frontiers in Public Health

METHODS
published: 30 September 2021
doi: 10.3389/fpubh.2021.688399

SCB-HC-ECC–Based Privacy Safeguard Protocol for Secure Cloud Storage of Smart Card–Based Health Care System

Sudha Senthilkumar[1], *K. Brindha*[2], *Natalia Kryvinska*[3]*, *Sweta Bhattacharya*[4]* and *Giridhar Reddy Bojja*[5]

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India, [2] School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India, [3] Head of Information Systems Department, Comenius University, Bratislava, Slovakia, [4] School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India, [5] College of Business and Information Systems, Dakota State University, Madison, SD, United States

The advent of the internet has brought an era of unprecedented connectivity between networked devices, making one distributed computing, called cloud computing, and popular. This has also resulted in a dire need for remote authentication schemes for transferring files of a sensitive nature, especially health-related information between patients, smart health cards, and cloud servers *via* smart health card solution providers. In this article, we elaborate on our proposed approach for such a system and accomplish an informal analysis to demonstrate the claim that this scheme provides sufficient security while maintaining usability.

Keywords: user anonymity, ECC, MAT tree, health care information, smart card

OPEN ACCESS

Edited by:
Patrick Siarry,
Universite Paris 12, France

Reviewed by:
Mohan Krishna Kagita,
The University of Queensland, Australia
Solomiia Fedushko,
Lviv Polytechnic, Ukraine

***Correspondence:**
Sweta Bhattacharya
sweta.b@vit.ac.in
Natalia Kryvinska
natalia.kryvinska@uniba.sk

Specialty section:
This article was submitted to Digital Public Health, a section of the journal Frontiers in Public Health

Received: *30 March 2021*
Accepted: *05 August 2021*
Published: *30 September 2021*

Citation:
Senthilkumar S, Brindha K, Kryvinska N, Bhattacharya S and Reddy Bojja G (2021) SCB-HC-ECC–Based Privacy Safeguard Protocol for Secure Cloud Storage of Smart Card–Based Health Care System. Front. Public Health 9:688399. doi: 10.3389/fpubh.2021.688399

INTRODUCTION

With the advent of cloud computing, we can rent servers and run geophysical modeling applications on the authoritative node present everywhere globally. We can securely store an enormous amount of data that can be accessed only by authorized users and applications (1–3). It enables us to rent a virtual server, switch it on or off, and expand it to fulfill users' immediate requirements. It increases association, adaptability, availability, and competency and speeds up the development process to imitate the deviations afforded to workload demand and also provides cost reduction over with efficient and optimized computations (4–8). As healthcare evolves, the need for innovative information system development is necessary (9, 10).

Cloud computing is the new paradigm for outdated conventional computing by adopting newer technology and many economic aspects. It is beneficial for both customers and service providers (2, 11). However, it has many advantages and disadvantages that restrict its usability. It includes architecture that supports many potential applications, programming models to support vast-scale data-centric computing, and provision for security and privacy protection of data. Security of data is challenged by both outside and inside threats (12–14). They can make use of a user's data for their benefit. Consequently, the popularity of cloud computing increases issues in security and privacy areas as well (15–17).

Consider a healthcare organization in which patients use a smart card that electronically holds patients' medical information. A smart card mechanism is used globally for secure identity, access, and payment applications. Smart health card solutions for patient and provider identity management are deployed worldwide and are accessible from various vendors (18, 19). A smart card mechanism offers a robust foundation for healthcare ID cards, empowering enhancement in

healthcare procedures and in-patient and provider identity verification while securing data and protecting privacy (20–22). Smart healthcare cards are available with two chips, one for the patient, and one for health professionals. Smart health cards can be an essential information source in case of an emergency when the patient is unresponsive. It could be the first source of information to know about the patient. However, smart cards are restricted in memory size, allowing the storage of only a limited amount of data. As such, the memory-intensive data, such as lab reports or diagnostic images and additional patient-related information, can be stored in a cloud server and accessed *via* the smart health card by healthcare professionals through the smart card solution provider (23–25).

Moving over to the cloud has proven to be helpful for both healthcare professionals and patients. The cloud also engages the patient with their health insurance plans by offering them generous access to their additional healthcare data that is not there in the smart health card, resulting in improved patient outcomes. Providing health care data in the cloud engages the interoperability of several segments of the health care industry, such as pharmaceuticals, insurance, and payments (13, 26, 27).

The following sections of the paper are organized as follows. Section II discusses related works on implementing and authentication of a smart card–based health care system with the cloud. Section III gives the preliminaries required for our work. Section IV gives an overview of the proposed system and system model. Section V describes the security and performance analysis of our scheme compared with other schemes. The conclusion is provided in Section VI.

RELATED WORKS

Many works have addressed implementing and authenticating smart card–based health care information systems. Moudgil et al. (1) designed a cloud-based smart health card monitoring system. Their proposed monitoring system helps health care providers, such as hospitals, physicians, and pharmacists, by managing all the patient data electronically, securely, and efficiently. It uses Bluetooth technology to transmit live patient monitoring data. It also supports off-line storage of medical and information and periodic updates to the cloud database. However, they do not focus on how the smart card and cloud servers are synchronized and how the mutual authentication happens between them. Yang et al. (28) design a MedShare system that publishes patient data to a cloud server using a two-way authorization process. They use the national identification card that patients swipe to publish data in the cloud. However, identification cards are only used for authentication purposes and do not carry any health care information. Li et al. (29) design a mutual authentication and privacy preservation protocol for the TMIS system. They use the AES encryption algorithm for encrypting patient information. Kausar et al. (30) design an intelligent card-based system using an iris-based biometric cryptosystem for an innovative card-based healthcare system. They focus only on how the patient data is stored and retrieved in the smart card. Their system does not include any security phases and is not integrated with cloud storage (31, 32).

Al-Saggaf et al. (33) propose a biometric-based remote authentication scheme using a smart card. They use a hashing function for transferring all the information. However, they do not mention the specific cryptographic technique for storing the data in the smart card. Kumari et al. (23) design an ESEAP system, which is an ECC-based mutual authentication protocol for the smart card. However, their system does not support the various phases, including health center data upload, medical data upload, and the lab technician phase. Ganesh et al. (34) propose the smart, automated health machine using IoT, which provides health services to the local area. They discuss the authentication phase using the smart card system to secure their privacy, but the system is not integrated with the cloud (35, 36).

The research work emphasizes the authentication to recognize that unauthorized users cannot access a user's private data but disregards an elusive privacy issue. In contrast, data sharing happens between the other users, such as the patient's smart card medical data and the cloud service provider. We propose a solution to address the data-sharing privacy issue for this type of environment.

The main contribution of the article is as follows:

1. Mutual access authority is attained by an anonymous access request matching approach with concern about security and privacy so that the cloud is not aware of who the patient is.
2. Mutual authentication between the healthcare organization that accesses the patient data using a smart card *via* the smart health card solution provider to the cloud server for further treatment.
3. The ECC-based encryption on the patient-related data in the cloud server and the smart health card.
4. Notification to the smart health card solution provider about changes in the patient data by the health care organization.

PRELIMINARIES

Elliptic Curve Cryptography

Elliptic-curve cryptography (**ECC**) is a technique for an asymmetric cryptosystem built on the algebraic structure of elliptic curves over finite fields (29).

Let p be a large prime number and E denote the elliptic curve over the prime finite field Z_P

$$E: y^2 = x^3 + c.x + d \pmod{p} \text{with(c, d)} \in Z_P \text{ and } 4c^3 + 27d^2 (mod\ p) \# 0$$

and produces grouping

$$E_p\ (c, d).$$

Base point G on the elliptic curve *has a large order n*, where n is a large prime number.

Encryption

1. Encode the message as (x,y) of point $\mathrm{P_m}$ $m \rightarrow P_m : (x, y)$ on the ECC

References	Method	Metrics	Limitation/research challenge
Moudgil et al. (1)	Smart card–based integrated electronic health record system	Biomedical parameters, such as blood pressure, diabetes mellitus and pulse oxygen.	Not focused on how the smart card and cloud servers are synchronized with each other and how the mutual authentication happens between them
Yang et al. (28)	MedShare system that uses two-way authorization techniques	The various phases are measured with respect to response time in milliseconds, throughput in bits/second and bandwidth in KB/second	Identification card only used for authentication purposes; does not carry any health care information
Li et al. (29)	Mutual authentication and privacy preservation protocol for TMIS system	Total cost of healthcare center upload phase, patient data upload phase, treatment and checkup phases are measured in seconds	Asymmetric encryption technique not used for encrypting the data
Kausar et al. (30)	A smart card–based system using an iris-based biometric cryptosystem for smart card–based healthcare system	Measurement of false rejection rate and false acceptance rate	They focus only on how the patient data is stored and retrieved in the smart card. The system does not include any security phases and is not integrated with cloud storage.
Al-Saggaf et al. (33)	Collision-resistant hash method	Computational cost of login and registration phases are measured in milliseconds	They use a hashing function for transferring all the information; however, they do not mention the specific cryptographic technique for storing the data in the smart card.
Kumari et al. (23)	ESEAP system that is an ECC-based mutual authentication protocol for smart cards	Communication cost measured in seconds	System does not support the various phases, which include health center data upload, mediclaim data upload, and Lab technician phase.
Divya et al. (34)	Smart automated health machine using IoT	Measurement of human heart rate, blood pressure, and ECG	Not focused on system integration with cloud
Sanjuan et al. (35)	Message queuing telemetry transport protocol using cryptographic smart card	Time spent for cryptographic operations measured in milliseconds	System performance is to be improved by using ECC algorithm instead of RSA.

