A Cloud-Assisted Medical Cyber-Physical System Using a Privacy-Preserving Key Agreement Framework and a Chebyshev Chaotic Map

B D Deebak, Seong Oun Hwang, *Senior Member IEEE,*

***Abstract*—At present, communication networks like the Internet of Things (IoT) are emerging with some of the latest technologies, such as artificial intelligence, big data, and cloud computing, to enable wireless edge infrastructures and seamless data migration. In particular, edge-based wireless communications help to gain new insights into the mitigation of potential communicable infections, e.g. COVID-19, via the use of IoT sensing devices. Of late, an evolving technology known as the cloud-assisted medical cyber-physical system (CA-MCPS) has explored various key agreement protocols to examine security weaknesses between sensing devices and medical experts. Unfortunately, the existing schemes address vulnerabilities such as impersonation, privileged-insider, and password guessing whereby the behavior of the system becomes nondeterministic when guarding against malicious intent. Also, failures, faults, and attacks may vary in the characteristic forms of the IoT and the MCPS, causing unforeseen impairments in the system and for users. Thus, this paper develops a privacy-preserving key agreement framework (PP-KAF) using the Chebyshev chaotic map mechanism to avoid privacy data disclosures and to protect session keys. The proposed PP-KAF exploits a strategy of two-way authentication not only to protect user identities but also to achieve untraceability from the remote server. Finally, a formal analytical model is applied to examine the properties of the key agreement protocol. Simulation results demonstrate that the proposed PP-KAF can offer better security efficiencies and can mitigate computation and communication overhead to guarantee improved quality metrics, namely, throughput rate and energy consumption.**

***Index Terms*—Cloud, Medical Cyber-Physical System, Privacy-Preserving, Untraceability, Security Efficiency.**

I. Introduction

Efficient electronic healthcare systems are in high demand for accurate medical decision-making. However, in conventional treatments, medical experts cannot provide better diagnoses for new in-patients because their medical histories and other relevant information are missing from real-time data centers. In order to improve the treatment process, modern healthcare allows medical experts to legally gain access to institute servers for the treatment process. Because patients' medical histories and subjective contents are entrusted with private information and confidential information of others, guarantees of data privacy, confidentiality, and integrity are essential to consider when allowing system access over public networks. Moreover, security requirements may vary between electronic healthcare systems or host institutes in order to comply with privacy legislation.

The jurisdiction of the electronic healthcare system includes the following: 1) The design of an Electronic Health Record (EHR) [1] maintains the patient's medical records to ease archiving services, including electronic prescriptions, clinic administration, online treatment bookings, etc; 2) A telemedicine and telehealth system stores a patient's medical data, providing access over the Internet to remotely provide medical diagnosis and treatment; 3) A clinical IT system provides medical imaging, surgery, radiology, nursing, diagnosis, and medical treatment planning. Moreover, the above systems can provide a better medical decision-making process; 4) Use of an IT health system [2] is to obtain patient information access to examine medical reports, including blood tests, cardiac stress tests, skin allergy tests, etc; and 5) Specifically, the electronic healthcare system uses a research team to collect and examine medical data so a bio-statistical program can identify an infection and related drug development for a positive outcome.

In a telecare medical information system (TMIS), preserving user anonymity plays a crucial role, and infringement on a patient's privacy may lead to serious legal complications. As a result, a distributed multimedia sensor network is preferred to collect and share the physiological data of a patient through a user terminal. To provide pervasiveness and high-quality medical services, a most promising segment known as mobile health (mHealth) was initiated that improves the quality and safety of the healthcare system through the advancement of mobile technology solutions [3]. Lately, the evolution of wireless devices and their related technologies has offered several unprecedented opportunities for pervasive mHealth that has emerged in several promising segments of electronic healthcare systems [4]. In addition, a control mechanism known as fine-grained access has significance for healthcare information, providing limited access to authorized users, i.e. for some specific attributes [5].

A. Research Motivation

As reported by Moody's Investor [6], an aging population around the world means 20% of the population is turning 65 and over owing to extended lifetimes, but the birth rates are worsening. For instance, 13 countries were predicted to have

*Corresponding Author: (Seong Oun Hwang, sohwang@gachon.ac.kr)

This work was supported by the National Research Foundation of Korea funded by the MSIT (Ministry of Science, ICT) under Grant 2022H1D3A2A02081848 and by the Gachon University research fund under Grant GCU-202206210001.

B D Deebak and Seong Oun Hwang are with the Department of Computer Engineering, Gachon University, 13120 Seongnam, South Korea (e-mail: deebak@gachon.ac.kr, sohwang@gachon.ac.kr)

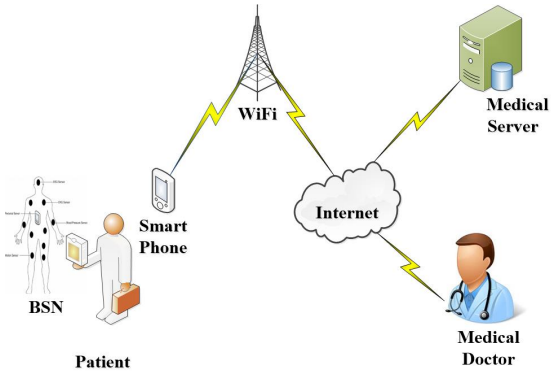


Fig. 1: Healthcare Application System Scenario.

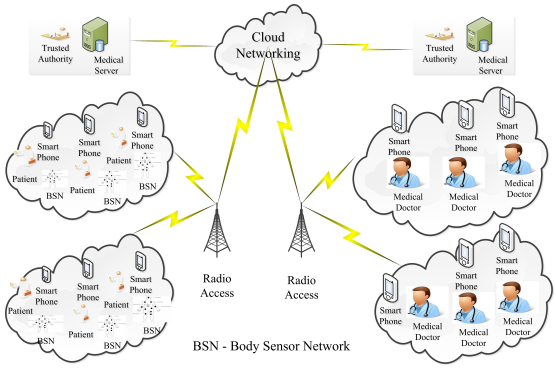


Fig. 2: A Typical Implementation of Medical Cyber-Physical Systems (MCPS).

more overage people by 2020, rising to 34 countries by 2034 [5]. This aging cohort is expected to put an extensive strain on existing healthcare applications where technologies play a vital role in healthcare industries. For instance, wireless body area networks (WBANs) are preferred where this new network paradigm provides periodic analysis to remotely monitor a patient's health. In general, patients wear a body sensor network (BSN) as assistive technology to improve health and personal safety. The BSN periodically collects personal healthcare information (PHI) such as heartbeat, temperature, blood pressure, etc. Subsequently, the collective PHI is sent via smart devices like smartphones, cognitive radio networks, Bluetooth, etc., to assist in proper medical diagnosis. The smart computing device may use a 4G or 5G communication network to record PHI in the healthcare center [7]. This communication setup utilizes radio technology that permits the medical practitioner (i.e. a medical expert) to analyze the patient's condition. Fig. 1 shows a healthcare application scenario.

In the electronic healthcare system, the patient wishes to obtain healthcare-related suggestions from a medical practitioner that are completely based on the patient's medical history. There may be a situation where the patient attempts to establish a communication service through a smart device that helps him/her to share current healthcare parameters with the medical server. This real-time setup can use wireless technologies to implement a heterogeneous IoT network using a medical cyber-physical system (MCPS) [8]. Fig. 2 shows an implementation of a mobile healthcare social network that includes a trusted authority to register patient information, i.e. $TA_P = \{TA_1, TA_2, TA_3, ..., ..., TA_N\}$. Importantly, wireless channels can easily be compromised by an adversary whereby modification, interception, insertion, delay, and relay can be exploited, damaging the reputation of the medical institute. On the other hand, resource-constrained medical devices have limited on-chip access to provide a sophisticated encryption protocol like public key infrastructure (PKI). As a consequence of this restriction, serious security threats (eavesdropping and modification) can be created while collecting and recording human data over a centralized server.

Over a decade, the implementation of the IoT has instituted several changes in the healthcare industry leading to significant improvements in remote patient monitoring. In health monitoring, massive numbers of smart computing devices are connected via active wireless channels to set up data collection and sharing. Due to inappropriate risk management in wireless infrastructures, hackers can take advantage of a vulnerability to expose sensitive health data within the information system. To address this issue, key properties such as authentication and privacy-preserving can be based on an assumption of a Chebyshev chaotic map [9]. This can secure sensitive health data before transmitting them over any public wireless channel. In practice, the chaotic framework includes properties such as pseudorandom behavior, sensitivity to initial conditions, etc., which are equivalent to a specific cryptographic primitive, i.e. a Chebyshev map. It has its own significant characteristics in strengthening the security level and reducing the communication overhead, compared to pairing-based and elliptic-curve [9] approaches. Therefore, the proposed privacy-preserving key agreement framework (PP-KAF) uses the Chebyshev chaotic map to protect sensitive data.

