

Received May 18, 2020, accepted June 4, 2020, date of publication June 9, 2020, date of current version June 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3001152

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

ADESH KUMARI<sup>1</sup>, VINOD KUMAR<sup>2</sup>, M. YAHYA ABBASI<sup>1</sup>, SARU KUMARI<sup>3</sup>, PRADEEP CHAUDHARY<sup>4</sup>, AND CHIEN-MING CHEN<sup>5</sup>, (Senior Member, IEEE)

<sup>1</sup>Department of Mathematics, Jamia Millia Islamia, New Delhi 110025, India

<sup>2</sup>Department of Mathematics, PGDAV College, University of Delhi, New Delhi 110065, India

<sup>3</sup>Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India

<sup>4</sup>Department of Statistics, Chaudhary Charan Singh University, Meerut 250004, India

<sup>5</sup>College 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

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

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 patient 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

anonymity, 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

TABLE 1. Notations.

Notation	Explanation	Notation	Explanation
RP	Registration phase	HUP	Healthcare center upload phase
PUP	Patient data upload phase	TP	Treatment phase
CP	Check up phase	EP	Emergency phase
$PW_P$	Password of $P$	$\mathcal{A}$	Attacker
$l$	The security parameter	$\mathcal{E}(F_q)$	Elliptic curve $\mathcal{E}$ over $F_q$
$q$	Large prime	$Z_q^*$	Multiplicative group of order $q - 1$
$P$	The patient	$ID_i$	The unique identity of entity $i$
$C$	The cloud	$NID_P$	Dynamic pseudo random value for $P$
$D$	The doctor	$h(\cdot)$	Secure one way hash function
$H$	The healthcare centre	$E_k(m)/D_k(m)$	Encryption/Decryption of information $m$ using key $k$
$PK_i$	Public key of entity $i$	$S_k(m)$	Signature of $m$ with using key $k$
$x \stackrel{?}{=} y$	Whether $x$ equals $y$	$V_k(m)$	Verified signature of $m$ with using key $k$
$PR_i$	Private key of entity $i$	$SK_{xy}(\cdot)$	The session key between participants $x$ and $y$
$\parallel$	Concatenation operation	$\oplus$	Bitwise XOR operation
$G$	Additive ECC group	$m_H$	Patient's inspection report generated by $H$
$g$	Base point of $G$	$m_B$	Patient's health data gathered by body sensor
$Sig_i$	The signature of $i^{th}$ participant	$m_D$	Patient's medical report generated by $D$
$F_q$	Prime finite field	$i \Rightarrow j : \{M\}$	$i$ sends information $M$ to $j$ through secure channel
$sn_P$	The sequence number for $P$	$i \rightarrow j : \{M\}$	$i$ sends information $M$ to $j$ through insecure channel

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. Even though key agreement frameworks [46], [47], [49], [50], [52], [53] have been provided over the last few years, their achievement is not yet sufficient. Also, these protocols disrupt the basic requirements of construction, so resulting in elemental omissions. In this paper, we aim to proposed a cloud-based secure and efficient mutual authentication framework using ECC for smart medical system.

C. RESEARCH CONTRIBUTIONS

The contributions of CSEF are as below:

- The proposed framework has different phases such as: Registration phase, Healthcare center upload phase, Patient data upload phase, Treatment phase, Check up phase and Emergency phase.
- The mutual authentication is established among patient, cloud server, healthcare center and doctor to build up the security of a architecture and communicating information.
- Further, CSEF satisfies different security attributes and secure against different attacks.
- The session key is established between patient and cloud, doctor and cloud, healthcare center and cloud, and healthcare center and patient.
- The comparative analysis proves the efficiency of CSEF. It is better than other frameworks in the same environment.

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  $v^2 = u^3 + \alpha u + \beta \pmod q$ , where  $\alpha, \beta \in F_q$ . The EC is said to be non singular if  $4\alpha^3 + 27\beta^2 \pmod q \neq 0$ .  $G$  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  $\nabla = (u, v) \in G$ , then defined  $-\nabla = (u, -v)$  and  $\nabla + (-\nabla) = \Phi$ .
2. If  $\nabla_1 = (u_1, v_1), \nabla_2 = (u_2, v_2) \in G$ , then  $\nabla_1 + \nabla_2 = (u_3, v_3)$ , where  $u_3 = \rho^2 - u_1 - u_2 \pmod q, v_3 = \rho(u_1 - u_3) - v_1 \pmod q$ , and

$$\rho = \begin{cases} \frac{v_2 - v_1}{u_2 - u_1} \pmod q & \text{if } \nabla_1 \neq \nabla_2 \\ \frac{3u_1^2 + \alpha}{2v_1} \pmod q & \text{if } \nabla_1 = \nabla_2 \end{cases}$$

3. Let  $\nabla = (u, v) \in G$  then, scalar multiplication in  $G$  such as:  $\eta \nabla = \nabla + \nabla + \nabla \dots + \nabla$  ( $\eta$  - 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  $\nabla_1, \nabla_2 \in G$  to find  $\mu \in Z_q^*$  such that  $\nabla_2 = \mu \nabla_1$ , is hard [69].
- \* **Definition 2. Elliptic curve computational Diffie-Hellman problem (ECCDHP):** For  $\alpha, \beta \in Z_q^*$  and  $g$

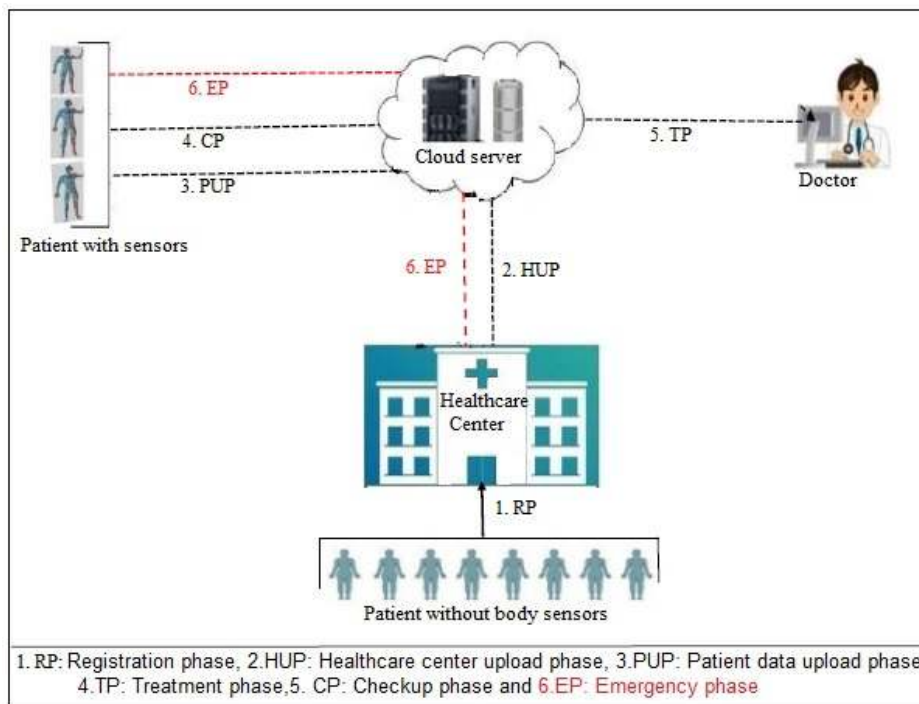


FIGURE 1. Architecture for CSEF with different phases.

