IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 May 2022, accepted 5 June 2022, date of publication 21 June 2022, date of current version 30 June 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3185016

CKMIB: Construction of Key Agreement Protocol for Cloud Medical Infrastructure Using Blockchain

SAMIULLA ITOO[1], AKBER ALI KHAN[2], VINOD KUMAR[3], AHMED ALKHAYYAT[4], MUSHEER AHMAD[1], AND JANGIRALA SRINIVAS[5], (Member, IEEE)

[1]Department of Applied Sciences and Humanities, Jamia Millia Islamia, New Delhi 110025, India
[2]B. S. Anangpuria Institute of Technology and Management, Faridabad, Haryana 121004, India
[3]Department of Mathematics, PGDAV College, University of Delhi, New Delhi 110065, India
[4]Department of Computer Technical Engineering, College of Technical Engineering, Islamic University, Najaf 54001, Iraq
[5]Jindal Global Business School, O. P. Jindal Global University, Sonipat, Haryana 131001, India

Corresponding author: Vinod Kumar (vinod.iitkgp13@gmail.com)

ABSTRACT In the traditional medical healthcare system, each medical facility is responsible for preserving its own records. Sharing such records with another medical establishment is difficult for them. To tackle this challenge, the traditional medical system leverages internet technology to transform into a modern electronic system. In electronic healthcare systems, managing the security and privacy of patient data becomes a major issue. As an alternative, the healthcare sector might use blockchain technology to exchange digitised healthcare data. Blockchain technology is characterised by anonymity, decentralisation, and immutability. It is hard to keep all electronic healthcare data on blockchain due to the expense and volume. Cloud computing is the best solution for storing this type of data and resolving problems like these. To address these concerns, we offer a blockchain-based key agreement protocol for cloud medical network systems that enhances privacy and security. We demonstrate a formal and informal security analysis of the proposed protocol that shows that the proposed protocol is both secure and communicative. We provide security verification of the proposed protocol by using the AVISPA software tool against man in the middle attack and replay attack. Finally, we compute the computation and communication costs of the proposed protocol and other existing protocols, the proposed protocol has less computation and communication costs than other existing protocols in the electronic healthcare system.

INDEX TERMS Elliptic curve cryptography, blockchain, mutual authentication, medical data, security and privacy.

I. INTRODUCTION

With embedded software and network connectivity, the medical health system is experiencing fast development. Modern medical systems constitute a separate type of cyber physical systems, which we call a Medical Cyber Physical Systems (MCPS). In current medical disciplines, the MCPS is a cyber physical system for integrated medical systems and distributed network systems with control devices that are utilised to display patient information. It uses embedded technologies, distributed computing and wireless communication networks to monitor and regulate the biological dynamics of patients. To certify each device and user identity and services, MCPS requires an independent and comprehensive security verification and authorization mechanism [1], [2]. Authorizing user access to each gadget, MCPS needs to create security gateways. Because of the growing complexity and scale, new design, validation, and verification approaches are required to modify the dynamic data of patients [3]. Thus, MCPS needs the creation of a secure authentication framework and a distributed computing network. With the growing MCPS complexity, conventional identifying authentication technology devices, on the other hand, are becoming excessively long and unsafe. Thus, the traditional authentication system has gone through several stage transitioning from single to multiphasic authentication systems. Traditional identification technology depend on a third-party authentication mechanism that has been criticized. Many heterogeneous networks, numerous types of gadgets, and various user nodes make up the MCPS complex environment. Security authentication across device

The associate editor coordinating the review of this manuscript and approving it for publication was Lo'ai A. Tawalbeh.

nodes in MCPS using various identity authentication systems is relatively rare and data security sharing is challenging to do. Therefore, we propose blockchain and ECC based authentication protocol CKMIB for cloud medical networks to guarantee data integrity, security and accessibility. Furthermore, the CKMIB protocol allows for secure data sharing in healthcare systems via a public channel.

A. RELATED WORK

Lee [4] stated that the traditional authentication system become complicated with the advancement of information technology so the traditional key framework is not reliable requires upgrading. Zhang *et al.* [5] suggested session initiate protocol authentication key framework. However, their SIP authentication not stand with security vulnerability trust. Tu *et al.* [6] suggested the improved smart card based session key authentication framework. Xu *et al.* [7] suggested a efficient and secure two factor mutual authentication key framework based on *ECC* for sharing patients healthcare data in medical system. Subsequently, with the help of crypt-analysis the improved two factor authentication framework primarily formulated on *ECC* is also suggested [8], [9]. Zhang *et al.* [5] organise the data supply secure certification problem based on blockchain and trusted SGX hardware. The certificateless signature framework for wireless network region suggested by Liu *et al.* [10] which is defined on the elliptic curve has security vulnerabilities. Thus, they returned to the earlier approach, which was entirely based on their own work, and proposed an upgraded authentication framework. Renuka *et al.* [11] proposed a three-factor USB-based authentication architecture for smart healthcare medical systems. Lin *et al.* [12] stated that the conventional authentication is improved due to the decentralization feature of block chain. The certificate for the present X.509 certificate standards is given by AI-Bassam [13], however cannot sign best identification characteristic statistics which is totally based on the smart agreement, with the passage of time it is improved and the feature records are authenticated [14]–[19]. Alexopoulos *et al.* [20] using open distributed ledger feature of blockchain technology for the secure authentication management system and design their model. Perera and Patel [21] introduced a multiple users verification in mobile active authentication, due to this the identification step and verification approach is introduced in multi-user system. Lin *et al.* [12] suggested a new TCUGA framework which strictly needs to use node signatures. The trapdoor hash function used in his framework allows the users to successfully update the certificate without resign the node. Fan *et al.* [22] introduced a block chain based information system management in medical healthcare system to record patients information, called as MedBlock. MedBlock accesses the electronic medical record of patients efficiently through the distributed ledger feature of blockchain and have secure access control protocols. As a result, it has the potential to play a critical role in the sharing of patient data in the medical health-care system. Li *et al.* [23] presented a prototype of a data preservation system built entirely on the blockchain ethereum technology. That provide an authentic storage solution in the medical healthcare system to ensure the verifiability and primitiveness of stored data. However, these blockchain-based protocols for the electronic healthcare system should take into account that maintaining or storing all electronic healthcare data in blockchain is too difficult because to the price and size of block chain [24]. Consequently, these protocols needs a cloud storage mechanism in the electronic health care system and decentralized mechanisms using blockchain. Latterly, many research studies have been done regarding the cloud-based electronic healthcare record using blockchain to solve storage problem that is associated with blockchain technology [25], [26]. Using blockchain Weng *et al.* [25] proposed electronic healthcare data sharing scheme that ensure data security by using proxy re-encryption. Sahoo *et al.* [27] proposed a mutual authentication framework for the electronic healthcare system in 2020 to solve security issues in similar existing schemes. They stated that their scheme can withstand attacks such as offline password guessing, and insider attacks. However, Ryu *et al.* [28] discovered that Sahoo *et al.* approach is still vulnerable to insider, privileged insider, and patient anonymity attacks and they proposed a three factor bio-metric based mutual authentication scheme for electronic healthcare system using ECC. Cheng *et al.* [29] proposed a mutual authentication framework for medical data sharing scheme based on block chain technology that also utilizing cloud technology. They using bilinear mapping for medical data sharing scheme. However, Itoo *et al.* [30] find some design flaws in Cheng *et al.* scheme. Later, Olakanmi and Odeyemi [31] proposed an improved key agreement approach for healthcare systems. It maintains the medical healthcare data in cloud stroage. However, these schemes [27]–[29], [31] cannot specifically considered for secure electronic health records based on cloud computing. Therefore, we proposed a CKMIB protocol that provides secure data sharing in electronic healthcare system viva public channel using ECC.

B. BLOCKCHAIN TECHNOLOGY

Nakamoto proposed blockchain in 2008 [34]. The blockchain is made up of blocks that are linked together in a chain. The block includes contains such as the block number, the previous blocks hash value, a nonce, and transaction data. The chain is formed by adding the hash value of the previous block in each block. The ledger is the label given to this chain. Figure 1 illustrates a basic blockchain ledger. Every network device has its own ledger. Blockchain utilizes agreement mechanisms to verify transactions and update the entire ledger [35]. When a new transaction is added to the ledger, all nodes in the network verify that information, if approved, then update their ledger with new transaction. Each user joins the network by registering a pair of public and private keys, which is accomplished through the recording of a transaction. The keys are kept in the wallets of each user. The blocks were built by miners. Miners are nodes in the blockchain network who are responsible for generating and approving

TABLE 1. Comparison of CKMIB with some correlate protocols.

