Q_3$, then he/she has to Compute $Q_6^*=(a.PK_{Pub3} \bmod P)$. Q_5, confirms $Q_6^*?=Q_6$, validates, computes $SK_U=h(ID_U||ID_{TMS}||Q_5||Q_6^*)$, $Q_7^*=h(PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_U)$ and can confirm $Q_7^*?=Q_7$ which is impossible. Therefore, a forgery attack is invalid for the RLKAS-TMS.

VII. PERFORMANCE EVALUATION

The performance metrics can be measured using storage, communication, and computation costs. Storage and processing limitations exist with the user-side devices, wearables, sensors, and related peripherals. To determine if the RLKAS-TMS approach can be executed on user-side devices in a suitable amount of time, it is necessary to count the total number of cryptographic and mathematical operations in the protocol. The proposed procedure is often implemented between two parties: a telemedicine system can represent one party, and a user can represent the other. The activities include a symmetric encryption function, hash function, message authentication, random number generator, encryption, decryption, ECC point multiplication, point addition, public keys, and an ECC-based private key. These are described one by one as follows:

A. STORAGE COSTS ANALYSIS

The storage costs are basically measured by looking at the parameters that are kept in the user's memory and on the telemedicine server during the registration process. Numerous parameters affect storage costs, such as random numbers, private keys, identities, hash images and mediums used, how frequently the data is accessed, and the degree of redundancy necessary. The cost of keeping unstructured data remains a significant concern for many protocols as the volume of credentials created can affect the storage costs. Therefore, to achieve this, the Table 3 represents the storage costs for the RLKAS-TMS, according to [38] and [39], the storage costs for different /credentials are as follows:

- ECC key is 160 bits
- Encryption/Decryption takes 192 bits of space
- Identity occupies 64 bits of space
- Random numbers 160 bits in length
- The timestamp is 32 bits in length
- Secret Key is 60 bits in size

TABLE 3. Storage overheads analysis.

Participant	Stored Parameters	Costs
TA	$\{ID_{TMS}, PK_{Pub2}\}$, $\{ID_U, PK_{Pub2}\}$	448
TMS	$\{ID_{TMS}, UK_{TMS}, PK_{TA}, ID_{TA}, PK_{Pub3}\}$	508
U	$\{ID_U, UK_U, PK_{TA}, ID_{TA}, PK_{Pub3}\}$	508
	Total Storage Costs in Bits	**1464**

The Table 3 demonstrated that trusted authority (TA) stored $\{ID_{TMS}, PK_{Pub2}\}$ credentials for the telemedicine server and $\{ID_U, PK_{Pub2}\}$ for the user. As stated above, any identity occupies 64-bit memory space; the ECC key is 160-bit, so the total costs are 448 bits.

The different parameters stored in the telemedicine server are $\{ID_{TMS}, UK_{TMS}, PK_{TA}, ID_{TA}, PK_{Pub3}\}$. In contrast, the private key occupies 60 bits, so the total costs for the telemedicine server are 508 bits. Finally, the user stored $\{ID_U, UK_U, PK_{TA}, ID_{TA}, PK_{Pub3}\}$ credentials with costs of 508 bits

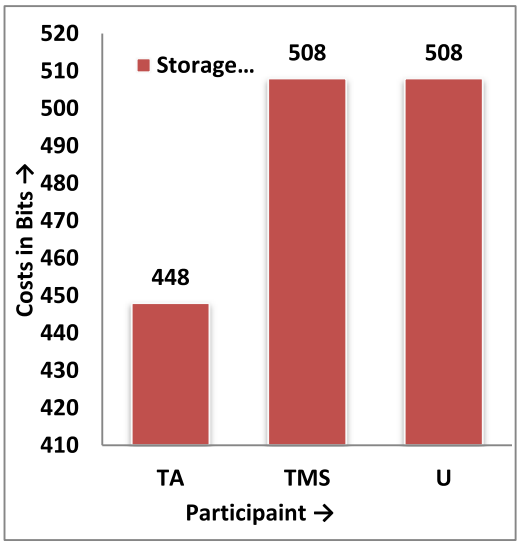

FIGURE 3. Storage overheads analysis.