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

ECC key size(Bits)	RSA key size(Bits)	Key size ratio
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

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  $\alpha, \beta \in Z_q^*$  and  $\sqrt[3]{1}, \sqrt[3]{2} = \alpha \sqrt[3]{1} + \beta \sqrt[3]{2} \in G$ , then to compute  $\alpha \sqrt[3]{1}$  and  $\beta \sqrt[3]{2}$  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 compare 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. DOLEV-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  $\mathcal{A}$ :

- \*  $\mathcal{A}$  can access the public network. He/she can modify, retrieve, replay, inject new message and can discard any communication network.
- \*  $\mathcal{A}$  is presumed to be protected, therefore cannot obtain the secret key of participants.
- \*  $\mathcal{A}$  knows the public identifier of all the participants.
- \*  $\mathcal{A}$  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 <i>P</i>	Healthcare center <i>H</i>
Inputs $ID_P, PW_P$ Computes $PWP = h(h(ID_P    PW_P)    ID_P    PW_P)$ Sends $\{ID_P, PWP, TR_1\}$ ..... $\Rightarrow$	Verifies $T_{R2} - T_{R1} \leq \Delta T$ Computes $NID_P = h(ID_P    PWP    TR_1)$ Generates $sn_P \in Z_q^*$ Store $NID_P, ID_P, sn_P$ in cloud database Encrypts $E_{P1} = E_{h(PWP    TR_1    ID_P)}(NID_P, ID_P, sn_P)$ Sends $\{E_{P1}\}$ ..... $\Leftarrow$
Decrypts $(NID_P, ID_P, sn_P) = D_{h(PWP    TR_1    ID_P)}(E_{P1})$ Stores $NID_P, ID_P, sn_P$	

TABLE 4. HUP of CSEF.

Healthcare center <i>H</i>	Cloud <i>C</i>
Generates $m_H = (ID_P, Data_P)$ Generates $a \in Z_q^*$ Inputs $ID_H$ and $a$ Encrypts $E_1 = E_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})}(ID_H, ag)$ Sends $M_1 = \{E_1, T_{H1}\}$ ..... $\rightarrow$	Verifies $T_{C1} - T_{H1} \leq \Delta T$ decrypts $(ID_H, ag) = D_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})}(E_1)$ Generates $b \in Z_q^*$ Computes $H_1 = h(ID_H    ag    bg    T_{H1})$ Encrypts $E_2 = E_{h(ID_H    ag    T_{H1}    T_{C2})}(bg, H_1)$ Sends $M_2 = \{E_2, T_{C2}\}$ ..... $\leftarrow$
Verifies $T_{H2} - T_{C2} \leq \Delta T$ Decrypts $(bg, H_1) = D_{h(ID_H    ag    T_{H1}    T_{C2})}(E_2)$ Computes $H_1^* = h(ID_H    ag    bg    T_{H1})$ Verifies $H_1^* \stackrel{?}{=} H_1$ Computes $SK_{HC} = h(ID_H    H_1^*    ag    T_{C2}    T_{H1})$ Encrypts $C_H = E_{h(ID_P    ID_H    NID_P)}(m_H)$ Computes $Sig_H = S_{PRH}(h(m_H))$ Computes $H_2 = h(SK_{HC}    C_H    Sig_H    T_{H3}    T_{C2})$ Encrypts $E_3 = E_{SK_{HC}}(ID_P, NID_P, sn_P, C_H, H_2, Sig_H)$ Sends $M_3 = \{E_3, T_{H3}\}$ ..... $\rightarrow$	Verifies $T_{C3} - T_{H3} \leq \Delta T$ Computes $SK_{CH} = h(ID_H    H_1    ag    T_{C2}    T_{H1})$ Decrypts $(ID_P, NID_P, sn_P, C_H, H_2, Sig_H) = D_{SK_{CH}}(E_3)$ Computes $H_2^* = h(SK_{CH}    C_H    Sig_H    T_{H3}    T_{C2})$ Verifies $H_2^* \stackrel{?}{=} H_2$ Stores $ID_P, C_H, Sig_H, NID_P, sn_P$

**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  $PWP = h(h(ID_P || PW_P) || ID_P || PW_P)$  and  $P \Rightarrow H : \{ID_P, PWP, TR_1\}$ .
- Step 2. On getting  $\{ID_P, PWP, TR_1\}$ , *H* checks  $T_{R2} - T_{R1} \leq \Delta T$ . *H* computes  $NID_P = h(ID_P || PWP || TR_1)$ , generates  $sn_P \in Z_q^*$ . Then, stores  $NID_P, ID_P, sn_P$  in cloud database. Further, *H* encrypts  $E_{P1} = E_{h(PWP || TR_1 || ID_P)}(NID_P, ID_P, sn_P)$  and  $H \Rightarrow P : \{E_{P1}\}$ .
- Step 3. Upon collecting  $\{E_{P1}\}$ , *P* decrypts  $(NID_P, ID_P, sn_P) = D_{h(PWP || TR_1 || ID_P)}(E_{P1})$  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 below:

- 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  $a$ . Further, *H* encrypts  $E_1 = E_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})}(ID_H, ag)$ . Then,  $H \rightarrow C : M_1 = \{E_1, T_{H1}\}$ .
- Step 2. On receiving  $M_1 = \{E_1, T_{H1}\}$ , *C* verifies  $T_{C1} - T_{H1} \leq \Delta T$ . Then, *C* decrypts  $(ID_H, ag) = D_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})}(E_1)$ , generates random number  $b \in Z_q^*$ , computes  $H_1 = h(ID_H || ag || bg || T_{H1})$ , encrypts  $E_2 = E_{h(ID_H || ag || T_{H1} || T_{C2})}(bg, H_1)$ . 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  $(bg, H_1) = D_{h(ID_H || ag || T_{H1} || T_{C2})}(E_2)$ , computes  $H_1^* = h(ID_H || ag || bg || T_{H1})$  and verifies  $H_1^* \stackrel{?}{=} H_1$ . Further, *H* computes session key  $SK_{HC} = h(ID_H || H_1^* || ag || T_{C2} || T_{H1})$ , encrypts  $C_H = E_{h(ID_P || ID_H || NID_P)}(m_H)$ , makes digital signature  $Sig_H = S_{PRH}(h(m_H))$ , computes  $H_2 = h(SK_{HC} || C_H || Sig_H || T_{H3} || T_{C2})$  and encrypts  $E_3 = E_{SK_{HC}}(ID_P, NID_P, sn_P, C_H, H_2, Sig_H)$ . Then,  $H \rightarrow C : M_3 = \{E_3, T_{H3}\}$ .
- Step 4. Upon collecting  $M_3 = \{E_3, T_{H3}\}$ , *C* verifies  $T_{C3} - T_{H3} \leq \Delta T$ . Then, computes  $SK_{CH} = h(ID_H || H_1 || ag || T_{C2} || T_{H1})$ , decrypts  $(ID_P, NID_P, sn_P, C_H, H_2, Sig_H) = D_{SK_{CH}}(E_3)$ , computes  $H_2^* = h(SK_{CH} || C_H || Sig_H || T_{H3} || T_{C2})$  and

TABLE 5. PUP of CSEF.