Features	Liu et al. [10]	Sahoo et al. [27]	Chang et al. [29]	Olankani et al. [31]	Renuka et al. [32]	Kim et al. [33]	CKMIB
ECC based	✓	✓	×	✓	✓	✓	✓
Hash based	✓	✓	✓	✓	✓	✓	✓
Secure protocol	✓	✓	×	×	×	✓	✓
Formal security proof	✓	✓	×	✓	✓	✓	✓
Password based approach	✓	✓	✓	×	✓	×	✓
Password update phase	✓	×	✓	×	×	×	✓
Security features based comparison	✓	×	×	×	×	✓	✓
Biometric based	×	✓	×	×	✓	×	✓
Biometric update phase	×	×	×	×	×	×	✓
Blockchain based	×	×	×	×	×	✓	✓
Cloud storage	×	✓	×	✓	×	✓	✓
Low computation cost	×	×	×	×	×	×	✓
Low communication cost	×	×	×	×	×	×	✓

Note : ✓ = having the feature and × = not having such feature.

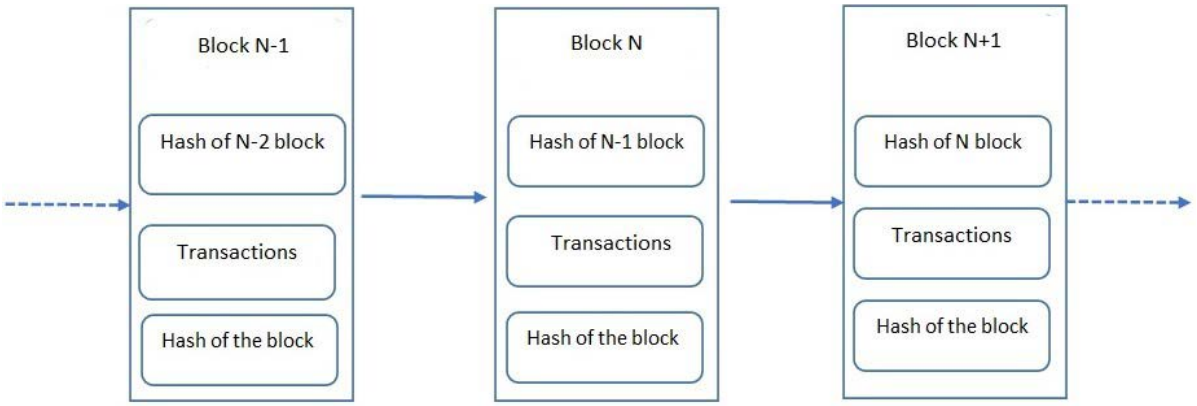

FIGURE 1. Blockchain mechanism of data storing.

blocks. To create a block, the associated node must first solve a difficult challenge. The public and private blockchains are the two forms of blockchain. On a public blockchain, everyone can participate in block generation and agreement, but only pre-approved nodes can do so on a private blockchain. Hyperledger is a private-type blockchain, whereas Bitcoin and Ethereum are public-type blockchains.

C. CLOUD BASED ELECTRONIC HEALTHCARE RECORD SYSTEM MODEL USING BLOCKCHAIN

In an electronic health care system, the patient medical record is stored. To maintain the security and efficiency of medical data it needs a secure model to share the electronic record. We built the system model electronic health care system based on four entities such as patient, medical center, network administrator and cloud server. The system model of the proposed protocol given in Figure 2.

- The patient visits the medical center to receive health care in order to receive health care it is a must to transmit the health data to the medical center through some devices and sensors. The patient health care data are saved in an electronic health care system with proper health care services provided by the medical center.
- A network administrator is a reliable administer that supervises the registration of any participant in the blockchain.
- The network administrator registers the medical center in the blockchain. The medical center stores the healthcare record of patients in a cloud server for sharing with another medical center. For any medical center to obtain the medical data of any medical center it needs to login the data request to the private blockchain in the form of a transaction.
- Cloud storage is a reliable entity that has enough capacity and computing power to manage and store electronic health care data and provide secure data sharing. It obtains data from the medical centre and distributes it to medical centres that have requested electronic health care data using the register secret key.

D. THE DESCRIPTION OF PROPOSED ELECTRONIC HEALTH CARE COMMUNICATION MODEL

- With the help of the network administrator the patient and doctor registering their identities for accessing electronic healthcare services.
- A session key is generating between patent and doctor for future communication.
- Medical center obtains the information from the patient with help of the session key. Then the electronic health record are generated by a medical centre. After that this record is uploaded in the block chain by medical centre.
- The electronic health record of the patient is encrypted through the medical center by using secret-key then send to the cloud server. The electronic health record is then decrypted by a cloud server and finally stores in the database.

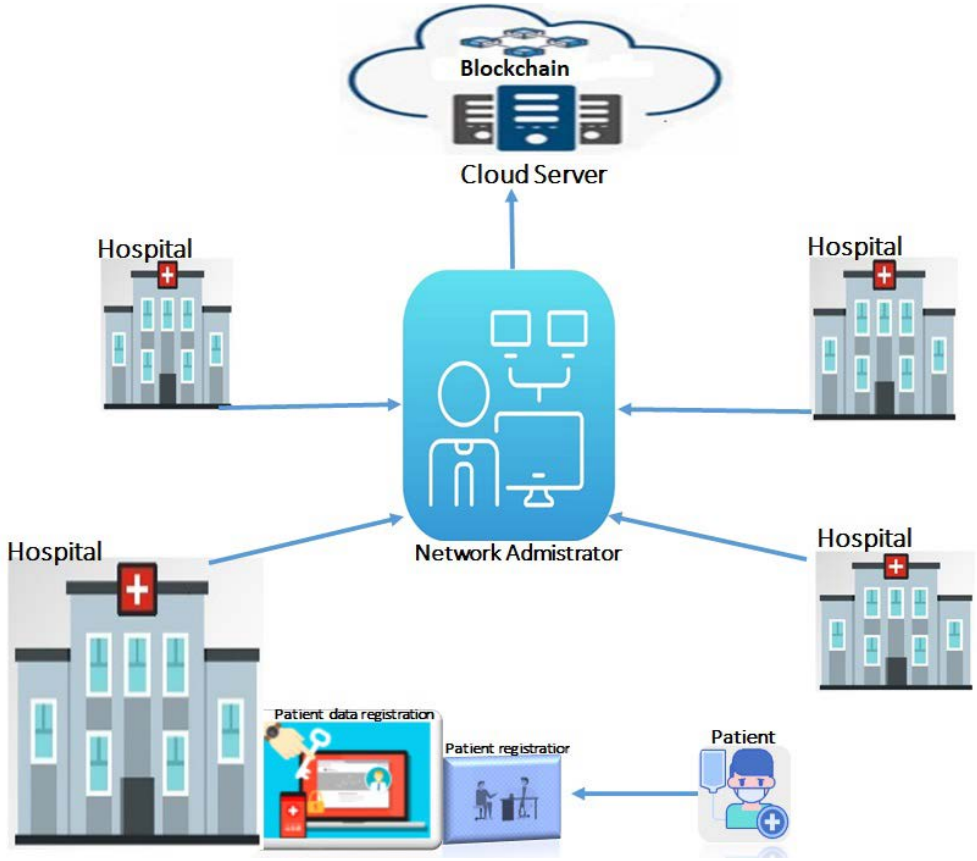

FIGURE 2. Cloud based electronic healthcare record system model.

- If the other medical center requests the data of the medical center to a cloud server. Then the cloud server encrypts the data with a secret key of medical center and sends it to the medical center through a secure channel.
- When the medical center receives the electronic health care data it decrypts first and then uploads the transaction of the patient and medical center identities, timestamp, and the signature in the blockchain.

E. MOTIVATION AND CONTRIBUTION

A technique must be used in the medical healthcare system to protect the system from misbehaving/compromised users. Doctors prefer to diagnose and monitor patients remotely using IoT-enabled wireless sensor nodes in electronic healthcare systems because of communicable diseases such as Covid19. As a consequence, the records were transferred to a digital healthcare device through wireless media. The security and privacy of patients sensitive information, as indicated in the preceding section remains a key concern. To do harm to medical devices, a hostile opponent may use sensitive information or gain control of medical equipment. Designers must develop a system that cannot misbehave/be hacked and is free of security dangers to avoid these security problems in medical systems. As a consequence, we develop a blockchain-based key agreement framework for cloud medical networks that employ ECC to provide secure data transmission in an electronic healthcare system through wireless channels. The proposed protocol is safe against a variety of cryptographic attacks, as well as eliminating side-channel attacks, reducing communication costs, and providing extra security features. We integrate cloud computing, blockchain, and authentication in CKMIB to enable safe key agreement authentication between network administrators and users, which makes it more suitable for electronic medical healthcare applications.