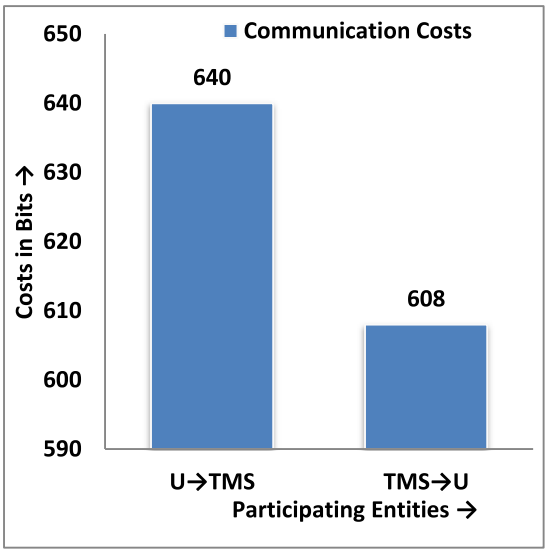

FIGURE 4. Communication costs analysis.

and the total storage costs for the RLKAS-TMS are 1464 bits and diagrammatically, the storage cost is plotted in Figure 3.

B. COMMUNICATION COSTS ANALYSIS

The messages exchanged in the key-agreement phase of the RLKAS-TMS are shown in Table 4, according to [39] and [40], the costs for the different parameters exchanged among participants are as follows:

- Hash Cryptographic Function is 256 bits
- ECC key is 160 bits
- Encryption/Decryption takes 192 bits of space
- The timestamp is 32 bits in length
- Private Key occupies 60 bits of space
- Identity is 64 bits in size
- Timestamp occupies 32 bits of space

TABLE 4. Communication costs analysis.

Participant	Message Exchanged	Values	Costs
U→TMS	$\{Q_1, Q_2, Q_3, T_U\}$	160+192+256+32	640
TMS→U	$\{Q_4, Q_6, Q_7, T_{TMS}\}$	160+160+256+32	608
	Total Communication Costs in Bits		**1248**

Table 4 illustrates that the message exchanged between a user and the telemedicine server is $\{Q_1, Q_2, Q_3, T_U\}$, whereas Q_1=a.PK_{Pub2}, encrypts Q_2=$E_{UKu}(ID_U \oplus Q_1)$, Q_3=h($PK_{Pub3}||T_U||ID_U||Q_1$) which means in Q_1 the ECC key is computed which is 160 bits in size, in Q_2 encryption is made through private key which is 192 bits weight, and Q_3 is the hash image, which is 256 bits. So, the commutative cost of the first message exchanged between a user and the telemedicine server is 640 bits.

Similarly, the message transmitted between a telemedicine server and the user is $\{Q_4, Q_6, Q_7, T_{TMS}\}$ whereas Q_5=b.PK_{Pub1}, Q_6=b.Q_4, SK_{TMS}=h($ID_{TMS}||ID_U||Q_5||Q_6$), Q_7=h($PK_{Pub3}||T_{TMS}||ID_{TMS}||SK_{TMS}$) in which Q_5 and Q_6 are ECC key of size 160 bits, Q_7 is a fixed-length hash image of size 256 bits and timestamp T_{TMS} is 32 bits size, so the commutative costs of the 2nd message exchanged between a telemedicine server and the user are 608 bits; in comparison, the total communication cots of the RLKAS-TMS are 1248 bits and is plotted in Figure 4.

TABLE 5. Computation costs analysis.

Peer	Different Operations	Values	Costs
U	$3T_X+1T_+ +1T_m+1T_{ed}+3T_h$	3(2.226)+0.262+0.539+0.0046+3(0.0023)	7.491
S	$3T_X+1T_+ +1T_m+1T_{ed}+3T_h$	3(2.226)+0.262+0.539+0.0046+3(0.0023)	7.491

TABLE 6. Comparative analysis (performance metrics).

