CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC

ADESH KUMARI¹, VINOD KUMAR², M. YAHYA ABBASI¹, SARU KUMARI³, PRADEEP CHAUDHARY⁴, AND CHIEN-MING CHEN⁵, (Senior Member, IEEE)

¹Department of Mathematics, Jamia Millia Islamia, New Delhi 110025, India
²Department of Mathematics, PGDAV College, University of Delhi, New Delhi 110065, India
³Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India
⁴Department of Statistics, Chaudhary Charan Singh University, Meerut 250004, India
⁵College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

Corresponding authors: Saru Kumari (saryusiirahi@gmail.com) and Chien-Ming Chen (chienmingchen@ieee.org)

ABSTRACT
Smart architecture is the concept to manage the facilities via internet utilization in a proper manner. There are various technologies used in smart architecture such as cloud computing, internet of things, green computing, automation and fog computing. Smart medical system (SMS) is one of the application used in architecture, which is based on communication networking along with sensor devices. In SMS, a doctor provides online treatment to patients with the help of cloud-based applications such as mobile device, wireless body area network, etc. Security and privacy are the major concern of cloud-based applications in SMS. To maintain, security and privacy, we aim to design an elliptic curve cryptography (ECC) based secure and efficient authentication framework for cloud-assisted SMS. There are six phases in the proposed protocol such as: patient registration phase, healthcare center upload phase, patient data upload phase, treatment phase, checkup phase and emergency phase. In CSEF, there are four entities like healthcare center, patient, cloud and doctor. In CSEF, mutual authentication establishes between healthcare center and cloud, patient and cloud, doctor and cloud, and patient and healthcare center by the using ECC and hash function. The CSEF is secure against security attacks, and satisfies many security attributes such as man-in-the-middle attack, impersonation attack, data non-repudiation, doctor anonymity, replay attack, known-key security property, message authentication, patient anonymity, data confidentiality, stolen-verifier attack, parallel session attack and session key security. Further, the CSEF is efficient in terms of computation and communication compared to others related frameworks. As a result, CSEF can be utilized in cloud-based SMS.

INDEX TERMS
Cloud-medical system, elliptic curve cryptography, mutual authentication, signature, security and privacy.

I. INTRODUCTION
In the smart cities, there are billions of devices which are associated with IoT framework for different applications. Smart city is the environment that designates to develop the facilities to citizen and government assistance by preparing internet technologies. With the rapid advancement of machine-to-machine and device-to-device communication, there is an exponential increment in the utilization of different smart applications, such as smart e-healthcare and smart education etc. IoT-based framework is being utilized worldwide in the construction of future smart cities [1] to provide services such as e-healthcare and smart transport system to the end clients. The cloud computing is a structure of resources using different applications. To offer favorable and quick network services, a new type of cloud computing association [2], [3] includes a large number of processors, high-speed networks, memories and various devices are presented by users via the internet server. Cloud services offer through a web browser to get online data information. These computing strategies can be obtained by the cloud stage. In addition, Tsai et al. [4] clarified that cloud services will be useful in the future. In this way, privacy and security of cloud have turned out to be important issues. Different research articles have
presented various issues of their misgivings, for example, cloud privacy [5], [6] and cloud services [7]. As given in [8]–[20] many operations are related to utilization and cloud services in cyber physical system.

With the speedy advancement of data innovation, the utilization of SMS is expanding step by step. SMS is one of the application which is used in cloud environment [21]. In SMS, a doctor provides online treatment to patients via cloud system. There are more information about healthcare system and its application in [22]–[24]. In SMS, patient and doctor communicated to each other via cloud server in insecure communication channel. It is major concern that cloud is not fully secure. For this system, there are many security issues like patent anonymity and unlinkability, doctor anonymity and unlinkability, data confidentiality, integrity, etc [25]–[27]. In SMS, users have unique access unambiguous and privilege in healthcare system. They save and recapture their data in cloud database. This data can be classified in many categories which manages user and system level obligations. Chatterjee et al. [28] presented biometric and access control based authentication framework for SMS with adapted structure, which does not maintain patient unlinkability and the medical information between patient and doctor in public channel. Amin et al. suggested an authentication framework for healthcare system [29] and patient authentication work using wireless sensor networks for medical system [30]. But, still there is a need to make secure and efficient authentication framework for the patient, doctor, medical data and other security aspects in medical system, so that any attacker could not find patient’s or doctor’s data information. Recently, there are many schemes proposed to recognized these issues [28], [29], [31], [32]. In the proposed framework, we develop a secure and efficient mutual authentication framework using ECC and cloud for SMS.

A. RELATED WORK

In recent years, there are many cloud based authentication protocols for TMIS [3], [33]–[42]. Islam et al. suggested authentication framework which is used for integrated method to user for information exchange in communication system [43]. Wazid et al. proposed anonymity preservation authentication and key agreement method for healthcare system [32]. Sutrala et al. suggested RSA-based patient anonymous authentication framework for TMIS and discuss that their scheme is secure over insecure channel with verifying security tools [44]. In 2012, Padhy et al. suggested approach for cloud-based in TMIS [45]. In 2014, Chen et al. provided a cloud-assisted data exchange framework [46]. In the same year, Chen et al. suggested a safe authentication framework for cloud-based healthcare system [47]. In 2015, Amin et al. proposed key agreement scheme for healthcare system [23], He et al. provided robust anonymous authentication framework for TMIS [34]. Zhou et al. offered a safe and efficient framework for cloud-assisted wireless body area network [48]. In 2016, Chiou et al. [49] provided cryptanalysis of Chen et al. framework and show that it fails to patient anonymit, message authentication and real-life application. Moreover, Chiou et al. suggested an enhanced framework in similar environment. In 2017, Mohit et al. [50] disclosed that Chiou et al. framework fails mobile stolen verifier attack and patient anonymity. Meanwhile, Mohit et al. suggested an enhanced key agreement framework for TMIS. In same the year, Jangirala et al. suggested user authentication work for health system which is based on medical sensor approach [6]. In 2018, Jangirala et al. proposed an authentication protocol for cloud-centric public safety device communications [51]. In the same year, Li et al. shows that Mohit et al. framework fails to patient anonymity and unlinkability, health report revelation attack, inspection report forgery attack and absence of medical relationship among them. Moreover, they provided an enhance protocol in the similar background [52]. In 2019, Chandrakar et al. proposed cloud-based authenticated scheme for healthcare monitoring system protocol which fails against patient unlinkability, impersonation attack and doctor unlinkability [53]. In same year, Kumari et al. [54] discussed design flaws and cryptanalysis of Mohit et al. [50] protocol. Ghani et al. [55] proposed a secure and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. This work is secure and efficient in communication system. Mahmood et al. [56] presented an enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure. Hussain et al. [57] discussed security weaknesses of Das et al.’s protocol [58] like traceability, stolen-verifier attack, stolen smart device attack and non provision of perfect forward secrecy. Mansoor et al presented securing IoT-based RFID systems: a robust authentication protocol using symmetric cryptography [59]. In this protocol, Mansoor et al. found security drawback of protocol [60] such as collision attack, stolen verifier attack and DoS attack. Further, They provided improved authentication protocol in same environment. Chaudhry et al. proposed correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems [61]. In this protocol, authors have discussed design flow and incorrectness of the Challa et al.’s protocol [62]. Further, Chaudhry et al. proposed enhanced protocol in cyber physical systems. In 2020, Chen et al. [63] proposed a secure electronic medical record authorization system for smart device application in cloud computing environments, Mo et al. [64] proposed an improved anonymous authentication protocol for wearable health monitoring systems and Alzahrani et al. [65] proposed a secure and efficient remote patient-monitoring authentication protocol for cloud-IoT.

B. MOTIVATIONS

With growth in science and engineering, different utilization scope of Smart-Physical System (SPS) are now opening due to their developing safety, usability, reliability efficiency and autonomy. For offering on-demand access to shared deal with utilizations, cloud environment is crucial in order to reduce infrastructure expenditures. However, the
communication between entities in cloud-based SMS is vulnerable to many attacks, such as replay, man-in-the-middle, impersonation, anonymity, known-key security, data confidentiality, data non-repudiation, message authentication, stolen-verifier attack, privileged-insider attack and parallel session attack. Thus, to ensure quality of service, information, security and privacy is an basic concern in cloud-based SMS.