2. Generate (pub,priv) key pair to be generated
3. Let k be the random number such as positive integer selected by A

$$C_m = (KG, P_m + kP_B)$$

where
P_m is the plain text point and $P_B = n_B * G$
where $n_B < n$ *which is private key*, P_B is the public key and C_m is the cipher text.

Decryption

1. Let us find $p_m = p_m + KP_B - n_B * kG$
2. $KP_B = k\left(n_{B*}G\right) = kn_B * kG$
3. Because of the multiplicative inverse property, $kn_B * kG$ can be written as $n_B * kG$
4. $p_m = p_m + n_B * kG - n_B * kG$

Finding the value of k or private key n_B is an elliptic curve discrete logarithmic problem (ECDLP) that requires a fully exponential running time. To compute the 160-bit key size of private key n_B, we require 8.5 * 10^{11} MIPS.

ECCDSA

The elliptic curve equivalent of the digital signature algorithm (DSA) is the elliptic curve digital signature algorithm (ECDSA). The ECDSA was first projected in 1992 by Scott Vanstone in response to NIST (37).

ECDSA has three phases: key generation, signature generation, and signature verification.

ECDSA Key Generation:

A is an entity that uses the key pair with a particular set of ECC domain parameters (p,q,g) that does the following:

1. Choose the pseudo random integer d in the interval $1 \leq d \leq q - 1$
2. Calculate $P = dG$
3. Choose P as its public key, and d is the private key

ECDSA Signature generation

A's message m is signed with domain parameters $D = \{q, FR, a, b, G, n.h\}$ and key pairs (P,d) perform the following steps:

1. Choose a random integer z, $1 \leq x \leq n - 1$
2. Calculate xG= $(x_{1,}y_1)$ and change $x1$ to an integer $\bar{x}_1$
3. Calculate $s = x_1 \ mod \ n$. If s=0, then go to step 1
4. Calculate $z^{-1} mod \ n$.

5. Calculate SHA-1(m) and convert the output to an integer f.
6. Calculate v= z^{-1}(f+ds) mod n. If v=0, then go to step 1.
7. A's signature for the message m is (s,v).

ECDSA Signature verification

To verify A's signature (s,v) on m, the entity B gets an authentic copy of A's domain parameters D = $\{q, FR, a, b, G, n.h\}$ and its public key P. B does the following:

1. Verify (s,v) are integers in the interval [1,n-1]
2. Calculate SHA-1 (m) and convert the output to an integer f
3. Calculate w = v^{-1}mod n
4. Calculate i_1 =fw mod n and i_2 =sw mod n
5. Calculate X = i_1G + i_2Q
6. Calculate X = 0; then reject the signature. Otherwise, convert x coordinate $x1$ of X to an integer and then $\bar{x}_1$ calculate u= $\bar{x}_1$ mod n
7. Accept the signature only if u = s

SHA-256

Secure hash algorithm-256 (SHA-256) is a cryptographic hash function with a message digest size of 256 bits. It is a keyless hash function; it detects the changes in the message called the manipulation detection code (MDC). A message is handled by blocks of 512 = 16 × 32 bits, in which each block is needful of 64 rounds (38–40).

It uses the Boolean operations AND, XOR, OR, and Bitwise complement that are indicated by $\wedge$, $\oplus$ and $\vee$, $^-$. Integer addition modulo 2^{32}, indicated by A + B.

The *RotR(A, m)* indicates the circular right shift of m bits of the binary word A.

The *ShR(A, m)* indicates the right shift of m bits of the binary word A.

$A||B$ denotes the concatenation of the binary words A and B.

SYSTEM MODEL

Architecture

The proposed system emphasizes the elimination of all the above stated factors that are discussed in the existing systems (23, 41, 42). The architecture of the proposed system is shown in **Figure 1**.

The system architecture shows that the patient goes to the health care professional, such as doctors or pharmacists, and health insurers and diagnosis lab technicians show how the interactions occur. First, both the patient and health care professional swipe their respective smart cards in the card reader: the patient's smart card by the patient and the professional smart card by the health care professional to mutually authenticate each other. Subsequently, the patient performs the second-factor authentication by entering a PIN or password or biometric. After the authentication phase, the patient's basic medical pieces of information are read from the patient's smart card. Suppose further detailed medical information is necessary to proceed with the next level, such as to take treatment from the doctor, to purchase medicine from the pharmacist, or to claim the insurance from the health insurer. In that case, the cloud server is contacted *via* the smart card solution provider (19, 43–45). The cloud server responds to the health professional's request by fetching the patient information and sending it to the health care professional. Later, when the patient data are modified or additional information needs to be added, the data are sent to the healthcare professional's cloud server. The following are the various phases of our proposed protocol.

Adversary Model

In this paper, we regard the adversarial model as follows:

1. X to capture the message transmitted on the cloud environment (46, 47).
2. The security parameters present in the smart card can be extracted by X (36, 48).
3. The password dictionary can be computed by X off-line (33, 48).

Notations	Description
U_i	User i
X	Adversary
R	Nonce
pwd_i	Password for user i
e_i	E-mail for user i
P	Elliptic curve base point
$h(\cdot)$	SHA-256 hash function
M_R	User registration message
S	Nonce $\in Z_{P*}$
Y	Public key
A	Nonce
T	Current time stamp
ΔT	Maximum transmission delay

Preliminary Phase

When the smart card is purchased from the smart card issuer, the patient's basic personal information or health care professional's information is stored in an encrypted form using ECC. To do that, the following ECC security parameters are chosen.

In this phase, the cryptographic algorithm ECC is chosen by the health care professional as well as by the smart card solution provider (SP) for encrypting the patient data in the patient's smart card and the detailed information of the patient's medical information stored in the cloud server.

Algorithm for Preliminary Phase

Input: ECC parameters
Output: Public key Y and private key s
1: Let p be a large prime number, and E denote the elliptic curve over the prime finite field Z_P.
2: Smart card SP chooses an ECC, $E: y^2 = x^3 + c.x + d$ (*mod p*) and generates grouping E_p (c, d) *having order n*, where *n* is a large prime number.
3: Then the smart card SP chooses base point,
$P = (x_0, y_0)$, where $n.P = O$ Later,
4: SP picks a nonce $s \in Z_{P*}$ as its private key and calculates the public key $Y = s.P$. All these computations are completed off-line.