Scheme → / Performance Metrics↓	[18]	[21]	[30]	[33]	[41]	RLKAS-TMS
Communication Costs in Bits	3456	1472	5312	1792	1328	1248
Computation Costs in Milliseconds	41.459	407.95	208.6	178.1	77.6	14.982

C. COMPUTATION COSTS ANALYSIS

It is necessary for the user to register with the TA if they wish to use the services of a telemedicine server with whom they are not yet enrolled. To utilize all the services of the telemedicine system, the user must register with the trusted authority (TA) once, according to our protocol. As a result, our protocol provides additional security features and greater ease. According to [40], the different execution times obtained from an experiment while using an Intel CPU of size 2.20GHz, 2GB RAM, and 32-bit Ubuntu OS, the execution time for different cryptographic operations are shown as follows:

- T_X represents the execution time for ECC point multiplication ≈2.226 ms
- T_+ represents the execution time for ECC point addition ≈0.262 ms

TABLE 7. Comparative analysis (security functionalities).

Scheme → / Security Functionalities ↓	[18]	[21]	[30]	[33]	[41]	RLKAS-TMS
A-Man-in-the-Middle Attack	√	x	x	x	x	x
B-DoS Attack	√	x	√	√	x	x
C-Replay Attack	x	√	x	x	√	x
D-Insider Attack	x	x	√	√	x	x
E-Spoofing Attack	x	√	v	x	x	x
F-Forgery Attacks	x	x	√	x	x	x
G-Traceability Attack	√	√	√	x	x	x
H-Brute Force Attack	x	√	x	√	x	x
I-Stolen-Verifier Attack	x	x	x	x	x	x
J-Password Guessing Attack	x	√	x	x	x	x
K-Anonymity violation	√	x	x	√	x	x
L-ESL Attack	v	x	√	x	√	x

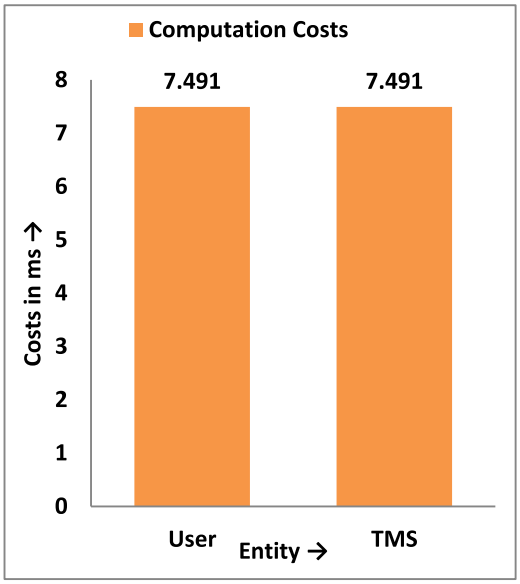

FIGURE 5. Computation costs analysis.

- T_{rm} represents the execution time for random number generation ≈0.539 ms
- T_{ed} represents the execution time for symmetric encryption/decryption ≈0.0046 ms
- T_h represents the execution time for collision-free one-way hash cryptographic function ≈ 0.0023 ms

For the RLKAS-TMS, the cumulative computation costs for the different cryptographic operations like point multiplication, addition, encryption/decryption, random number generation, and hash function are shown in Table 5 and are plotted in Figure 5.