B. Research Contributions

The major objectives of the proposed system are to enhance robustness in the presence of interference and to provide seamless authentication to the nodes of the sensing devices using a fast hash function [10]. As a result, each function uses a preset key and an idea of a one-time password to compute a new hash value. This computed value is applied to the generated sources including key and message requests which are operated among the base station/mobile sink and IoT devices to resolve the issue of time synchronization. A time-synchronization mechanism is applied to regulate clock synchronization based on roundtrip problems between real-time entities to solve the difficulty of the time margin caused by network latency and delay. The major contributions of the proposed PP-KAF are as stated below:

1) We propose PP-KAF using a Chebyshev chaotic map mechanism for CA-MCPS without the intervention of a mobile sink. Moreover, this proposed PP-KAF evaluates the properties including collision and randomness effectively using a faster hash function to improve the efficiency of CA-MCPS.

2) The proposed PP-KAF uses two-factor authentication with a secure token credential session to access the healthcare service in order to address the problem of clock synchronization.
3) In addition, the proposed PP-KAF employs a smart strategy in a context-aware mechanism, where each user tries to satisfy the demands of communication networks to obtain patient information. To provide reliable and secure data transmission over insecure public networks, this research presents a secure two-way authentication mechanism with direct access control of IoT devices.
4) Compared to the recent authentication schemes, the proposed PP-KAF consumes lower communication costs to meet the requirements of resource-constraints medical IoT devices i.e., processing and storage.

C. Paper Organization

The remaining sections are as follows. Section II reviews the challenges of the existing work. Section III discusses the mathematical assumptions, any threats, and the framework model itself. Section IV presents the privacy-preserving key agreement framework using the Chebyshev chaotic map mechanism. Section V discusses the security and performance analysis. Section VI concludes the research.

II. Related Work

Of late, the mutual authentication and key agreement (M-AKA) protocol has become a solution for the protection of network-based application systems like wireless medical sensor networks (WMSNs) [11]. M-AKA protocols are widely used in multi-server systems [12], satellite communications [13], and RFID [14]. Wazid et al. [15] designed lightweight authentication for an edge-based IoT environment. Sharma and Kalra [16] proposed an efficient secure authentication scheme for healthcare services. Zhou et al. [17] introduced lightweight IoT-based authentication for smart computing devices. However, these schemes could not offer better transmission efficiency to meet a key constraint on smart devices. Chiou et al. [22] demonstrated the key features of the Chen et al. framework in [23] to determine security weaknesses such as authentication and anonymity.

To address the issues of Chen et al., Chiou et al. devised a strategy for a cloud-based medical information model. Mohit et al. [24] proved that the Chiou et al. method cannot resist vulnerabilities such as the stolen verifier and client anonymity. To enhance the security level of the medical information system, Mohit et al. constructed a lightweight authentication model. Li et al. [25] and Kumar et al. [26] analyzed the challenges for the Mohit et al. model, such as impersonation and stolen verifiers, to probe the deficiency factors of a shared session key. Lately, Kumar and colleagues [27] reviewed the security attributes of the Li et al. research, such as data confidentiality, message authentication, data non-repudiation, and impersonation, because Li et al. could not preserve the session key in the upload phase. To acquire a privacy-preserving attribute, Kumar et al. constructed a desired prerequisite in the data upload phase that can even manage performance efficiencies from computation and communication to meet TMIS requirements. Deebak and Al-Turjman [28] constructed a security mechanism for a cloud-health infrastructure using the IoMT. It uses smart service authentication to analyze weaknesses in a common secret session key.

Chen et al. [29] designed a key agreement protocol using radio-frequency identification for epidemic emergency management systems. This agreement protocol enhanced the version of Mansoor et al. [30] to improve automation and decision-making processes. Chen et al. [31] presented an efficient privacy-preserving authentication scheme. It uses temporary identities to preserve privacy and patient medical histories. However, the Chen et al. authentication scheme did not consider a few quality metrics, such as latency, resource utilization, and energy consumption, to address the practical difficulties. Chatterjee et al. [18] employed a biometric-based authentication using the Chebhyshev chaotic map to achieve higher computation efficiency in a multi-server environment. Zhang et al. [19] designed an authentication scheme based on Chebyshev chaotic map to offer fast authentication while preserving anonymity using proper negotiation. Lee et al. [19] constructed a lightweight authentication using an extended chaotic map to derive a strong group in order to guarantee the practical features of wireless sensor networks such as perfect secrecy and known key security [20]. Regardless of its design strategy using Chebyshev and chaotic map, the authentication schemes namely Chatterjee et al., Zhang et al., and Lee et al. still invoke a few additional message rounds to perform a proper key validation.

Yupapin et al. [21] utilized a fractional chaotic map to design secure authentication which does not invoke any additional message round to validate the server keys. However, Yupapin et al. failed to prove the security efficiency of the verifier-based authentication protocol. In compliance with Table I, a few existing schemes (lightweight authentication using an elliptic curve [15], [16], [22], crypto-hashing [28], Chebyshev [18], [19], and chaotic map [20], [21]) were preferred to analyze a property message authentication and integrity which not only support known key security and anonymity but also prevent the vulnerabilities such as impersonation and password guessing [32]. Moreover, the evaluated schemes proved that they can reduce cost efficiencies (computation and communication) using theoretical evaluation, however, their schemes do not consider any operational factors involved in a real-time deployment.

Therefore, this paper constructs a privacy-preserving framework using a Chebyshev chaotic map not only to manage security and privacy but also to prove its efficiency in real-time systems.

III. Preliminaries

This section discusses mathematical assumptions, threats, and framework models related to the cloud-assisted MCPS.

A. Mathematical Assumption

Enhanced Chebyshev Chaotic Maps [10]: For a given degree $<n>$, an enhanced Chebyshev polynomial $T_n(x)$ can be

TABLE I: Summarized Key Attributes Of Related Works In Authentication Frameworks Based On Medical Cyber-Physical Systems

Prior Works	Technique Applied	Practical Domains	Real-Time Analysis	Properties							Attacks							
				Support of Key Freshness	Support of User Anonymity	Support of Proper Mutual Authentication/Inegrity	Support of Unlinkability	Support of Non-Repudiation	Conditional Traceability	Support of Perfect Secrecy	Resilient To Replay Attack	Resilient To Impersonation Attack	Resilient To offline guessing Attack	Resilient To Stolen Verifier Attack	Resilient To Mobile Device Loss Attack	Resilient To Device Compromise Attack	Resilient To Denial of Service Attack	Resilient To De-Synchronization Attack
[15]	Lightweight Authentication, Key Management, and Elliptic Curve Cryptography	Edge Computing and IoT	Simulation Using NS2	✖	✖	✖	✖	✖	✖	✖	✔	✔	✖	✖	✖	✖	✖	✖
[16]	Lightweight Authentication and Cryptographic Hash Function	Cloud and Healthcare Services	Not Considered	✔	✔	✔	✖	✖	✖	✖	✔	✔	✖	✖	✖	✖	✖	✔
[17]	Lightweight Authentication and Cryptographic Hash Function	Cloud and IoT	Not Considered	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✔
[18]	Biometric-based Authentication and Chebyshev Chaotic Map	Multiserver Environments	Not Considered	✖	✔	✔	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖
[19]	Energy Efficient Authentication and Chebyshev Chaotic Map	Smart Grid Environment	Not Considered	✖	✖	✔	✔	✖	✖	✔	✔	✖	✖	✔	✖	✖	✖	✖
[20]	Lightweight Identity-based Authentication and Extended Chaotic Map	Wireless Sensor Networks	Not Considered	✖	✖	✔	✖	✖	✖	✔	✔	✔	✔	✖	✖	✖	✖	✖
[21]	Verifier-based Authentication and Fractional Chaotic Map	Telecare Medical Information Systems	Not Considered	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
Proposed PP-KAF	Privacy Preserving, Key Agreement, and Chebyshev Chaotic Map	IoT, Cloud and MCPS	Considered	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
✔ - Proven; ✖ - Not Proven																		

expressed as follows:

$$T_n(x) = \begin{cases} 1, & \text{n=0} \\ x \mod p, & \text{n=1} \\ (2x.T_{n-1}(x) - T_{n-1}(x)) \mod p, & \text{n} \geq 2 \end{cases} \quad (1)$$

where $x \in (-\infty, +\infty)$, and p represents a large prime integer to satisfy the semi-group property:

$$T_r(T_s(x)) = T_{rs}(x) = T_s(T_r(x)) \; \forall s, r \in \mathbb{Z}^+ \quad (2)$$

Complex Assumption: The enhanced Chebyshev polynomial problem is associated with three computational problems that are applied in the proposed PP-KAF. They are as follows. Extended Chaotic-Map-based Discrete Logarithm (ECM-DL): given $x, y, T(x)$, and p, it is complex to find out if it is computationally infeasible for random integer r:

$$Y = T_r \mod p \quad (3)$$

The functional benefit of A_{dv} to solve *ECM-DL* is defined as $A_{dv}^{ECM-CDH}(t_2) = P_r[A_{dv}(x, y) = r : r \in \mathbb{Z}_p^*, y = T_r(x) \mod p$. As referred to [18], A_{dv} may find a deterministic solution using interger function s using the equation $T_{s'}(x) = T_s(x)$ in case of obtaining the values of $T_s(x)$ and $x(x \in [-1, +1])$ using a strategical function $s' = \frac{arccos(T_s(x)) + 2k\pi}{arccos(x)}$, $k \in \mathbb{Z}$ where $\mathbb{Z}$ is an integer set.