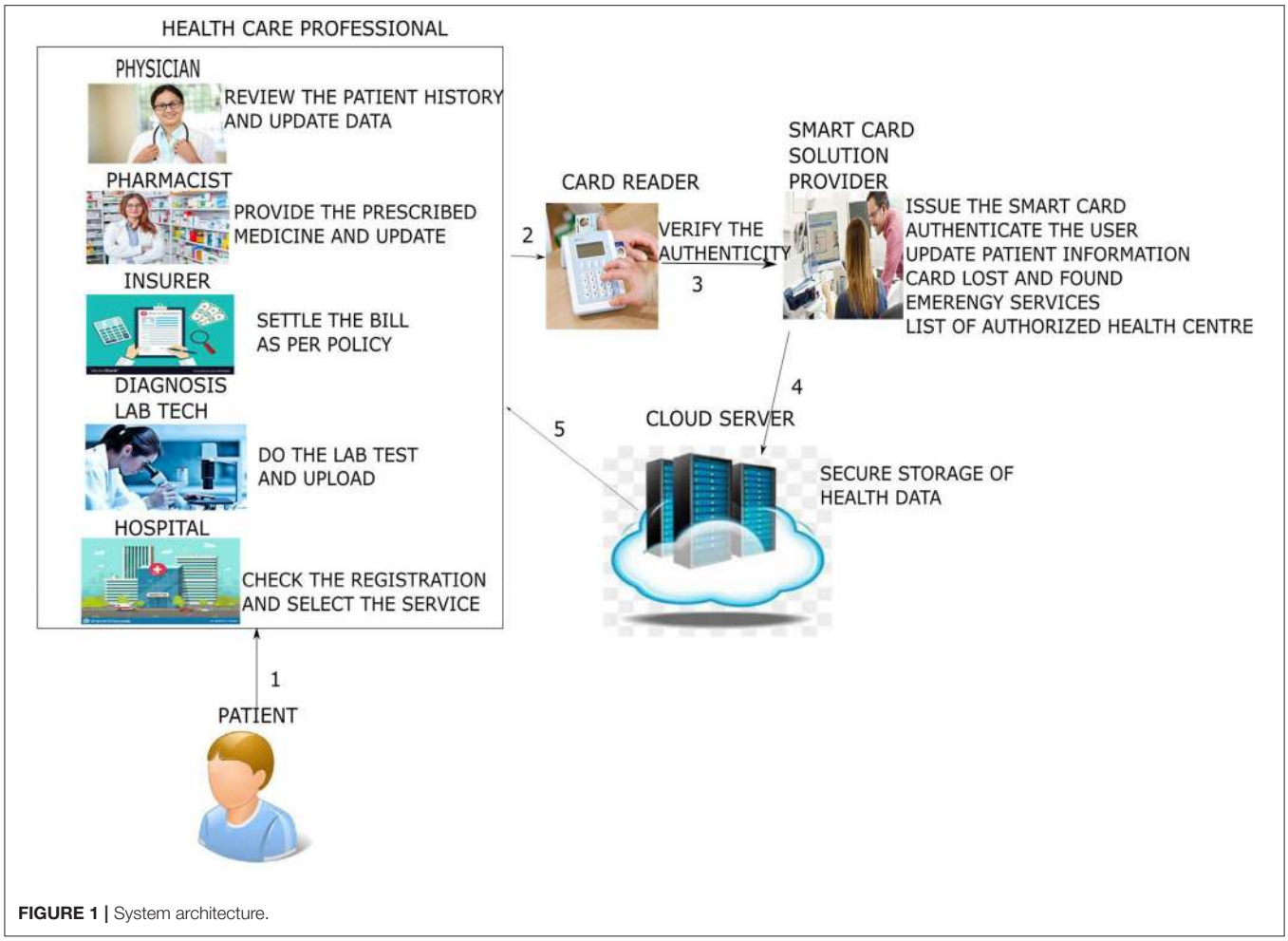

FIGURE 1 | System architecture.

Registration Phase

A new user U_i such as a patient or health care professional purchases the smart card from the SP *and registers* it as follows:

Algorithm for registration:

Input: Password pwd_i, nonce r, and ID.
Output: Encrypted personal information
1: U_i selects password pwd_i and a nonce r, and then U_i transfers the *ID* and computes

a. $A = h(pwd_i \| r)$

and sends it to the smart card *SP* along with an e-mail e_i. Adding the nonce in the pwd_i ensures it does not reveal the sensitive information even to the smart card SP.
2: The smart card SP, after getting *ID*, e_i, and A from the user U_i, it computes

a. $M = h(s \oplus ID)$
b. $B = M \oplus A$

3: *SP* also finds the category U_i belongs to, such as patient or health care professional, and sends $\{E_p, P, Y, B, Category\}$ to U_i, which it stores locally along with r in its smart cards.
4: The personal information that is entered by the SP is encrypted by the smart card using the public key Y and stored in it.

a. Smart card <- E_Y(personal_info)

Login Phase

The login phase is common to patient and health care professional cards issued by the smart card SP.

The user U_i (patient or health care professional) logs in with the system to access the information stored in the smart card as follows:

Algorithm for login:

Input: ID and pwd_i
Output: Login Access Request
1: U_i provides ID and pwd_i, and then the smart card computes,

a. $A = h(pwd_i \| r)$
b. $M = B \oplus A$
c. $C1 = a.P$
d. $C2 = a.Y$
e. $TID = ID \oplus h(C2)$
f. $f = h(ID \| M \| T)$

Here, a is a secret nonce picked by U_i, and T is the current time stamp.
2: U_i then transmits the login access request message

a. $msg_1 = \{C1, TID, f, T\}$ to SP.

Authentication Phase

The authentication steps are as follows: Algorithm for authentication

Input: Message msg_1
Output: Unencrypted form of medical data
1: Upon receiving msg_1 from U_i, SP checks whether

a. $T' - T \leq \Delta T$

where ΔT is the maximum transmission delay. If the validity fails, SP rejects the session. Else, SP uses its private key s to compute

b. $C2' = s.C1$
c. $ID' = TID \oplus h1\ (C2')$
d. $M' = h(s \oplus ID')$,
e. $f' = h(ID' \| M' \| T)$

SP then checks whether $f' \stackrel{?}{=} f$. If true, then U_i, either the patient or health care professional, is a legitimate user. Else, abort.
2: SP then computes

a. $D1 = c.P, D2 = c.C1$

The session key

b. $SK = h(ID \| h1\ (D2) \| M')$ and
c. $G = h(SK \| M' \| T_2)$

where, c is a nonce selected by SP, and T_2 is the current time stamp. Then, SP transfers

d. $msg_2 = \{D1, G, T_2\}$ to U_i.

3: Upon receiving msg_2, U_i checks whether T_2

a. $T' - T_2 \leq \Delta T$ is valid or not. If it is valid, U_i calculates
b. $D2' = a.D1$
c. $SK = h(ID \| h1\ (D2') \| M)$ for future correspondence.

4: After the mutual authentication, the current information of the patient from the smart card and the cloud server are fetched for proceeding with further treatment. In both cases, the patient's medical data are stored in the encrypted form. The data are fetched in the same form and then decrypted at the smart card to view in the unencrypted form by the health care professional.

Password Update Phase

U_i performs the following steps to update a password:
Algorithm for password update:

Input: ID and pwd_i
Output: Updated password
1: U_i inputs ID and pwd_i and then calculates

a. $A = h(pwd_i \| r)$
b. $M = B \oplus A$

2: Then, U_i is prompted to input the new password pwd_{new} and computes

a. $A_{new} = h(pwd_{new} \| r)$
b. $B_{new} = A_{new} \oplus M$

and replaces B with B_{new}; thus, the password is updated successfully.

According to the category, the health care professional belongs to the type of data retrieved, and data that is being synchronized with the cloud server differs. The below phases denote per the type of health care professional what type of data can be accessed or modified in the patient data.

Data Synchronization Phase

This phase starts when patient data is altered by the health care professional and should be synchronized with the cloud server to maintain consistency between the data stored in the cloud and the smart card and to store additional information that could not be stored in the cloud due to memory constraints. The following are the cases when the patient data should be synchronized with a cloud server.

(i) The doctor uploads an e-health prescription into the cloud after consulting with the patient and identify the health problem.
(ii) When the doctor requires further diagnosis, the doctor refers the patient to the diagnosis center.
(iii) From the diagnosis center, the test results are uploaded into the cloud database to help the doctor view the test results.
(iv) The insurance provider can update the cloud database when the particular treatment bill is claimed.

(v) Similarly, additional health care professional information also can be stored in a cloud server.

After performing a successful login, the health care professional gets an option to store the information as follows:

Algorithm: Data Synchronization

Input: Msg_1, different type of patient information
Output: Signature sig and encrypted file
1: The HCP defines the permissions for the patient document from the smart card used by the patient, for example, the pharmacist can view only the prescription information alone and that information is divided into chunks of byte arrays (B_1... B_n).
2: *HCP* then computes a. $MSG_1 = \{ Category, scope\} \oplus SK$
b. $B_1 = B_1 \oplus SK$
$B_n = B_n \oplus SK$
c. $MSG_2 = h\,(ID \parallel Y) \oplus SK$
3: *HCP* reconstitutes the file from byte arrays (B_1... B_n).
4: The *Category* is added to the file to denote whether the information pertains to the patient, doctor, insurer, or diagnostician. This help the cloud server while searching the different data according to their category.

a. If the category belongs to the patient, then it is further identified as to whether it is a prescription, test results, or insurance-related information.

5: HCP then computes an ECCDSA hash of the file to act as checksum and encrypts the file with its public key *Y* and sends the {Sig, F1,MSG2} to the cloud server S (48).

a. FD<-h(F),
b. Sig=S_y [FD]
c. $F1=E_y[F]$

Data Retrieval Phase

This phase starts when patient data needs to be retrieved by the health care professional to study the patient's medical history and diagnose the disease to proceed with further treatment. The following are the cases when the patient data should be retrieved from the cloud server.

(i) The doctor wants to view the patient's previous history to know more in depth about the health problem.
(ii) The pharmacist can sell the medicine according to the prescription uploaded in the cloud server.
(iii) The insurance provider can check the hospital bill to process the claim for the medical expenditure.