Section II, The CSEF framework. Section IV, The security evaluation. Section V, performance evaluation. Finally, we have given conclusion. Further, we have provided Table.1 for the useful notations in the paper.

II. MATHEMATICAL PRELIMINARIES

A. ELLIPTIC CURVE CRYPTOGRAPHY OVER FINITE FIELD

Let where \( q \) be the large prime number and \( \mathcal{E}(F_q) \) denotes an elliptic curve (EC) over prime finite field \( F_q \). An equation of elliptic curve over \( F_q \) is given by \( v^2 = u^3 + \alpha u + \beta \mod q \), where \( \alpha, \beta \in F_q \). The EC is said to be non singular if \( 4\alpha^3 + 27\beta^2 \mod q \neq 0 \). \( G \) is the group under addition which is defined as \( G = \{ (u, v) : u, v \in F_q, (u, v) \in \mathcal{E} \} \cup \{ \Phi \} \), where the point \( \Phi \) is known as a zero member of \( G \).

The followings properties of \( G \) are defined as [66], [67]:
1. Let \( \bigvee = (u, v) \in G \), then defined \( - \bigvee = (u, -v) \) and \( \bigvee + (-\bigvee) = \Phi \).
2. If \( \bigvee_1 = (u_1, v_1), \bigvee_2 = (u_2, v_2) \in G \), then \( \bigvee_1 + \bigvee_2 = (u_3, v_3) \), where \( u_3 = \rho^2 - u_1 - u_2 \mod q, v_3 = \rho(u_1 - u_3) - v_1 \mod q \), and
   \[
   \rho = \begin{cases} 
   \frac{v_2 - v_1}{u_2 - u_1} \mod q & \text{if } \bigvee_1 \neq \bigvee_2 \\
   \frac{3u_1^2 + \alpha}{2v_1} \mod q & \text{if } \bigvee_1 = \bigvee_2 
   \end{cases}
   \]
3. Let \( \bigvee = (u, v) \in G \) then, scalar multiplication in \( G \) such as: \( \eta \bigvee = \bigvee + \bigvee + \bigvee + \ldots + \bigvee \) \( (\eta \times \text{times}) \).
4. If \( g \) is the generator of \( G \) with order \( \eta \), then \( \eta g = \Phi \).

For more details, we refer [66], [68].

B. ECC BASED COMPUTATIONAL HARD PROBLEM

* Definition 1. Elliptic curve discrete logarithms problem (ECDLP): For given \( \bigvee_1, \bigvee_2 \in G \) to find \( \mu \in \mathbb{Z}_q^* \) such that \( \bigvee_2 = \mu \bigvee_1 \) is hard [69].

* Definition 2. Elliptic curve computational Diffie-Hellman problem (ECDHP): For \( \alpha, \beta \in \mathbb{Z}_q^* \) and \( g \)

D. ORGANIZATION OF THE PAPER

The remaining part of the paper is mapped as follows. Section II, we describe the Mathematical preliminaries. Section III, The CSEF framework. Section IV, The security evaluation. Section V, performance evaluation. Finally, we have given conclusion. Further, we have provided Table.1 for the useful notations in the paper.

### II. MATHEMATICAL PRELIMINARIES

#### A. ELLIPTIC CURVE CRYPTOGRAPHY OVER FINITE FIELD

Let where \( q \) be the large prime number and \( \mathcal{E}(F_q) \) denotes an elliptic curve (EC) over prime finite field \( F_q \). An equation of elliptic curve over \( F_q \) is given by \( v^2 = u^3 + \alpha u + \beta \mod q \), where \( \alpha, \beta \in F_q \). The EC is said to be non singular if \( 4\alpha^3 + 27\beta^2 \mod q \neq 0 \). \( G \) is the group under addition which is defined as \( G = \{ (u, v) : u, v \in F_q, (u, v) \in \mathcal{E} \} \cup \{ \Phi \} \), where the point \( \Phi \) is known as a zero member of \( G \).

The followings properties of \( G \) are defined as [66], [67]:
1. Let \( \bigvee = (u, v) \in G \), then defined \( - \bigvee = (u, -v) \) and \( \bigvee + (-\bigvee) = \Phi \).
2. If \( \bigvee_1 = (u_1, v_1), \bigvee_2 = (u_2, v_2) \in G \), then \( \bigvee_1 + \bigvee_2 = (u_3, v_3) \), where \( u_3 = \rho^2 - u_1 - u_2 \mod q, v_3 = \rho(u_1 - u_3) - v_1 \mod q \), and
   \[
   \rho = \begin{cases} 
   \frac{v_2 - v_1}{u_2 - u_1} \mod q & \text{if } \bigvee_1 \neq \bigvee_2 \\
   \frac{3u_1^2 + \alpha}{2v_1} \mod q & \text{if } \bigvee_1 = \bigvee_2 
   \end{cases}
   \]
3. Let \( \bigvee = (u, v) \in G \) then, scalar multiplication in \( G \) such as: \( \eta \bigvee = \bigvee + \bigvee + \bigvee + \ldots + \bigvee \) \( (\eta \times \text{times}) \).
4. If \( g \) is the generator of \( G \) with order \( \eta \), then \( \eta g = \Phi \).

For more details, we refer [66], [68].

#### B. ECC BASED COMPUTATIONAL HARD PROBLEM

* Definition 1. Elliptic curve discrete logarithms problem (ECDLP): For given \( \bigvee_1, \bigvee_2 \in G \) to find \( \mu \in \mathbb{Z}_q^* \) such that \( \bigvee_2 = \mu \bigvee_1 \) is hard [69].

* Definition 2. Elliptic curve computational Diffie-Hellman problem (ECDHP): For \( \alpha, \beta \in \mathbb{Z}_q^* \) and \( g \)
A. Kumari et al.: CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC

FIGURE 1. Architecture for CSEF with different phases.

TABLE 2. ECC and RSA key size compassion [68], [70].

| ECC key size (Bits) | RSA key size (Bits) | Key size ratio |
|---------------------|--------------------|---------------|
| 163                 | 1024               | 1.6           |
| 256                 | 3072               | 1.2           |
| 384                 | 7680               | 1.2           |
| 512                 | 15360              | 1.3           |

is the base of $G$, given $(g, \alpha g, \beta g)$, then to compute $\alpha\beta g$ is hard in group $G$ [69].

* Definition 3. Elliptic curve factorization problem (ECFP): For $\alpha, \beta \in \mathbb{Z}_q^*$ and $\sqrt{1}, \sqrt{2} = \alpha \sqrt{1} + \beta \sqrt{2} \in G$, then to compute $\alpha \sqrt{1}$ and $\beta \sqrt{2}$ is hard in group $G$ [70].

We assume that the three problems above are intractable. That is, there is no polynomial time algorithm that can solve these problems with non-negligible probability. Next, we explain why we adopted ECC to design the authentication protocol for smart medical system networks.

- More complex: Since ECC can be implemented in different ways rather than a single encryption algorithm, it is more complex compared to RSA. Moreover, ECDLP is more difficult to break than the factorization and discrete logarithm problem. Although many authors have tried to attack ECC. But, it is still infeasible to break ECC with existing computational resources. Thus, the security strength of ECC is much stronger than other public key cryptosystems like as Diffie-Hellman (D-H) or RSA [70].

- Smaller key size: As displayed in Table 2, we compare RSA and ECC offers equivalent security with smaller key sizes which implies lower power, bandwidth, and computational requirements. These advantages are very important when public-key cryptography is implemented for low power environments [70].

- Computational efficiency: ECC is much more efficient than RSA and D-H public protocols in terms of computation, since implementing scalar multiplication in software and hardware is much more feasible than performing multiplications or exponentiations in them [70].

Thus, according to above attractive properties of ECC, we chose it to design the proposed CSEF.

C. DOELEV-YAO (DY) THREAT MODEL

In CSEF, we consider the Dolev-Yao (DY) model which has discussed in [71]. There are following assumptions for the capacities of any adversary $A$:

- $A$ can access the public network. He/she can modify, retrieve, replay, inject new message and can discard any communication network.