Extended Chaotic Map Computational Diffie-Hellman (ECM-CDH): given $T_r(x)$, $T_s(x)$, x, $T(.)$, and p, it is hard to calculate whether it is computationally infeasible for $r, s \geq 2, x \in (-\infty, +\infty)$:

$$T_{rs}(x) \equiv T_r(T_s(x)) \equiv T_s(T_r(x)) \mod p \quad (4)$$

Extended Chaotic Map Decisional Diffie-Hellman (ECM-DDH): given $T_r(x)$, $T_s(x)$, $T_z(x)$, x, $T(.)$, and p, it is difficult to decide whether it is computationally infeasible or not:

$$T_{rs}(x) \equiv T_z(x) \mod p \quad (5)$$

B. Threat Model

This subsection discusses an adversarial model to infer the capabilities of the adversary A_{dv}. In general, the adversary is assumed to possess the following qualities as referred to [18] and [21].

1) A_{dv} could easily deduce any user's confidentiality level through the exploration of malicious smartcard readers using a side-channel attack [11].
2) A_{dv} may try to execute offline and online guessing attacks after the successful deduction of user confidential information from a smartcard.
3) It is always evident that the security protocol cannot be held back from adversaries.
4) The information from eavesdropping on any user may be stolen, fabricated, deleted, redirected, or retransmitted to cover the original form.
5) A_{dv} may track down the involvement of any user if the invoked security protocol of the user has used constant parameters during session establishment.
6) A_{dv} may be available implicitly in the target organization or maybe a legitimate user trying to undermine the trustworthiness of reputed third-party systems.
7) A_{dv} may be aware of the execution of a security protocol.
8) A_{dv} may extract storage information about a smartcard by using the power analysis techniques referred to in [33] and [34].

TABLE II: NOTATIONS USED IN PROPOSED PP-KAF

Parameter	Definition
j,k,and q	Session Keys with a key size of 256 bits
gw_{node}	Gateway Node
ms_{node}	Mobile Sink Node
U_{id}	User Identity
U_{pwd}	User Password
SK	Long-Term Secret Key of gw_{node}
id_g	Gateway Identity
D_B	Database
Reg_{Centre}	Registration Center
Med_{Expert}	Medical Expert
MS_{kit}	Medical Sensor Kit
P_{id}	Patient's Identity
ms_{node}	Medical Sensor Node
$<RC_{SID_j}, PRC_{SID_j}>$	Unique Pseudo Identities
t_U, t_G, t_S	Timestamp
$Session_{Key}$	Secure Session Key

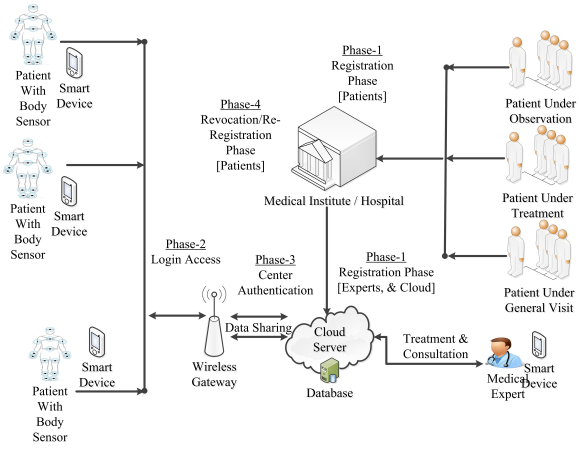


Fig. 3: Framework for a Cloud-assisted Medical Cyber-Physical System using the IoT.

C. A Framework for a Cloud-assisted Medical Cyber-Physical System

Fig. 3 shows a framework model for cloud-assisted medical cyber-physical systems using the IoMT where the real-time entities are trusted health centers, medical practitioners, patients, cloud servers, and wireless gateways. Before processing a telemedicine requisition, patients are outfitted with body sensor networks that record health information such as blood pressure, pulse rate, body movements, breathing, etc. After reading the health information successfully, the patient's data would be transmitted to a cloud server through a wireless gateway. By then, the medical practitioner gains access privileges via a smart device to observe the patient's medical information in order to recommend medical treatment, follow-up procedures, or medical assistance.

Finally, using a smartphone, patients may receive health information to follow up on medical prescriptions or treatments. The cloud-aided MCPS is composed of medical expert registration, patient registration, system login, center authentication, and password updates. Descriptive details of each phase are as follows:

Patient Registration: In general, patients visit a health center to undergo medical observation, treatment, or a general checkup, which requires prior registration with the health center. By then, the patients are subject to medical treatment involving report generation, inspection, and medical recommendations. Finally, a summary report on the patient would be recorded on the cloud server.

After uploading healthcare information to the cloud server, the patient may gain authenticated access to download the summary report. According to the medical recommendations, the patient may again undergo treatment that would generate new medical data to be collected and shared with the cloud server.

Medical Expert: Upon successful collection of patient healthcare data in the cloud server, the medical practitioner may obtain privileged access to the server to read the patient's records. Subsequently, the practitioner would generate a diagnostic report on the patient, i.e. medical treatment or advice, and would then upload the same to the cloud server.

Center Authentication: In pursuit of medical treatment, a telehealth services facility can be enabled on the patient's dashboard. To access medical services, the patient acquires device connectivity with the cloud server to view and download the doctor's diagnosis reports, medical prescriptions, and follow-up treatment advice.

User Revocation and Re-Registration: Any legitimate $User$ may revoke its accessing services in pursuit of the expiry of the registration period in order to perform a proper re-registration process.

Password Update: In the proposed PP-KAF, Reg_{Centre} is essential to load necessary parameters in $User$ and C_S during the registration phase to minimize the cost efficiency (computation) involved in login and authentication phases.

IV. The Proposed PP-KAF Mechanism

The proposed PP-KAF scheme uses three different session keys, j, k, and q, with a key size of $256bits$. This mechanism uses key agreement strategies [15-19] to share $SK_{gs} \parallel id_g)$ between gateway node gw_{node} and mobile sink node ms_{node}. Table II shows the important notation used in the proposed PP-KAF. The phases are as follows.

Medical Expert Registration: In the hospital registration center, the medical expert registers his/her information in gw_{node} as follows.

Step 1: Over a secure channel, $User$ furnishes his/her credentials, namely U_{id} and U_{pwd}.

Step 2: Upon receiving the user ID and password $\{U_{id}, U_{pwd}\}$, gw_{node} performs the following computation: $C_{gw} = E_j(U_{id} \parallel id_g \parallel T_{x_i}(K_{User_i}))$ and $N_{id} = H(U_{id} \oplus U_{pwd} \oplus SK)$ where $K_{User_i} \in \{-\infty, +\infty\}$ computes the Chebyshev polynomial $T_{x_i}(K_{User_i})$ and $T_{x_i}(K_{User})$.

Step 3: gw_{node} stores $\{H(.), C_{gw}, N_{id}, SK, T_{x_i}(K_{User_i})\}$ into database D_B to provide $D_B = \{H(.), C_{gw}, N_{id}, SK, T_{x_i}(K_{User_i})\}$ to $User$, where SK is the long-term secret key of gw_{node}.

Patient Registration: In the registration center Reg_{Centre} of the hospital, the patient submits his/her credentials, such as a user name. Upon receiving the name of the patient, Reg_{Centre} provides details on a medical expert Med_{Expert}

along with medical sensor kit MS_{kit}. By then, Reg_{Centre} feeds the patient's identity, P_{id}, into MS_{kit} and sends him/her to Med_{Expert}. Finally, Med_{Expert} fuses ms_{node} in the patient's body to analyze his/her physiological data.

Cloud Server Registration: The execution steps are as follows.

Step 1: Reg_{Centre} provides unique and pseudo identities, such as $\{RC_{SID_j}, PRC_{SID_j}\}$, to the cloud server C_S over a secure network.

Step 2: C_S calculates $C_1 = H(PRC_{SID_j} \parallel C_{ID} \parallel x \parallel T_{x_i}(K_{User_i})$ and $C_2 = H(RC_{SID_j} \parallel x \parallel T_{x_i}(K_{User_i})$, and stores RC_{SID_j} in Reg_{Centre}. Last, it sends system parameters $\{C_1, C_2, C_{ID}, T_{x_i}(K_{User_i}\}$ to Reg_{Centre} over a secure channel.

Step 3: Reg_{Centre} stores the communication parameters $\{C_1, C_2, C_{ID}, PRC_{SID_j}, RC_{SID_j}, T_{x_i}(K_{User_i}\}$ to validate the storage data and service access.

System Login: Med_{Expert} logs in to the system to access the medical information of patients via medical sensor networks. Then, to gain access to Reg_{Centre}, Med_{Expert} provides his/her credentials: U_{id} and U_{pwd}. This information will in turn be used with the subsequent procedures as follows.

Step 1: Initially, Reg_{Centre} performs the computation $N^*_{id} = H(U_{id} \oplus U_{pwd} \oplus SK)$ to compare with N_{id}. If $N^*_{id} = N_{id}$, then Reg_{Centre} continues with the rest of the steps. Otherwise, it terminates the login session.