In section 1.1, we review the numerous authentication protocol proposed by various researchers for the medical health system. While some of them are based on ECC, none of them meet all of the security requirements in the electronic health care system. We proposed a blockchain-based key agreement architecture for cloud medical networks as a way to improve things. Table 1 shows the comparative study of the procedures with our suggested protocols. The following are the key aspects of the CKMIB protocol:

- We propose new key agreement and authentication protocol for cloud medical system using blockchain.
- The proposed protocol is secure in many security attacks such as impersonation attack, eavesdropping attack, stolen verifier attack, insider assault attack, replay attack, and man in the middle attack. Furthermore,

TABLE 2. Symbol and their meaning.

Symbol	Meaning	Symbol	Meaning
ECC	Elliptic curve cryptography	SK_p	Session key of patient
G	Additive group	SK_{MC}	The session key of MC
q	Prime number	$\mathcal{A}$	An adversary
g	Group generator	$h(.)$	Hash function
D_K	Decryption using secret key K	$\triangle T_i$	Time span
ID_p	The unique identity of patient p	$\|\|$	Concatenation operation
PW_p	Password of patient p	$\oplus$	Bitwise XOR operation
$Z_q^\star$	Group of order $q-1$ under multiplication	$\mathcal{T}$	Error tolerance
B_p	Biometrics information of patient p	$\rightarrow$	Public channel
E_K	Encryption using secret key k	$\Rightarrow$	Secure channel
τ_p	Public reproduction data	σ_p	Reproduce biometric key
C_p	Counter for patient	C_{cm}	Counter for medical center
r_q	Prime number belongs to $Z_q^\star$	NA	Network administrator
y	Secret key of NA	MC	Medical center
$Adv_{CKMIB}(\mathcal{A})$	Advantage of attacker in CKMIB	p	The patient
eHR_i	Electronic healthcare record	H_{ID_i}	Health identity of patient i
T_{access}	Electronic healthcare record accessing time	R_x	Data-log

proposed protocol manages various security properties such as, patient anonymity, unlinkability, mutual authentication, traceability, key freshness, and perfect forward security.
- We perform a formal security analysis of the proposed protocol using a random oracle model.
- We use simulation tool AVISPA "Automated Validation of Inter-net Security Protocols and Applications" for the verification of security against replay and man-in-the-middle attacks.
- The proposed protocol have much less communication and computation costs than other existing protocols [10], [27], [29], [31]–[33] in same environment.
- In the proposed protocol user can easily update his/her password through proposed protocol.

F. ADVERSARY MODEL

We follow Dolev-Yao model [36] throughout the proposed protocol CKMIB to perform the security analysis. Dolev-Yao (DY) model is based on the following assumptions:
- An attacker $\mathcal{A}$ can delete the message, injects the unwanted messages and intercept the message that is transmitted throughout the public channel.
- An attacker $\mathcal{A}$ may endeavor numerous attacks such as eavesdropping attack, session key stolen attack, replay attack, prevention of insider attack and so on.

G. ORGANISATION OF THE PAPER

The remaining work of this paper is organised as follows: the preliminaries are given in the section 2, that will helpful to demonstrate the proposed scheme. We presented the proposed scheme in the section 3. In the section 4, we perform the security analysis of proposed protocol using formal and informal security analysis. The overall performance evaluation of the proposed scheme with the associated schemes is given in section 5. Finally, we draw the conclusion.

II. PRELIMINARIES

In this section, we give the required mathematical terminologies and notations which are helpful for explanation of this paper.

A. NOTATIONS

In Table 2, we give the meaning of each useful notation or symbol that are used in the proposed paper.

B. ELLIPTIC CURVE OVER FINITE PRIME FIELD

Let $E_q(i,j) : v^2 = w^3 + iw + j \bmod q$ [37] be a non singular elliptic curve over a finite field $Z_q^\star$ where $i, j \in Z_q^\star$ with $4i^3 + 27j^2 \bmod q \neq 0$ and $G = \{(w,v) : v, w \in Z_q, (w,v) \in E\} \cup \{\theta\}$, where θ is group identity under addition.

1. Let $M = (w,v) \in G$, then define $-M = (w,-v)$ and $M + (-M) = \theta$
2. Let $M = (w,v) \in G$ then the scalar multiplication is defined as: $tM = M + M + M \ldots\ldots\ldots\ldots\ldots + M$ $(t - times)$.
3. If $M = (w_1, v_1)$, $N = (w_2, v_2)$, then $M + N = (w_3, v_3)$, where $w_3 = \lambda^2 - w_1 - w_2 \; mod \; p$ and $v_3 = \lambda(w_1 - w_2) - v_1 \; mod \; q$, with

$$\lambda = \begin{cases} \dfrac{v_2 - v_1}{w_2 - w_1} \; mod \; \text{q} \; if \; M \neq N \\ \dfrac{3w_1^2 + i}{2v_1} \; mod \; \text{q} \; if \; M = N \end{cases}$$

C. ECDLP: ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

For the given pair (Y, eY), where $e \in Z_q^\star$, $Y \in G$, It is hard to find e by any polynomial bounded algorithm. The probability that the attacker can evaluate $ECDLP$ as $Adv_{ECDLP}(\mathcal{A}) = Prob[\mathcal{A}(Y, eY) = e : e \in Z_q^\star, Y \in G]$. Also, $Adv_{ECDLP}(\mathcal{A})$ is negligible that is $Adv_{ECDLP}(\mathcal{A}) \leq \epsilon$,where ϵ is comparatively so small.

TABLE 3. Patient registration phase.

p	**NA**
Input ID_p, PW_p and imprint B_p Generates $r_q \in Z_q^\star$ Computes $(\sigma_p, \tau_p) = Gen(B_p)$ Computes $A = h(PW_p \| \sigma_p) \oplus r_q$ Sends $\{ID_p, A\}$ $\cdots\cdots\cdots\cdots\cdots\cdots \Longrightarrow$	
	Computes $B = h(ID_p \| C_p \| y)$ Stores $\{ID_p, C_p\}$ in database Computes $\alpha = B \oplus A$ Store $\{\alpha, C_p\}$ and ID_p in database Sends $\{\alpha, C_p\}$ $\Longleftarrow \cdots\cdots\cdots\cdots\cdots\cdots$
Computes $\alpha_1 = \alpha \oplus \sigma_p$ Computes $\alpha_2 = h(ID_p \| PW_p \| \alpha_1)$ Store $\{\tau_p, \alpha, \alpha_1, \alpha_2, C_p\}$ in database	

D. ECDHP:ELIPITIC CURVE DEFFIE-HELLMAN PROBLEM

For $eY, dY \in G$ and for all $\{e, d\} \in Z_q^\star$ it is hard to compute edY. The probability that the attacker can solve $ECDHP$ as: $Adv_{ECDHP}(\mathcal{A}) = prob[\mathcal{A}(eY, dY) = edY : e, d \in Z_q^\star, Y \in G]$. The probabilistic time-bounded polynomial $Adv_{ECDHP}(\mathcal{A})$ is comparatively negligible *i.e* $Adv_{ECDHP}(\mathcal{A}) \leq \epsilon$ where ϵ is comparatively very small positive quantity.

E. BIOMETRIC FUZZY EXTRACTOR

Fuzzy extractor is defined in pair of function in which one function uses to generate the uniform random bits from the pre-defined input values and the other one uses to retrieve the string from the input value that is close to the authentic input value within the pre-defined approach.The mathematical representation of fuzzy extractor is $(\mathcal{L}, \mathcal{J}, \mathcal{M})$ where, $\mathcal{M}$ is bio-metric input of data of metric-space of finite dimension and $\mathcal{L}$ bit length of output string. The fuzzy extractor also consists of two algorithms which are $Rep(.)$ and $Gen(.)$ [38].

- $Gen(.)$: The $Gen(.)$ is probabilistic method which takes bio-metric $B_i \in \mathcal{M}$ input and gives secret key data $\Re_i \in \{0, 1\}^l$ as output and τ_i a public reproduction variable for the bio-metric input data $B_i \in \mathcal{M}$. Where $Gen(B_i) = \{\Re_i, \tau_i\}$.
- $Rep(.)$: A deterministic approach that takes bio-metric data $B_i' \in \mathcal{M}, \mathcal{T}$ and the attribute τ_i then replicate bio-metric key $\Re$ that is $Rep(\tau_i, B_i') = \Re_i$, provided $d(B_i, B_i') \leq \mathcal{J}$

III. THE PROPOSED PROTOCOL

The proposed protocol CKMIB is based on three phases such as initialization phase, registration phase and authentication phase that are explained as bellow:

A. INITIALIZATION PHASE

In the proposed protocol *CKMIB*, *NA* selects a random number q on elliptic curve $E_q(i, j) : v^2 = w^3 + iw + j \bmod q$ where $i, j \in Z_q^\star$ such that $4i^3 + 27j^2 \bmod q \neq 0$, $g \in G$ and her/his hash function $h(.)$, also the biometeric is executed by using the algorithm of fuzzy extractor [39]. The $Gen(.)$ and $Rep(.)$ algorithms are executed during the login. Further, *NA* generates a random value $y \in Z_q^\star$, selects it as his/her private key and computes public key as $P_{pub} = yg$. Furthermore, *NA* publish the attributes $\{\tau_p(.), \sigma(.), q, g, h(.), E_q(s, t)\}$

B. REGISTRATION PHASE

There are two phase in CKMIB protocol, first is patient registration phase and second is medical centre registration phase which are describes as follows:

1) PATIENT REGISTRATION PHASE

To receive the medical diagnosis the patient must have to register his/her identity with the network administrator. The NA help patient to register his/her public and private key and this is executed over a secure channel. The details of the registration section are mentioned below and shown in Table 3.