Algorithm: Data retrieval

Input: Signature Sig, Encrypted file
Output: Unencrypted file
1: Data retrieval starts after the smart card authentication is over with the card issuer and request made for accessing additional information by the health professional.

2: After receiving the request, the cloud server S searches the data over the encrypted form from its database using the MCKS-MAT scheme (49). We have constructed the multiattribute tree (MAT) for the partient or health care professional record set by choosing the category as the root of the tree. File search is considered to be a separate phase.
3: The cloud server retrieves the data and then transfers it to the smart card SP. The decryption performed at the smart card solution provider by using s also computes and checks its ECCDSA hash to detect any tampering. If the check fails stop, divide the patient documents into chunks of byte arrays (B_1... B_n) and send it to the patient smart card

a. V=Ver_s(Sig)
b. F=D_s(F1)
c. ($B_1 \oplus SK$)…($B_n \oplus SK_{))}$ =Split(F)

$B_1 \oplus SK$
$B_n \oplus SK$

4: The smartcard then decrypts the stream of messages and reconstitutes the file from byte arrays (B_1... B_n).

File Search

To search the patient records in the cloud server, we adopt the MCKS-MAT scheme (49) by which we have constructed the MAT for the patient record set. The number of levels in the MAT index tree L is equal to the number of attributes in the patient file. The MAT index tree is encrypted using the ECC encryption algorithm. Along with the patient files, the encrypted MAT tree is stored in the cloud server, which protects the cloud server against a cipher text attack, known plaintext attack and known background attack. The construction and explanation of the MCKS-MAT scheme is beyond the scope of our work.

INFORMAL ANALYSIS

We have assessed that the proposed method has the ability to protect the user from different cryptographic attacks.

User Anonymity

Our scheme provides user anonymity, such as patient and health care professional (doctor, lab technician, and insurer) anonymity, for example, during the entirety of the phases, the user's ID is always masked and unattainable even from any trapped messages. Hence, the smart card SP, after getting ID, e_i, and A from the user U_i, it computes $M = h(s \oplus ID)$ and B= $M \oplus A$ and discloses it to the user. Furthermore, the ID is not revealed to anyone. Hence, our scheme confers the property of user anonymity.

Forward Secrecy

Our scheme confers the forward secrecy property as each session key is fresh due to the randomness of *c*. *SP* computes $D1 = c.P$, $D2 = c.C1$. From that, it computes the session key $SK = h(ID \parallel h1\,(D2) \parallel M')$. Thus, each session key is completely autonomous of other sessions. Thus, even in the

TABLE 1 | Security feature comparison of various protocols.

Security attack	Li et al. (29)	Kumar et al. (12)	Kumar et al. (23)	Proposed
Man-in-the-middle attack	√	√	√	√
Replay attack	√	√	√	√
Patient anonymity	×	√	√	√
Patient unlinkability	×	√	√	√
Doctor unlinkability	×	×	√	√
Data non-repudiation	√	√	√	√
Data confidentiality	√	√	√	√
Message authentication	×	√	√	√
Impersonation attack	×	√	√	√
Stolen smart card attack	×	×	×	√
Session key security	×	√	√	√
Off-line password guessing attack	×	√	√	√
Forward secrecy	×	×	×	√

√ - *Security attack protected by the protocols.*
× - *Security attack not protected by the protocols.*

TABLE 2 | Execution time of various cryptographic operations.

Notations	Descriptions	Execution time (s)
T_{kgen}	Key generation time	0.219
T_{enc}	ECC encryption time	0.3057
T_{dec}	ECC decryption time	0.015
T_{kgen1}	ECCDSA key generation time	0.466
T_{siggen}	Time for generating the signature	0.0009
$T_{sigverify}$	Time for verifying the signature	0.0053
T_M	Time for performing multiplication.	0.0053 s
T_H	Time for calculating one-way hash function	0.0005 s
T_S	Time for calculating symmetric encryption/decryption time	0.0087 s

unlikely case that a session key is compromised, it does not affect other sessions.

Replay Attack

Our scheme protects against replay attacks by providing sufficient checks of validity for each transmitted message. Thus, our scheme is able to withstand a replay attack as it includes the time stamp in the transmitted message. Kumar et al. (12) does not sustain doctor unlinkability. Kumar et al. (12, 23) does not support forward secrecy, stolen smart attacks. Our scheme protects against several known security attacks (50).

Man-in-the-Middle Attack

Our scheme prevents the man-in-the-middle attack as each datum that we are transferring between the entities is associated with the time stamp and hash conditions. In case any adversary A verifies the time stamp, it further has to verify $f' = f$, which is impossible due to the characterization of the one-way hash function.

Data Confidentiality

In case any adversary tries to read the patient's or health care professional's information, it needs to decrypt the information, which is not possible without knowing the key and hash value. The freshness of s and one-way hash function ECCDSA ensures data confidentiality.

Data Non-repudiation

The proposed protocol supports data non-repudiation in various phases. During the data synchronization phase, the signature is calculated as FD<-h(F), Sig=S_y [FD] and sends it to the cloud server along with the encrypted file { Sig, F1}. At the data retrieval phase, it verifies the signature as V=Ver_s(Sig) by the smart card SP. This ensures that the authenticity cannot be denied by the health care professional.

Patient and Doctor Unlinkability

Patient/doctor unlinkability means that adversary *E* should not reveal the medical association between the patient and the doctor *via* the communication channel. Because of the proposed protocol, both the patient's and doctor's information are stored in the encrypted form as $F1=E_y[F]$ and does not reveal the

TABLE 3 | Computation cost of SCB-HC protocol with relevant protocols.

Phases	Li et al. (29)	Kumar et al. (12)	Kumar et al. (23)	Proposed
Preliminary	NA	NA	NA	$1T_{kgen}$ 0.219
Registration	$3T_H$ 0.0015 s	$3T_H$ 0.0015 s	$3T_H$ 0.0015 s	$2T_H + 1T_{Enc}$ 0.3067 s
HUP (health center data upload phase) (Login+ Authentication+ Data synchronization)	$11T_H + 1T_{sign} + 3T_s$ 0.3543 s	$10T_H + 1T_{sign} + 3T_s$ 0.3538 s	$10T_H + 1T_{sign} + 5T_s$ 0.3628 s	$12T_H + 1T_{sig_{gen}} + 5T_M + 1T_{Enc}$ 0.339 s
TUP (treatment upload phase) (Login+ Authentication+ Data synchronization)	$3T_{sign} + 6T_{s+}10T_H$ 0.7128 s	$2T_{sign} + 6T_{s+}10T_H$ 0.7026 s	$3T_{sign} + 6T_{s+}11T_H$ 1.0528 s	$12T_H + 1T_{sig_{gen}} + 5T_M + 1T_{Enc}$ 0.339 s
MRP (medi reclaim phase) (Login+ Authentication+ Data Retrieval)	NA	NA	NA	$12T_H + 1T_{sig_{ver}} + 5T_M + 1T_{Dec}$ 0.0528 s
LUP (lab technician phase) (Login+ Authentication+ Data Retrieval+ Data Synchronization)	NA	NA	NA	$12T_H + 1T_{sig_{gen}} + 1T_{sig_{ver}} + 5T_M + 1T_{Dec} + 1T_{Enc}$ 0.3594 s
Password update	NA	NA	NA	$2T_H = 0.001$ s
Total time	1.0686 s	1.0579 s	1.4171 s	1.6169 s

TABLE 4 | Communication cost of various components in bits.

Component	Cost in bits
Time stamp	48
Generated random number	48
Symmetric encryption/decryption operation	128
Asymmetric encryption/decryption operation	163
Modular multiplication and inverse operation	128
Cryptographic hash function	160
Executing/verifying a signature	256

information even to the cloud server, so the unlinkability is preserved between the doctor and patient.

PERFORMANCE ANALYSIS

We performed various cryptographic operations on a machine with a dual core processor of 2:4 GHz and equipped with 2 GB RAM running with the windows 10 operating system. Because of the other processes executing on the system, the execution time recollected in this article is the average time after a certain number of executions of the different cryptosystems based on article (51). The encryption and decryption of the ECC algorithm uses the key with the length of 163 bits. The security, communication, and execution cost of the proposed protocol with other relevant protocols are discussed in this article. In the following section, the security feature and communication and execution costs of the proposed protocol are compared with the Kumar et al. (12, 23) scheme. The evaluation made in this section delivers an effectiveness of the proposed protocol compared with the other relevant protocol.