- $A$ is presumed to be protected, therefore cannot obtain the secret key of participants.

- $A$ knows the public identifier of all the participants.

- $A$ can be an intruder or can be an insincere entity of the underlying communication system.

III. THE CSEF FRAMEWORK

A. ARCHITECTURE

There are four entities in this framework like Patient, Doctor, Cloud server and Healthcare center. The architecture of CSEF is shown in the Figure 1.
TABLE 3. RP of CSEF.

| Patient P | Healthcare center H |
|-----------|---------------------|
| Inputs $ID_P$, $PW_P$ | Sends $(ID_P, PW_P, T_{R1})$ |
| Computes $PW_P = h(h(ID_P \| PW_P) \| ID_P \| PW_P)$ | $\Rightarrow$ |
| Sends $(ID_P, PW_P, T_{R1})$ | $\Rightarrow$ |
| Verifies $T_{R2} = T_{R1} \leq \Delta T$ |
| Computes $NID_P = h(ID_P \| PW_P \| T_{R1})$ |
| Generates $sn_P \in Z_q^*$ |
| Stores $NID_P, ID_P, sn_P$ in cloud database |
| Encrypts $E_{P1} = E_h(ID_P \| PW_P \| T_{R1} \| ID_P \| PW_P, sn_P)$ |
| Sends $(E_{P1})$ |

Decryption $D_{h}(PW_P \| T_{R1} \| ID_P \| E_{P1})$:

Step 1. $H$ generates medical record $m_H = (ID_P, Data_P)$ and random value $a \in Z_q^*$. Then, $H$ inputs $ID_H$ and $a$.

Step 2. $C$ on getting $M_1 = \{E_1, T_{H1}\}, C$ verifies $T_{C1} - T_{H1} \leq \Delta T$. Then, $C$ decrypts $(ID_H, ag) = D_h(PKW_h \| T_{H1} \| PKC \| T_{H1})(E_1)$, generates random number $b \in Z_q^*$, computes $H_1 = h(ID_H \| bl \| bg \| T_{H1}),$ encrypts $E_2 = E_h(ID_H \| bl \| bg \| T_{H1}\| T_{C2}(bg, H_1)$, after that, $C \rightarrow H : M_2 = \{E_2, T_{C2}\}$.

Step 3. On getting $M_2 = \{E_2, T_{C2}\}$, $H$ verifies $T_{H2} - T_{C2} \leq \Delta T$. Then, $H$ decrypts $(bg, H_1) = D_h(PKW_h \| T_{H1} \| PKC \| T_{H1})(E_2)$, computes $H_2^* = h(ID_H \| bg \| T_{H1})$ and verifies $H_1^* = H_2^*$. Further, $H$ computes session key $SK_{CH} = h(ID_H \| m_H \| abg)$ in cloud database, encrypts $C_1 = E_h(ID_H \| m_H \| T_{C2}(bg, H_1)$, makes digital signature $S_i_{H} = SP_{R}(h(m_H))$, computes $H_3 = h(SK_{CH} \| C_1 \| S_i_{H} \| T_{C2})$, and encrypts $E_3 = E_{SK_{CH}}(ID_P, NID_P, sn_P, C_1, H_2, S_i_{H})$, after that, $H \rightarrow C : M_3 = \{E_3, T_{H2}\}$.

Step 4. Upon collecting $M_3 = \{E_3, T_{H3}\}, C$ verifies $T_{C3} - T_{H3} \leq \Delta T$. Then, $C$ decrypts $(ID_P, NID_P, sn_P, C_1, H_2, S_i_{H}) = D_{SK_{CH}}(E_3)$, computes $H_4^* = h(SK_{CH} \| C_1 \| S_i_{H} \| T_{H3})$ and stores $(ID_P, NID_P, C_1, H_2, S_i_{H})$ in database.

TABLE 4. HUP of CSEF.

| Healthcare center H | Cloud C |
|---------------------|---------|
| Generates $m_H = (ID_P, Data_P)$ | Verifies $C_{T1} - T_{H1} \leq \Delta T$ |
| Generates $a \in Z_q^*$ | Decrypts $(ID_H, ag) = D_h(PKW_h \| T_{H1} \| PKC \| T_{H1})(E_1)$ |
| Inputs $ID_H$ and $a$ | Generates $b \in Z_q^*$ |
| Encrypts $E_1 = E_h(PKW_h \| T_{H1} \| PKC \| T_{H1})(E_1)$ | Computes $H_1 = h(ID_H \| bg \| T_{H1})$ |
| Sends $M_1 = \{E_1, T_{H1}\}$ | $\Rightarrow$ |
| $\Rightarrow$ | Verifies $H_1 \neq H_2$ |
| $\Rightarrow$ | Computes $SK_{CH} = h(ID_H \| m_H \| abg)$ |
| $\Rightarrow$ | Decrypts $(ID_P, NID_P, sn_P, C_1, H_2, S_i_{H}) = D_{SK_{CH}}(E_3)$ |
| $\Rightarrow$ | Computes $H_2^* = h(SK_{CH} \| C_1 \| S_i_{H} \| T_{C2})$ |
| $\Rightarrow$ | Verifies $H_2^* = H_3^*$ |
| $\Rightarrow$ | Stores $(ID_P, C_1, H_2, S_i_{H}, NID_P, sn_P)$ |

B. PROTOCOL DESCRIPTION

There are five phases in CSEF: (1) RP, (2) HUP, (3) PUP, (4) TP, (5) CP and (6) EP. The details of these phases are as below:

1) REGISTRATION PHASE

In this phase, $P$ gets registration with the help of $H$. The detail of this phase is shown in Table 3 and described as below:

Step 1. $P$ inputs $ID_P, PW_P$ and executes $PW_P = h(h(ID_P \| PW_P) \| ID_P \| PW_P)$ and $P \Rightarrow H : (ID_P, PW_P, T_{R1})$.

Step 2. On getting $(ID_P, PW_P, T_{R1}), H$ checks $T_{R2} - T_{R1} \leq \Delta T$. $H$ computes $NID_P = h(ID_P \| PW_P \| T_{R1})$, generates $sn_P \in Z_q^*$. Then, stores $NID_P, ID_P, sn_P$ in cloud database. Further, $H$ encrypts $E_{P1} = E_h(PKW_P \| T_{R1})(NID_P, ID_P, sn_P)$ and $H \Rightarrow P : (E_{P1})$.

Step 3. Upon collecting $(E_{P1}), P$ decrypts $(NID_P, ID_P, sn_P) = D_h(PKW_P \| T_{R1})(E_{P1})$ and stores parameters $(NID_P, ID_P, sn_P)$ in database.

2) HEALTHCARE CENTER UPLOAD PHASE

In HUP, $H$ and $C$ manage the session key $H$ sends $P$’s medical data to $C$. The information of this phase is shown in Table 4 and explained as above:
TABLE 5. PUP of CSEF.

| Patient $P$ | Cloud $C$ |
|--------------|------------|
| Generates $m_B = (ID_P, Database)$ | Verifies $T_{C6} - T_{P1} ≤ ΔT$ |
| Inputs $ID_P, NID_P$ | $(ID_P, NID_P) = E_h(ID_P||NID_P||T_{P1})(E_4)$ | |
| Encrypts $E_4 = E_h(ID_P||NID_P||T_{P1})(ID_P, NID_P)$ | Generates $c ∈ Z^*_q$ | |
| Sends $M_4 = (ID_P, T_{P1})$ | Computes $H_3 = h(IDP ||sn_ID ||CID ||SigH ||c ||T_{C5} ||T_{P1})$ | |
| | Encrypts $E_5 = E_h(sn_{ID} ||CID ||SigH ||c ||T_{C5} ||T_{P1})(E_4)$ | |
| | Sends $M_5 = (E_5, T_{C5})$ | Stores $CP, ID_P, SK_P$ in database |

verifies $H_3^* = H_3$. After that, $C$ stores parameters $ID_P, CID, SigH, NID_P, sn_P$ in database.