- **Step 1:** p_i request network administrator for registration. p_i inputs ID_p, password PW_p and imprint his biometric B_p. Then generates $r_q \in Z_q^\star$. Computes $(\sigma_p, \tau_p) = Gen(B_p)$, computes $A = h(PW_p \| \sigma_p) \oplus r_q$ and sends $\{ID_p, A\}$ to *NA* viva secure channel to the network administrator.
- **Step 2:** On received message, *NA* computes $B = h(ID_p \| C_p \| y)$ where y is secret key of network administrator and stores $\{ID_p, C_p\}$ in his data base for further communication and then computes again $\alpha = B \oplus A$ and stores $\{\alpha, C_p\}$ in his data base for corresponding ID_p then sends $\{\alpha, C_p\}$ to patient.
- **Step 3:** The user computes $\alpha_1 = \alpha \oplus \sigma_p$ and $\alpha_2 = h(ID_p \| PW_p \| \alpha_1)$. Finally patient stores $\{\tau_p, \alpha, \alpha_1, \alpha_2, C_p\}$ in his data base.

2) MEDICAL CENTRE REGISTRATION PHASE

The medical centre must have to register with the network administration to have the accesses for exchange the

TABLE 4. Medical centre registration phase.

MC	NA
Input $\{ID_{MC}\}$ Sends $\{ID_{MC}\}$ $\cdots\cdots\cdots\cdots\cdots\Longrightarrow$	
	Computes $\beta = h(ID_{MC}\|C_{MC}\|y)$ stores $\{ID_{MC}, C_{MC}\}$ in database Sends $\{\beta, C_{MC}\}$ $\Longleftarrow\cdots\cdots\cdots\cdots\cdots$
Store $\{\beta, C_{MC}\}$ in database	

information with other medical centre. The detail of the medical centre registration phase are given below and illustrated in Table 4.

- **Step 1:** *MC* choices his identity ID_{MC} and sends his unique identity to network administrator viva secure channel
- **Step 2:** *NA* computes $\beta = h(ID_{MC}\|C_{MC}\|y)$ and stores $\{ID_{MC}, C_{MC}\}$ in data base. The network administrator sends $\{\beta, C_{MC}\}$ to medical center viva secure channel.
- **Step 3:** Medical centre store $\{\beta, M_{MC}\}$ in his data base for future communication system.

C. LOGIN AND AUTHENTICATION PHASE

In the authentication phase, p communicates with *NA* and *MC* in public channel. The detailed illustration of login and authentication phase are given below and shown in Table 5:

- **Step 1:** p login with $ID_{p^\star}, PW_{p^\star}$ and biometric $B_{p^\star}$. The p get $\sigma_{p^\star} = Rep(B_{p^\star}, \tau_{p^\star})$. The p computes $\alpha_1^\star = \alpha \oplus \tau_{p^\star}$ and $\alpha_2^\star = h(ID_{p^\star}\|PW_{p^\star}\|\alpha_1^\star)$. User verifies $\alpha_2^\star \stackrel{?}{=} \alpha_2$ if yes then generates $a \in Z_q^\star$, computes $K_1 = h(A\|C_p)$, $H_1 = h((A \oplus ag)\|K_1)$ and computes $E_1 = E_{K_1}(ID_p, ag, H_1)$. The p again computes $H_2 = h(ID_p\|C_p\|T_1)$ and encrypts $E_2 = E_{K_2}(E_1, H_2)$ where $K_2 = h(A\|\alpha_1\|ID_p)$. Finally sends $M_1 = \{E_2, T_1\}$ to *NA*.
- **Step 2:** *NA* verifies the time span $T_2 - T_1 \leq \triangle T$ aborts if not fresh otherwise computes $K_2^\star = h(A\|\alpha\|I_p)$ and Decrypts $(E_1, E_2) = D_{K_2^\star}(E_1)$. *NA* computes $H_2^\star = h(ID_p\|C_p\|T_1)$ and verifies $H_2^\star \stackrel{?}{=} H_2$ if yes then computes $K_3 = h(ID_{cm}\|C_{cm})$ and $H_3 = h(\beta\|C_{cm}\|K_3\|ID_{cm})$. The user *NA* Encrypt $E_3 = E_{K_3}(E_1, A, H_3, C_p)$ and sends $M_2 = \{E_3, T_3\}$ to *MC*.
- **Step 3:** On received the message, *MC* verifies $T_4 - T_3 \leq \triangle T$. If yes, then computes $K_3 = h(ID_{cm}\|C_{cm})$ and computes $(E_1, A, H_3) = D_{K_3^\star}(E_3)$. *MC* verifies $H_3^\star \stackrel{?}{=} H_3$ if yes then computes $K_1^\star = h(A\|C_p)$ and decrypts $(ID_p, ag, H_1) = D_{K_1^\star}(E_1)$, computes $H_1^\star = h(A \oplus ag\|K_1^\star)$. *MC* again verifies $H_1 \stackrel{?}{=} H_2$. If yes, then generates $b \in Z_q^\star$ and computes $K_4 = h(C_p\|C_{cm}\|H_1^\star)$, $H_4 = h(K_4\|C_p\|C_{cm}\|\beta\|bg\|T_5)$. *MC* computes session key $SK_{MC} = h(H_4\|ID_p\|ID_{cm}\|bag\|\beta\|T_5)$ and encrypts $E_4 = E_{K_4}(bg, \beta, T_5, ID_{cm}, H_4)$. The medical centre sends back $M_3 = \{E_4, T_5\}$ to *NA* viva public channel.
- **Step 4:** *NA* verifies $T_6 - T_5 \leq \triangle T$ and sends $M_4 = \{M_3, T_7\}$ to p.
- **Step 5:** p verifies $T_8 - T_7 \leq \triangle T$. If valid, then computes $K_4^\star = h(C_p\|C_{cm}\|H_1)$ and decrypts $(bg, \beta, T_5, ID_{cm}, H_4) = D_{K_4^\star}(E_4)$ and computes $H_4^\star = h(K_4^\star\|C_p\|C_{cm}\|\beta\|bg\|T_5)$. Further, p verifies $H_4^\star \stackrel{?}{=} H_4$, and computes his/her his session key $SK_p = h(H_4^\star\|ID_p\|ID_{cm}\|abg\|\beta\|T_5)$. Hence, matches his session key $SK = SK_p = SK_{cm}$

D. ELECTRONIC HEALTHCARE RECORD STORING PHASE

The medical centre generates eHR_i and stores eHR_i in CS. Detailed steps are as follows:

- Step 1: The medical centre generates eHR_i, which includes H_{ID_i} and health record information of patient. MC computes $MC_R = h(eHR_i||H_{ID_i})$. Then MC sends $\{T_{access}, MC_R\}$ to cloud server.
- Step 2: On recieving MC_R, cloud server stores eHR_i and H_{ID_i} into the server database.

E. UPLOADING DATA-LOG IN BLOCKCHAIN

On receiving $MC_R = h(eHR_i||H_{ID_i})$ from MC, cloud server computes $R_x = (H_{ID_i}||T_{access}||eHR_i\}$ and create a data-log and uploads it in blockcahin as shown in fig 1. Finally cloud server stores the data in his data base.

F. UPDATING OF PASSWORD AND BIOMETRIC PHASE

When p wants to update his/her password. He/she takes following steps:

- **Step 1:** The p inputs $ID_{p^\star}, B_{p^\star}$ and $PW_{p^\star}$ and gets $\sigma_{p^\star} = Rep(\tau_{p^\star}, B_{p^\star})$ then, p computes $\alpha_1^\star = \alpha \oplus \tau_{p^\star}$ and $\alpha_2^\star = h(ID_{p^\star}\|PW_{p^\star}\|\alpha_1^\star)$. p verifies $\alpha_2^\star \stackrel{?}{=} \alpha_2$ holds or not. If it is not, then terminates session. Otherwise p selects his /her new password and bio-metric as (B_p^{new}, PW_p^{new}). Then p computes $(\tau_p^{new}, \sigma_p^{new}) = Gen(B_p^{new})$, $\beta_p^{new} = h(PW_p^{new}\|\sigma_p^{new}) \oplus r_q$ and sends $M_1' = \{ID_p^{new}, \beta_p^{new}\}$ to *NA*.
- **Step 2:** *NA* verifies $\{ID_p, C_p\}$ in data base then, computes $\lambda_{new} = \{B \oplus \beta_p^{new}\}$ and sends $M_2' = \{\lambda^{new}, C_p\}$ to p.
- **Step 3:** When p receives $M_2' = \{\lambda^{new}, C_p\}$ then, computes $\lambda_1^{new} = \lambda^{new} \oplus \sigma_p^{new}$ and $\lambda_2^{new} = h(ID_p\|PW_p^{new}\|\lambda_1^{new})$. Then, p replace his old password

TABLE 5. Login and authentication phase.