Step 2: Upon successful comparison of $N^*_{id} = N_{id}$, Reg_{Centre} generates random integer r_m to compute $User_{id} = E_k(H(U_{id}) \parallel r_m \parallel ms_{node} \parallel C_{gw} \parallel t_U \parallel T_{x_i}(K_{User_i}))$.

Step 3: Finally, it requests login access $\{User_{id}, t_U, T_{x_i}(K_{User_i})\}$ to gw_{node} with current timestamp t_U.

Center Authentication: Upon receiving login access information $\{User_{id}, t_U, T_{x_i}(K_{User_i})\}$, gw_{node} validates the request by $User$ to compute a transmission message to the legal ms_{node}. The authentic processes of gw_{node} are as follows.

Step 1: To process a login request, it primarily processes the current timestamp t_U to validate $(t^{'}_G - t_U > \triangle t)$ to terminate the login request. If timestamp t_U is verified as fresh, it will proceed.

Step 2: To acquire $\{H(U_{id})^s, r_m, ms_{node}, C_{gw}, t^s_U\}$, gw_{node} decrypts $User_{id}$ as $D_{crypt}(U_{id})$. Besides, it uses C_{gw} as $D_{crypt}(C_{gw})$ to acquire $\{U^*_{id}, id^*_g\}$.

Step 3: Then, gw_{node} computes $H(U_{id})^*$ and verifies that $H(U_{id})^* = H(U_{id})^s$, $id^*_g = id_g$, and $t_U = t^s_U$ to validate similarities and process the login request. If the validation fails, the login request will be terminated. Otherwise, it will be processed.

Step 4: Finally, gw_{node} obtains $t^{'}_G$ to compute a valid authentication, $A_v = E_{SK_{gs}}(H(U_{id}) \parallel r_m \parallel ms_{node} \parallel t_G \parallel t_U \parallel T_{x_i}(K_{User_i}))$, and sends authentication computation $\{A_v, t_G\}$ to ms_{node}. Upon receiving authentication of $\{A_v, t_G, T_{x_i}(K_{User_i})\}$ from gw_{node}, the authentication process for ms_{node} follows.

Step 5: ms_{node} gets current timestamp $t^{'}_S$ from $(t^{'}_S - t_U) > \triangle t$ to check whether it should be discarded or processed.

Step 6: Then, ms_{node} invokes decryption $D_{SK_{gs}}(A_v)$ to acquire $(H(U_{id})^* \parallel r^*_m \parallel ms^*_{node} \parallel t^*_G \parallel t^*_U \parallel T_{x_i}(K_{User_i}))$ to verify whether it has a valid login request from gw_{node}.

Step 7: Upon verification, ms_{node} and t_G validate the information with ms^*_{node} and t^*_G to verify the login request as valid with respect to its current timestamp.

Step 8: After validating the current timestamp, ms_{node} performs a computation with the secure session key, $Session_{Key} = (H(U_id)^* \parallel r^*_m \parallel ms^*_{node} \parallel t^*_U \parallel T_{x_i}(K_{User_i}))$. To compute $L = E_{Session_{Key}}(r^*_m \parallel ms_{node} \parallel t_S \parallel T_{x_i}(K_{User_i}))$, ms_{node} needs alternate timestamp t_S. Finally, ms_{node} sends $\{L, t_S, T_{x_i}(K_{User_i})\}$ to U_{ser}. While U_{ser} receives $\{L, t_S\}$ from ms_{node}, Reg_{Centre} executes the following steps.

Step 9: To verify the current timestamp $t^{'}_U$, the timestamp of a recent message is checked with $t^{'}_U = t_S > \triangle t$ to either discard the process or proceed.

Step 10: Eventually, Reg_{Centre} computes a shared session key, $Key_{User-ms_{node}} = H((U_{id}) \oplus r_m \oplus ms_{node} \oplus t_U)$. By then, it performs the computation of decryption $D_{Key_{User-ms_{node}}}(L)$ to acquire ms_{node} and r^*_m. Reg_{Centre} checks the equivalencies of ms_{node} with ms^*_{node} and r_m with r^*_m to establish a shared session key securely between the users.

User Revocation and Re-registration: While the connectivity of any $User$ is lost or intruded via gw_{node} to gain the access privilege with ms_{node}, an authentic revocation and re-registration are required to preserve the source attributes of the proposed PP-KAF. In case of any intrusion or interception with ms_{node}, the proposed PP-KAF holds the execution of revocation and re-registration with reserved $User$ to maintain a consistent identity. On this account, $User$ intends to revoke their existing account and reinstate the registration without changing their identity U_{id}. In consideration of revocation, $User$ claims to contribute a parameter U_{pwd} and compute N_{id} and C_{gw} to verify the process of computation with SK. The detailed flow structure of revocation and re-registration is as follows:

Step 1: In virtue of revocation, Reg_{Centre} securely delivers a revocation message request including $\{User_{id}, t_U, C_{gw}, T_{x_i}(K_{User_i})\}$to each computing server in order to perform a proper user revocation $User$. Upon obtaining this message request, C_S openly escalates a flag of revocation to $User$ in their registered database.

Step 2: Over the course of verification using *Center Authentication*, C_S determines $H(U_{id})^*$ to verify whether the registered database has any authorized revocation flag or not. Otherwise, C_S disowns the authenticated message request to the respective $User$ with a refusal notice.

Step 3: If there is a genuine $User$ desires to re-enroll with similar identity $User_{id}$, then Reg_{Centre} initially confirms the identity $User_{id}$ using N_{id} to extract C_{gw}, t_U, and $T_{x_i}(K_{User_i})$. In case of successful confirmation, Reg_{Centre} carries out an execution of the registration phase in order to re-issue the corresponding account of $User$.

Password Update: $User$ is allowed to change his/her password through the execution of the following steps.

Step 1: $User$ submits his/her credentials in the Reg_{Centre} to

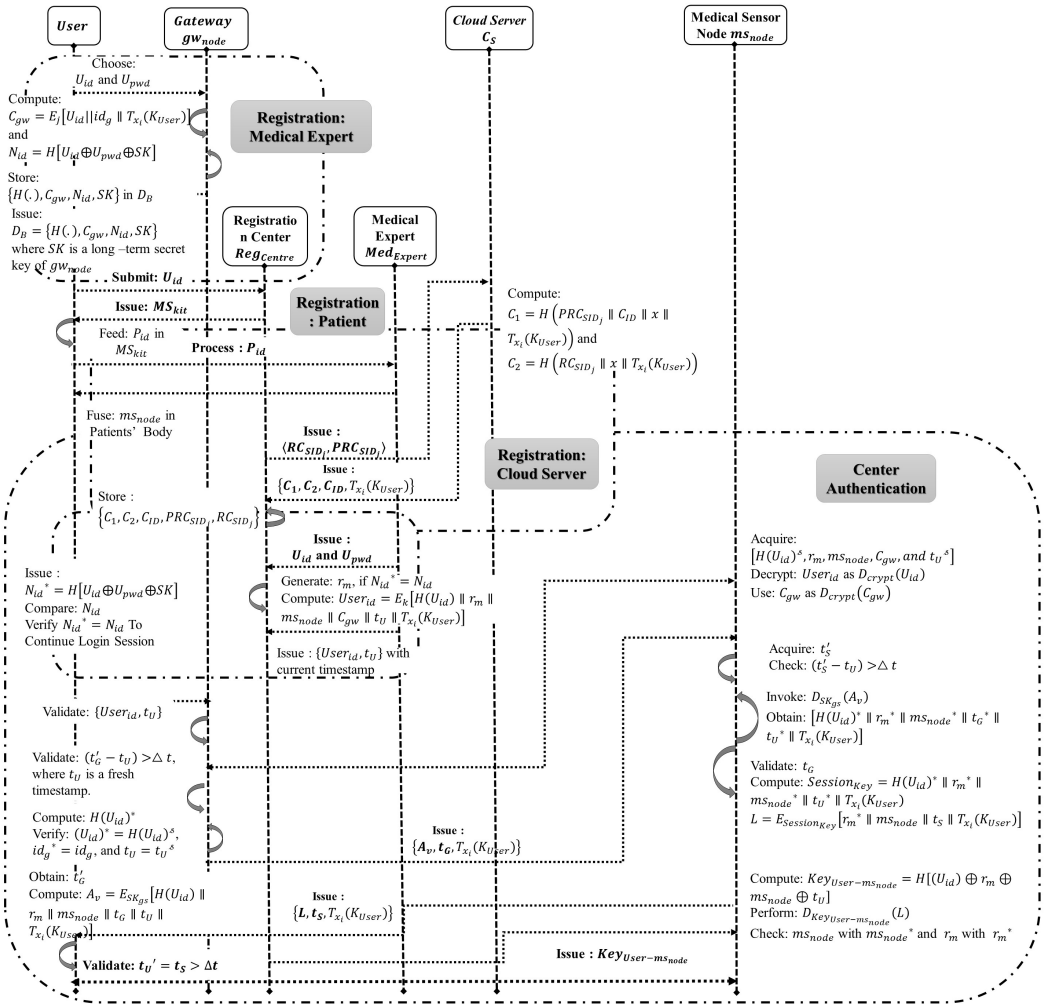


Fig. 4: Communication Phases of the Proposed PP-KAF.

process parameters U_{id} and U_{pwd}.