D. COMPARATIVE ANALYSIS

Upon comparing the RLKAS-TMS with state-of-the-art works, it has been demonstrated that the proposed scheme is better in terms of performance metrics and security functionalities against its competitors. In terms of performance metrics, the result is shown in Table 6 and plotted in Figures 6 and 7, respectively. The communication cost of Son et al. [18] is 3456 bits, which means that the proposed protocol is 63.88% better than [18] in terms of communication cost. The computation cost of Son et al. [18] is 41.459 ms, which means that the proposed protocol is also 63.86% better in terms of computation costs. The communication cost of Ryu et al. [21] is 1472 bits, and the computation cost is 407.95 ms; so the proposed protocol is 15.21% better in terms of communication and 96.32% in terms of computation costs. Mohit et al. [30] have 5312 bits, and the proposed protocol is 1248 bits, which means the proposed protocol is 76.50% better in terms of communication and 92.81% better in terms of computation cost; The proposed protocol is 30.35% improved in terms of communication and 91.58% smaller than Sahoo et al. [33] scheme. Finally, the proposed scheme is 6.02% improved in communication against Abbasi et al. [41] and 79.66% better in computation costs. This means that the RLKAS-TMS is lightweight at a maximum of 76.50% and a minimum of 6.02% against its competitors.

In addition, when comparing the proposed scheme with Mohit et al. [30], Son et al. [18], Ryu et al. [21], Sahoo et al. [33], and Abbasi et al. [41] in terms of security functionalities, including A-Man-in-the-Middle Attack, B-DoS Attack, C-Replay Attack, D-Insider Attack, E-Spoofing Attack, F-Forgery Attack, G-Traceability Attack, H-Brute Force Attack, I-Stolen-Verifier Attack, J-Password Guessing Attack, K-Anonymity, and L-ESL Attack while √-Supported, x–Not Supported. The result shows that the proposed protocol provides maximum security, as shown in Table 7. The result obtained shows that [18] has anonymity issues and suffers from MITM and DoS attacks; [21] is not safe against brute-force, insider and replay attacks; [30] is vulnerable to ESL, DOS, and Insider threats; [33] is not shown resistance to DoS, insider and brute-force attacks and has anonymity issues; [41] is vulnerable to potential replay and ESL attacks while the proposed protocol is robust against all the mentioned vulnerabilities.

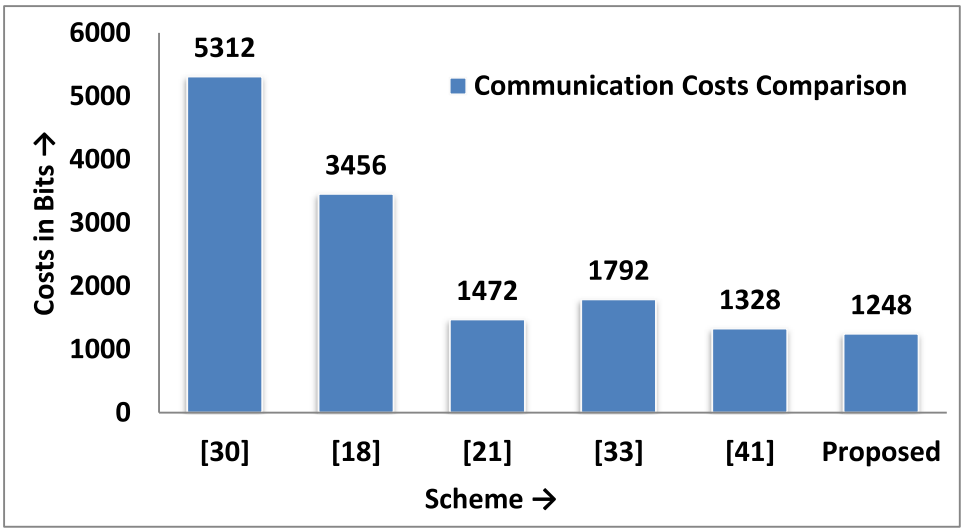

FIGURE 6. Communication costs comparison.