3) PATIENT DATA UPLOAD PHASE

In PUP, $P$ requests body sensor to collect the fresh medical record of $P$ and sends to $P$’s mobiles device. The details of this phase is shown in the Table 5 and explained as below:

Step 1. $P$ medical record $m_R = (ID_P, Database)$ from sensor. Then, $P$ inputs $ID_P, NID_P$ and encrypts $E_4 = E_h(ID_P||NID_P||T_{P1})(ID_P, NID_P)$. Then, $P → C : M_4 = (ID_P, T_{P1})$.

Step 2. Upon getting $M_4 = (ID_P, T_{P1})$, $C$ checks $T_{C4} - T_{P1} ≤ ΔT$. Then, $C$ decrypts $(ID_P, NID_P) = E_h(ID_P||NID_P||T_{P1})(E_4)$, generates random number $c ∈ Z^*_q$, computes $H_3 = h(IDP ||sn_ID ||CID ||SigH ||c ||T_{C5} ||T_{P1})$ and encrypts $E_5 = E_h(sn_{ID} ||CID ||SigH ||c ||T_{C5} ||T_{P1})(E_4)$. Then, $C → P : M_5 = (E_5, T_{C5})$.

Step 3. On collecting $M_5 = (E_5, T_{C5})$, $P$ verifies $T_{P2} - T_{C5} ≤ ΔT$. Then, $P$ decrypts $(SigH, CID, H_3, ID_P, T_{C5}) = E_h(sn_{ID} ||CID ||SigH ||c ||T_{C5} ||T_{P1})(E_5)$, computes $H_3^* = h(IDP ||sn_ID ||CID ||SigH ||c ||T_{C5} ||T_{P1})$ and verifies $H_3^* = H_3$. Further, $P$ generates random number $d ∈ Z^*_q$, computes $SK_{PC} = h(IDP ||ID_H ||CID ||H_3^* ||T_{C5} ||T_{P1})$, decrypts $m^*_H = D_h(IDP||ID_H||CID)(P_C)$, verifies $m^*_H = h(IDP ||ID_H ||CID ||H_3^* ||T_{C5} ||T_{P1})$ and encrypts $H_4 = h(SK_{PC} ||CP ||SigP ||T_{P3} ||T_{C5})$ and encrypts $E_6 = E_h(sn_{ID} ||CID ||SigH ||c ||T_{C5} ||T_{P1})(E_4)$. Then, $P → C : M_6 = (E_6, T_{P3})$.

Step 4. On getting receiving $M_6 = (E_6, T_{P3})$, $C$ checks $T_{C6} - T_{P3} ≤ ΔT$. Then, $C$ decrypts $(dg, SnA, SigP, CP) = D_h(sn_{ID} ||CID ||SigH ||c ||T_{C5} ||T_{P1})(E_5)$ and computes session key $SK_{CP} = h(IDP ||ID_H ||CID ||H_3^* ||T_{C5} ||T_{P1})$. Further, $C$ computes $H_4^* = h(SK_{PC} ||CP ||SigP ||S3 ||ID_P ||ID_H ||T_{C5} ||T_{P1} ||T_{C5})$ and verifies $H_4^* = H_4$. Then, $C$ stores parameters $CP, ID_P, SigP$ in database.

4) TREATMENT PHASE

The information of TP shown in Table 6 and explained as below:

Step 1. $D$ generates random $r ∈ Z^*_q$, encrypts $E_7 = E_h(pk_D ||pk_C ||pk_T ||T_{D1})(ID_D, rg)$ and $D → C : M_7 = (E_7, T_{D1})$.

Step 2. On getting $M_7 = (E_7, T_{D1})$, $C$ verifies $T_{C7} - T_{D1} ≤ ΔT$. Then, $C$ decrypts $(ID_D, rg) = D_h(pk_D ||pk_C ||pk_T ||T_{D1})(E_7)$, generates random number $s ∈ Z^*_q$, computes $H_5 = h(IDP ||ID_D ||SigH ||SigP ||CP ||T_{C8} ||T_{D1})$ and encrypts $E_8 = E_{sk_D}(SigP, SigH, NID_P, CP, ID_D, H_5)$. After that $C → D : M_8 = (E_8, E_{sk_D}(T_{C8}))$.

Step 3. On receiving $M_8 = (E_8, E_{sk_D}(T_{C8}))$, $D$ checks $T_{D2} - T_{C8} ≤ ΔT$. Then, $D$ computes $J = I ⊕ h(ID_D ||rg ||T_{D1})$, decrypts $(SigP, SigH, NID_P, CP, ID_D, H_5, sg) = D_j(E_8)$, computes $H_5^* = h(IDP ||ID_D ||SigH ||SigP ||CP ||T_{C8} ||T_{D1})$ and verifies $H_5^* = H_5$. Further, $D$ computes report $m_B = D_h(sn_{ID} ||ID_P ||ID_H)(CP)$ and verifies digital signature $V_{PK_P}(SigP) = h(m_B)$. Furthermore, $D$ inputs $m_D = (ID_P, Database)$.
Verifies $T_{C7} - T_{D1} \leq \Delta T$
Decryps $(ID_{D}, r_{9}) = D_{K}(h(ID_{D}) || P_{ID} || ID_{P})$
Generates $s \in \mathbb{Z}_{q}^{*}$
Computes $H_{6} = h(ID_{P}) || ID_{P} || ID_{D} || C_{P} || C_{D} || T_{C8} || T_{D1}$
Encrypts $E_{9} = E_{m_{P}}(S_{ID_{P}}, Sig_{P}, ID_{P}, H_{9}, s_{9})$
Sends $M_{9} = \{E_{8}, T_{C8}\}$

Step 4. Upon getting $M_{12} = \{E_{12}, T_{P6}\}$, C verifies $T_{C12} - T_{P5} \leq \Delta T$. Then, C decrypts $(S_{ID_{P}}, C_{P}, H_{9}) = E_{m_{P}}(E_{9})$, computes

$H_{6}' = h(ID_{P}) || ID_{D} || ID_{P} || C_{D} || Sig_{ID} || Sig_{I_{D}} || T_{C8}$

and verifies $H_{6}' = H_{6}$. Further, C computes session key $S_{K_{CD}} = h(H_{6}'' || ID_{P} || ID_{ID} || Sig_{ID} || Sig_{ID} || T_{C8})$ and stores parameters $C_{P}, Sig_{ID}$ in database.

5) CHECKUP PHASE

The details of CP is shown in Table 7, and discussed as below:

Step 1. $P$ inputs $ID_{P}, NID, sn_{p}$ generates random value $x \in \mathbb{Z}_{q}^{*}$, encrypts $E_{10} = E_{SK_{PC}}(ID_{P}, NID, sn_{p}, x)$ and $P \rightarrow C : M_{10} = \{E_{10}, T_{P4}\}$.

Step 2. Upon collecting $M_{10} = \{E_{10}, T_{P4}\}$, C verifies $T_{C10} - T_{P4} \leq \Delta T$ and decrypts $(ID_{P}, NID, sn_{p}, x)$ = $D_{SK_{PC}}(E_{10})$. Further, C generates random number $y \in \mathbb{Z}_{q}^{*}$, computes $H_{1} = h(SK_{PC} || ID_{P} || ID_{D} || C_{P} || xy || Sig_{ID} || T_{C11} || T_{P4})$ and encrypts $E_{11} = E_{SK_{PC}}(H_{1}, ID_{D}, Sig_{D}, C_{D}, y)$. Then, $C \rightarrow P : M_{11} = \{E_{11}, T_{C11}\}$.

Step 3. On getting $M_{11}, P$ verifies $T_{P4} - T_{C11} \leq \Delta T$. Then, decrypts $(H_{7}, ID_{D}, Sig_{D}, C_{D}, y)$ = $D_{SK_{PC}}(E_{11})$, computes $H_{7}' = h(SK_{PC} || ID_{D} || ID_{P} || C_{D} || xy || Sig_{ID} || T_{C11} || T_{P4})$ and verifies $H_{7}' = H_{7}$. Further, $P$ decrypts $(m_{9}, m_{8}, m_{D}) = D_{h(ID_{D}) || ID_{P} || NID} || ID_{P})(C_{P})$ and verifies $V_{PK_{D}}(Sig_{D}) = h(m_{P})$. Further, $P$ encrypts $C_{E} = E_{m_{P}}(ID_{P} || ID_{D} || Sig_{P} || ID_{P})(m_{9}, m_{8}, m_{D})$, computes $H_{8} = h(SK_{PC} || H_{7}'' || C_{E} || Sig_{ID} || Sig_{ID} || xy || T_{P6} || T_{C11})$, also encrypts $E_{12} = E_{SK_{PC}}(C_{E}, H_{8})$ and $P \rightarrow C : M_{12} = \{E_{12}, T_{P6}\}$.