Patient <i>P</i>	Cloud <i>C</i>
Generates $m_B = (ID_P, Data_B)$	
Inputs $ID_P, NID_P$	
Encrypts $E_4 = E_{h(ID_P  NID_P  T_{P1})}(ID_P, NID_P)$	Verifies $T_{C4} - T_{P1} \leq \Delta T$
Sends $M_4 = \{ID_P, T_{P1}\}$	$(ID_P, NID_P) = E_{h(ID_P  NID_P  T_{P1})}(E_4)$
.....→	Generates $c \in Z_q^*$
	Computes $H_3 = h(NID_P  sn_i  C_H  Sig_H  cg  T_{C5}  T_{P1})$
	Encrypts $E_5 = E_{h(sn_P  NID_P  T_{C5}  T_{P1})}(Sig_H, C_H, H_3, ID_H, cg)$
	$M_5 = \{E_5, T_{C5}\}$
	←.....
Verifies $T_{P2} - T_{C5} \leq \Delta T$	
Decrypts $(Sig_H, C_H, H_3, ID_H, cg) = E_{h(sn_P  NID_P  T_{C5}  T_{P1})}(E_5)$	
Computes $H_3^* = h(NID_P  sn_i  C_H  Sig_H  cg  T_{C5}  T_{P1})$	
Verifies $H_3^* \stackrel{?}{=} H_3$	
Generates $d \in Z_q^*$	
Computes $SK_{PC} = h(ID_P  ID_H  C_H  H_3^*  cdg  T_{C5}  T_{P1})$	
Decrypts $m_H^* = D_{h(ID_P  ID_H  NID_P)}(C_H)$	
Verifies $m_H^* \stackrel{?}{=} m_H$	
Verifies $V_{PK_H}(Sig_H) \stackrel{?}{=} h(m_H)$	
Encrypts $C_P = E_{h(sn_P  NID_P  ID_P)}(m_H, m_B)$	
Computes $Sig_P = S_{PRP}(h(m_B))$	
Computes $H_4 = h(SK_{PC}  C_P  Sig_P  H_3^*  cdg  T_{P3}  T_{C5})$	
Encrypts $E_6 = E_{h(sn_P  NID_P  ID_P)}(dg, H_4, Sig_P, C_P)$	
Sends $M_6 = \{E_6, T_{P3}\}$	
.....→	
	Verifies $T_{C6} - T_{P3} \leq \Delta T$
	Decrypts $(dg, S_4, Sig_P, C_P) = D_{h(sn_P  NID_P  ID_P)}(E_6)$
	Computes $SK_{CP} = h(ID_P  ID_H  C_H  H_3  cdg  T_{C5}  T_{P1})$
	Computes $H_4^* = h(SK_{PC}  C_P  Sig_P  S_3  cdg  T_{P3}  T_{C5})$
	verifies $H_4^* \stackrel{?}{=} H_4$
	Stores $C_P, ID_P, Sig_P$ in database

verifies  $H_2^* \stackrel{?}{=} H_2$ . After that, *C* stores parameters  $ID_P, C_H, Sig_H, NID_P, sn_P$  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  $m_B = (ID_P, Data_B)$  from body 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,  $P \rightarrow C : M_4 = \{ID_P, T_{P1}\}$ .
- Step 2. Upon getting  $M_4 = \{ID_P, T_{P1}\}$ , *C* checks  $T_{C4} - T_{P1} \leq \Delta T$ . Then, *C* decrypts  $(ID_P, NID_P) = E_{h(ID_P||NID_P||T_{P1})}(E_4)$ , generates random number  $c \in Z_q^*$ , computes  $H_3 = h(NID_P||sn_i||C_H||Sig_H||cg||T_{C5}||T_{P1})$  and encrypts  $E_5 = E_{h(sn_P||NID_P||T_{C5}||T_{P1})}(Sig_H, C_H, H_3, ID_H, cg)$ . Further,  $C \rightarrow P : M_5 = \{E_5, T_{C5}\}$ .
- Step 3. On collecting  $M_5 = \{E_5, T_{C5}\}$ , *P* verifies  $T_{P2} - T_{C5} \leq \Delta T$ . Then, *P* decrypts  $(Sig_H, C_H, H_3, ID_H, cg) = E_{h(sn_P||NID_P||T_{C5}||T_{P1})}(E_5)$ , computes  $H_3^* = h(NID_P||sn_i||C_H||Sig_H||cg||T_{C5}||T_{P1})$  and verifies  $H_3^* \stackrel{?}{=} H_3$ . Further, *P* generates random number  $d \in Z_q^*$ , computes  $SK_{PC} = h(ID_P||ID_H||C_H||H_3^*||cdg||T_{C5}||T_{P1})$ , decrypts  $m_H^* = D_{h(ID_P||ID_H||NID_P)}(C_H)$ , verifies  $m_H^* \stackrel{?}{=} m_H$  and  $V_{PK_H}(Sig_H) \stackrel{?}{=} h(m_H)$ . Furthermore, *P* encrypts  $C_P = E_{h(sn_P||NID_P||ID_P)}(m_H, m_B)$ , makes digital signature  $Sig_P = S_{PRP}(h(m_B))$ , computes  $H_4 = h(SK_{PC}||C_P||Sig_P||H_3^*||cdg||T_{P3}||T_{C5})$  and encrypts  $E_6 = E_{h(sn_P||NID_P||ID_P)}(dg, H_4, Sig_P, C_P)$ . Then,  $P \rightarrow C : M_6 = \{E_6, T_{P3}\}$ .

- Step 4. On getting receiving  $M_6 = \{E_6, T_{P3}\}$ , *C* checks  $T_{C6} - T_{P3} \leq \Delta T$ . Then, *C* decrypts  $(dg, S_4, Sig_P, C_P) = D_{h(sn_P||NID_P||ID_P)}(E_6)$  and computes session key  $SK_{CP} = h(ID_P||ID_H||C_H||H_3||cdg||T_{C5}||T_{P1})$ . Further, *C* computes  $H_4^* = h(SK_{PC}||C_P||Sig_P||S_3||cdg||T_{P3}||T_{C5})$  and verifies  $H_4^* \stackrel{?}{=} H_4$ . Then, *C* stores parameters  $C_P, ID_P, Sig_P$  in database.

4) TREATMENT PHASE

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

- Step 1. *D* generates random  $r \in Z_q^*$ , encrypts  $E_7 = E_{h((PK_D \oplus PK_C) \oplus T_{D1})}(ID_D, rg)$  and  $D \rightarrow C : M_7 = \{E_7, T_{D1}\}$ .
- Step 2. On getting  $M_7 = \{E_7, T_{D1}\}$ , *C* verifies  $T_{C7} - T_{D1} \leq \Delta T$ . Then, decrypts  $(ID_D, rg) = D_{h((PK_D \oplus PK_C) \oplus T_{D1})}$ , computes  $I = sn_P \oplus h(ID_D||r||T_{D1})$ , generates random number  $s \in Z_q^*$ , computes  $H_5 = h(ID_P||ID_D||Sig_H||Sig_P||C_P||T_{C8}||T_{D1})$  and encrypts  $E_8 = E_{sn_P}(Sig_P, Sig_H, NID_P, C_P, ID_P, H_5, s)$ . After that  $C \rightarrow D : M_8 = \{E_8, I, T_{C8}\}$ .
- Step 3. On receiving  $M_8 = \{E_8, I, T_{C8}\}$ , *D* checks  $T_{D2} - T_{C8} \leq \Delta T$ . Then, *D* computes  $J = I \oplus h(ID_D||rg||T_{D1})$ , decrypts  $(Sig_P, Sig_H, NID, C_P, ID_P, H_5, sg) = D_J(E_8)$ , computes  $H_5^* = h(ID_P||ID_D||Sig_H||Sig_P||C_P||T_{C8}||T_{D1})$  and verifies  $H_5^* \stackrel{?}{=} H_5$ . Further, *D* computes report  $(m_H, m_B) = D_{h(sn_P||NID_P||ID_P)}(C_P)$  and verifies digital signature  $V_{PK_P}(Sig_P) \stackrel{?}{=} h(m_B)$ . Furthermore, *D* inputs  $m_D = (ID_P, Data_D)$ ,

TABLE 6. TP of CSEF.