Step 2: Upon entry of U_{id} and U_{pwd}, Reg_{Centre} performs the computation $N_{id}^* = H(U_{id} \oplus U_{pwd} \oplus SK)$ and verifies it against N_{id}. If verification is successful, then $User$ is allowed to change to a new U_{pwd}. Otherwise, Reg_{Centre} discards the process.

Step 3: Last, Reg_{Centre} performs the computation $N_{id}^{New} = H(U_{id} \oplus U_{pwd}^{New} \oplus SK)$ and replaces N_{id} with N_{id}^{New}.

V. Security and Performance Analysis

In this section, the authentication centre considers a tree-node distribution structure using formal analysis including heuristics (shown in APPENDIX A) and random oracle models to analyze the transmission efficiency of the system.

A. Formal Analysis Using Random Oracle Model

This section demonstrates the formal analysis of the proposed PP-KAF using a random oracle model to prove the property of mutual authentication between $User$ and C_S. This analysis uses semantic security to prove that A_{dv} has the following potential to execute the adversarial model presented in [35].

- In the registration phase, Reg_{centre} records the system parameters $\{C_1, C_2, C_{ID}, PRC_{(SID_j)}, RC_{(SID_j)}, T_{x_i}(K_{User_i})\}$ whereas gw_{node} stores $\{H(.), C_{gw}, N_{id}, SK, T_{x_i}(K_{User_i})\}$ in the database of the $User_i$ to verify the integrity of data access. Additionally, $User_i$ chooses the strong password U_{pwd_i} from an uniformly distributed finite dictionary $\mathbb{D}$ with a key size $|\mathbb{D}|$. $User_i$ acquires their identity U_{id} and one-way hash function $H(.)$ with variable length input string to obtain the unique output.
- We deliberately observe two participants of the proposed PP-KAF including Reg_{centre} and gw_{node} to assess the trust efficiency of a long-term secret key SK. With the aim of eliminating the ambiguity, the entities including Reg_{centre} and gw_{node} are commonly defined as $\mathcal{P}$. To attack the proposed PP-KAF $\mathcal{P}$, let us assume an adversary A_{dv} be a probabilistic polynomial time that has the ability to execute a few oracle queries in an attempt to interact with the t^{th} instances of the enforcing participant $\mathcal{P}^t$. An oracle query agrees with three feasible outcomes: (a) Obtains an appropriate message request (*accept*), (b)

Observes an inappropriate message request (*reject*), (c) Make no attempt to attain any desired result, i.e., no findings are achieved ($\perp$).

- A malicious A_{dv} has an absolute right to control the message transmission over a dedicated communication channel. As a result, A_{dv} has the capacity to block, intercept, modify or extract the processed message msg transmitted between $User_i$ and C_{S_j}.
- Once A_{dv} obtains the access privilege of $User_i$, A_{dv} can apply the power analysis attacks to extract the significant parameters stored in Reg_{centre} and gw_{node}.

In an attempt to violate the security of the proposed PP-KAF, A_{dv} carries out a few simulation attacks based on Oracle queries. They are as discussed below. *Execute ($User_i$,C_{S_j}):* Using passive attack, A_{dv} may overhear or eavesdrop the message transmission msg connected between $User_i$ and C_{S_j} in a practical execution of the proposed PP-KAF protocol $\mathcal{P}$. *Send ($User_i$/C_{S_j},msg):* Using active attack, A_{dv} enables to receive an actual reply message processed by the participant $\mathcal{P}^t$. According to the rules of the proposed PP-KAf, A_{dv} sends a message request msg to $\mathcal{P}^t$ and also obtains the corresponding replies to gain channel access. *Reveal($\mathcal{P}^t$):* The query *Reveal* exhibits the actual shared session key $Key_{User-ms_{node}}$ acquired by $\mathcal{P}^t$ (and its associate entity) to A_{dv}. *Corrupt($User_i$,c):* The query model *Corrupt* simulates the capabilities of A_{dv} to extract the secret parameters of $User_i$, thereby the proposed PP-KAF is corrupted on the basis of:

- When $c = 1$, the query recovers the actual password of $User_i$ to A_{dv}.
- When $c = 2$, the query reinstates the significant parameters of $User_i$ to $A + dv$.
- When $c = 3$, the query observes the database of $User_i$ in order to return the accessible parameters to A_{dv}.

Test($\mathcal{P}^t$) The query model *Test* can be forced to invoke only once in order to show the actual strength of the semantic security on the ground of obtaining the shared session key $Key_{User-ms_{node}}$. With the aim of proper analysis, A_{dv} provides this query model to $\mathcal{P}^t$. In case of no shared session key, a value of *null* is reoccured. Otherwise, $\mathcal{P}^t$ holds a proper decision according to the results obtained by an unbiased flipped coin f. While $f = 1$, $\mathcal{P}^t$ recovers the current $Key_{User-ms_{node}}$ to A_{dv}. Otherwise, $\mathcal{P}^t$ (i.e., $b = 0$) reinstates a random string with similar key length to A_{dv}.

Definition 1: A representative $\mathcal{P}^t$ is known to be approved, in case of obtaining the last awaited protocol message successfully returned into *accept* state. Also, the systematic concatenations are placed in an ordered form to communicate with the messages preferably *send and receiver* operation using an instance $\mathcal{P}^t$ to discover a session identity (s_{id}) of the protocol $\mathcal{P}^t$, especially for the ongoing session.

Definition 2: Two representatives $User_i^{t_1}$ and $C_{S_j}^{t_2}$ are known to be the associative partners, in case of satisfying three authentic conditions at the same time: 1) both entities $User_i^{t_1}$ and $C_{S_j}^{t_2}$ are available to share their parameters in *accept* state; 2) both entities $User_i^{t_1}$ and $C_{S_j}^{t_2}$ agree to perform mutual authentication in order to share the similar identity S_{id}; and 3) both entities $User_i^{t_1}$ and $C_{S_j}^{t_2}$ act as the associative partners mutually.

Definition 3: (Key Freshness) A representative $\mathcal{P}^t$ is known to be with a property of key freshness, in case of satisfying three basic conditions collectively: 1) $\mathcal{P}^t$ exists in *accept* state; 2) The query model *Reveal($\mathcal{P}^t$)* has never been able to present to its representative or associative partner $\mathcal{P}^t$; and 3) precisely not more than two query models *Corrupt($\mathcal{P}^t$,c)* has been presented to $\mathcal{P}^t$, while $\mathcal{P} \in User_i$. Alternatively, while $\mathcal{P} \in C_{S_j}$, precisely not more than two query models *Corrupt($\mathcal{P}^t$,c)* has been presented to the associative partner $\mathcal{P}$.

Definition 4: (Semantic Security) Let's assume that A_{dv} defines an incidental event where A_{dv} may execute a single *Test ($\mathcal{P}^t$)* query with a preferable choice of f controlling c in order to generate a new instance $\mathcal{P}^t$ along with query outcomes c generating a guess bit $F^{'}$. In case $f^{'} = f$, A_{dv} can successfully break the semantic security of the proposed PP-KAF. As a result, the functional benefits of A_{dv} breaking the semantic security using a correct guessing bit $f^{'}$ is determined by $Adv^{PP-KAF}(A_{dv}) = |2P_r[Succ(A_{dv}] - 1| = ||2P_r[f = f^{'} - 1]$.

Definition 5: A privacy-preserving based authentication can be semantically secure if the functional benefit $Adv^{PP-KAF}(A_{dv})$ is nominally exceeding the value of $maxq_s(\frac{1}{|\mathbb{D}|}, \frac{1}{2^{l_f}}, \varepsilon_{fmsg})$, where q_s is the available number of *Send* queries, $|\mathbb{D}|$ is the actual size of the password dictionary, l_f is the string length extracted from $user$ password, and ε_{fmsg} is the probability of *false positivity* in the chosen bit f over a transmitted message msg.

Definition 6: The functional benefit of $A_{dv}^{ECM-CDH}(t_{A_{dv}}) \leq \epsilon$, for any negligible function $\epsilon > 0$.

Theorem 1. Assume A_{dv} is a polynomial-based time deterministic adversary operating with the upper time bound $t_{A_{dv}}$. In order to violate the semantic security of the proposed PP-KAF $\mathcal{P}$, A_{dv} constructs *Send* queries at the most q_s times, *Execute* queries at the most q_e times, and *Hash* queries at the most q_H times, respectively. Accordingly, the deterministic adversary A_{dv} obtains $A_{dv}^{ECM-CDH}(t_{A_{dv}}) \leq \frac{q_h^2}{2^{l_h}} + 2.maxq_s(\frac{1}{|\mathbb{D}|}, \frac{1}{2^{l_f}}, \varepsilon_{fmsg} + \frac{(q_s+q_e)^2+4q_s}{2^{l_r}} + 4q_H(1+(q_s+q_e)^2)A_{dv}^{ECM-CDH}(t_{A_{dv}})$, where l_h is the length of the hash string, l_r is the length of the random integer, l_f is the length of the $User_i$ password, ε_{fmsg} is the possibility of obtaining the *False Positivity*, $\mathbb{D}$ is the dictionary with the key size $|\mathbb{D}|$, and $A_{dv}^{ECM-CDH}(t_{A_{dv}})$ is the probability of A_{dv} in violating the assumption made by ECM-CDH.