Patient	Network administration	Medical center
Login with $ID_{p^\star}, PW_{p^\star}$ and $B_{p^\star}$ And gets $\sigma_{p^\star} = Rep(B_{p^\star}, \tau_{p^\star})$ Computes $\alpha_1^\star = \alpha \oplus \tau_{p^\star}$ Computes $\alpha_2^\star = h(ID_{p^\star} \| PW_{p^\star} \| \alpha_1^\star)$ Verifies $\alpha_2^\star \stackrel{?}{=} \alpha_2$ if yes then: Generates $a \in Z_q^\star$ Computes $K_1 = h(A \| C_p)$ Computes $H_1 = h((A \oplus ag) \| K_1)$ Encrypts $E_1 = E_{K_1}(ID_p, ag, H_1)$ Computes $H_2 = h(ID_p \| C_p \| T_1)$ Encrypts $E_2 = E_{K_2}(E_1, H_2)$ Where $K_2 = h(A \| \alpha_1 \| ID_p)$ Sends $M_1 = \{E_2, T_1\}$ . . . . . $\longrightarrow$	Verifies $T_2 - T_1 \leq \triangle T$, aborts if not fresh Computes $K_2^\star = h(A \| \alpha \| I_p)$ Decrypts $(E_1, H_2) = D_{K_2^\star}(E_1)$ Computes $H_2^\star = h(ID_p \| C_p \| T_1)$ Verifies $H_2^\star \stackrel{?}{=} H_2$ if yes Computes $K_3 = h(ID_{cm} \| C_{cm})$ Computes $H_3 = h(\beta \| C_{cm} \| K_3 \| ID_{cm})$ Encrypts $E_3 = E_{K_3}(E_1, A, H_3, C_p)$ Sends $M_2 = \{E_3, T_3\}$ . . . . . $\longrightarrow$ Verifies $T_6 - T_5 \leq \triangle T$ Sends $M_4 = \{M_3, T_7\}$ $\longleftarrow$	Verifies $T_4 - T_3 \leq \triangle T$ Computes $K_3 = h(ID_{cm} \| C_{cm})$ Computes $(E_1, A, H_3) = D_{K_3^\star}(E_3)$ Computes $H_3^\star = h(\beta \| C_{cm} \| K_3^\star \| ID_{cm})$ Verifies $H_3^\star \stackrel{?}{=} H_3$ Computes Computes $K_1^\star = h(A \| C_p)$ Decrypt $(ID_p, ag, H_1) = D_{K_1^\star}(E_1)$ Computes $H_1^\star = h(A \oplus ag \| K_1^\star)$ Verifies $H_1 \stackrel{?}{=} H_2$ if yes Generates $b \in Z_q^\star$ Computes $K_4 = h(C_p \| C_{cm} \| H_1^\star)$ Computes $H_4 = h(K_4 \| C_p \| C_{cm} \| \beta \| bg \| T_5)$ Computes $SK_{MC} = h(H_4 \| ID_p \| ID_{cm} \| bag \| \beta \| T_5)$ Encrypts $E_4 = E_{K_4}(bg, \beta, T_5, ID_{cm}, H_4)$ Sends $M_3 = \{E_4, T_5\}$ $\longleftarrow$ . . . . .
Verifies $T_8 - T_7 \leq \triangle T$ Computes $K_4^\star = h(C_p \| C_{cm} \| H_1)$ Decrypts $(bg, \beta, T_5, ID_{cm}, H_4) = D_{K_4^\star}(E_4)$ Computes $H_4^\star = h(K_4^\star \| C_p \| C_m \| \beta \| bg \| T_5)$ Verifies $H_4^\star \stackrel{?}{=} H_4$ Computes $SK_p = h(H_4^\star \| ID_p \| ID_{cm} \| abg \| \beta \| T_5)$ Hence $SK = SK_p = SK_{cm}$		

PW_p and B_p with new password PW_p^{new} and B_p^{new} and stores $\{\tau_p^{new}, \lambda, \lambda_1^{new}, \lambda_2^{new}\}$ respectively in data base.

IV. SECURITY ANALYSIS

In this section, we analysis of CKMIB. We prove that CKMIB is secure against various malicious security attacks. We also prove that CKMIB is secure against replay attacks and MITM by using random oracle model.

A. INFORMAL SECURITY ANALYSIS

We did analysis informal security of CKMIB and show that CKMIB is secure against various security threats. Moreover, CKMIB assure the patient's confidentiality and secure authentication.

1) IMPERSONATION ATTACK

$\mathcal{A}$ attempt to attack a authorized p to acquire the sensitive information. To impersonate the p, $\mathcal{A}$ to compute a message $M_1 = \{E_2, T_1\}$. However, E_2 is encrypted by secret key K_2 and adversely cannot compute the secret key because it is encrypted by $K_2 = h(A \| \alpha_1 \| ID_p)$. Therefore, the CKMIB is secure against impersonation attack.

2) EAVESDROPPING ATTACK

According to the eavesdropping attack, $\mathcal{A}$ can intercept the all messages convey through insecure medium. Therefore, $\mathcal{A}$ can intercept messages. But in the proposed protocol all the parameters are protected by hash function and also fresh random number which are chosen in every round of authentication. So, $\mathcal{A}$ neither get any parameter nor get identity of user. In addition of this the $\mathcal{A}$ cannot calculate $SK_p = h(H_4^\star \| ID_p \| ID_{cm} \| abg \| \beta \| T_5)$. Therefore $\mathcal{A}$ cannot obtain ID_p, M_i and SK_p.

3) SESSION KEY DISCLOSURE ATTACK

If $\mathcal{A}$ tries to obtain the session key $SK_p = h(H_4^\star \| ID_p \| ID_{cm} \| abg \| \beta \| T_5)$, the adversely must know the random number's a, b, and base point of elliptic curve g which is hard to obtain and know the identity of p and as well as of medical center MC. Therefore, CKMIB is secure against the session key disclosure.

4) KEY FRESHNESS

Key freshness is likely about when the new keys are generated so that future interconnection cannot be deformed even if the old keys are compromised. Therefore, for the utilization of freshness of keys in the cryptography always take two principal values such as selecting random number and time stamp. In CKMIB in each step, we chose fresh random number as well as fresh timestamp. Therefore, the freshness of key agreement is maintained in CKMIB.

5) PERFECT FORWARD SECRECY

If by chance $\mathcal{A}$ knows the private secret key, $\mathcal{A}$ cannot obtain the previous key $SK_p = h(H_4^\star \| ID_p \| ID_{cm} \| abg \| \beta \| T_5)$ because the previous key does not contain SK_{NA}. Further, if the parameters $K_2^\star$ and $K_3^\star$ are compromised, but $\mathcal{A}$ cannot obtain abg,which is compute to hard as Deffie-Hellman problem.

6) REPLAY ATTACK

$\mathcal{A}$ tries to transmit a massage to perform a reply attack. But $\mathcal{A}$ cannot perform reply attack because the transmitted messages includes verifying conditions, random number and secure hash function. Thus, CKMIB can resist the reply attack.

7) INSIDER ATTACK

The massage transmitted by p is conformed by NA and then upload to cloud based blockchain. After receiving $p's$ message in blockchain, the $p's$ identity still remains mask by p private key K_1. The p private key remains always secret that can be known only by p. The other entity cannot obtain the patient information because it is masked by the secret key. The patient only can decrypts the massage by his/her secret key. Therefore, the attacker fails to use his/her identity to obtain the other user information or the users identity password for other services login attempts. Therefore, CKMIB is secure against the insider attack.

8) PATIENT ANONYMITY

$\mathcal{A}$ cannot known the patient real identity because it is masked by hash function or encrypted with random number or secret key. Therefore, in CKMIB the users identity is secure.

9) TRACEABILITY

An attacker monitors the authentication request messages from two different sessions and compares them to see if they are similar. If both messages are identical, the authentication request messages have the same origin, indicating that the user/patient for both requests is the same. The adversary cannot track the user/patient in our scheme even after listening/stealing the authentication messages $M_i = \{E_i, , t_i\}$ because these messages contain encrypted parameters $E_{K_1}(ID_p, ag, H_1)$ with a private key K_1, one way hash function, and current timestamp t_i that are chosen a fresh timestamp for each new session, resulting in the formation of new M_i. Hence, the identity of the user/patient and medical center cannot be traced. Thus, our scheme is resistant to untraceability attacks.