Doctor <i>D</i>	Cloud <i>C</i>
Inputs $ID_D$ Generates $r \in Z_q^*$ Encrypts $E_7 = E_{h((PK_D \oplus PK_C) \oplus T_{D1})}(ID_D, rg)$ Sends $M_7 = \{E_7, T_{D1}\}$ .....→	Verifies $T_{C7} - T_{D1} \leq \Delta T$ Decrypts $(ID_D, rg) = D_{h((PK_D \oplus PK_C) \oplus T_{D1})}(E_7)$ Computes $I = sn_P \oplus h(ID_D    rg    T_{D1})$ Generates $s \in Z_q^*$ Computes $H_5 = h(ID_P    ID_D    Sig_H    Sig_P    C_P    T_{C8}    T_{D1})$ Encrypts $E_8 = E_{sn_P}(Sig_P, Sig_H, NID_P, C_P, ID_P, H_5, sg)$ Sends $M_8 = \{E_8, I, T_{C8}\}$ ←.....
Verifies $T_{D2} - T_{C8} \leq \Delta T$ Computes $J = I \oplus h(ID_D    rg    T_{D1})$ Decrypts $(Sig_P, Sig_H, NID, C_P, ID_P, H_5, sg) = D_J(E_8)$ Computes $H_5^* = h(ID_P    ID_D    Sig_H    Sig_P    C_P    T_{C8}    T_{D1})$ Verifies $H_5^* \stackrel{?}{=} H_5$ Decrypts $(m_H, m_B) = D_{h(sn_P    NID_P    ID_P)}(C_P)$ Verifies $V_{PK_P}(Sig_P) \stackrel{?}{=} h(m_B)$ Generates $m_D = (ID_P, Data_D)$ Encrypts $C_D = E_{h(ID_P    ID_D    sn_P    NID_P)}(m_H, m_B, m_D)$ Computes $Sig_D = S_{PR_D}(h(m_D))$ Computes $H_6 = h(ID_P    ID_D    C_D    Sig_D    Sig_P    T_{D3}    T_{C8})$ Computes $SK_{DC} = h(H_6    ID_P    ID_D    Sig_D    Sig_P    rs_g    T_{D3}    T_{C8})$ Encrypts $E_9 = E_J(Sig_D, C_D, H_6)$ Sends $M_9 = \{E_9, T_{D3}\}$ .....→	Verifies $T_{C9} - T_{D3} \leq \Delta T$ Decrypts $(Sig_D, C_D, H_6) = E_{sn_P}(E_9)$ Computes $H_6^* = h(ID_P    ID_D    C_D    Sig_D    Sig_P    T_{D3}    T_{C8})$ Verifies $H_6^* \stackrel{?}{=} H_6$ Computes $SK_{CD} = h(H_6^*    ID_P    ID_D    Sig_D    Sig_P    rs_g    T_{D3}    T_{C8})$ Stores $C_D, Sig_D$ in database

encrypts  $C_D = E_{h(ID_P || ID_D || sn_P || NID_P)}(m_H, m_B, m_D)$ , makes digital signature  $Sig_D = S_{PR_D}(h(m_D))$ , computes  $H_6 = h(ID_P || ID_D || C_D || Sig_D || Sig_P || T_{D3} || T_{C8})$ , computes session key  $SK_{DC} = h(H_6 || ID_P || ID_D || Sig_D || Sig_P || rs_g || T_{D3} || T_{C8})$  and encrypts  $E_9 = E_J(Sig_D, C_D, H_6)$ . After that,  $D \rightarrow C : M_9 = \{E_8, T_{D3}\}$ .

Step 4. On getting  $M_9 = \{E_8, T_{D3}\}$ ,  $C$  verifies  $T_{C9} - T_{D3} \leq \Delta T$ . Then,  $C$  decrypts  $(Sig_D, C_D, H_6) = E_{sn_P}(E_9)$ , computes  $H_6^* = h(ID_P || ID_D || C_D || Sig_D || Sig_P || T_{D3} || T_{C8})$  and verifies  $H_6^* \stackrel{?}{=} H_6$ . Further,  $C$  computes session key  $SK_{CD} = h(H_6^* || ID_P || ID_D || Sig_D || Sig_P || rs_g || T_{D3} || T_{C8})$  and stores parameters  $C_D, Sig_D$  in database.

decrypts  $(m_H, m_B, m_D) = D_{h(ID_P || ID_D || sn_P || NID_P)}(C_D)$  and verifies  $V_{PK_D}(Sig_D) \stackrel{?}{=} h(m_D)$ . Furthermore,  $P$  encrypts  $C_E = E_{h(ID_P || ID_D || sn_P || NID_P || Sig_P)}(m_H, m_B, m_D)$ , computes  $H_8 = h(SK_{PC} || H_7^* || C_E || Sig_P || Sig_D || xy_g || T_{P6} || T_{C11})$ , 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  $(C_E, S_8) = D_{SK_{CP}}(E_{12})$ , computes  $H_8^* = h(SK_{CP} || S_7 || C_E || Sig_P || Sig_D || xy_g || T_{P6} || T_{C11})$  and verifies  $H_8^* \stackrel{?}{=} H_8$ . After that  $C$  stores parameter  $C_E$  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  $x \in Z_q^*$ , encrypts  $E_{10} = E_{SK_{PC}}(ID_P, NID_P, sn_P, xg)$  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  $(ID_P, NID_P, sn_P, xg) = D_{SK_{CP}}(E_{10})$ . Further,  $C$  generates random number  $y \in Z_q^*$ , computes  $H_7 = h(SK_{CP} || ID_P || ID_D || C_D || xy_g || Sig_P || T_{C11} || T_{P4})$  and encrypts  $E_{11} = E_{SK_{CP}}(H_7, ID_D, Sig_D, C_D, yg)$ . 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  $(H_7, ID_D, Sig_D, C_D, yg) = D_{SK_{PC}}(E_7)$ , computes  $H_7^* = h(SK_{PC} || ID_P || ID_D || C_D || xy_g || Sig_P || T_{C11} || T_{P4})$  and verifies  $H_7^* \stackrel{?}{=} H_7$ . Further,  $P$

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  $H_9 = h(H_6 || ID_P || T_{EP1})$ . Further,  $P$  generates a random number as  $\alpha \in Z_q^*$ , encrypt  $E_{13} = E_{SK_{PC}}(H_9, \alpha, EP_{request})$ . 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  $(H_9, \alpha, EP_{request}) = D_{SK_{CP}}(E_{13})$  and verifies  $H_9^* \stackrel{?}{=} h(H_6^* || ID_P || T_{EP1})$ . Then,  $C$  computes  $H_{10} = h(H_2^* || ID_H || ID_P || T_{EP3})$  and encrypts  $E_{14} = E_{SK_{CHS}}(EP_{request}, ID_P, H_{10}, \alpha, H_9^*)$ . 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  $(EP_{request}, ID_P, H_{10}, \alpha, H_9^*) = D_{SK_{HC}}(E_{14})$ . Further,  $C$  verifies  $H_{10}^* \stackrel{?}{=} h(H_2 ||$

TABLE 7. CP of CSEF.

Patient <i>P</i>	Cloud <i>C</i>
Inputs $ID_P, NID_P, sn_P$ Generates $x \in Z_q^*$ Encrypts $E_{10} = E_{SK_{PC}}(ID_P, NID_P, sn_P, xg)$ Sends $M_{10} = \{E_{10}, T_{P4}\}$ .....→	Verifies $T_{C10} - T_{P4} \leq \Delta T$ Decrypts $(ID_P, NID_P, sn_P, xg) = D_{SK_{CP}}(E_{10})$ Generates $y \in Z_q^*$ Computes $H_7 = h(SK_{CP}    ID_P    ID_D    C_D    xyg    Sig_P    T_{C11}    T_{P4})$ Encrypts $E_{11} = E_{SK_{CP}}(H_7, ID_D, Sig_D, C_D, yg)$ Sends $M_{11} = \{E_7, T_{C11}\}$ ←.....
Verifies $T_{P5} - T_{C11} \leq \Delta T$ Decrypts $(H_7, ID_D, Sig_D, C_D, y) = D_{SK_{PC}}(E_7)$ Computes $H_7^* = h(SK_{PC}    ID_P    ID_D    C_D    xyg    Sig_P    T_{C11}    T_{P4})$ Verifies $H_7^* \stackrel{?}{=} H_7$ Decrypts $(m_H, m_B, m_D) = D_{h(ID_P    ID_D    sn_P    NID_P)}(C_D)$ Verifies $V_{PK_D}(Sig_D) \stackrel{?}{=} h(m_D)$ Encrypts $C_E = E_{h(ID_P    ID_D    sn_P    NID_P    Sig_P)}(m_H, m_B, m_D)$ Computes $H_8 = h(SK_{PC}    H_7^*    C_E    Sig_P    Sig_D    xyg    T_{P6}    T_{C11})$ Encrypts $E_{12} = E_{SK_{PC}}(C_E, H_8)$ Sends $M_{12} = \{E_{12}, T_{P6}\}$ .....→	Verifies $T_{C12} - T_{P6} \leq \Delta T$ Decrypts $(C_E, S_8) = D_{SK_{CP}}(E_{12})$ Computes $H_8^* = h(SK_{CP}    S_7    C_E    Sig_P    Sig_D    xyg    T_{P6}    T_{C11})$ Verifies $H_8^* \stackrel{?}{=} H_8$ stores $C_E$ in database

$ID_H || ID_P || T_{EP3}$ ). Then,  $H$  computes  $SK_{HP} = h(H_9^* || ID_P || ID_H || \alpha\beta g || T_{EP3} || T_{EP5})$ ,  $H_{11} = h(H_7^* || ID_H || ID_P || \alpha g || T_{EP5})$ ,  $K_H = h(ID_H || ID_P || H_7^* || \alpha g)$  and encrypts  $E_{15} = E_{K_H}(\beta, H_{11}, EP_{replay}, T_{EP3}, T_{EP5})$ . Finally,  $H \rightarrow C : M_{15} = \{E_{15}, T_{EP5}\}$ .