Proof. We specify a deterministic sets of game G_i where $i = 0, 1, 2, 3, 4, 5$ initiating by G_0 and terminating at G_5. Suppose $Succ_i$ is a coincidental event defined as a successful guessing bit f in the query model *Test($\mathcal{P}^t$)* which corresponds to each game G_i defined by A_{dv}.

Game G_0. In random oracle, G_0 and the authentic protocol are presumed to be similar as the entities cannot compute any hash input on their own. Hence, we derive,

$$A_{dv}^{ECM-CDH}(t_{A_{dv}}) = |aP_r[Succ_0] - 1|. \quad (6)$$

Game G_1 Using G_1, the oracle queries simulate textitReveal, *Execute*, *Corrupt*, *Test*, and textitHash excluding *Send* to obtain a coherent solution in some arbitrary order. The working procedures of the query model are characterized in APPENDIX B to show the systematic flows of the proposed PP-KAF along with its simulation scenario using $Sendquery$. Additionally, G_1 generates three prominent lists: 1) Register R_H to satisfy the execution of *Hash* query; 2) Record R_H to store the corresponding outputs of the query model; and 3) Return R_H to file the message transcripts between $User_i$ and C_{S_j}. In connection with indistinguishability over G_1 and the authentic protocol, we obtain,

$$P_r[Succ_1] = P_r[Succ_0] \tag{7}$$

Game G_2**.** Using G_2, a collision resistance with hash values and the random integers in the transcripts of the message request msg_1 and msg_2 are considered to find whether it is computationally infeasible or not. In accordance with the birthday paradox attack, the oracle *Hash* query has a collision probability of at most $\frac{q_H^2}{2^{(l_h+1)}}$. Considering this probability, the message requests msg_1 and msg_2 contain r_m as a random integer to obtain the probability of its collision at the most $\frac{(q_s+q_e)^2}{2^{(l_r+1)}}$. Hence, we obtain,

$$|P_r[Succ_2] - P_r[Succ_1]| \leq \frac{(q_s+q_e)^2}{2^{(l_r+1)}} + \frac{q_H^2}{2^{(l_h+1)}} \tag{8}$$

Game G_3**.** Using G_3, a specific situation like message transcript is considered where A_{dv} holds the proper transcripts msg_1 and msg_2 without any active associative partner of *Hash* query. This query observes two primary cases to classify in G_3 as the communication phases of the proposed PP-KAF process two message requests during login and authentication $\mathcal{P}$.

Case 1. The observed query $Send(C_{S_j}, msg_1)$ carefully protects the message transcript msg_1 which has a *Hash* value $H(U_{id})^* = H(U_{id})^s \in R_{A_{dv}}$ to perform a process of computation with the session key. In case of successful computation, the maximum probability of obtaining the session establishment is at the most $\frac{q_H}{2^{l_h}}$. Otherwise, the current process terminates the session. Further, a few more computation processes like $Session_{Key} = (H(U_id)^* \parallel r_m^* \parallel ms_{node}^* \parallel t_U^* \parallel T_{x_i}(K_{User_i}))$ and $L = E_{Session_{Key}}(r_m^* \parallel ms_{node} \parallel t_S \parallel T_{x_i}(K_{User_i}))$ are considered to verify their probabilities of success which are at the most $\frac{q_H}{2^{l_h}}$ and $\frac{q_h}{2^{l_h}}$, respectively. Lastly, the message transcript $msg_1 \in R_T$ verifies its current session with t_U and t_G to validate the integrity of the session. Otherwise, the session terminates. Regarding this process, the computation probability is at the most $\frac{q_s}{2^{l_r}}$.

Case 2. In an effort to respond to the oracle query $Send(User_i, msg_2)$, a few more computation $A_v = E_{SK_{gs}}(H(U_{id}) \parallel r_m \parallel ms_{node} \parallel t_G \parallel t_U \parallel T_{x_i}(K_{User_i}))$ and $(T_{x_j}(T_{Session_{Key1}}) \parallel H(U_{id})^* \parallel r_m^* \parallel ms_{node}^* \parallel t_U^* \parallel T_{x_i}(K_{User_i})) \in R_{A_{dv}}$ are observed to verify whether the transcript msg_2 holds the overall probability $\frac{2.q_H}{2^{l_r}}$ or not. Lastly, for a message transcript msg_2, the maximum probability can be obtained as $\frac{q_H}{2^{l_r}}$. In considering both cases, we obtain,

$$|P_r[Suuc_3] - P_r[Succ_2]| \leq \frac{2.q_s}{2^{l_r}} + \frac{5.q_H}{2^{l_r}} \tag{9}$$

Game G_4**.** This game G_4 considers the guessing attacks including online and offline performed by A_{dv} which uses the property of three-factor authentication to analyze the robustness of the proposed PP-KAF. Moreover, this property considers a few assumptions such as passwords and pre-deterministic key computation to derive the suitable cases.

Case 1. The observed queries always start with either passwords U_{pwd_i} or pre-deterministic key SK to observe the essential parameters reserved in $User_i$ database. Achieving this, A_{dv} performs a query execution $Corrupt(User_i, 3)$ which has two sub-cases to deal with.

Case 1.1. In support of password guessing, A_{dv} operates a query $Corrupt(User_i, 1)$ which chooses a suitable password offhand using a dictionary $|\mathbb{D}|$. Moreover, this query runs its probability at the most q_s times to process the query defined by $Send(C_{S_j}, msg_1)$. Hence, the maximum probability of this case is $\frac{q_s}{|\mathbb{D}|}$.

Case 1.2. In the interest of obtaining the pre-deterministic key SK, A_{dv} permits to process a query $Corrupt(User_i, 2)$. This query obtains its maximum probability as $\frac{1}{2^{l_f}}$ where l_f is the secret key length of the extracted string. Moreover, this query considers a few more coincidental guessing with the possibility of *'False Positivity'* to relate the events with ε_{fmsg}. In general, the pre-computation is observed with $\varepsilon_{fmsg} \approx 2^{-14}$ to relate the maximum probability at the most $max\{q_s\frac{1}{2^{l_f}}, \varepsilon_{fmsg}\}$.

Case 2. With the aim of launching the guessing (offline) attack, A_{dv} runs over $(User_i, 3)$ in conjunction with other two queries $Corrupt(User_i, 1)$ and $Corrupt(User_i, 2)$ to obtain either $Execute(User_i, C_{S_j})$ or successive *Send* with its respective *Hash* query. As a result, the proposed PP-KAF considers two pre-computation keys $Session_{Key1}$ and $Session_{Key2}$ to create the *Hash* values using the parameters of chaotic-map. Moreover, A_{dv} already uses *ECM-CDH* to solve the problem in relevant with *Hash* oracle simulation which has a maximum probability $2q_H A_{dv}^{ECM-CDH}(t_{A_{dv}})$.

It is apparent that the simulation game G_3 and G_4 are not perceptible without proper execution of the aforementioned password guessing attacks. Hence, we have,

$$|P_r[Succ_4] - P_r[Succ_3]| \leq maxq_s(\frac{1}{2^{l_f}}, \varepsilon_{fmsg}) + 2q_H A_{dv}^{ECM-CDH}(t_{A_{dv}}). \tag{10}$$

Game G_5**.** The final game G_5 observes a strong property of forward security which simulates *Execute*, *Send*, and *Hash* queries over the old message transcript msg_1 and msg_2. As a consequence of this, two primary indices $\alpha\beta \in \{1, 2, ..., ..., (q_s + q_e)\}$ are chosen. In this case, the game may be terminated when the *Test* query cannot return any valid key $Session_{Key}$ for α^{th} instance of $User_i$ or β^{th} instance of C_{S_j}, respectively. In accordance with G_4 analysis, we achieve that,

$$|P_r[Succ_5] - P_r[Succ_4]| \leq 2q_H(q_s+q_e)^2 \times A_{dv}^{ECM-CDH}(t_{A_{dv}}). \tag{11}$$

Considering the aforementioned games G_0 to G_5, it is so certain to declare that A_{dv} has no advantageous gain to guess an appropriate bit f. Hence, we obtain,

$$P_r[Succ_5] = \frac{1}{2}. \tag{12}$$

Applying the property of triangular inequality, we have the successive probability to optimize the computation problem.

$$\begin{aligned}|P_r[Succ_0] - \frac{1}{2}| &= |P_r[Succ_1] - P_r[Succ_5]| \\ &\leq |P_r[Succ_1] - P_r[Succ_2]| \\ &+|P_r[Succ_2] - P_r[Succ_5]| \\ &\leq |P_r[Succ_1] - P_r[Succ_2]| \\ &+|P_r[Succ_2] - P_r[Succ_3]| \\ &+|P_r[Succ_3] - P_r[Succ_4]| \\ &\leq |P_r[Succ_1] - P_r[Succ_2]| \\ &+|P_r[Succ_2] - P_r[Succ_3]| \\ &+|P_r[Succ_3] - P_r[Succ_4]| \\ &+|P_r[Succ_4] - P_r[Succ_5]|.\end{aligned} \tag{13}$$

From the above equation Eq. (6) - Eq. (13), we derive,

$$\begin{aligned}\frac{1}{2}A_{dv_{\mathcal{P}}}^{ECM-CDH}(t_{A_{dv}}) &= |P_r[Succ_0] - \frac{1}{2}| \\ &\leq \frac{(q_s+q_e)^2}{2^{(l_r+1)}} + \frac{q_H^2}{2^{(l_h+1)}} \\ &+\frac{2q_s}{2^{l_r}} + \frac{5.q_H}{2^{l_h}} \\ &+max\left\{q_s\left(\frac{1}{|\mathbb{D}|}, \frac{1}{2^{l_f}}, \varepsilon_{fmsg}\right)\right\} \\ &+2q_H A_{dv_{A_{dv}}}^{ECM-CDH} \\ &+2q_H(q_s+q_e)^2 A_{dv_{A_{dv}}}^{ECM-CDH}.\end{aligned} \tag{14}$$

Finally, while multiplying opposite sides by 2 in Eq. (14) and re-arranging the substitute terms, the desired result can be obtained. Hence, *Theorem 1* is proved. ■

B. Performance Analysis

In this subsection, the experimental configuration was carefully devised to analyze the efficiency rate of the proposed PP-KAF with other existing schemes shown in Table III.