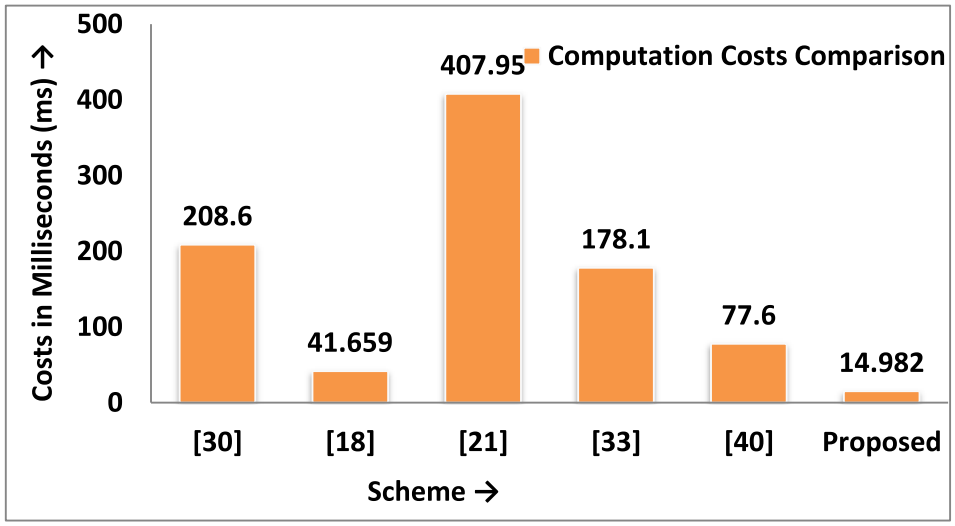

FIGURE 7. Computation costs comparison.

VIII. CONCLUSION

In this article, an asymmetric-based key cryptographic primitive called ECC has been used for securely authenticating a remote user (patient, doctor, laboratory, embedded sensors, and other wearables) with the telemedicine server. This research demonstrated the importance of such a system for uplifting human lives in the recent technological world, where physical access to the healthcare system creates hurdles and maximizes the rush on available resources. The security of the proposed ECC-based security framework has been scrutinized through the real-or-random (RoR) model and ProVerif software toolkit. At the same time, the performance has been measured by considering storage, computation, and communication costs. The result from the comparison analysis shows that the scheme is efficient and effective and can strongly be recommended for practical implementation in the real-world telehealth system. In the future, the researcher plans to work on the verifiability of centralized ledger databases and develop a system based on blockchain to authenticate LedgerDB and VeDB strongly and deploy them in a cloud-based e-healthcare system.

ACKNOWLEDGMENT

The author would like to thank the University of Jeddah for its technical support.

REFERENCES

[1] W. K. Dong, Y. C. Jin, and H. H. Keun, "Risk management-based security evaluation model for telemedicine systems," *BMC Med. Inform. Decis. Making*, vol. 20, no. 1, p. 106, 2020.

[2] A. S. Albahri, J. K. Alwan, Z. K. Taha, S. F. Ismail, R. A. Hamid, A. A. Zaidan, O. S. Albahri, B. B. Zaidan, A. H. Alamoodi, and M. A. Alsalem, "IoT-based telemedicine for disease prevention and health promotion: State-of-the-art," *J. Netw. Comput. Appl.*, vol. 173, Jan. 2021, Art. no. 102873.