Step 4. Upon getting $M_{12} = \{E_{12}, T_{P6}\}$, C verifies $T_{C12} - T_{P5} \leq \Delta T$. Then, C decrypts $(C_{E}, S_{9}) = D_{SK_{PC}}(E_{12})$, computes $H_{8}' = h(SK_{PC} || H_{7}'' || C_{E} || Sig_{ID} || Sig_{ID} || xy || T_{P6} || T_{C11})$ and verifies $H_{8}' = H_{8}$. After that C stores parameter $C_{E}$ in database.

6) EMERGENCY PHASE

When, $P$ has emergency or heart attack position, body sensor attack inform to $C$ and $C$ informs to $H$. The details of EP is shown Table 8 and discussed as below:

Step 1. $P$ input $ID_{P}, EP_{request}$ and computes $H_{9} = h(H_{9} || ID_{D} || T_{EP1})$. Further, $P$ generates a random number as $a \in \mathbb{Z}_{q}^{*}$ encrypt $E_{13} = E_{SK_{PC}}(H_{9}, a, EP_{request})$. Then, $P \rightarrow C : M_{13} = \{E_{13}, T_{EP1}\}$.

Step 2. On getting $M_{13}, C$ checks $T_{EP2} - T_{EP1} \leq \Delta T$. Then, decrypts $(H_{9}, a, EP_{request}) = D_{SK_{PC}}(E_{13})$, computes $H_{9}' = h(SK_{PC} || H_{9}'' || ID_{D} || T_{EP1})$. Then, C decrypts $H_{10} = h(H_{9}'' || ID_{D} || ID_{P} || T_{EP3})$ and encrypts $E_{14} = E_{SK_{CHS}}(EP_{request}, ID_{P}, H_{10}, a, H_{9}'')$. Finally, $C \rightarrow H : M_{14} = \{E_{14}, T_{EP3}\}$.

Step 3. On receiving $M_{14}, H$ verifies $T_{EP4} - T_{EP3} \leq \Delta T$. Then, $H$ decrypts $(EP_{request}, ID_{P}, H_{10}, a, H_{9}'') = D_{SK_{PC}}(E_{14})$. Further, $C$ verifies $H_{10}' = h(H_{2} || P_{ID} || P_{ID})$. 

| Doctor $D$ | Cloud $C$ |
|-----------------|-----------------|
| **Inputs $ID_{D}$** | **Verifies $T_{C7} - T_{D1} \leq \Delta T$** |
| Generates $r \in \mathbb{Z}_{q}^{*}$ | **Decryps $(ID_{D}, r_{9}) = D_{K}(h(ID_{D}) || P_{ID} || ID_{P})$** |
| Encrypts $E_{7} = E_{h(ID_{D} \oplus P_{KC}) \oplus T_{D1}}(ID_{D}, r_{9})$ | **Generates $s \in \mathbb{Z}_{q}^{*}$** |
| Sends $M_{7} = \{E_{7}, T_{D1}\}$ | **Computes $H_{5} = h(ID_{P}) || ID_{P} || ID_{D} || C_{P} || C_{D} || T_{C8} || T_{D1}$** |
| | **Encrypts $E_{8} = E_{m_{P}}(Sig_{P}, Sig_{H}, NID_{P}, C_{D}, ID_{P}, H_{9}, s_{9})$** |
| | **Sends $M_{8} = \{E_{8}, T_{C8}\}$** |

**TABLE 6. TP of CSEF.**
TABLE 7. CP of CSEF.

| Patient $P$ | Cloud $C$ |
|-------------|-----------|
| **Inputs** $ID_P, NID_P, sn_P$ | Verifies $T_{C10} - T_{P4} \leq \Delta T$ |
| Generates $x \in Z_p^*$ | Decrypts $(ID_P, NID_P, sn_P, zg) = D_{SKCP}(E_{10})$ |
| Encrypts $E_{10} = E_{SKCP}(ID_P, NID_P, sn_P, zg)$ | Generates $y \in Z_p^*$ |
| Sends $M_{10} = \{E_{10}, T_{P4}\}$ | Computes $H_7 = h(SK_{CP}||ID_D||ID_P||C_D||xyg||Sig_P||T_{C11}||T_{P4})$ |
| | Encrypts $E_{11} = E_{SKCP}(H_7, ID_D, Sig_D, C_D, yg)$ |
| | Sends $M_{11} = \{E_{11}, T_{C11}\}$ |

Verifies $T_{P3} - T_{C11} \leq \Delta T$  
Decrypts $(ID_D, Sig_D, C_D, C_T) = D_{SKCP}(E_{11})$  
Generates $y \in Z_p^*$  
Computes $H_5 \equiv h(SK_{CP}||ID_D||ID_P||C_D||xyg||Sig_P||T_{C11}||T_{P4})$  
 Encrypts $E_{11} = E_{SKCP}(H_7, ID_D, Sig_D, C_D, yg)$  
Sends $M_{11} = \{E_{11}, T_{C11}\}$

Verifies $T_{C12} - T_{P6} \leq \Delta T$  
Decrypts $(C_E, Sig_C) = D_{SKCP}(E_{12})$  
Computes $H_5 \equiv h(SK_{CP}||Sig_C||Sig_D||xyg||T_{P6}||T_{C11})$  
 Verifies $H_5 \equiv H_6$  
stores $C_E$ in database

$ID_P || ID_D || T_{EP3}$. Then, $H$ computes $SK_{HP} = h(H_5^* || ID_P || ID_H || abg || T_{EP3} || T_{EP5})$. $H_1 = h(H_5^* || ID_H || ID_P || abg || T_{EP3} || T_{EP5})$, $K_H = h(ID_H || ID_P || H_1 || abg)$ and encrypts $E_{15} = E_{K_H} \{\beta, H_1, EP_{replay}, T_{EP3}, T_{EP5}\}$. Finally, $H \rightarrow C : M_{15} = \{E_{15}, T_{EP5}\}$.

Step 4. On getting $M_{15}$, $C$ checks $T_{EP5} - T_{EP5} \leq \Delta T$ and $C \rightarrow P : M_{16} = \{E_{16}, T_{EP7}\}$.

Step 5. On receiving $M_{16}$, $P$ verifies $T_{EP5} - T_{EP7} \leq \Delta T$. Then, computes $K_P = h(ID_H || ID_P || H_7 || abg)$, decrypts $(\beta, H_1, EP_{replay}, T_{EP3}, T_{EP5}) = D_{K_P}(E_0)$ and also verifies $H_1 = h(H_5^* || ID_H || ID_P || abg || T_{EP5})$. Further, $P$ computes $SK_{PH} = h(H_6 || ID_H || ID_P || abg || T_{EP3} || T_{EP5})$.

In EP, P and H agree on session key $SK_{PH} = SK_{HP}$.

IV. SECURITY ANALYSIS

In this session, we evaluate CSEF, it has capacity to resist several security features and attributes. The details of security analysis is explained as below:

A. MAN-IN-THE-MIDDLE ATTACK

This attack make the task of keeping data secure and private particularly challenging since attacks can be mounted from remote computers with fake addresses in network system [72]. In CSEF, we adopted method to avoid this attack with help [47], [50], the details for this as follows:

- In HUP, on receiving message $M_1 = \{E_1, T_{H1}\}$, $C$ verifies $T_{C1} - T_{H1} \leq \Delta T$ and sends $M_2 = \{E_2, T_{C2}\}$ to $H$. On receiving $M_2$, $H$ verifies $T_{H2} - T_{C2} \leq \Delta T$, computes $H_1 = h(ID_H || abg || bkg || T_{H1})$, verifies $H_1 = H_1$ and sends $M_3 = \{E_2, T_{H2}\}$ to $C$. On getting $M_3$, $C$ verifies $T_{C3} - T_{H2} \leq \Delta T$ and $H_2 = H_2$.