TABLE III: Configuration of Testing Devices

System Detail	Configuration Features
Desktop	Operating System: Windows 10 64-bit CPU: Core (6), 2.9 to 4.3 GHz (Cache) RAM: 8 GB HDD: 1 TB
Mobile Device	System: Meizu 16th OS: Android Oreo 8 Processor Core: Octa Clock Speed: 2.8 GHz RAM: 8 GB
Conversion Code	Board: STM (32) F (107) Kernel: Cortex-M(3) 32-bit, 76 MHz Flash: 256 KB and RAM: 64 KB

To calculate the consumption of resources, operations such as one-way cryptographic hash H_{ash}, elliptic-curve point multiplication ECC_M, a symmetric session key encryption/decryption S_{ED}, and $(T_n(x) \mod p)$ in Chebyshev polynomial computation T_{CP} are considered. As referred to in [18], [36], the elliptic-curve signature requires $30.67ms$ to complete installation on an Intel PXA-270 processor in a Linux personal assistant at a rate of $0.624GHz$. In the authentication process, client entities such as a trusted network, $'Ben'$, and $'Jas'$ participated. Two-way authentication between $'Ben'$ and $'Jas'$ executed $H_{ash} \approx 0.0005sec$, $ECC_M \approx 0.063075sec$, $S_{ED} \approx 0087ms$, and $T_{CP} \approx 0.02102sec$, respectively. We neglect the cost computation of XOR as it is significantly lower compared to other cost operations. Table IV summarizes the computation efficiencies of the proposed PP-KAF compared with other existing mechanisms [15]–[19], [21], [32].

TABLE IV: Comparison of Computation Efficiency.

Authentication Scheme	Smart/ User Device	Gateway Node	Registration Centre	Total Cost (ms)
Proposed PP-KAF	$2H_{ash}$	$4H_{ash}$ + $1T_{CP}$	$4H_{ash}$ + $1T_{CP}$	$10H_{ash}$ + $2T_{CP}$ ≈ 42.05
[15]	$13H_{ash}$	$19H_{ash}$	$11H_{ash}$	$32H_{ash}$ ≈ 21.5
[16]	$11H_{ash}$	$8H_{ash}$	$14H_{ash}$	$23H_{ash}$ ≈ 16.5
[17]	$10H_{ash}$	$7H_{ash}$	$19H_{ash}$	$36H_{ash}$ ≈ 18
[18]	$9H_{ash}$+2 T_{CP}	$7H_{ash}$ + $2T_{CP}$	$7H_{ash}$ + 2 T_{CP}	$23H_{ash}$ + $6T_{CP}$ ≈ 126.13
[19]	$7H_{ash}$ + $5T_{CP}$	$5H_{ash}$ + $2T_{CP}$	Not Available	$12H_{ash}$+7 T_{CP} ≈ 147.15
[32]	$12H_{ash}$ + $7T_{ECC-M}$	$11H_{ash}$ + $5T_{ECC-M}$	Not Available	$23H_{ash}$ + $12T_{ECC-M}$ ≈ 756.91
[21]	$8H_{ash}$	$8H_{ash}$	$10H_{ash}$	$26H_{ash}$ ≈ 13

In the execution of the authentication and key agreement, the proposed PP-KAF's total cost was $10H_{ash} + 2T_{CP} \approx 42.05ms$, whereas the other schemes [15]–[19], [21], [32] need more total execution time at $32H_{ash} \approx 21.5ms$, $23H_{ash} \approx 16.5ms$, $36H_{ash} \approx 18ms$, $23H_{ash} + 6T_{CP} \approx 126.13ms$, $12H_{ash} + 7T_{CP} \approx 147.15ms$, $23H_{ash} + 12T_{ECC-M} \approx 756.91ms$, $26H_{ash} \approx 13ms$, respectively. In accordance with the computation of total cost, the proposed PP-KAF has a lower computation cost $\approx 42.05ms$ than other Chebyshev chaotic map-based authentication [18], [19], [32], improving system efficiency. However, the other authentication schemes [15]–[17], [21] utilize lightweight operations like one-way hashing to improve their cost efficiencies. Since this study considers medical cyber-physical systems with a cloud computing environment, the proposed PP-KAF processes limited length of the message transmission on end users i.e., two message rounds to meet the practical requirements of battery-operated medical IoT devices. Considering this essential factor, the lightweight authentication schemes [15]–[17], [21] cannot fulfill the practical requirements of IoT devices as they are bound to perform more message transmission on end IoT devices.

TABLE V: Comparison of Communication Efficiency.

Authentication Scheme	Message Rounds	Total Transmission Cost $(bits)$
Proposed PP-KAF	2	992
[15]	4	2400
[16]	4	2912
[17]	4	3840
[18]	2	1280
[19]	3	1312
[32]	4	2208
[21]	6	2464

Table V depicts a comparison of communication efficiency. As referred to in [20], system parameters such as client identity, a random nonce, a hash digest, and a time stamp were $160bits$, $128bits$, $160bits$, and $32bits$, respectively. It was

also proven that $1024bits$ for $RSApublickeycryptosystem$ provided a security level similar to the $160bits$ for $ECCpublickeycryptosystem$ [20]. The proposed PP-KAF had $A_v = E_(SK_{gs})(H(U_{id}) \parallel r_m \parallel ms_{node} \parallel t_G \parallel t_U)$ and $L = E_(Session_{Key})(r_m^* \parallel ms_{node} \parallel t_S)$, incurring a cost of $[128 + 160 + 160 + 160 + 32] \approx 640bits$ and $[160 + 160 + 32] \approx 352bits$, respectively. Hence, the total communication cost of the proposed PP-KAF was $992bits$, whereas the schemes in [15], [16], [17], [18], [19], [32], and [21] consumed $2400bits$, $2912bits$, $3840bits$, $1280bits$, $1312bits$, $2208bits$, and $2464bits$, respectively. Table V shows that the proposed PP-KAF achieved better communication efficiency than the other authentication schemes.

For the experimental analysis, the system was equipped with the real-time setup shown in Table III. To analyze the throughput rate, a simple message transmission of $\approx 4KB$ was preferred between the smart device and the registration center through a trusted network. The throughput rate is generally defined as the number of transmitted bits per unit of time, which is mathematically expressed as $\frac{(v_r|\rho|)}{T_D}$, where T_D is the total packet size, v_r is the total number of packets received, and ρ is the individual packet size. From Fig. 5(a), we see that the proposed PP-KAF achieved better throughput than the other schemes. Since it has lower computation and communication costs, it can manage smart devices more effectively to establish a reliable connection with Reg_{Centre}. After establishing a reliable connection with Reg_{Centre}, the hub of computing devices has more frames in the queue to transmit or retransmit data packets during a limited time interval. The average delay can be expressed as follows:

$$A_D = T_{CU} + T_{Pro} + T_{Frame} \tag{15}$$

where T_{CU} is the cumulative delay of the successfully transmitted frame, T_{Pro} is the propagation delay, and T_{Frame} is the total frame duration. To analyze the efficiency rate, the average delay varies with different transmission rates $\approx 971.4kbps$. Each computing device uniformly utilizes a random value from the given interval to analyze the data traffic. It has low and high user priorities to schedule the access intervals, which not only acquires a channel but also establishes a hub association. However, the expected transmission time verifies the guard time with the remaining time slots to release the current transmission. Therefore, the proposed PP-KAF had a lower transmission delay, improving system efficiency compared to other schemes, as shown in Fig. 5(b). To evaluate the energy cost, the proposed PP-KAF and the other schemes assumed the power capacity of the computing device to be $\approx 10.88W$. The energy cost is expressed as:

$$E_C = CC_T \times P_C \tag{16}$$

where CC_T is the calculated computation cost, and P_C is the maximum power capacity of the computing device.

The other schemes could not lessen the computation cost because it is based on asymmetric cryptography. However, the proposed PP-KAF consumes lower computation and communication costs to control access functionalities, including computing devices, time stamps, and temporary identities. The proposed PP-KAF handles data transmissions effectively to reduce the exchange of computation parameters, which adopts the computing device to offload data traffic. As a result, the proposed PP-KAF uses less energy over time, improving the consumption ratio of the eHealth system as shown in Fig. 5(c).