10) UNLINKABILITY

The identity and location of the user/patient are two important privacy concerns. Adversary must be kept in the dark about the patient identity and associated information. It is impossible for the adversary to deduce the patient identity in the proposed protocol CKMIB, because we uses anonymous identity $ID_{p^\star}$ and also encrypted it with private key K_1 as $E_1 = E_{K_1}(ID_p, ag, H_1)$. In addition, each session uses a distinct temporary identity $ID_{p^\star}$ to protect p privacy. Outsiders have no knowledge who is communicating with MC because $ID_{p^\star}$ is unlinkable. The adversary has no idea about the identity involved in two runs of protocol is same are different. Therefore, the proposed scheme prevents the leakage of user identity and protects users privacy.

11) MAN IN THE MIDDLE ATTACK

$\mathcal{A}$ can endeavor to utilize the past messages of login in the server side. $\mathcal{A}$ replays $M_1 = \{E_2, T_1\}$ where $E_2 = E_{K_2}(E_1, H_2)$ is encrypted by K_2 which is masked by hash function $K_2 = h(A\|\alpha_1\|ID_p)$. When the NA receives the message it verifies the timestamp $T_2 - T_1 \leq \triangle T$ and $H_2^\star \stackrel{?}{=} H_2$. Similarly, the MC also verifies the timestamp $T_4 - T_3 \leq \triangle T$ and $H_3^\star \stackrel{?}{=} H_3$. Thus, $\mathcal{A}$ is not competent to compute with original entity because we uses fresh random values and anonymous identity. Hence our proposed protocol withstands against this attack.

12) EPHEMERAL SECURITY LEAKAGE ATTACK

Let $\mathcal{A}$ can obtain access to the secret parameters short-term (ephemeral) and long-term (permanent) values. After that, $\mathcal{A}$ can try to calculate $SK_p = h(H_4^\star\|ID_p\|ID_{cm}\|abg\|\beta\|T_5)$ between the patient and the medical centre. The two cases are illustrated below.

- Assume that $\mathcal{A}$ knows about the short-term secret parameters a and b. Then $\mathcal{A}$ tries to calculate SK, that cannot be computed without the long-term secret parameters K_1 and K_2, even though $\mathcal{A}$ can compute abg with the short-term secret parameters but cannot calculate $H_4^\star$.
- Assume that $\mathcal{A}$ has access to the long-term secret parameters K_1 and K_2. On the other hand, $\mathcal{A}$ is still unable to compute SK since she is unaware of the short-term secret parameters a and b, which is impossible due to ECDHM.

To create the right SK in the above two cases, $\mathcal{A}$ must be aware of both short-term and long-term secret factors. As a result, ephemeral security leakage attack is not possible in our proposed framework CKMIB.

13) DoS ATTACK

During the login phase in the proposed protocol CKMIB, p inputs $ID_{p^\star}, B_{p^\star}$ and $PW_{p^\star}$ and gets $\sigma_{p^\star} = Rep(\tau_{p^\star}, B_{p^\star})$ and NA computes $H_2^* = h(ID_p^*\|C_p\|T_1)$ and verifies $H_2^* \stackrel{?}{=} H_1$. The session is terminated if this condition is not met. Thus, the authentication request is only sent to p if NA confirms authenticity. p also protects against replay attacks by checking the messages freshness. Therefore, even if attacker tries to overload NA by replaying numerous valid legitimate users past login requests, NA rejects these requests by checking the message freshness. Hence, CKMIB is resistant to DoS attacks.

14) SIDE CHANNEL ATTACK

In well-known shared key encryption, there are several side channel attacks. The side channel attack can be used to get the AES encryption key used in the challenge-response for a single password based authentication scheme. The AES encryption key in our protocol is made up of numerous keys that have been xored together, and those keys cannot be recovered from the encryption key. An attacker cannot determine the values of the keys used in authentication simply by knowing the encryption key. As a result, a side channel

TABLE 6. Simulation of oracles.

Simulation of oracle
For $send(\Upsilon_p^i, start)$ query, the Υ_p^i oracle first login the server as: Generates $a \in Z_q^\star$ Computes $\alpha_1^\star = \alpha \oplus \tau_{p^\star}$ Computes $\alpha_2^\star = h(ID_{p^\star} \| PW_{p^\star} \| \alpha_1^\star)$ Computes $K_1 = h(A \| C_p)$ Computes $H_1 = h((A \oplus ag) \| K_1)$ Encrypts $E_1 = E_{K_1}(ID_p, ag, H_1)$ Computes $H_2 = h(ID_p \| C_p \| T_1)$ Encrypts $E_2 = E_{K_2}(E_1, H_2)$ Then it answers $M_1 = \{E_2, T_1\}$
For $send(\Upsilon_p^i, \{E_2, T_1\}$ query, the Υ_{NA}^j oracle simulates as: Verifies $T_2 - T_1 \leq \triangle T$, aborts if not fresh Computes $K_2^\star = h(A \| \alpha \| I_p)$ Decrypts $(E_1, H_2) = D_{K_2^\star}(E_1)$ Computes $H_2^\star = h(ID_p \| C_p \| T_1)$ Verifies $H_2^\star \stackrel{?}{=} H_2$ if yes Computes $K_3 = h(ID_{cm} \| C_{cm})$ Computes $H_3 = h(\beta \| C_{cm} \| K_3 \| ID_{cm})$ Encrypt $E_3 = E_{K_3}(E_1, A, H_3, C_p)$ Then it answers with $M_2 = \{E_3, T_3\}$
For $send(\Upsilon_{NA}^j, \{E_3, T_3\})$ query, The Υ_{MC}^k oracle simulate as: Verifies $T_4 - T_3 \leq \triangle T$ Computes $K_3 = h(ID_{cm} \| C_{cm})$ Decrypts $(E_1, A, H_3) = D_{K_3}^\star(E_3)$ Computes $H_3^\star = h(\beta \| C_{cm} \| K_3^\star \| ID_{cm})$ Verifies $H_3^\star \stackrel{?}{=} H_3$ Computes $K_1^\star = h(A \| C_p)$ Decrypt $(ID_p, ag, H_1) = D_{K_1^\star}(E_1)$ Computes $H_1^\star = h(A \oplus ag \| K_1^\star)$ Verifies $H_1 \stackrel{?}{=} H_2$ if yes Generates $b \in Z_q^\star$ Computes $K_4 = h(C_p \| C_{cm} \| H_1^\star)$ Computes $H_4 = h(K_4 \| C_p \| C_{cm} \| \beta \| bg \| T_5)$ Computes $SK_{MC} = h(H_4 \| ID_p \| ID_{cm} \| bag \| \beta \| T_5)$ Encrypts $E_4 = E_{K_4}(bg, \beta, T_5, ID_{cm}, H_4)$ Then it answer with $M_3 = \{E_4, T_5\}$
For $send(M\Upsilon_{MC}^k, \{E_4, T_5\})$ query, the Υ_{NA}^j oracle simulates as: Verifies $T_6 - T_5 \leq \triangle T$ Then it answers with $M_4 = \{M_3, T_7\}$
For $send(\Upsilon_{NA}^j, \{M_3, T_7\})$ query, The Υ_p^i oracle simulates as : Verifies $T_8 - T_7 \leq \triangle T$ Computes $K_4^\star = h(C_p \| C_{cm} \| H_1)$ Decrypts $(bg, \beta, T_5, ID_{cm}, H_4) = D_{K_4^\star}(E_4)$ Computes $H_4^\star = h(K_4^\star \| C_p \| C_m \| \beta \| bg \| T_5)$ Verifies $H_4^\star \stackrel{?}{=} H_4$ Computes $SK_p = h(H_4^\star \| ID_p \| ID_{cm} \| abg \| \beta \| T_5)$ Verifies $SK = SK_p = SK_{cm}$ If verified, then it accept the session key.
For execute $(\Upsilon_p^i, \Upsilon_{NA}^j, \Upsilon_{MC}^k)$ query, by using the send query and obtain $\{E_2, T_1\} \longleftarrow$ send $(\Upsilon_p^i, start)$ $\{E_3, T_3\} \longleftarrow$ send $(\Upsilon_p^i, \{E_2, T_1\}$ $\{E_4, T_5\} \longleftarrow$send $(\Upsilon_{NA}^j, \{E_3, T_3\})$ $\{M_3, T_7\} \longleftarrow$send $(M\Upsilon_{MC}^k, \{E_4, T_5\})$, then returns to $\mathcal{A}$
For the Session key Reveal Υ_i query, returns the session key if Υ_i has actually formed the session key and both Υ_i and its partner have not asked by a test query, otherwise returns null.
For $Test(\Upsilon^i)$, a bit e will be developed randomly, creates this query, if the session key comes up, for example Υ^i returns the original session key when $e = 1$, or returns random number of same length to $\mathcal{A}$.

attack cannot be used to obtain the entire secure vault by construct a duplicate device or insert a false message into the channel.