The Li et al. (29) scheme does not support patient anonymity, patient unlinkability, doctor unlinkability message authentication, or session key security. It does not protect from the impersonation attack, stolen smart card attack, or off-line password guessing attack. Kumar et al. (12) does not support doctor unlinkability and forward secrecy. Kumar et al. (23) does not support forward secrecy. However, all the schemes do not support the stolen smart card attack as it is focusing on telecare medicine information system. In summary, our scheme provides support for several security features and protects against several known attacks.

Computation Cost

In this section, we project performance of our proposed framework with the related schemes that operated in the cloud computing environment to enable secure medical data communication, such as the Kumar et al. and Li et al. techniques. **Table 1** shows security feature comparison of various protocols. We have embraced different cryptographic operations in this article established on the details appropriate in Kumar et al. and Li et al. to assess the computation cost of the proposed protocol. **Table 2** presents the execution time of various cryptographic operations, such as key generation, signature generation, ECC encryption/decryption, and symmetric cryptographic operations. **Table 3** shows the computation cost of the SCB-HC protocol with other relevant protocols. The computation cost of the

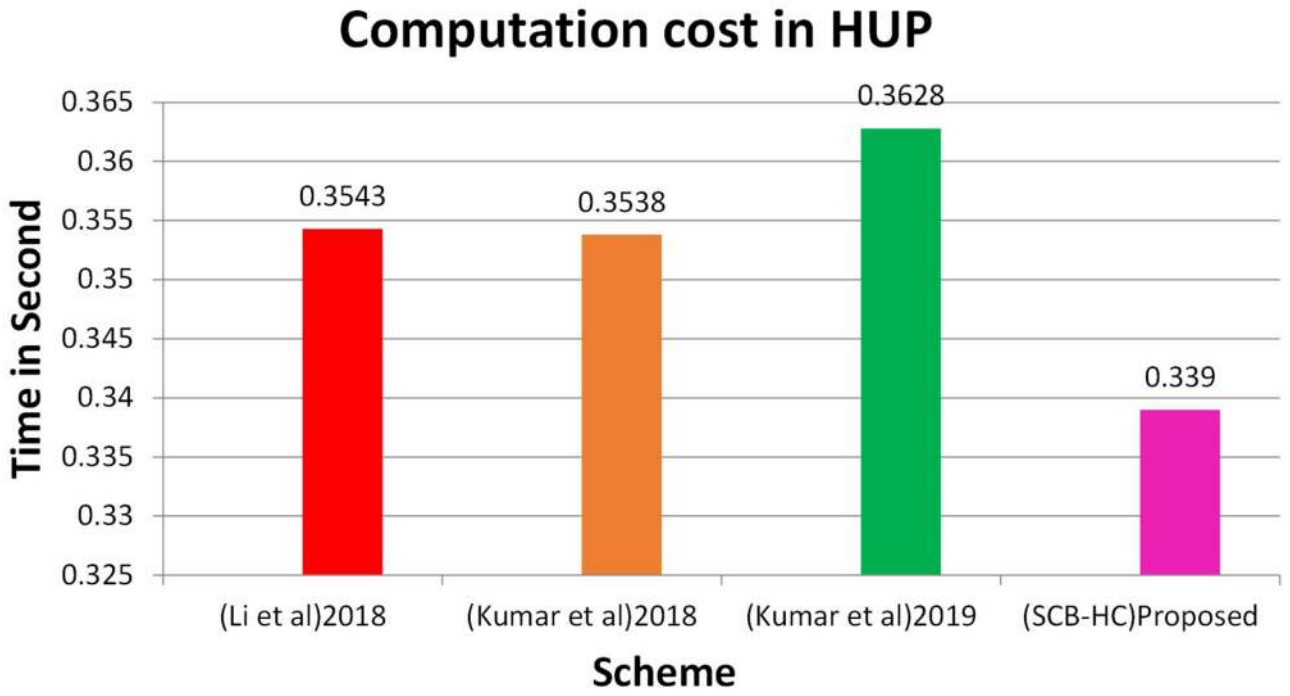

FIGURE 2 | HUP computation cost.

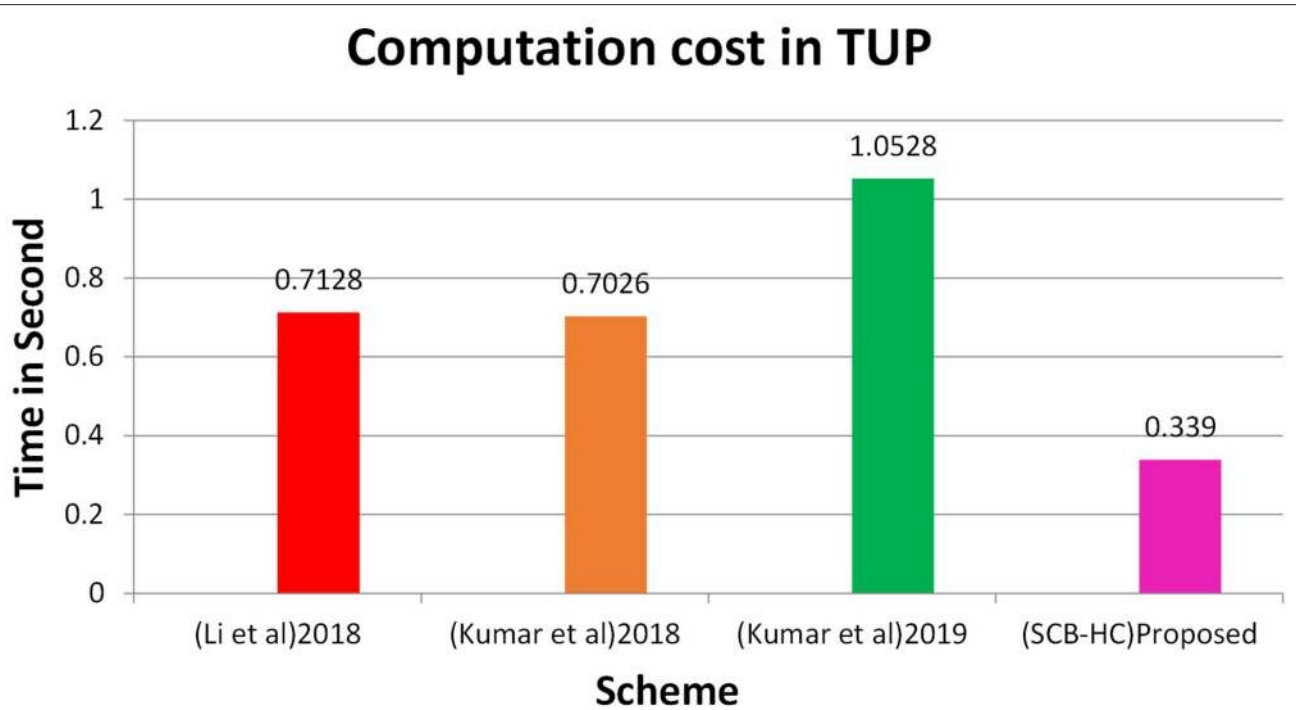

FIGURE 3 | TUP computation cost.

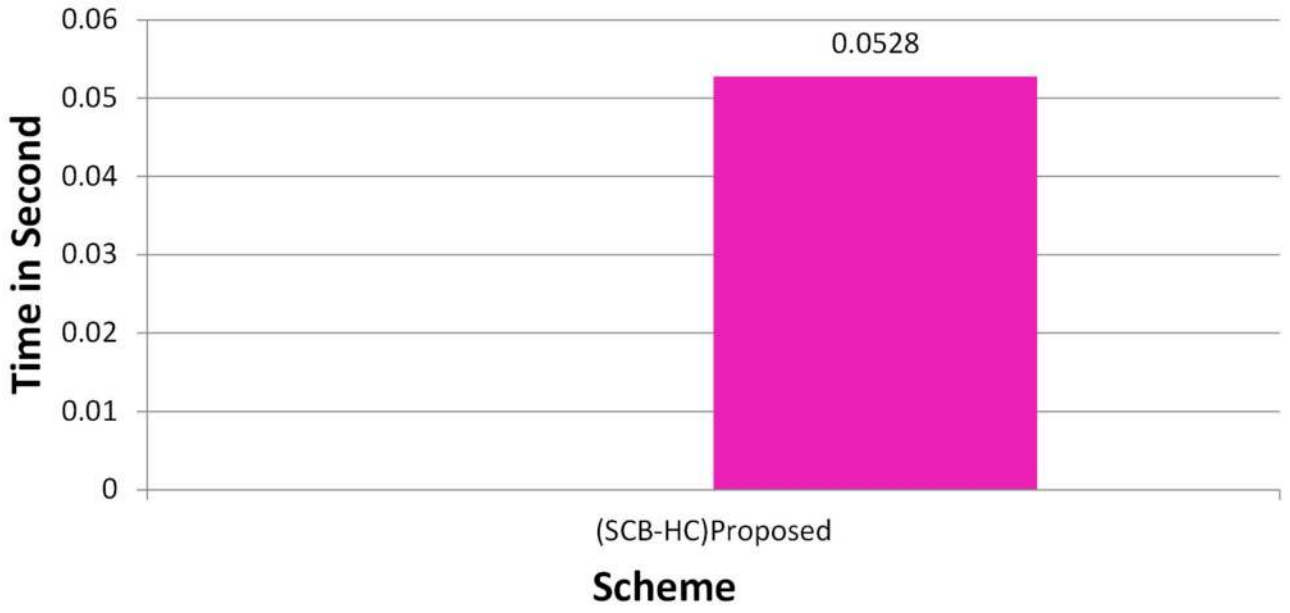

FIGURE 4 | MRP computation cost.