Step 4. On getting  $M_{15}$ ,  $C$  checks  $T_{EP6} - T_{EP5} \leq \Delta T$  and  $C \rightarrow P : M_{16} = \{E_{16}, T_{EP7}\}$ .

Step 5. On receiving  $M_{16}$ ,  $P$  verifies  $T_{EP8} - T_{EP7} \leq \Delta T$ . Then, computes  $K_P = h(ID_H || ID_P || H_7 || \alpha g)$ , decrypts  $(\beta, H_{11}, EP_{replay}, T_{EP3}, T_{EP5}) = D_{K_P}(E_9)$  and also verifies  $H_{11}^* \stackrel{?}{=} h(H_9 || ID_H || ID_P || \alpha g || T_{EP3})$ . Further,  $P$  computes  $SK_{PH} = h(H_9 || ID_P || ID_H || \alpha\beta g || T_{EP3} || T_{EP5})$ .

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 below:

- 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  $H_1^* = h(ID_H || ag || bg || T_{H1})$ , verifies  $H_1^* \stackrel{?}{=} H_1$  and sends  $M_3 = \{E_2, T_{H3}\}$  to  $C$ . On getting  $M_3$ ,  $C$  verifies  $T_{C3} - T_{H3} \leq \Delta T$  and  $H_2^* \stackrel{?}{=} H_2$ .

Any  $\mathcal{A}$  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  $E_3 = E_{SK_{HC}}(ID_P, NID_P, sn_P, C_H, H_2, Sig_H)$  and only be decrypt by  $C$ ,  $(ID_P, NID_P, sn_P, C_H, H_2, Sig_H) = D_{SK_{CH}}(E_3)$  with using  $SK_{CH} = h(ID_H || H_1 || abg || T_{C2} || T_{H1})$  and verifies  $H_2^* \stackrel{?}{=} H_2$  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



TABLE 8. EP of CSEF.

Patient P	Cloud C	Healthcare center H
Input $ID_P, EP_{request}$ Computes $H_9 = h(H_6    ID_P    T_{EP1})$ Select $\alpha \in Z_q^*$ Encrypt $E_{13} = E_{SK_{PC}}(H_9, \alpha, EP_{request})$ Sends $M_{13} = \{E_{13}, T_{EP1}\}$ ..... $\rightarrow$	Checks $T_{EP2} - T_{EP1} \leq \Delta T$ Decrypt $(H_9, \alpha, EP_{request}) = D_{SK_{CP}}(E_{13})$ Checks $H_9 \stackrel{?}{=} h(H_6^*    ID_P    T_{EP1})$ Computes $H_{10} = h(H_2^*    ID_H    ID_P    T_{EP3})$ Encrypt $E_{14} = E_{SK_{CHS}}(EP_{request}, ID_P, H_{10}, \alpha, H_9^*)$ Sends $M_{14} = \{E_{14}, T_{EP3}\}$ ..... $\rightarrow$	Checks $T_{EP4} - T_{EP3} \leq \Delta T$ Decrypts $(EP_{request}, ID_P, H_{10}, \alpha) = D_{SK_{HC}}(E_{14})$ Verifies $H_{10}^* \stackrel{?}{=} h(H_2    ID_H    ID_P    T_{EP3})$ Generates $\beta \in Z_q^*$ computes $SK_{HP} = h(H_9^*    ID_P    ID_H    \alpha \beta g    T_{EP3}    T_{EP5})$ Computes $H_{11} = h(H_9^*    ID_H    ID_P    \alpha g    T_{EP5})$ Computes $K_H = h(ID_H    ID_P    H_7^*    \alpha g)$ Encrypts $E_{15} = E_{K_H}(\beta, H_{11}, EP_{replay}, T_{EP3}, T_{EP5})$ Sends $M_{15} = \{E_{15}, T_{EP5}\}$ ..... $\leftarrow$
Verifies $T_{EP8} - T_{EP7} \leq \Delta T$ Computes $K_P = h(ID_H    ID_P    H_7    \alpha g)$ Decrypts $(\beta, H_{11}, EP_{replay}, T_{EP3}, T_{EP5}) = D_{K_P}(E_{15})$ Verifies $H_{11}^* \stackrel{?}{=} h(H_9    ID_H    ID_P    \alpha g    T_{EP3})$ Computes $SK_{PH} = h(H_9    ID_P    ID_H    \alpha \beta g    T_{EP3}    T_{EP5})$	Verifies $T_{EP6} - T_{EP5} \leq \Delta T$ Sends $M_{16} = \{E_{15}, T_{EP7}\}$ ..... $\leftarrow$	

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  $SK_{PC} = h(ID_P || ID_H || C_H || H_3^* || cdg || T_{C5} || T_{P1})$  and  $C$  computes  $SK_{CP} = h(ID_P || ID_H || C_H || H_3 || cdg || T_{C5} || T_{P1})$ .
- In TP,  $D$  executes  $SK_{DC} = h(H_6 || ID_P || ID_D || Sig_D || Sig_P || rsg || T_{D3} || T_{C8})$  and  $C$  key  $SK_{CD} = h(H_6^* || ID_P || ID_D || Sig_D || Sig_P || rsg || T_{D3} || T_{C8})$ .
- In EP,  $H$  computes  $SK_{HP} = h(H_9^* || ID_P || ID_H || \alpha \beta g || T_{EP3} || T_{EP5})$  and  $P$  computes  $SK_{PH} = h(H_9 || ID_P || ID_H || \alpha \beta g || T_{EP3} || T_{EP5})$ .

Here,  $A$  cannot find session key in different phases. Hence, CSEF has manages known-key security.

**F. DATA CONFIDENTIALITY**

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

- In HUP,  $H$  encrypts as  $E_1 = E_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})}(ID_H, ag)$  with using key  $h((PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1}))$  and forwards to  $C$ . Further,  $C$  decrypts  $(ID_H, ag) = D_{h(PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1})}(E_1)$  with using key  $h((PK_H \oplus T_{H1}) \oplus (PK_C \oplus T_{H1}))$ . Furthermore,  $C$  encrypts  $E_2 = E_{h(ID_H || ag || T_{H1} || T_{C2})}(bg, H_1)$  with using key  $h(ID_H || ag || T_{H1} || T_{C2})$  and uploads to  $H$ . Furthermore,  $H$  decrypts  $(bg, H_1) = D_{h(ID_H || ag || T_{H1} || T_{C2})}(E_2)$  with using key  $h(ID_H || ag || T_{H1} || T_{C2})$ , encrypts  $C_H = E_{h(ID_P || ID_H || NID_P)}(m_H)$  with using key  $h(ID_P || ID_H || NID_P)$ ,  $E_3 = E_{SK_{HC}}(ID_P, NID_P, sn_P, C_H, H_2, Sig_H)$  with using key  $SK_{HC}$  and sends to  $C$ . On receiving,  $C$  decrypts  $(ID_P, NID_P, sn_P, C_H, H_2, Sig_H) = D_{SK_{CH}}(E_3)$  with using key  $SK_{CH}$  and verifies  $H_2^* \stackrel{?}{=} H_2$ . Then, stores parameters  $ID_P, C_H, Sig_H, NID_P, sn_P$  in database.