Any $A$ cannot enter in these phases because these parameters are the essential components/techniques of ECC based communication system. Thus, CSEF protects the man-in-middle attack in this phase.

Similarity, PUP, TP, CP and EP of CSEF maintain against this attack.

B. PATIENT ANONYMITY

We explain $P$’s anonymity in HUP of CSEF as below:

- During HUP, $P$’s $ID_P$ is encrypted by screening actual identifier. Then, $ID_P$ in encrypted with $SK_{HC} = h(ID_H || H_1 || abg || T_{C2} || T_{H1})$, as get $E_3 = E_{SKHC}(ID_P, NID_P, sn_P, C_H, H_2, Sig_H)$ and only be decrypt by $C$, $(ID_D, NID_P, sn_P, C_H, H_2, Sig_H) = D_{SKCH}(E_3)$ with using $SK_{CH} = h(ID_H || abg || T_{C2} || T_{H1})$ and verifies $H_2 = H_2$ then, stores $ID_P, C_H, Sig_H, NID_P, sn_P$. Hence, $P$ anonymity manages in HUP.

Similarly, $P$ maintains anonymity in PUP, TP, CP and EP. Hence, CSEF maintains $P$ anonymity in SMS.

C. DOCTOR ANONYMITY

We discuss $D$ anonymity in TP of CSEF:

- During TP, $D$’s identity $ID_P$ is encrypted by screening actual $ID_D$. Here, $ID_P$ in encrypted with key $h(PK_D || PK_C || T_{D1})$, as get $E_7 = E_{h(PK_D || PK_C || T_{D1})}(ID_D, rg)$ and only be decrypt by $C$, $(ID_D, rg) = D_{h(PK_D || PK_C || T_{D1})}(E_7)$ with using key $h(PK_D || PK_C || T_{D1})$. Then, $C$ stores parameters $C_D, Sig_D$ in database.

Therefore, CSEF provides $D$’s anonymity in SMS.

D. STRONG REPLAY ATTACK

In CSEF, we use the time-stamp condition $T_i - T_j \leq \Delta T$ and random values as a counter-measure every phase. In CSEF, $\Delta T$ is the valid time length. Further, random number and current time value are used to computing hash value, encryption, decryption, session keys and different keys. In ECC, one way
107846

In CSEF, we discuss the details of data confidentiality as free from reply attack. In CSEF, there are different session keys which are explained by hash function is secure in network system. Hence, CSEF is free from reply attack.

**E. KNOWN-KEY SECURITY PROPERTY**

In CSEF, there are different session keys which are explained as below:

- In HUP, H computes \( SK_{HC} = h(ID_H || H_1^* || abg || T_{C2} || T_{H1}) \) and C computes \( SK_{CH} = h(ID_H || H_1 || abg || T_{C2} || T_{H1}) \).
- In PUP, P executes \( SK_{PC} = h(ID_P || ID_H || CH || H_2^* || cdg || T_{C5} || T_{P1}) \) and C computes \( SK_{CP} = h(ID_P || ID_H || CH || H_3 || cdg || T_{C5} || T_{P1}) \).
- In TP, D executes \( SK_{DC} = h(H_6 || ID_P || ID_D || Sig_D || Sig_D || rsg || T_{D3} || T_{C8}) \) and C key \( SK_{CD} = h(H_6 || ID_P || ID_D || Sig_D || rsg || T_{D3} || T_{C8}) \).
- In EP, H computes \( SK_{HP} = h(H_3 || ID_P || ID_H || abg || T_{EP3} || T_{EP5}) \) and P computes \( SK_{PH} = h(H_3 || ID_P || ID_H || abg || T_{EP3} || T_{EP5}) \).

Here, \( A \) cannot find session key in different phases. Hence, CSEF has managed known-key security.

**F. DATA CONFIDENTIALITY**

In CSEF, we discuss the details of data confidentiality as below:

- In HUP, H encrypts as \( E_1 = E_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})} \) with using key \( h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1}) \) and forwards to C. Further, C decrypts \( ID_H, ag \) as \( D_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})}(E_1) \) with using key \( h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1}) \). Furthermore, C encrypts \( E_2 = E_{h(ID_H \oplus T_{H1} \oplus T_{C2})}(bg_1,H_1) \) with using key \( h(ID_H \oplus T_{H1} \oplus T_{C2}) \) and uploads to H. Furthermore, H decrypts \( (bg_1,H_1) = D_{h(ID_H \oplus T_{H1} \oplus T_{C2})}(E_2) \) with using key \( h(ID_H \oplus T_{H1} \oplus T_{C2}) \).

**TABLE 8. EP of CSEF.**

| Patient P | Cloud C | Healthcare center H |
|-----------|---------|---------------------|
| Input \( ID_P, E_{P_{request}} \) | Computes \( H_3 = h(H_6 || ID_P || T_{EP1}) \) | Checks \( T_{EP3} - T_{EP2} \leq \Delta T \) |
| Select \( \alpha \in Z_q^* \) | Encrypts \( E_{\alpha T_{P_{request}}} = E_{SK_{HC}}(H_9, \alpha, E_{P_{request}}) \) | Decrypts \( (E_{P_{request}}, ID_P, H_{10}, \alpha) \) = \( D_{SK_{HC}}(E_{\alpha T}) \) |
| Encrypts \( M_{13} = \{E_{\alpha T}, T_{EP1}\} \) | | Verifies \( H_{13} = h(H_2 || ID_H || ID_P || T_{EP3}) \) |

Similarly, CSEF data confidentiality maintains in PUP, TP, CP and EP. Hence, CSEF offers data confidentiality.

**G. DATA NON-REPUDIATION**

In CSEF, we explains data non-repudiation in every phases as below:

- In HUP, H computes digital signature \( Sig_H = S_{PR_H}(h(m_H)) \).
Thus, P inputs ID_P, PW_P and computes PWP = h(h(ID_P || PW_P) || ID_P || PW_P) and P sends message {ID_P, PWP, T_R1} to H via secure channel.
- On getting message, H verifies T_R2 - T_R1 ≤ ΔT. Then, H computes NID_P = h(ID_P || PWP || T_R1), generates sn_P ∈ Z_q^*. Then, stores NID_P, ID_P, sn_P in cloud database. Further, H encrypts E_P1 = E[h(PWP || T_R1 || ID_P) || NID_P, ID_P, sn_P] and sends {E_P1} to P via secure channel.
- Upon obtain {E_P1}, P decrypts {NID_P, ID_P, sn_P} = D[h(PWP || T_R1 || ID_P) || E_1] and stores parameters NID_P, ID_P, sn_P in database.

Here, A can not access password and dynamic pseudo random of P. Because, we use hash value, dynamic pseudo random, encryption and decryption methods. Hence, CSEF is free from stolen-verifier attack. • Chen et al.’s [47] fails in PU, DC, PA, DU, OG, RP and EP. • Chen et al.’s [46] fails in SS, PA, KK, OG, RP and EP. • Chiu et al.’s [49] fails in PU, PA, DU, KK, IM, RP and EP. • Mohit et al.’s [50] fails in PU, SS, IM, OG, RP and EP. • Li et al.’s [52] fails in PU, SS, PA, DU, MI, IM, RP and EP. • Chandraker et al.’s [53] fails in PU, IM, DR and EP.

K. SESSION KEY SECURITY

In this session, we examine the session key security in HUP of CSEF.

* During HUP, SK_HC = h(h(ID_H || H_1 || abg || T_C2 || T_H1) and SK_CH = h(h(ID_H || H_1 || abg || T_C2 || T_H1) are the session key between H and C, where SK_HC = SK_CH. A cannot execute SK_HC or SK_CH, where H_1 = h(h(ID_H || abg || bg || T_H1)) and H_1 = h(h(ID_H || abg || bg || T_H1)). According as impersonation attack, H_1 and H_1 cannot be computed by A. Further, For a, b ∈ Z_q^* and g is the generator of G, for given (g, a, b), then executes abg is hard for G by ECDHP in the ECC. So, SK can only be executed by the valid participant.