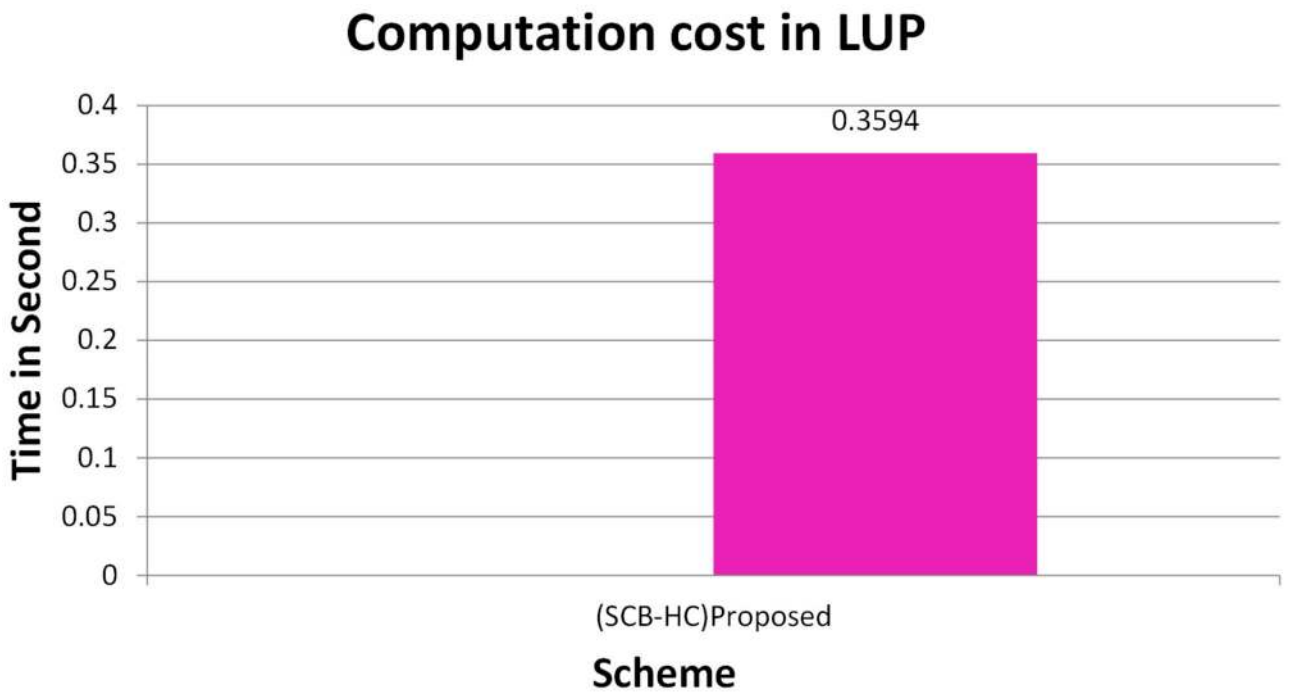

FIGURE 5 | LUP computation cost.

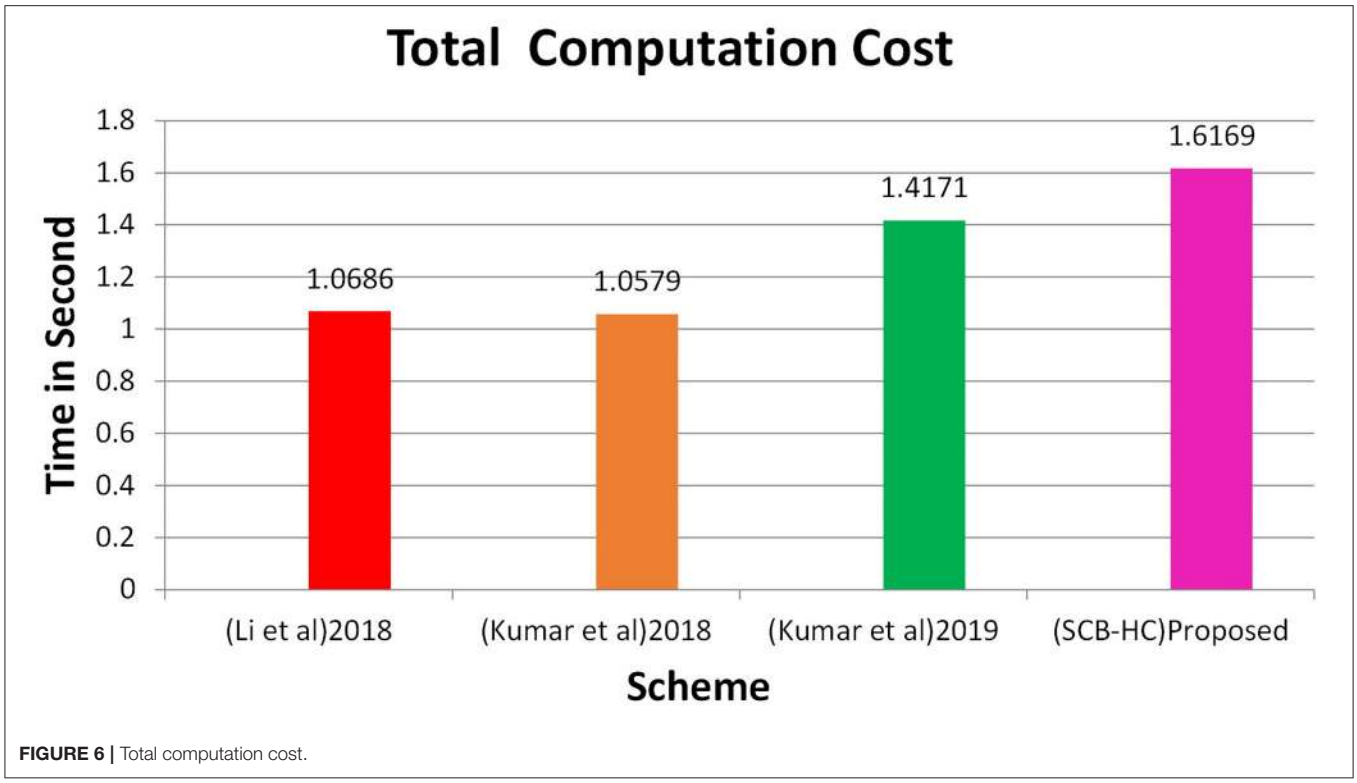

FIGURE 6 | Total computation cost.

TABLE 5 | Communication cost comparison for SCB-HC with other related schemes.

Protocol	Li et al. (29)	Kumar et al. (12)	Kumar et al. (23)	Proposed (SCB-HC)
Preliminary	NA	NA	NA	211
Registration	208	208	208	371
HUP	592	624	496	755
TUP	720	544	544	755
MRP	NA	NA	NA	755
LUP	NA	NA	NA	755
PUP	1,232	544	496	NA
CP	1,232	596	592	NA
EP	NA	704	NA	NA
Total cost in bits	3,984	3,220	2,336	3,602

HUP, Health center data upload phase; TUP, Treatment Upload phase; MRP, Medi reclaim phase; LUP, Lab Technician phase; PUP, Patient data upload phase; CP, Checkup Phase; EP, Emergency Phase.

proposed protocol is 1.6169, which is slightly higher than the existing protocols. However, our scheme adopts the ECC cryptographic operations, **Table 4** shows the communication cost of various components in bits which are not used in any of the existing schemes. Because it uses ECC operations, our scheme is more against the existing scheme. The efficiency of the proposed protocol in each phase is shown with other relevant protocols (52).