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  $Sig_H = S_{PR_H}(h(m_H))$ .

- In PUP,  $P$  verified  $H$ 's digital signature by  $V_{PK_H}(Sig_H) \stackrel{?}{=} h(m_H)$ . Then,  $P$  executes digital signature  $Sig_P = S_{PR_P}(h(m_B))$ .
- In TP,  $D$ 's checked  $P$ 's digital signature by  $V_{PK_P}(Sig_P) \stackrel{?}{=} h(m_B)$  and computes digital signature  $Sig_D = S_{PR_D}(h(m_D))$ .
- In CP,  $P$  checked  $D$ 's digital signature  $V_{PK_D}(Sig_D) \stackrel{?}{=} h(m_D)$ .

Thus,  $P$  verifies the health records. Hence, CSEF maintains data non-repudiation.

## H. MESSAGE AUTHENTICATION

We explain message authentication in HUP as below:

- In HUP,  $H$  collects  $M_2 = \{E_2, T_{C2}\}$  and checks the authenticity by checking  $T_{H2} - T_{C2} \leq \Delta T$  and  $H_1^* \stackrel{?}{=} H_1$ . Similarly,  $C$  gets  $M_3 = \{E_2, T_{H3}\}$  and verifies the validity by verifying  $T_{C3} - T_{H3} \leq \Delta T$ , and  $H_2^* \stackrel{?}{=} H_2$ . If any  $\mathcal{A}$  endeavors alter any charge of the information,  $C$  will recognize it.

Similarly, message authentication verified in PUP, TP, CP and EP. Therefore, CSEF manages this property in each phase.

## I. IMPERSONATION ATTACK

We explain this attack in HUP as:

- Any attacker  $\mathcal{A}$  tries to masquerade as an authenticated  $C$ , and eavesdrop the transmitted  $M_2 = \{E_2, T_{C2}\}$  and tries to executes  $h(ID_H \| ag \| T_{H1} \| T_{C2})$ ,  $H_1^* = h(ID_H \| ag \| bg \| T_{H1})$ .  $E$  cannot execute  $H_1^*$ , which is the hash value contain attributes  $ID_H$ ,  $ag$ ,  $bg$ ,  $T_{H1}$  where  $ID_H$  is identifier of the  $H$ ,  $ag$  and  $bg$  scalar multiplication of ECC which are computed by the  $H$  and  $C$ . Further,  $E$  cannot compute  $H_2 = h(SK_{HC} \| C_H \| Sig_H \| T_{H3} \| T_{C2})$  by secure hash function. Thus, any  $\mathcal{A}$  cannot impersonate as an authenticate  $C$ .
- $\mathcal{A}$  adversary tries to impersonate as a healthcare center. If,  $\mathcal{A}$  verifies  $T_{H2} - T_{C2} \leq \Delta T$ , guesses  $ID_H$  of  $H$  as  $ID_{\mathcal{A}} = ID_H$ , random number  $a$  and executes  $ag$ . Then, calculates  $H_2 = h(SK_{HC} \| C_H \| Sig_H \| T_{H3} \| T_{C2})$  and checks  $H_2^* \stackrel{?}{=} H_2$ . Which is not possible, as  $H_2^* = h(SK_{CH} \| C_H \| Sig_H \| T_{H3} \| T_{C2})$  is the hash value of parameters  $SK_{CH}$ ,  $C_H$ ,  $Sig_H$ ,  $T_{H3}$ ,  $T_{C2}$ . Thus,  $H_2^*$  has safe value. Thus,  $\mathcal{A}$  cannot impersonate as an authenticate  $H$ .

Similarly, impersonation attacks cannot work in PUP, TP, CP and EP phases. Thus, CSEF is free from this attack.

## J. STOLEN-VERIFIER ATTACK

The stolen-verifier attack means that  $\mathcal{A}$  who steals a password from the cloud server can use it directly to impersonate a legitimate participant in an authentication process. In fact,  $\mathcal{A}$  who has a verifies password may further mount a guessing attack. In CSEF, we discuss verification of stolen-verifier attack as below:

- $P$  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  $T_{R2} - T_{R1} \leq \Delta T$ . Then,  $H$  computes  $NID_P = h(ID_P \| PWP \| T_{R1})$ , generates  $sn_P \in Z_q^*$ . Then, stores  $NID_P$ ,  $ID_P$ ,  $sn_P$  in cloud database. Further,  $H$  encrypts  $E_{P1} = E_{h(PWP \| T_{R1} \| ID_P)}(NID_P, ID_P, sn_P)$  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,  $\mathcal{A}$  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  $EP$ . • Chiou 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  $EP$ . • Chandrakar 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,  $SK_{HC} = h(ID_H \| H_1^* \| abg \| T_{C2} \| T_{H1})$  and  $SK_{CH} = h(ID_H \| H_1 \| abg \| T_{C2} \| T_{H1})$  are the session key between  $H$  and  $C$ , where  $SK_{HC} = SK_{CH}$ .  $\mathcal{A}$  cannot execute  $SK_{HC}$  or  $SK_{CH}$ , where  $H_1^* = h(ID_H \| ag \| bg \| T_{H1})$  and  $H_1 = h(ID_H \| ag \| bg \| T_{H1})$ . According as impersonation attack,  $H_1$  and  $H_1^*$  cannot be computed by  $\mathcal{A}$ . Further, For  $a, b \in Z_q^*$  and  $g$  is the generator of  $G$ , for given  $(g, ag, bg)$ , then executes  $abg$  is hard for  $G$  by ECCDHP 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  $\mathcal{A}$  reuse historical message in insecure channel to make a fresh request, then impersonates the understandable participant to compute session key. In CSEF,  $\mathcal{A}$  has to know the components reposed of the information then,  $\mathcal{A}$  can form the suitable request or keys. As this analysis,  $\mathcal{A}$  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], Chiou 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	×	✓	×	×	×	×	✓
DU	✓	✓	✓	✓	✓	✓	✓
SS	✓	×	✓	✓	×	✓	✓
PA	×	×	×	×	×	✓	✓
DU	×	✓	×	×	×	✓	✓
RA	✓	✓	✓	✓	✓	✓	✓
KK	✓	×	×	✓	✓	✓	✓
MI	✓	✓	✓	✓	✓	✓	✓
IM	✓	✓	×	×	×	×	✓
MA	✓	✓	✓	✓	×	✓	✓
DR	✓	✓	✓	✓	✓	×	✓
OF	×	×	✓	×	✓	✓	✓
RP	×	×	×	×	×	✓	✓
EP	×	×	×	×	×	×	✓

Note  $\implies$  ✓: Attributes satisfied by the framework and ×: 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-repudiation, OF : Off-line 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	$\approx 0.0005$
$T_{Sign}$	Execute/verify a signature	$\approx 0.3317$
$T_P$	Bilinear pairing operation	$\approx 0.0621$
$T_A$	Asymmetric encryption/ decryption operation	$\approx 0.3057$
$T_M$	Multiplication operation	$\approx 0.0503$
$T_S$	Symmetric encryption/ decryption operation	$\approx 0.0087$

TABLE 11. Comparison of the computation cost in seconds .