[3] M. Y. Peter, "Successfully developing a telemedicine system," *J. Telemed. Telecare*, vol. 11, no. 7, pp. 331–335, 2005.
[4] C. S. Pattichis, E. Kyriacou, S. Voskarides, M. S. Pattichis, R. Istepanian, and C. N. Schizas, "Wireless telemedicine systems: An overview," *IEEE Antennas Propag. Mag.*, vol. 44, no. 2, pp. 143–153, Apr. 2002.
[5] M. C. Batistatos, G. V. Tsoulos, and G. E. Athanasiadou, "Mobile telemedicine for moving vehicle scenarios: Wireless technology options and challenges," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 1140–1150, May 2012.
[6] S. K. Margaret, J. Todd, and K. Zachrison, "Digital disparities: Designing telemedicine systems with a health equity aim," *Emergency Med. J.*, vol. 38, no. 6, pp. 474–476, 2021.
[7] D. Falco, I. D. Cioppa, A. Koutny, T. Krcma, M. Scafuri, and E. Tarantino, "Genetic programming-based induction of a glucose-dynamics model for telemedicine," *J. Netw. Comput. Appl.*, vol. 119, pp. 1–13, Oct. 2018.
[8] T.-W. Lin and C.-L. Hsu, "FAIDM for medical privacy protection in 5G telemedicine systems," *Appl. Sci.*, vol. 11, no. 3, p. 1155, Jan. 2021.
[9] A. Celesti, A. Bagula, I. De Falco, P. Brandão, and G. Sannino, "Emerging networked computer applications for telemedicine," *J. Netw. Comput. Appl.*, vol. 130, pp. 104–106, Mar. 2019.
[10] H. Chen, D. Ding, L. Zhang, C. Zhao, and X. Jin, "Secure and resource-efficient communications for telemedicine systems," *Comput. Electr. Eng.*, vol. 98, Mar. 2022, Art. no. 107659.
[11] A. Sharifi Kia, M. Rafizadeh, and L. Shahmoradi, "Telemedicine in the emergency department: An overview of systematic reviews," *J. Public Health*, vol. 31, no. 8, pp. 1193–1207, Aug. 2023.
[12] C. Ankur, H. Thuong, and N. Beyene, "A W3H2 analysis of security and privacy issues in telemedicine: A survey study," in *Proc. ACM Southeast Conf.*, 2023, pp. 47–55.
[13] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2439–2461, Aug. 2015.
[14] L. Zheng, Y. Zhang, R. Zhang, J. Chen, M. Cui, and C. Song, "An improved authentication protocol in telemedicine system," in *Algorithms and Architectures for Parallel Processing*, Guangzhou, China. Springer, 2018, pp. 177–184.
[15] C. T. Li, D. H. Shih, and C. C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems," *Comput. Methods Programs Biomed.*, vol. 157, pp. 191–203, Apr. 2018.
[16] R. Amin, S. H. Islam, P. Gope, K. R. Choo, and N. Tapas, "Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system," *IEEE J. Biomed. Health Informat.*, vol. 23, no. 4, pp. 1749–1759, Jul. 2019.
[17] Y. B. Dwi and S. Estri, "Multi-tier model with JSON-RPC in telemedicine devices authentication and authorization protocol," in *Proc. 7th Int. Conf. Eng., Appl. Sci. Technol. (ICEAST)*, Apr. 2021, pp. 213–216.
[18] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das, and Y. Park, "Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain," *IEEE Access*, vol. 8, pp. 192177–192191, 2020.
[19] C.-L. Lei and Y.-H. Chuang, "Privacy protection for telecare medicine information systems with multiple servers using a biometric-based authenticated key agreement scheme," *IEEE Access*, vol. 7, pp. 186480–186490, 2019.
[20] D. Dharminder, U. Kumar, and P. Gupta, "A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services," *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2531–2542, Oct. 2021.
[21] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, "Secure ECC-based three-factor mutual authentication protocol for telecare medical information system," *IEEE Access*, vol. 10, pp. 11511–11526, 2022.
[22] M. Ramadan and S. Raza, "Secure equality test technique using identity-based signcryption for telemedicine systems," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16594–16604, Sep. 2023.
[23] M. Bellare, "Practice-oriented provable-security," in *School Organized by the European Educational Forum*. Springer, 1998, pp. 1–15.
[24] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "ProVerif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial," in *Version From*, 2018, pp. 5–16.