VI. Conclusion

This paper presented a privacy-preserving key agreement framework (PP-KAF) mechanism for cloud-assisted medical cyber-physical systems, which applies two-way authentication to guarantee transmission security. Theoretical analysis showed that the proposed PP-KAF proved it yields better security and user privacy. Moreover, performance analysis demonstrated that the proposed PP-KAF incurs lower communication costs, improving system efficiency in terms of throughput, average delay, and energy cost to satisfy the practical necessities of battery-operated medical IoT devices. In the future, the development of the Internet of Medical Things will be integrated in order to consider a strong security evaluation that may influence a better mobility scenario for ambient assisted living.

References

[1] D. McGlade and S. Scott-Hayward, "Ml-based cyber incident detection for electronic medical record (emr) systems," *Smart Health*, vol. 12, pp. 3–23, 2019.

[2] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in iot," *IEEE Access*, vol. 7, pp. 135 632–135 649, 2019.

[3] B. D. Deebak, F. Al-Turjman, and L. Mostarda, "Seamless secure anonymous authentication for cloud-based mobile edge computing," *Computers & Electrical Engineering*, vol. 87, p. 106 782, 2020.

[4] K. N. Mishra, "An efficient approach towards enhancing the performance of m-health using sensor networks and cloud technologies," *Internet of Things (IoT) Concepts and Applications*, pp. 491–513, 2020.

[5] S. Xu, Y. Li, R. H. Deng, Y. Zhang, X. Luo, and X. Liu, "Lightweight and expressive fine-grained access control for healthcare internet-of-things," *IEEE Transactions on Cloud Computing*, vol. 10, no. 1, pp. 474–490, 2019.

[6] J. Chen, M. C. Fu, W. Zhang, and J. Zheng, "Supporting real-time covid-19 medical management decisions: The transition matrix model approach," *arXiv preprint arXiv:2007.01201*, 2020.

[7] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[8] Q. He, N. Zhang, Y. Wei, and Y. Zhang, "Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems," *Computer Networks*, vol. 140, pp. 163–173, 2018.

[9] L. Zhang, Y. Zhu, W. Ren, Y. Wang, and N. N. Xiong, "An energy efficient authentication scheme using chebyshev chaotic map for smart grid environment," *arXiv preprint arXiv:2008.11366*, 2020.

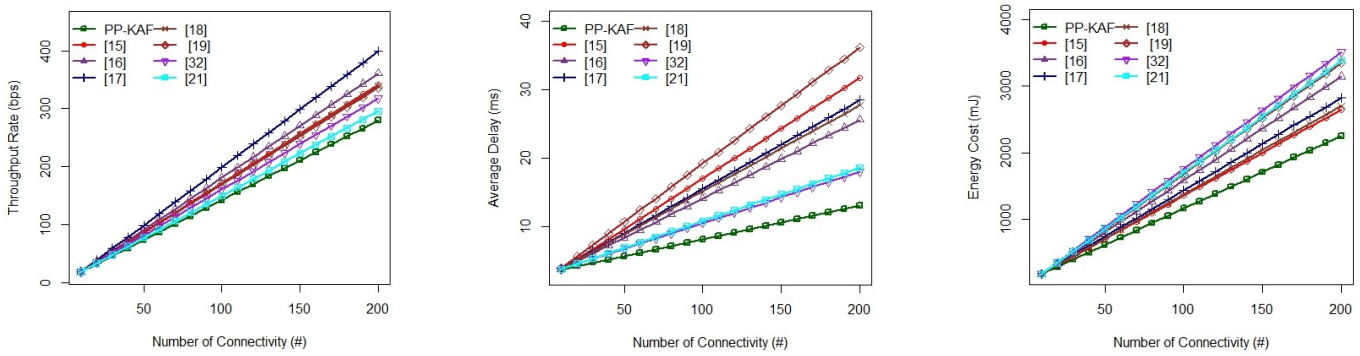
[10] J. Li, N. Zhang, J. Ni, J. Chen, and R. Du, "Secure and lightweight authentication with key agreement for smart wearable systems," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7334–7344, 2020.

[11] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 39–50, 2019.

[12] M. Qi and J. Chen, "Anonymous biometrics-based authentication with key agreement scheme for multi-server environment using ecc," *Multimedia Tools and Applications*, vol. 78, pp. 27 553–27 568, 2019.

[13] I. Altaf, M. Arslan Akram, K. Mahmood, S. Kumari, H. Xiong, and M. Khurram Khan, "A novel authentication and key-agreement scheme for satellite communication network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, e3894, 2021.

[14] D. BD, F. Al-Turjman, and L. Mostarda, "A hash-based rfid authentication mechanism for context-aware management in iot-based multimedia systems," *Sensors*, vol. 19, no. 18, p. 3821, 2019.



(a) Throughput Rate (bps) (b) Average Delay (ms) (c) Energy Cost (mJ)

Fig. 5: Examined the number of connectivity (#) in a configured testing device

[15] M. Wazid, A. K. Das, S. Shetty, J. JPC Rodrigues, and Y. Park, "Ldakm-eiot: Lightweight device authentication and key management mechanism for edge-based iot deployment," *Sensors*, vol. 19, no. 24, p. 5539, 2019.

[16] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-iot based healthcare services," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, pp. 619–636, 2019.

[17] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight iot-based authentication scheme in cloud computing circumstance," *Future generation computer systems*, vol. 91, pp. 244–251, 2019.

[18] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 824–839, 2016.

[19] L. Zhang, Y. Zhu, W. Ren, Y. Wang, K.-K. R. Choo, and N. N. Xiong, "An energy-efficient authentication scheme based on chebyshev chaotic map for smart grid environments," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 17 120–17 130, 2021.

[20] T.-F. Lee and M. Chen, "Lightweight identity-based group key agreements using extended chaotic maps for wireless sensor networks," *IEEE Sensors Journal*, vol. 19, no. 22, pp. 10 910–10 916, 2019.

[21] 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 Computing*, pp. 1–15, 2023.

[22] S.-Y. Chiou, Z. Ying, and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *Journal of medical systems*, vol. 40, pp. 1–15, 2016.

[23] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, "A privacy authentication scheme based on cloud for medical environment," *Journal of medical systems*, vol. 38, pp. 1–16, 2014.

[24] P. Mohit, R. Amin, A. Karati, G. Biswas, and M. K. Khan, "A standard mutual authentication protocol for cloud computing based health care system," *Journal of medical systems*, vol. 41, pp. 1–13, 2017.

[25] C.-T. Li, D.-H. Shih, and C.-C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems," *Computer methods and programs in biomedicine*, vol. 157, pp. 191–203, 2018.

[26] V. Kumar, S. Jangirala, and M. Ahmad, "An efficient mutual authentication framework for healthcare system in cloud computing," *Journal of medical systems*, vol. 42, pp. 1–25, 2018.

[27] V. Kumar, M. Ahmad, and A. Kumari, "A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted tmis," *Telematics and Informatics*, vol. 38, pp. 100–117, 2019.

[28] B. D. Deebak and F. Al-Turjman, "Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 346–360, 2020.

[29] X. Chen, X. Zhang, D. Geng, L. Zhou, J. Chen, F. Lu, *et al.*, "A rfid authentication protocol for epidemic prevention and epidemic emergency management systems," *Journal of Healthcare Engineering*, vol. 2021, 2021.

[30] K. Mansoor, A. Ghani, S. A. Chaudhry, S. Shamshirband, S. A. K. Ghayyur, and A. Mosavi, "Securing iot-based rfid systems: A robust authentication protocol using symmetric cryptography," *Sensors*, vol. 19, no. 21, p. 4752, 2019.

[31] Y. Chen and J. Chen, "An efficient and privacy-preserving mutual authentication with key agreement scheme for telecare medicine information system," *Peer-to-Peer Networking and Applications*, pp. 1–13, 2022.

[32] L. Xiong, T. Peng, F. Li, S. Zeng, and H. Wu, "Privacy-preserving authentication scheme with revocability for multi-wsn in industrial iot," *IEEE Systems Journal*, 2022.

[33] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, pp. 4767–4779, 2011.

[34] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ecc-based mutual authentication and session key generation scheme for healthcare applications," *Journal of medical systems*, vol. 43, no. 1, p. 10, 2019.

[35] S. Han, T. Jager, E. Kiltz, *et al.*, "Authenticated key exchange and signatures with tight security in the standard model," in *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part IV 41*, Springer, 2021, pp. 670–700.

[36] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2016.

B D Deebak received his Ph.D. degree in computer science from SASTRA Deemed University, Thanjavur, India, in 2016. He is currently a Brain Pool Fellow with the Department of Computer Engineering, Department Computer Engineering, Gachon University, Seongnam 13120, Korea. He is an Active Member of professional societies like IE (I), CSI, and ISTE. His research interests include multimedia networks, network security, the Internet of Things, and machine learning.

SEONG OUN HWANG (Senior Member, IEEE) received his Ph.D. degree in computer science from the Korea Advanced Institute of Science and Technology, in 2004, South Korea. He is currently a Full Professor at the Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea. His research interests include cryptography, cybersecurity, data-centric artificial intelligence, and artificial intelligence.