Similarly, SK are managed in other phases. Thus, the proposed framework manages the session key security.

L. PARALLEL SESSION ATTACK

This attack commonly happens when A reuse historical message in insecure channel to make a fresh request, then impersonates the understandable participant to compute session key. In CSEF, A has to know the components reposed of the information then, A can form the suitable request or keys. As this analysis, A cannot obtain SK. Hence, CSEF is free from this attack.

V. PERFORMANCE EVALUATION

In this section, we discuss the performance evaluation as below:

A. COMPARISON OF THE SECURITY AND FUNCTIONALITY FEATURES

Here, we discuss the security attributes comparison of CSEF with similar framework, like Chen et al. [47], Chen et al. [46], Chiu et al. [49], Mohit et al. [50], Li et al. [52]
TABLE 9. Comparison the security and functionality features.

| Protocol | Ref [47] | Ref [46] | Ref [49] | Ref [50] | Ref [52] | Ref [53] | CSEF |
|----------|----------|----------|----------|----------|----------|----------|------|
| PU       | x        | v        | x        | x        | x        | x        | v    |
| DU       | v        | v        | v        | v        | v        | v        | v    |
| SS       | v        | x        | v        | x        | x        | x        | v    |
| PA       | x        | x        | x        | x        | x        | x        | v    |
| DU       | x        | v        | x        | x        | x        | x        | v    |
| RA       | v        | v        | v        | v        | v        | v        | v    |
| KK       | v        | x        | x        | x        | x        | x        | v    |
| MI       | v        | v        | v        | v        | v        | v        | v    |
| IM       | v        | v        | v        | v        | v        | v        | v    |
| MA       | v        | v        | v        | v        | v        | v        | v    |
| DR       | v        | v        | v        | v        | v        | v        | v    |
| OF       | x        | x        | x        | x        | x        | x        | v    |
| RP       | x        | x        | x        | x        | x        | x        | v    |
| EP       | x        | x        | x        | x        | x        | x        | v    |

Note: ✓ Attributes satisfied by the framework and x: Attributes not satisfied by the framework
PU: Patient unlinkability, SS: Session key security, DC: Data confidentiality, PA: Patient anonymity, DU: Doctor unlinkability, RA: Replay attack, KK: Known-key security property, MI: Man-in-the-middle attack, IM: Impersonation attack, MA: Message authentication, DR: Data non-reputation, OF: Offline guessing attack, RP: Patient registration phase and EP: Emergency phase

TABLE 10. Computing time of the different operation computations.

| Notations | Descriptions | Execution time (Second) |
|-----------|--------------|-------------------------|
| T_H       | One-way hash function | ≈ 0.0005               |
| T_Signer  | Execute/verify a signature | ≈ 0.3317               |
| T_p       | Bilinear pairing operation | ≈ 0.0621               |
| T_A       | Asymmetric encryption/decryption operation | ≈ 0.3057               |
| T_M       | Multiplication operation | 0.0005                  |
| T_S       | Symmetric encryption/decryption operation | ≈ 0.0087               |

TABLE 11. Comparison of the computation cost in seconds.

| Protocol | Ref [47] | Ref [46] | Ref [49] | Ref [50] | Ref [52] | Ref [53] | CSEF |
|----------|----------|----------|----------|----------|----------|----------|------|
| HCP      | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H |
| PUP      | 1T_{Sign} + 2T_M + 4T_H | 1T_{Sign} + 2T_M + 4T_H | 1T_{Sign} + 2T_M + 4T_H | 1T_{Sign} + 2T_M + 4T_H | 1T_{Sign} + 2T_M + 4T_H | 1T_{Sign} + 2T_M + 4T_H | 1T_{Sign} + 2T_M + 4T_H |
| TP       | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H |
| CP       | NA       | NA       | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H |
| EP       | NA       | NA       | NA       | NA       | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H | 1T_{Sign} + 2T_M + 2T_p + 4T_H |

Total cost: 6T_{Sign} + 2T_M + 2T_p + 4T_H

Total time: ≈ 4.7091 Second

6T_{Sign} + 37T_S + 56T_H ≈ 2.3401 second. The comparison of computation expenditure with related protocols are discussed as below:

- The computation expenditure of Chen et al.’s [47] is 3T_{Sign} + 3T_M + 6T_p + 15T_S + 2.7091 second, which is approximate 101.24% grater than CSEF computation expenditure.
- The computation expenditure of Chen et al.’s [46] is 6T_{Sign} + 12T_M + 15T_p + 15T_S + 22T_H + 2T_A ≈ 4.2782 second, which is approximately 82.83% grater than CSEF computation expenditure.
- The computation expenditure of Chou et al.’s [49] is 5T_{Sign} + 4T_M + 13T_p + 10T_S + 33T_H ≈ 2.7705 second, which is approximately 15.53% grater than CSEF computation expenditure.

and Chandrakar et al. [53] protocol. The evaluation offers an insight capability of CSEF with other frameworks. The Table 9 is shown comparison of the security and functionality features of CSEF and other related frameworks.

B. COMPARISON OF THE COMPUTATION EXPENDITURE

In this section, we measure the computation cost of CSEF with the similar framework in same environment such as Chen et al., Chen et al., Chou et al., Mohit et al. Li et al. and Chandrakar et al. frameworks. We have taken various cryptographic functions in CSEF and other protocols based on the relevant information in [49], [50]. Table 10. is displayed the computation cost of different cryptographic operations. From Table 11., the computation expenditure of CSEF is
C. COMPARISON OF THE COMMUNICATION EXPENDITURE

In this section, we discuss communication expenditure of CSEF with associated frameworks. Here, we adopt the methods based on framework [49], [50] for communication expenditure. We epitomize the communication expenditure in Table 12, the communication cost of CSEF is 2976 bits. The comparison of communication expenditure is discussed as below:

- The communication expenditure of Mohit et al.’s [50] is $6T_{\text{Sign}} + 9T_{S} + 35T_{H} \approx 2.086$ second, which is approximately 10.85% less than CSEF computation expenditure and Mohit et al.’s framework is not secure against, off-line guessing attack, impersonation attack, fails patient anonymity, fails doctor unlinkability and fails in common session security.
- The computation expenditure of Li et al.’s [52] is $7T_{\text{Sign}} + 15T_{S} + 39T_{H} \approx 2.4719$ second, which is approximately 5.42% greater than CSEF computation expenditure.
- The computation expenditure of Chandrakar et al.’s [53] is $7T_{\text{Sign}} + 15T_{S} + 39T_{H} \approx 3.5031$ second, which is approximately 49.698% greater than CSEF computation expenditure.

The efficiency of CSEF and other related frameworks are shown in Figure 2.

The CSEF is productive in terms of communication expenditure. The comparison of communication expenditure of CSEF and other relevant frameworks is displayed in Figure 3.

VI. CONCLUSION

Security and privacy are two essential concerns to establish a secure authentication framework in smart medical system. The paper is the construction of an ECC-based suitable framework for smart medical system in cloud environment. In this paper, we have discussed six different phases such as registration phase, healthcare center upload phase, patient data upload phase, treatment phase, check up phase and emergency phase. The paper has shown the security analysis of the presented framework. Further, we have demonstrated that the proposed framework manages better security and privacy features and attributes compared to related frameworks in the similar environment. Also, we have shown that the proposed framework is more efficient in term of computation and communication expenditure compared with related protocols in SMS. Hence, CSEF is the real life application in cloud-based smart medical system.

REFERENCES

[1] M. V. Moreno, F. Terroso-Saenz, A. Gonzalez-Vidal, M. Valdes-Vela, A. F. Skarmeta, M. A. Zamora, and V. Chang, “Applicability of big data techniques to smart cities deployments,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 800–809, Apr. 2017.
[2] D. Bajpai, M. Vardhan, S. Gupta, R. Kumar, and D. S. Kushwaha, “Security service level agreements based authentication and authorization model for accessing cloud services,” in *Advances in Computing and Information Technology*. Chennai, India: Springer, 2012, pp. 719–728.
A. A. Khan, V. Kumar, M. Ahmad, and D. Mishra, “PALK: Password-based anonymous lightweight key agreement framework for smart grid,” Int. J. Electr. Power Energy Syst., vol. 100, pp. 241–248, Feb. 2019.