[25] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[26] B. Preneel, "Cryptographic hash functions," *Eur. Trans. Telecommun.*, vol. 5, no. 4, pp. 431–448, 1994.
[27] A. Cilardo, L. Coppolino, N. Mazzocca, and L. Romano, "Elliptic curve cryptography engineering," *Proc. IEEE*, vol. 94, no. 2, pp. 395–406, Feb. 2006.
[28] S. Niu, B. Kang, A. Li, Y. Huo, and X. Zuo, "Analysis and improvement of a privacy-preserving authentication scheme for telecare medical information system environment," *Wuhan Univ. J. Natural Sci.*, vol. 28, no. 6, pp. 531–540, Dec. 2023.
[29] S. Yu and K. Park, "SALS-TMIS: Secure, anonymous, and lightweight privacy-preserving scheme for IoMT-enabled TMIS environments," *IEEE Access*, vol. 10, pp. 60534–60549, 2022.
[30] P. Mohit, R. Amin, A. Karati, G. Biswas, and M. K. Khan, "A standard mutual authentication protocol for cloud computing based health care system," *J. Med. Syst.*, vol. 41, p. 50, Feb. 2017.
[31] A. K. Das, V. Odelu, and A. Goswami, "A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS," *J. Med. Syst.*, vol. 39, p. 92, Aug. 2015.
[32] P. Yupapin, C. Meshram, S. K. Barve, R. W. Ibrahim, and M. A. Akbar, "An efficient provably secure verifier-based authentication protocol using fractional chaotic maps in telecare medicine information systems," *Soft Comput.*, vol. 27, no. 10, pp. 6033–6047, May 2023.
[33] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *J. Ambient Intell. Humanized Comput.*, vol. 12, pp. 1419–1434, Jul. 2021.
[34] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, vol. 31. Springer, 2008.
[35] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori, "An inside job: Remote power analysis attacks on FPGAs," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 38, no. 3, pp. 58–66, Jun. 2021.
[36] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proc. 4th Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, 2005, pp. 91–98.
[37] K. Suzuki, D. Tonien, K. Kurosawa, and K. Toyota, "Birthday paradox for multi-collisions," in *Proc. 9th Int. Conf.*, Busan, South Korea. Springer, 2006, pp. 29–40.
[38] B. Lynn, "On the implementation of pairing-based cryptosystems," in *Visualizing Deep Learning*, 2007.
[39] M. Scott, "Miracle-multiprecision integer and rational arithmetic C/C++ library," Shamus Softw., Dublin, Ireland, Tech. Rep., 2003.
[40] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1005–1023, 2nd Quart., 2014.
[41] I. A. Abbasi, S. U. Jan, A. S. Alqahtani, A. S. Khan, and F. Algarni, "A lightweight and robust authentication scheme for the healthcare system using public cloud server," *PLoS ONE*, vol. 19, no. 1, Jan. 2024, Art. no. e0294429.
[42] X. Yang, S. Wang, F. Li, Y. Zhang, W. Yan, F. Gai, B. Yu, L. Feng, Q. Gao, and Y. Li, "Ubiquitous verification in centralized ledger database," in *Proc. IEEE 38th Int. Conf. Data Eng. (ICDE)*, Kuala Lumpur, Malaysia, May 2022, pp. 1808–1821.
[43] X. Yang Y. Zhang S. Wang B. Yu F. Li Y. Li and W. Yan, "LedgerDB: A centralized ledger database for universal audit and verification," *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, 2020.
[44] X. Yang, R. Zhang, C. Yue, Y. Liu, B. C. Ooi, Q. Gao, Y. Zhang, and H. Yang, "VeDB: A software and hardware enabled trusted relational database," *Proc. ACM Manag. Data*, vol. 1, no. 2, pp. 1–27, 2023.

ABULRAHMAN ALZAHRANI received the bachelor's degree in computer science, the master's degree in computer science, engineering management, information systems and technology, and business administration, and the Ph.D. degree in information systems and technology.

He is currently an Assistant Professor with the Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia. He is also the Head of the Department of Computer Engineering and Network. He teaches several courses to the bachelor's and master's students. His research interests include information security and innovations in data science, machine learning, health informatics, the Internet of Things (IoT), and the Internet of Drones (IoD).