B. FORMAL SECURITY ANALYSIS

In the following subsection, we define the formal security analysis for CKMIB. The proposed security model is acceptable and appropriate based on literature [40]. In CKMIB, we define the three factors p, NA and MC. In addition, Υ_p^i, Υ_{NA}^j and Υ_{MC}^k represent the occurrence of i, j and k of p, NA and MC accordingly, called as oracles.

The attacker can make the following queries and are illustrated in Table 6:

- *Execute* $(\Upsilon_p^i, \Upsilon_{NA}^j, \Upsilon_{MC}^k)$: This inquiry is used to model the eavesdropping attack,*i.e* the attacker can intercept all message's that are convey through this channel by this request.
- *Reveal* (Υ^i): This inquiry is used to model the session key disclosure attack. The attacker can redeem the session key in the current session generated by (Υ_p^i).
- *Send* $(\Upsilon^i, \Upsilon^j, message(m)$: This inquiry imitates an active attack by attacker. The attacker behaves as Υ_p^i and communicate a message (m) to Υ^j. If m is authenticate, then following the protocol, the attacker can retrieve a corresponding message as feedback message, otherwise the inquire is terminated.

- *Test*(Υ^i): This inquiry is a model of lingual security of the session key among p and NA. Earlier than this, a bit e is developed randomly, and the output is secret to attacker. When $\mathcal{A}$ creates this query, if Sk comes up, for example Υ^i returns the original Sk when $e = 1$, or random number of same length as the Sk when $e = 0$ otherwise the production is null and void.

Finally, the simatic security of the Sk is defined. In the proposed model, a attacker desires to differentiate whether the session key between Υ_p^i and Υ_{NA}^j is actual or a random variety. Attacker could make the check question to the instances Υ_p^i or Υ_{NA}^j, and then verify the constancy of its output with the random bit e. Subsequently, attacker wishes to guess a bit e'. When $e' = e$ is satisfied, it means that attacker wins the game. The $succ$ is used to represent the event that attacker wins the game. The probability that $\mathcal{A}$ breaks through the semantic safety of the protocol to obtain an advantage is described $Adv_{CKMIB}(\mathcal{A}) = |2.prob[Succ] - 1|$, where $prob$ represents the probability of occurrence of the event E. If $Adv_{CKMIB}(\mathcal{A})$ is negligible, protocol is considered secure on this proposed model.

Theorem: Let the attacker ongoing in a polynomial time in the proposed model against the proposed protocol. Assume NA is not negotiated, so the dominance of attacker in breaking the semantic security of protocol for obtaining the session key between the p and NA is:

$$Adv_{CKMIB}(\mathcal{A}) \leq \frac{Q_h^2}{2^{l_s}} + \frac{(Q_s + Q_e)^2}{n}$$

where Q_s, Q_h, Q_e, n and l_s represents execute queries, hash oracle queries, range space of the random number generation, and the length of the hash function output value.

Proof: In this proof we take three factor game which are G_i, where $i = 1, 2, 3$. Let $Succ_i$ denotes the event that the $\mathcal{A}$ successfully evaluate the bit e in the game G_i.

- G_1 : The attacker execute attack on protocol. Before the game starts e is selected randomly, we get

$$Adv_{CKMIB}(\mathcal{A}) = |2.prob[Succ_1] - 1| \quad (1)$$

- G_2: The attacker executes an eavesdropping attack on protocol. The attacker first makes *Execute* queries and then make a *Test* query. The session key in the proposed protocol is $SK_p = h(H_4^\star \| ID_p \| ID_{cm} \| abg \| \beta \| T_5)$. The attacker have to differentiate whether the result returned after performing *Test* query is actually a random number or a session key, it can get all the parameters $\{E_2, T_1, M_3, T_7, E_4, T_5\}$ transmitted in the channel by making *execute* queries, but cannot obtain SK_p. Hence, eavesdropping attacks do not increase the probability of attacker winning, therefore we obtain:

$$prob(succ_1) = prob(succ_2) \quad (2)$$

- G_3 : During the authentication phase G_2 simulates the random number and all hash collisions. The session key is generated by hash function and random numbers in the proposed protocol. According to the birthday paradox, probability of a random number collision is $\frac{(Q_s+Q_e)^2}{2n}$ and $\frac{Q_h^2}{2^{l_s+1}}$ is the probability of hash collision.Therefore, we have

$$|prob(succ_2) - prob(succ_3)| \leq \frac{Q_h^2}{2^{l_s+1}} + \frac{(Q_s + Q_e)^2}{2n} \quad (3)$$

All the queries are simulated in G_2. The session key is independently generated between p and NA in the proposed protocol. Therefore, the attacker cannot get any information about bit e. The attacker can win game only if attacker get bit e after making *test* query. Thus, it is obtained:

$$prob(succ_4) = 1/2. \quad (4)$$

The following result is obtained from equation (1),(2) and (4):

$$\begin{aligned} \frac{1}{2}Adv_{CKMIB}(\mathcal{A}) &= |prob(succ_1) - \frac{1}{2}| \\ &= |prob(succ_2) - prob(succ_3)| \end{aligned} \quad (5)$$

From the equation (3) and (5) following results are obtained:

$$Adv_{CKMIB}(\mathcal{A}) \leq \frac{Q_h^2}{2^{l_s}} + \frac{(Q_s + Q_e)^2}{n} \quad (6)$$

C. SIMULATION STUDY USING AVISPA TOOL

Formal verification of the proposed work is performed using the AVISPA software tool, which uses a formal and modular language to express the security protocol needs and features. Further, the AVISPA is a one-button tool for Automated Validation of Internet Security Protocols and Applications [41]. The goal of this tool is to create a rich language for describing threat models and security objectives. Additionally, AVISPA helps security organisations to identify weaknesses and risks in authentication protocols. In order to perform security verification of security framework is modeled in a modular and role-based language called the High Level Protocol Specification Language (HLPSL). This formal language supports the specification of structures, intruder models, crypto primitives with their complex properties. Eventually, there is a translator in AVISPA namely, HLPSL2IF which automatically translates HLPSL specification into equivalent Intermediate Format (IF). Later, which are in turn fed to one of the backends in AVISPA to display a result.