S. K. H. Islam, R. Amin, G. P. Biswas, M. S. Farash, X. Li, and S. Kumari, “An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments,” J. King Saud Univ. Comput. Inf. Sci., vol. 29, no. 3, pp. 311–324, Jul. 2017.

A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, “Orthogonal authentication and provably secure anonymity preserving three-factor user authentication and key agreement scheme for E-healthcare systems,” J. King Saud Univ. Comput. Inf. Sci., vol. 29, no. 4, pp. 796–805, Aug. 2017.

R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and X. Li, “Cryptanalysis and enhancement of anonymity preserving key agreement protocol for healthcare systems,” IEEE Access, vol. 5, pp. 7012–7030, 2017.

M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, “Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for telecare medicine information systems,” IEEE Access, vol. 5, pp. 10995–11004, 2017.

R. Guo and H. Shi, “Confidentiality-preserving personal health records in cloud-based healthcare system using authenticated certificateless encryption,” IET Netw., vol. 9, no. 6, pp. 955–964, Nov. 2019.

D. He, N. Khan, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeoh, “Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks,” Multimedia, vol. 21, no. 1, pp. 49–60, Feb. 2015.

V. Kumar, M. Ahmad, and A. Kumari, “A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS,” Lect. Notes Comput. Sci., vol. 10274, no. 1, pp. 129–147, 2017.

C.-T. Li, C.-C. Lee, C.-Y. Weng, and S.-J. Chen, “A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-Healthcare systems,” J. Med. Syst., vol. 42, no. 8, pp. 1–11, Aug. 2018.

C.-H. Liu and Y.-F. Chiang, “Secure user authentication scheme for wireless healthcare sensor networks,” Comput. Electr. Eng., vol. 59, pp. 250–261, Apr. 2017.

C.-T. Li, C.-C. Lee, C.-C. Wang, T.-H. Yang, and S.-J. Chen, “Design flaws in a secure medical data exchange protocol based on cloud environments,” in Proc. Int. Conf. Algorithms Archit. Parallel Process. Zhangjiajie, China: Springer, 2015, pp. 435–444.

C.-T. Li, D.-H. Shih, and C.-C. Wang, “On the security of a privacy authentication scheme based on cloud for medical environment,” in Proc. Int. Conf. Inf. Sci. Appl. Chengdu, China: Springer, 2017, pp. 24–28.

C.-T. Li, C.-C. Lee, and C.-Y. Weng, “A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems,” J. Med. Syst., vol. 38, no. 9, pp. 77–91, Sep. 2014.

V. Kumar, S. Jangirala, and M. Ahmad, “An efficient mutual authentication framework for healthcare system in cloud computing,” J. Med. Syst., vol. 42, no. 8, pp. 140–151, Aug. 2018.

S. A. Chaudhry, H. Naqvi, T. Shon, M. Sher, and M. S. Farash, “Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems,” J. Med. Syst., vol. 39, no. 6, pp. 58–75, Jun. 2015.

S. H. Islam, M. K. Khan, and X. Li, “Security analysis and improvement of ‘a more secure anonymous user authentication scheme for the integrated EPR information system,’” PLoS ONE, vol. 10, no. 8, Aug. 2015, Art. no. e0131368.
[44] A. K. Sutrula, A. K. Das, V. Odelu, M. Wazid, and S. Kumari, “Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems,” Comput. Methods Programs Biomed., vol. 155, pp. 167–185, Oct. 2016.

[45] R. P. Patil, M. R. Patra, and S. C. Satapathy, “Design and implementation of a cloud based rural healthcare information system model,” Univers. J. Appl. Comput. Sci. Technol., vol. 2, no. 1, pp. 149–157, 2012.

[46] C.-L. Chen, T.-T. Yang, and T.-F. Shih, “A secure medical data exchange protocol based on cloud environment,” J. Med. System., vol. 38, no. 9, p. 112, Sep. 2014.

[47] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, “A privacy authentication scheme based on cloud for medical environment,” J. Med. System., vol. 38, no. 11, p. 143, Nov. 2014.

[48] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, “4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks,” Inf. Sci., vol. 314, pp. 258–276, Sep. 2015.

[49] S.-Y. Chiou, Z. Ying, and J. Liu, “Improvement of a privacy authentication scheme based on cloud for medical environment,” J. Med. System., vol. 40, no. 4, p. 101, Apr. 2016.

[50] P. Mohit, R. Amin, A. Karati, G. P. Biswas, and M. K. Khan, “A standard mutual authentication protocol for cloud computing based health care system,” J. Med. System., vol. 41, no. 4, p. 50, Apr. 2017.

[51] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, “Cloud centric authentication for wearable healthcare monitoring system,” IEEE Trans. Depend. Sec. Comput., early access, Apr. 19, 2018, doi: 10.1109/ TDSC.2018.2828306.

[52] 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.

[53] P. Chandrakar, S. Sinha, and R. Ali, “Cloud-based authenticated protocol for healthcare monitoring system,” J. Ambient Intell. Humanized Comput., pp. 1–17, Oct. 2019, doi: 10.1007/s12652-019-01537-2.

[54] A. Kumari, M. Y. Abbasi, V. Kumar, and M. Alam, “Design flaws and cryptanalysis of a standard mutual authentication protocol for cloud computing-based healthcare system,” in Advances in Data Sciences, Security and Applications. New Delhi, India: Springer, 2020, pp. 99–109.

[55] A. Ghani, K. Manosoor, S. Mehmoon, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, “Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key,” Int. J. Commun. Syst., vol. 32, no. 16, p. e4139, Nov. 2019.

[56] S. Mehmoon, J. Arshad, S. A. Chaudhry, and S. Kumari, “An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure,” Int. J. Commun. Syst., vol. 32, no. 16, Nov. 2019, Art. no. e4137.

[57] J. V. Alzahrani, A. Arshad, and M. M. Alsharif, “Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems,” Comput. Commun., vol. 153, pp. 527–537, Mar. 2020.

[58] S. Challia, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, “Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems,” Future Gener. Comput. Syst., vol. 1058, pp. 1267–1286, Jul. 2020, doi: 10.1016/j.future.2018.04.019.

[59] C.-L. Chen, P.-T. Huang, Y.-Y. Deng, H.-C. Chen, and Y.-C. Wang, “A secure electronic medical record authorization system for smart device application in cloud computing environments,” Hum.-Centric Comput. Inf. Sci., vol. 10, no. 1, pp. 1–31, Dec. 2020.
SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012. She is currently an Assistant Professor with the Department of Mathematics, Chaudhary Charan Singh University. She has published more than 133 research articles in reputed International journals and conferences, including 115 publications in SCI-indexed journals. Her current research interests include information security and applied cryptography. She is a Technical Program Committee member for many International conferences. She has served as a Lead/Guest Editor of four special issues in SCI journals of Elsevier, Springer, and Wiley. She is on the Editorial Board of more than 12 journals of international repute, including seven SCI journals.

PRADEEP CHAUDHARY received the M.Sc. (Hons.), M.Phil. (Hons.), and Ph.D. degrees in statistics from Chaudhary Charan Singh University, Meerut, India, in 1996, 1998, and 2004, respectively. He has served as a Research Assistant, the Director of the Institutional Finance and Sarvhit Bima, Government of Uttar Pradesh, India, and as an Assistant Director of the Rural Development Department, State Institute of Rural Development, Government of Uttar Pradesh. He is currently an Assistant Professor with the Department of Statistics, CCS University. His current research interests include reliability and applied cryptography.

CHIEN-MING CHEN (Senior Member, IEEE) received the Ph.D. degree from National Tsing Hua University, Taiwan. He is currently an Associate Professor with the Shandong University of Science and Technology, China. His current research interests include network security, the mobile Internet, the IoT, and cryptography. He also serves as an Associate Editor for IEEE Access and an Executive Editor for the International Journal of Information Computer Security.