Figure 2 shows the computation cost in HUP in which our proposed scheme SCB-HC takes 0.339 seconds, which is less than the Li et al. (29) and Kumar et al. (12, 23) schemes even though our scheme SCB-HC is more secure compared with existing schemes. **Figure 3** shows the computation cost of TUP. It also takes 0.339 seconds, which is less than the existing schemes. **Figures 4**, **5** shows the computation cost of MRP and LUP, which take 0.0528 and 0.3594, respectively. Only SCB-HC has this phase as it deals with the medi reclaim and lab technician upload phases, and this is the added advantage in the SCB-HC scheme that is not available in any of the existing phases. **Figure 6** shows the total communication cost of all the scheme. The total cost of the SCB-HC scheme is 1.6169 s as it includes additional phases MRP and LUP, which are not present in any of the existing schemes. Also, SCB-HC uses ECC encryption and decryption and the ECCDSA signature algorithm, which is more secure and efficient compared with the existing schemes.

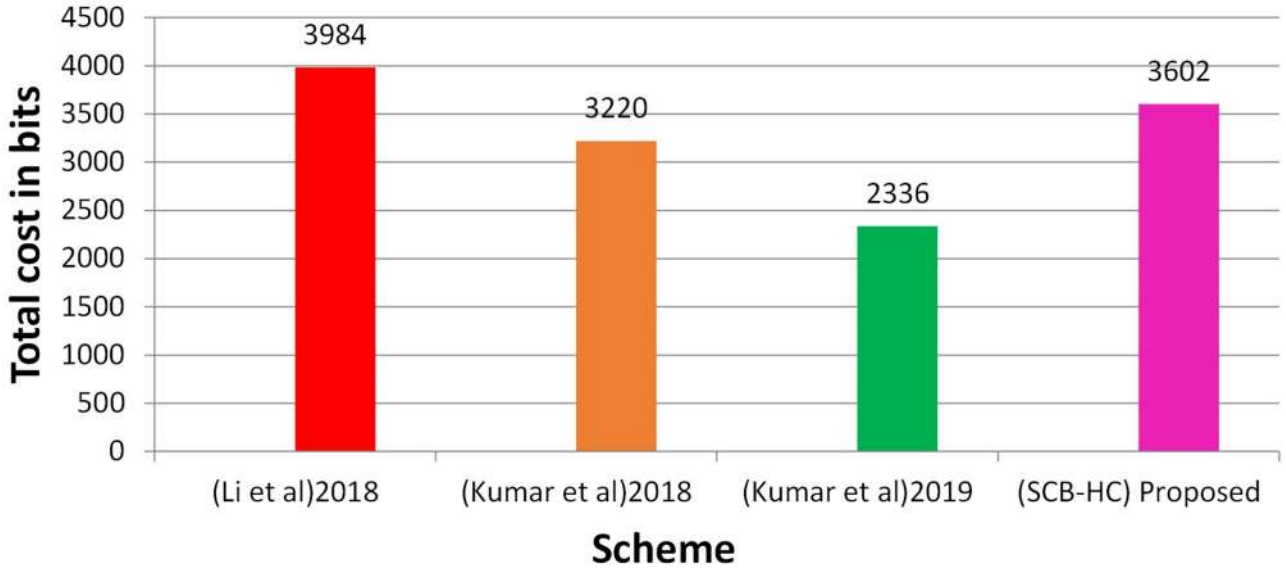

FIGURE 7 | Communication cost for various schemes.

Communication Cost Comparison

We analyze the communication cost of the SCB-HC protocol with other relevant protocols.

Table 5 shows the communication cost comparison of the various schemes in which SCB-HC has the communication cost of 3,602 bits and other relevant schemes are 3,984, 3,220, and 2,336 bits, respectively. **Figure 7** shows the communication cost comparison for SCB-HC with various schemes. The SCB-HC has slightly higher cost compared with the Kumar et al. (12, 23) schemes as our scheme has various additional phases and the ECC cryptographic technique, which is not supported by other schemes.

CONCLUSION

We elaborated our suggested methodology for a remote authentication scheme with the smart card–based health care information using the ECC algorithm in the present article. We performed an informal analysis to substantiate the claim that our scheme provides sufficient security while maintaining usability. Maintaining user anonymity also maintains that others cannot access data without prior approval of the file owner. It also supports file integrity with the help of ECCDSA. Furthermore, we show that our proposed protocol is effective in terms of the communication and computation cost in secure cloud storage of smart card–based health care information.

The current work only involves integrating remote authentication with the smart card. In the future, we will focus on designing a smart card with a higher capacity to store large information, such as X-ray films and SCAN images.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author/s.

AUTHOR CONTRIBUTIONS

SS and KB: conception or design of the work and data collection. SS, KB, and SB: data analysis, interpretation, and drafting the article. NK and GR: critical revision of the article and funding and final approval of the version to be published. All authors contributed to the article and approved the submitted version.

FUNDING

This research was supported by the Faculty of Management of Comenius University in Bratislava, Slovakia.