Protocol	Ref [47]	Ref [46]	Ref [49]	Ref [50]	Ref [52]	Ref [53]	CSEF
HUP	$1T_{Sign}+1T_M+2T_P + 4T_S+2T_H+3T_A$	$1T_{Sign}+4T_M+4T_P + 2T_S+6T_H+1T_A$	$1T_{Sign}+3T_P + 2T_S+7T_H$	$1T_{Sign}+3T_S + 11T_H$	$1T_{Sign}+3T_S + 11T_H$	$1T_{Sign}+4T_S + 10T_H$	$1T_{Sign}+7T_S + 12T_H$
PUP	$1T_M + 2T_P + 4T_S + 2T_H+3T_A$	$1T_{Sign} + 4T_M + 4T_P + 3T_S+6T_H + 1T_A$	$1T_{Sign}+4T_P + 2T_S+12T_H$	$+ 2T_{Sign}+2T_S + 10T_H$	$2T_{Sign}+4T_S + 10T_H$	$2T_{Sign}+7T_S + 9T_H$	$2T_{Sign}+8T_S + 15T_H$
TP	$2T_{Sign}+1T_M+2T_P + 7T_S+2T_H+4T_A$	$2T_{Sign}+4T_M+4T_P + 4T_S+6T_H$	$2T_{Sign}+4T_M+4T_P + 4T_S + 6T_H$	$+ 2T_{Sign} + 2T_S + 9T_H$	$3T_{Sign} + 6T_S + 10T_H$	$5T_{Sign}+5T_S + 22T_H$	$2T_{Sign}+8T_S + 13T_H$
CP	NA	NA	$1T_{Sign}+2T_P + 2T_S+8T_H$	$1T_{Sign} + 2T_S + 5T_H$	$1T_{Sign} + 2T_S + 8T_H$	$2T_{Sign}+2T_S + 8T_H$	$1T_{Sign}+8T_S + 6T_H$
EP	NA	$2T_{Sign} + 2T_P + 6T_S + 4T_H$	NA	NA	NA	NA	$10T_H + 6T_S$
Total cost	$3T_{Sign}+3T_M+6T_P + 15T_S+6T_H+10T_A$	$6T_{Sign}+12T_M+15T_P + 15T_S+22T_H+2T_A$	$5T_{Sign}+4T_M+13T_P + 10T_S+33T_H$	$+ 6T_{Sign} + 9T_S + 35T_H$	$7T_{Sign} + 15T_S + 39T_H$	$10T_{Sign}+18T_S + 59T_H$	$6T_{Sign}+37T_S + 56T_H$
Total time	$\approx 4.7091$ Second	$\approx 4.2782$ Second	$\approx 2.7705$ Second	$\approx 2.086$ Second	$\approx 2.4719$ Second	$\approx 3.5031$ Second	$\approx 2.3401$ Second

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., Chiou 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

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

- The computation expenditure of Chen et al.'s [47] is  $3T_{Sign}+3T_M+6T_P+15T_S+6T_H+10T_A \approx 4.7091$  second, which is approximate 101.24% grater than CSEF computation expenditure.
- The computation expenditure of Chen et al.'s [46] is  $6T_{Sign} + 12T_M + 15T_P + 15T_S + 22T_H + 2T_A \approx 4.2782$  second, which is approximately 82.83% grater than CSEF computation expenditure.
- The computation expenditure of Chiou et al.'s [49] is  $5T_{Sign} + 4T_M + 13T_P + 10T_S + 33T_H \approx 2.7705$  second, which is approximately 15.53% grater than CSEF computation expenditure.

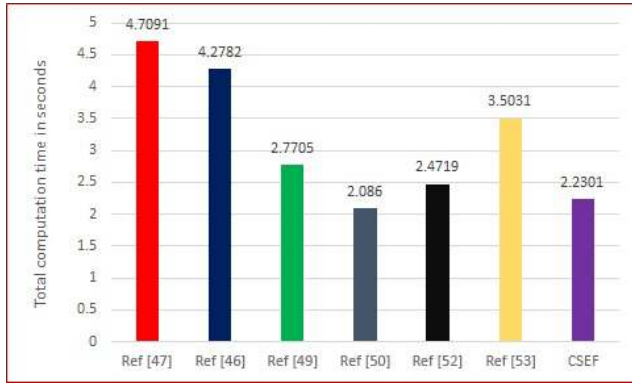


FIGURE 2. Comparison of the computation cost in seconds.

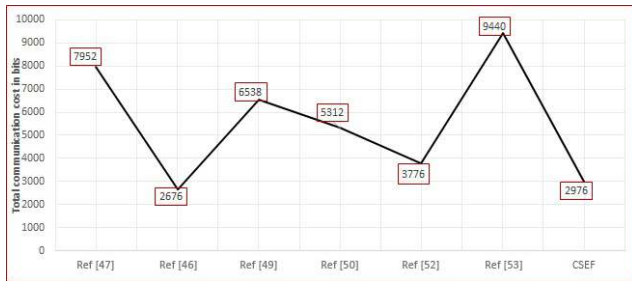


FIGURE 3. Comparison the communication cost in bits.

- The computation expenditure of Mohit *et al.*'s [50] is  $6T_{Sign} + 9T_S + 35T_H \approx 2.086$  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  $7T_{Sign} + 15T_S + 39T_H \approx 2.4719$  second, which is approximately 5.42% greater than CSEF computation expenditure.
- The computation expenditure of Chandrakar *et al.*'s [53] is  $7T_{Sign} + 15T_S + 39T_H \approx 3.5031$  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.

### 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:

TABLE 12. Comparison the communication cost in bits.

Protocol	Ref [47]	Ref [46]	Ref [49]	Ref [50]	Ref [52]	Ref [53]	CSEF
HUP	1936	816	704	592	592	800	528
PUP	2064	816	1600	1744	1232	1120	528
TP	2192	944	2112	1792	720	5296	688
CP	NA	NA	2122	1184	1232	2224	528
EP	1760	NA	NA	NA	NA	NA	704
Total cost in bits	7952	2576	6538	5312	3776	9440	2976

- The communication expenditure of Chen *et al.* [47] is 7952 bits, which is approximately 167.20% greater than CSEF communication cost.
- The communication expenditure of Chen *et al.* [46] is 2576 bits, which is approximately 15.52% greater than CSEF communication cost.
- The communication expenditure of Chiou *et al.* [49] is 6538 bits, which is approximately 119.69% greater than CSEF communication cost.
- The communication expenditure of Mohit *et al.* [50] is 5312 bits, which is approximately 78.5% greater than CSEF communication cost.
- The communication expenditure of Li *et al.* [52] is 3776 bits, which is approximately 26.88% greater than CSEF communication cost.
- The communication expenditure of Chandrakar *et al.* [53] is 9440 bits, which is approximately 217.0% greater than CSEF communication cost.