REFERENCES

1. Moudgil K, Maheshwari R, Parekh HB, Devadkar K. Cloud-based secure smartcard healthcare monitoring and tracking system. In: *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. Coimbatore: IEEE (2017). p. 1–8. doi: 10.1109/ICECCT.2017.8117869
2. Rathnayaka A, Al Mamun MA, Wu F, Curtis SJ, Stewardson AJ, Yuce MR. Protecting health care workers from infectious diseases using physical proximity networks (PPN). In: *2020 IEEE Sensors*. IEEE (2020). p. 1–4. doi: 10.1109/SENSORS47125.2020.9278701
3. Deng F, Wang Y, Peng L, Xiong H, Geng J, Qin Z. Ciphertext-policy attribute-based signcryption with verifiable outsourced designcryption for sharing personal health records. *IEEE Access.* (2018) 6:39473–86. doi: 10.1109/ACCESS.2018.2843778
4. Saho NJG, Ezin EC. Comparative study on the performance of elliptic curve cryptography algorithms with cryptography through RSA algorithm. In: *CARI 2020-Colloque Africain sur la Recherche en Informatique et en Mathématiques Apliquées*. Thies senegal (2020).
5. Rashid M, Singh H, Goyal V. Cloud storage privacy in health care systems based on IP and geo-location validation using K-mean clustering technique. *Int J E-Health Med Commun.* (2019) 10:54–65. doi: 10.4018/IJEHMC.2019100105
6. Ganiga R, Pai RM, Pai MMM, Sinha RK. Private cloud solution for securing and managing patient data in rural healthcare system. *Proc Comput Sci.* (2018) 135:688–99. doi: 10.1016/j.procs.2018.08.217
7. Singh I, Kumar D, Khatri SK. Improving the efficiency of E-Healthcare system based on cloud. In: *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE (2019). p. 930–3. doi: 10.1109/AICAI.2019.8701387
8. Shabaan M, Arshad K, Yaqub M, Jinchao F, Zia MS, Boja GR, et al. Survey: smartphone-based assessment of cardiovascular diseases using ECG and PPG analysis. *BMC Med Inform Decis Mak.* (2020) 20:1–16. doi: 10.1186/s12911-020-01199-7
9. Bojja GR, Liu J. Impact of it investment on hospital performance: a longitudinal data analysis. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*. Maui (2020). doi: 10.24251/HICSS.2020.438
10. Rehman ZU, Zia MS, Bojja GR, Yaqub M, Jinchao F, Arshid K. Texture based localization of a brain tumor from MR-images by using a machine learning approach. *Med Hypotheses.* (2020) 141:109705. doi: 10.1016/j.mehy.2020.109705
11. Idoga PE, Toycan M, Nadiri H, Çelebi E. Factors affecting the successful adoption of e-health cloud based health system from healthcare consumers' perspective. *IEEE Access.* (2018) 6:71216–28. doi: 10.1109/ACCESS.2018.2881489
12. Kumar V, Jangirala S, Ahmad M. An efficient mutual authentication framework for healthcare system in cloud computing. *J Med Syst.* (2018) 42:142. doi: 10.1007/s10916-018-0987-5
13. Benil T, Jasper J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput Netw.* (2020) 178:107344. doi: 10.1016/j.comnet.2020.107344
14. Maganti PK, Chouragade PM. Secure application for sharing health records using identity and attribute based cryptosystems in cloud environment. In: *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. Tirunelveli: IEEE (2019). p. 220–3. doi: 10.1109/ICOEI.2019.8862540
15. Zhang L, Zhang Y, Ma H. Privacy-preserving and dynamic multi-attribute conjunctive keyword search over encrypted cloud data. *IEEE Access.* (2018) 6:34214–25. doi: 10.1109/ACCESS.2018.2823718
16. Sasubilli SM, Kumar A, Dutt V. Improving health care by help of internet of things and bigdata analytics and cloud computing. In: *2020 International Conference on Advances in Computing and Communication Engineering (ICACCE)*. IEEE (2020). p. 1–4. doi: 10.1109/ICACCE49060.2020.9155042
17. Wang X, Bai L, Yang Q, Wang L, Jiang F. A dual privacy-preservation scheme for cloud-based eHealth systems. *J Inform Secur Appl.* (2019) 47:132–8. doi: 10.1016/j.jisa.2019.04.010
18. Zhang Y, Zheng D, Deng RH. Security and privacy in smart health: efficient policy-hiding attribute-based access control. *IEEE Internet Things J.* (2018) 5:2130–45. doi: 10.1109/JIOT.2018.2825289
19. Krishnan SSR, Manoj MK, Gadekallu TR, Kumar N, Maddikunta PKR, Bhattacharya S, et al. A blockchain-based credibility scoring framework for electronic medical records. In: *2020 IEEE Globecom Workshops (GC Wkshps)*. Taipei: IEEE (2020). p. 1–6.
20. Sánchez-Gallegos DD, Galaviz-Mosqueda A, Gonzalez-Compean JL, Villarreal-Reyes S, Perez-Ramos AE, Carrizales-Espinoza D, et al. On the continuous processing of health data in edge-fog-cloud computing by using micro/nanoservice composition. *IEEE Access.* (2020) 8:120255–81. doi: 10.1109/ACCESS.2020.3006037
21. Yao X, Lin Y, Liu Q, Zhang J. Privacy-preserving search over encrypted personal health record in multi-source cloud. *IEEE Access.* (2018) 6:3809–23. doi: 10.1109/ACCESS.2018.2793304
22. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE Access.* (2019) 7:66792–806. doi: 10.1109/ACCESS.2019.2917555
23. Kumari A, Jangirala S, Abbasi MY, Kumar V, Alam M, ESEAP. ECC based secure and efficient mutual authentication protocol using smart card. *J Inform Secur Appl.* (2020) 51:102443. doi: 10.1016/j.jisa.2019.102443
24. Zhang X, Tang Y, Cao S, Huang C, Zheng S. Enabling identity-based authorized encrypted diagnostic data sharing for cloud-assisted E-health information systems. *J Inform Secur Appl.* (2020) 54:102568. doi: 10.1016/j.jisa.2020.102568
25. Azeez NA, Van der Vyver C. Security and privacy issues in e-health cloud-based system: a comprehensive content analysis. *Egypt Informa J.* (2019) 20:97–108. doi: 10.1016/j.eij.2018.12.001
26. Gautam P, Ansari MD, Sharma SK. Enhanced security for electronic health care information using obfuscation and RSA algorithm in cloud computing. *Int J Inform Secur Priv*. (2019) 13:59–69. doi: 10.4018/IJISP.2019010105
27. Jayaraman I, Panneerselvam AS. A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. *J Ambient Intell Human Comput*. (2020) 2020:1–14. doi: 10.1007/s12652-020-01931-1
28. Yang Y, Li X, Qamar N, Liu P, Ke W, Shen B, et al. Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers. *IEEE Access.* (2018) 6:46949–61. doi: 10.1109/ACCESS.2018.2865535
29. Li C-T, Shih D-H, Wang C-C. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. *Comput Methods Programs Biomed.* (2018) 157:191–203. doi: 10.1016/j.cmpb.2018.02.002
30. Kausar F. Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egypt Informat J.* (2021). 1:4. doi: 10.1016/j.eij.2021.01.004
31. Xu C, Wang N, Zhu L, Sharif K, Zhang C. Achieving searchable and privacy-preserving data sharing for cloud-assisted E-healthcare system. *IEEE Internet Things J.* (2019) 6:8345–56. doi: 10.1109/JIOT.2019.2917186
32. Jin LP, Dong J. Intelligent health vessel ABC-DE: an electrocardiogram cloud computing service. *IEEE Trans Cloud Comput.* (2018) 8:861–74. doi: 10.1109/TCC.2018.2825390
33. Al-Saggaf AA, Sheltami TR. Renewable and anonymous biometrics-based remote user authentication scheme using smart cards for telecare medicine information system. In: *2019 Advances in Science and Engineering Technology International Conferences (ASET)*. IEEE (2019). p. 1–6. doi: 10.1109/ICASET.2019.8714479
34. Ganesh D, Seshadri G, Sokkanarayanan S, Bose P, Rajan S, Sathiyanarayanan M. AutoImpilo: smart automated health machine using IoT to improve telemedicine and telehealth. In: *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*. Bengaluru (2020). p. 487–93. doi: 10.1109/ICSTCEE49637.2020.9277223
35. Sanjuan EB, Cardiel IA, Cerrada JA, Cerrada C. Message queuing telemetry transport (MQTT) security: a cryptographic smart card approach. *IEEE Access.* (2020) 8:115051–62. doi: 10.1109/ACCESS.2020.3003998
36. Afrizal SH, Handayani PW, Eryando T, Sartono A. Primary care functional requirements of a health information system in Indonesia. In: *2018 Third International Conference on Informatics and Computing (ICIC)*. Tirunelveli: IEEE (2018). p. 1–7. doi: 10.1109/IAC.2018.8780501

37. Monteiro K, Rocha E, Silva E, Santos GL, Santos W, Endo PT. Developing an e-health system based on IoT, fog and cloud computing. In: *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)*. IEEE (2018). p. 17–8. doi: 10.1109/UCC-Companion.2018.00024
38. Abiodun AS, Anisi MH, Khan MK. Cloud-based wireless body area networks: managing data for better health care. *IEEE Consumer Electr Magazine.* (2019) 8:55–9. doi: 10.1109/MCE.2019.2892244
39. Kamoona MA, Altamimi AM. Cloud E-health systems: a survay on security challenges and solutions. In: *2018 8th International Conference on Computer Science and Information Technology (CSIT)*. Amman: IEEE (2018). p. 189–94. doi: 10.1109/CSIT.2018.8486167
40. Numan M, Subhan F, Khan WZ, Hakak S, Haider S, Reddy GT, et al. A systematic review on clone node detection in static wireless sensor networks. *IEEE Access.* (2020) 8:65450–61. doi: 10.1109/ACCESS.2020.2983091
41. Senthilkumar S, Viswanatham VM, HB-PPAC. Hierarchy-based privacy preserving access control technique in public cloud. *Int J High Perform Comput Netw.* (2017) 10:13–22. doi: 10.1504/IJHPCN.2017.083196
42. Gadekallu TR, Kumar N, Hakak S, Bhattacharya S. Blockchain based Attack detection on machine learning algorithms for IoT based E-health applications. *arXiv preprint arXiv:2011.01457*. (2020).
43. Sureshkumar V, Anitha R, Rajamanickam N, Amin R. A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity. *Comput Electr Eng.* (2017) 57:223–40. doi: 10.1016/j.compeleceng.2016.07.014
44. Deebak BD, Al-Turjman F, Aloqaily M, Alfandi O. An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. *IEEE Access.* (2019) 7:135632–49. doi: 10.1109/ACCESS.2019.2941575
45. Sarwar MA, Bashir T, Shahzad O, Abbas A. Cloud-based architecture to implement electronic health record (EHR) system in Pakistan. *IT Prof.* (2019) 21:49–54. doi: 10.1109/MITP.2018.2882437
46. Islam SH, Amin R, Biswas GP, Farash MS Li X, Kumari S. An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments. *J King Saud Univ Comput Inform Sci.* (2017) 29:311–24. doi: 10.1016/j.jksuci.2015.08.002
47. Senthilkumar S, Viswanatham VM. ERAC-MAC efficient revocable access control for multi-authority cloud storage system. *Int J Internet Technol Secured Trans.* (2019) 9:221–41. doi: 10.1504/IJITST.2019.101824
48. Chinnasamy P, Deepalakshmi P. Design of secure storage for health-care cloud using hybrid cryptography. In: *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE (2018). p. 1717–20. doi: 10.1109/ICICCT.2018.8473107
49. Prince PB, Lovesum SJ. Privacy enforced access control model for secured data handling in cloud-based pervasive health care system. *SN Comput Sci.* (2020) 1:1–8. doi: 10.1007/s42979-020-00246-4
50. Bae WI, Kwak J. Smart card-based secure authentication protocol in multi-server IoT environment. *Multimed Tools Appl.* (2020) 79:15793–811. doi: 10.1007/s11042-017-5548-2
51. Brindha K, Jeyanthi N. Securing portable document format file using extended visual cryptography to protect cloud data storage. *IJ Netw Secur.* (2017) 19:684–93. doi: 10.6633/IJNS.201709.19(5).05
52. Akter M, Gani A, Rahman MO, Hassan MM, Almogren A, Ahmad S. Performance analysis of personal cloud storage services for mobile multimedia health record management. *IEEE Access.* (2018) 6:52625–38. doi: 10.1109/ACCESS.2018.2869848

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.