### 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.

- [3] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.
- [4] Y. Tsai, "Cloud computing security," *Commun. CCISA*, vol. 18, no. 2, pp. 62–68, 2012.
- [5] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, and S. Loureiro, "A security analysis of Amazon's elastic compute cloud service," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN)*, Jun. 2012, pp. 1427–1434.
- [6] J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," *J. Med. Syst.*, vol. 41, no. 5, p. 80, May 2017.
- [7] B.-Q. Cao, B. Li, and Q.-M. Xia, "A service-oriented QoS-assured and multi-agent cloud computing architecture," in *Proc. IEEE Int. Conf. Cloud Comput. Bengaluru, India: Springer*, Dec. 2009, pp. 644–649.
- [8] C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 8, pp. 3133–3142, Aug. 2019.
- [9] E. Casalicchio and L. Silvestri, "Mechanisms for SLA provisioning in cloud-based service providers," *Comput. Netw.*, vol. 57, no. 3, pp. 795–810, Feb. 2013.
- [10] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. K. Khan, "SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing," *Int. J. Commun. Syst.*, Jul. 2019, Art. no. e4103, doi: 10.1002/dac.4103.
- [11] A. K. Sangaiah, D. V. Medhane, T. Han, M. S. Hossain, and G. Muhammad, "Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4189–4196, Jul. 2019.
- [12] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Gener. Comput. Syst.*, vol. 83, pp. 629–637, Jun. 2018.
- [13] D. Mishra, V. Kumar, and S. Mukhopadhyay, "A pairing-free identity based authentication framework for cloud computing," in *Proc. Int. Conf. Netw. Syst. Secur. Madrid, Spain: Springer*, 2013, pp. 721–727.
- [14] V. Kumar, A. A. Khan, and M. Ahmad, "Design flaws and cryptanalysis of elliptic curve cryptography-based lightweight authentication scheme for smart grid communication," in *Advances in Data Sciences, Security and Applications*. New Delhi, India: Springer, 2020, pp. 169–179.
- [15] V. Kumar, M. Ahmad, and P. Kumar, "An identity-based authentication framework for big data security," in *Proc. 2nd Int. Conf. Commun., Comput. Netw. Chandigarh, India: Springer*, 2019, pp. 63–71.
- [16] A. A. Khan, V. Kumar, and M. Ahmad, "An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach," *J. King Saud Univ. Comput. Inf. Sci.*, to be published, doi: 10.1016/j.jksuci.2019.04.013.
- [17] A. Kumari, V. Kumar, M. YahyaAbbasi, and M. Alam, "The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for IOT and cloud servers," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 321–325.
- [18] A. K. Sangaiah, M. Sadeghilalimi, A. A. R. Hosseinabadi, and W. Zhang, "Energy consumption in point-coverage wireless sensor networks via bat algorithm," *IEEE Access*, vol. 7, pp. 180258–180269, 2019.
- [19] D. Mishra, V. Kumar, D. Dharminder, and S. Rana, "SFVCC: Chaotic map-based security framework for vehicular cloud computing," *IET Intell. Transp. Syst.*, vol. 14, no. 4, pp. 241–249, Apr. 2020.
- [20] C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, and M.-E. Wu, "A secure authenticated and key exchange scheme for fog computing," *Enterprise Inf. Syst.*, pp. 1–16, Jan. 2020, doi: 10.1080/17517575.2020.1712746.
- [21] A. G. Reddy, D. Suresh, K. Phaneendra, J. S. Shin, and V. Odelu, "Provably secure pseudo-identity based device authentication for smart cities environment," *Sustain. Cities Soc.*, vol. 41, pp. 878–885, Aug. 2018.
- [22] S. H. Islam and M. K. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 10, p. 135, Oct. 2014.
- [23] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and M. S. Obaidat, "Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system," *J. Med. Syst.*, vol. 39, no. 11, p. 137, Nov. 2015.
- [24] C.-M. Chen, C.-T. Li, S. Liu, T.-Y. Wu, and J.-S. Pan, "A provable secure private data delegation scheme for mountaineering events in emergency system," *IEEE Access*, vol. 5, pp. 3410–3422, 2017.
- [25] P. Gope and R. Amin, "A novel reference security model with the situation based access policy for accessing EPHR data," *J. Med. Syst.*, vol. 40, no. 11, p. 242, Nov. 2016.
- [26] 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.
- [27] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "PALK: Password-based anonymous lightweight key agreement framework for smart grid," *Int. J. Electr. Power Energy Syst.*, vol. 121, Oct. 2020, Art. no. 106121.
- [28] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, A. G. Reddy, K. Park, and Y. Park, "On the design of fine grained access control with user authentication scheme for telecare medicine information systems," *IEEE Access*, vol. 5, pp. 7012–7030, 2017.
- [29] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and X. Li, "Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for E-health care systems," *J. Med. Syst.*, vol. 39, no. 11, p. 140, Nov. 2015.
- [30] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 80, pp. 483–495, Mar. 2018.
- [31] Z.-Y. Wu, Y.-J. Tseng, Y. Chung, Y.-C. Chen, and F. Lai, "A reliable user authentication and key agreement scheme for Web-based hospital-acquired infection surveillance information system," *J. Med. Syst.*, vol. 36, no. 4, pp. 2547–2555, Aug. 2012.
- [32] 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 TMIS," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 1983–2001, Sep. 2016.
- [33] R. Guo and H. Shi, "Confidentiality-preserving personal health records in tele-healthcare system using authenticated certificateless encryption," *IJ Netw. Secur.*, vol. 19, no. 6, pp. 995–1004, 2017.
- [34] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, Feb. 2015.
- [35] V. Kumar, M. Ahmad, and A. Kumari, "A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS," *Telematics Informat.*, vol. 38, pp. 100–117, May 2019.
- [36] 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. 40, no. 11, p. 233, Nov. 2016.
- [37] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 59, pp. 250–261, Apr. 2017.
- [38] 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.
- [39] 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. Macao, China: Springer*, 2017, pp. 241–248.
- [40] 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, p. 77, Sep. 2014.
- [41] 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, p. 142, Aug. 2018.
- [42] 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, p. 66, Jun. 2015.
- [43] 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. Sutrala, 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. 135, pp. 167–185, Oct. 2016.
- [45] R. P. Padhy, 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. Syst.*, 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. Syst.*, 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. 255–276, 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. Syst.*, 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. Syst.*, 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. Mansoor, S. Mehmood, 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] K. Mahmood, 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] S. Hussain and S. A. Chaudhry, "Comments on 'biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment,'" *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10936–10940, Dec. 2019.
- [58] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.
- [59] K. Mansoor, A. Ghani, S. Chaudhry, S. Shamshirband, S. Ghayyur, and A. Mosavi, "Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography," *Sensors*, vol. 19, no. 21, p. 4752, Nov. 2019.
- [60] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," *Comput. Secur.*, vol. 55, pp. 271–280, Nov. 2015.
- [61] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. 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.
- [62] S. Challa, 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.
- [63] 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.
- [64] J. Mo, W. Shen, and W. Pan, "An improved anonymous authentication protocol for wearable health monitoring systems," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–13, Apr. 2020.
- [65] B. A. Alzahrani, A. Irshad, K. Alsubhi, and A. Albeshri, "A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT," *Int. J. Commun. Syst.*, Apr. 2020, Art. no. e4423.
- [66] H. Darrel, M. Alfred, and V. Scott, "Guide to elliptic curve cryptography," in *Springer Professional Computing*, H. D. Hankerson, A. J. Menezes, V. Scott, eds. Springer, 2004, p. 311.
- [67] A. Kumari, M. Y. Abbasi, V. Kumar, and A. A. Khan, "A secure user authentication protocol using elliptic curve cryptography," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 521–530, May 2019.
- [68] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100213.
- [69] A. Kumari, S. Jangirala, M. Y. Abbasi, V. Kumar, and M. Alam, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," *J. Inf. Secur. Appl.*, vol. 51, Apr. 2020, Art. no. 102443.
- [70] L. Zhang, S. Tang, and H. Luo, "Elliptic curve cryptography-based authentication with identity protection for smart grids," *PLoS ONE*, vol. 11, no. 3, Mar. 2016, Art. no. e0151253.
- [71] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
- [72] S. Gangan, "A review of man-in-the-middle attacks," 2015, *arXiv:1504.02115*. [Online]. Available: <http://arxiv.org/abs/1504.02115>



**ADESH KUMARI** received the master's degree in mathematics from Maharshi Dayanand University (MDU), Rohtak, India. She is currently pursuing the Ph.D. degree from the Department of Mathematics, Jamia Millia Islamia, New Delhi, India. She has authored or coauthored ten research articles in reputed international journals and conferences. Her research interests include remote user authentication protocols, smart card security, information security, and cloud computing.



**VINOD KUMAR** received the Master of Philosophy degree in mathematics from Chaudhary Charan Singh University, Meerut, India, and the Master of Technology degree from IIT Kharagpur, in 2013. He is currently working as an Assistant Professor with the Department of Mathematics, PGDAV College, University of Delhi, New Delhi, India. He has authored or coauthored of 20 research articles in reputed international journals and conferences. He is a reviewer of many reputed journals. His research interests include remote user authentication protocols, information and network security, cloud computing, cryptographic security protocols, vehicular networking, and applied mathematics.



**M. YAHYA ABBASI** received the Ph.D. degree from the Department of Mathematics, Aligarh Muslim University, Aligarh, India. He is currently an Assistant Professor with the Department of Mathematics, Jamia Millia Islamia, New Delhi, India. He is edited two books and published more than 40 research articles in reputed international journals and conferences. His research interests include abstract algebra, application of algebra, and cryptography.



**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.



**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*.

• • •



**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.