V. PERFORMANCE ANALYSIS

In the following section we exhibit the performance of CKMIB with the corresponding schemes [10], [27], [29], [31]–[33]. We analysis the computation as well as communication cost of the related scheme with the CKMIB.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/CKMIB.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.8s
  visitedNodes: 4 nodes
  depth: 2 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/CKMIB.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.35 seconds
  Computation: 0.00 seconds
```

FIGURE 3. Results of AVISPA employing OFMC and ATSE.

TABLE 7. The comparison of proposed protocol with related protocols.

Feature	Liu et al. [10]	Sahoo et al. [27]	Chang et al. [29]	Olankani et al. [31]	Renuka et al. [32]	Kim et al. [33]	CKMIB
Traceability	×	×	✓	×	×	×	✓
Impersonation Attack	×	✓	×	✓	✓	✓	✓
Session Key Disclosure Attack	×	✓	✓	×	✓	✓	✓
Perfect Forward Secrecy	×	✓	✓	✓	✓	×	✓
Replay Attack	✓	✓	×	×	✓	✓	✓
Prevention of Insider Attack	×	×	×	×	✓	✓	✓
Patient Anonymity	✓	×	✓	✓	✓	✓	✓
Mutual Authentication	×	✓	✓	✓	✓	✓	✓
Unlinkability	×	×	×	×	×	×	✓
Man in the middle attack	×	×	×	×	×	×	✓
Eavesdropping Attack	×	×	×	×	×	×	✓

Note : ✓ Means Secure against features × Means does not secure against features.

A. SECURITY ATTRIBUTES COMPARISON

The comparative security analysis of CKMIB with related schemes [10], [27], [29], [31]–[33] in the same environment are shown in Table 7. Thus, CKMIB with stand against the following attacks such as: impersonation attack, prevention of insider attack, eavesdropping attack, replay attack and man in middle attack and having the security features such as session key disclosure, forward secrecy, patient anonymity, unlinkability and traceability.

B. COMPUTATION COST COMPARISON

We have evaluate the computation cost of proposed protocol with other existing protocols [10], [27], [29], [31]–[33], the time analysis of different operation in milliseconds are as: hash function t_h has 0.0001ms, bilinear pairing t_{bp} has 4.211ms, bilinear pairing operation of scaler multiplication t_{bp-sm} has 1.709ms, bilinear pairing operation of addition t_{bp-ad} has 0.0071ms, elliptic curve operation of scalar multiplication t_{ec-sm} has 0.442ms, exponential t_{exp} has 3.886ms, elliptic curve decryptions t_{ec-dec} has 0.7399ms, elliptic curve encryption t_{ec-enc} has 0.5102ms, elliptic curve addition t_{ec-ad} has 0.0018ms. The computation cost of the proposed protocol and other existing protocols based on Kim *et al.* [33] in which they performed these simulation on laptop with an Intel Core i5 processor, 8 GB of RAM, and a GeForce 920M graphics card for simulating. This device can calculate 250 K hashes per second. The first two components of the simulations focus on transaction processing time. The outcome is solely determined by the total number of transactions. We correlate the computation costs of CKMIB throughout the authentication phase between the medical center and the patient with the corresponding schemes are as:

- Liu *et al.* [10] scheme consists of six bilinear pairing operation of scaler multiplication, three bilinear pairing operation of addition, two exponential operation and six hash functions used that has total computation cost approximately 22.2583 ms.
- Sahoo *et al.* [27] scheme consists of three elliptic curve encryption and three elliptic curve decryptions, seven elliptic curve scalar multiplication and fifteen hash functions that has total computation cost approximately 6.8458 ms.
- Chang *et al.* [29]scheme consists of eight bilinear pairing operation of scaler multiplication, two bilinear pairing operation of addition, one exponential operation and six hash functions that has total computation cost approximately 17.5728 ms.
- Olakanmi and Odeyemi [31] scheme consists of two elliptic curve scalar multiplication, two bilinear pairing operations and four hash functions that has total computation cost approximately 9.3064 ms.
- Renuka *et al.* [32] scheme consists of nine elliptic curve operation of scalar multiplication, one elliptic curve encryption, two elliptic curve decryptions and fifteen hash functions that has total computation cost approximately 5.2296 ms.
- Kim *et al.* [33] scheme consists of two elliptic curve encryption, two elliptic curve decryptions, two elliptic curve scaler addition operations, two elliptic curve scaler multiplication operation and ten hash functions that has total computation cost approximately 3.3878 ms.

TABLE 8. Computation cost comparison.

Protocols	Operations	Computation cost (milliseconds)
Liu et al. [10]	$6t_{bp-sm} + 3t_{bp-ad} + 2t_{exp} + t_{bp} + 6t_h$	$\approx$ 22.2583 ms
Sahoo et al. [27]	$3t_{ec-enc} + 3t_{ec-dec} + 7t_{ec-sm} + 15t_h$	$\approx$ 6.8458 ms
Chang et al. [29]	$8t_{bp-sm} + 2t_{bp-ad} + t_{exp} + 6t_h$	$\approx$ 17.5728 ms
Olankani et al. [31]	$4t_h + 2t_{ec-sm} + 2t_{bp}$	$\approx$ 9.3064 ms
Renuka et al. [32]	$9t_{ec-sm} + t_{ec-enc} + 2t_{ec-dec} + 15t_h$	$\approx$ 5.2296 ms
Kim et al. [33]	$2t_{ec-enc} + 2t_{ec-dec} + 2t_{ec-sm} + 2t_{ec-ad} + 10t_h$	$\approx$ 3.3878 ms
CKMIB	$2t_{ec-enc} + 2t_{ec-dec} + 15t_h$	$\approx$ 2.5017 ms

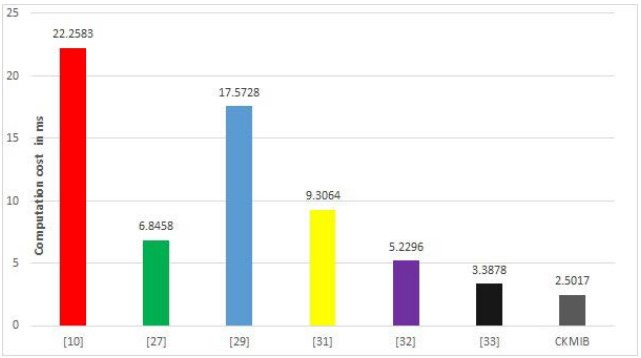

FIGURE 4. Computation cost comparison.

TABLE 9. Communication cost comparison.

Protocols	Communication cost (bits)
Liu et al. [10]	3424
Sahoo et al. [27]	1792
Chang et al. [29]	1984
Olankani et al. [31]	2290
Renuka et al. [32]	1184
Kim et al. [33]	864
CKMIB	704

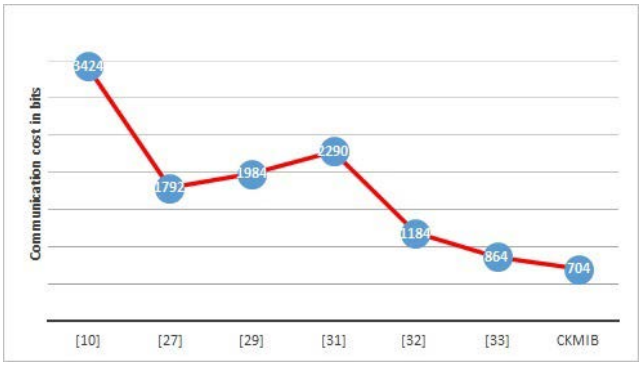

FIGURE 5. Communication cost comparison.

- The proposed scheme consists of two elliptic curve encryption, two elliptic curve decryptions and fifteen hash functions that has total computation cost approximately 2.5017 ms.

The detailed illustration are shown in Table 8 and the efficiency of proposed protocol and other existing protocol given in Figure 4.

C. COMMUNICATION COST COMPARISON

We evaluate the communication cost of proposed protocol and other existing protocols [10], [27], [29], [31]–[33]. For communication cost we take the message authentication code is 160 bits, identity is 128 bits, hash function 160 bits, timestamp 32 bits, additive group G_1 is 1024 bits, multiplicative group G is 320 bits, the symmetric-key encryption is 256 bits and ECC-based encryption is 320 bits. We compute the communication cost of the proposed framework based on [33]. The communication cost of CKMIB and the related schemes are shown in Table 9. Here, communication cost of our proposed protocol is much less than the other existing protocol. Thus, the proposed protocol is more efficient in communication than the other existing protocol. The efficiency of proposed protocol and other existing protocol given in Figure 5.

VI. CONCLUSION

In this article, we have proposed an effective blockchain and cloud based mutual authentication protocol for electronic healthcare systems. The proposed CKMIB security system protects user privacy, anonymity, and is also resistance to various attacks. In the electronic healthcare system, every record is being replaced by electronic files due to the rapid advancement of technology. These electronic healthcare records contain personal information about patients, they must be kept secure. In this paper, we presented a secure CKMIB protocol based on blockchain and cloud computing technologies. The proposed protocol is secure under the random oracle model. In addition, formal security verification and validation has been performed through AVISPA using HLPSL. The proposed protocol is also more secure and has more security measures than other similar schemes in the same context. Hence, the proposed protocol is lightweight, efficient, possess less communication and computational cost as compared to the other existing authentication protocols in a similar environment. Our proposed framework opens the door to new opportunities in the future. This ECC-based authentication protocol can be used to securely transfer data for applications such as aerospace, smart vehicles, national security, the Internet of Things (IoT), wireless networks, online voting systems, and other government schemes.

REFERENCES

[1] A. Ouaddah, H. Mousannif, and A. Ait Ouahman, "Access control models in IoT: The road ahead," in *Proc. IEEE/ACS 12th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2015, pp. 1–2.

[2] 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.
[3] 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.
[4] E. A. Lee, "Cyber physical systems: Design challenges," in *Proc. 11th IEEE Int. Symp. Object Compon.-Oriented Real-Time Distrib. Comput. (ISORC)*, May 2008, pp. 363–369.
[5] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 270–282.
[6] H. Tu, N. Kumar, N. Chilamkurti, and S. Rho, "An improved authentication protocol for session initiation protocol using smart card," *Peer–Peer Netw. Appl.*, vol. 8, no. 5, pp. 903–910, Sep. 2015.
[7] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 1, p. 9994, Jan. 2014.
[8] S. A. Chaudhry, K. Mahmood, H. Naqvi, and M. K. Khan, "An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography," *J. Med. Syst.*, vol. 39, no. 11, p. 175, Nov. 2015.
[9] 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.
[10] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for WirelessBody area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332–342, Feb. 2014.
[11] K. Renuka, S. Kumari, and X. Li, "Design of a secure three-factor authentication scheme for smart healthcare," *J. Med. Syst.*, vol. 43, no. 5, p. 133, May 2019.
[12] C. Lin, D. He, X. Huang, M. Khurram Khan, and K.-K.-R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," *IEEE Access*, vol. 6, pp. 28203–28212, 2018.
[13] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, 2017, pp. 35–40.
[14] M. Tanveer, A. U. Khan, T. Nguyen, M. Ahmad, and A. Abdei-Latif, "Towards a secure and computational framework for internet of drones enabled aerial computing," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 15, 2022, doi: 10.1109/TNSE.2022.3151843.
[15] M. Tanveer, A. U. Khan, H. Shah, A. Alkhayyat, S. A. Chaudhry, and M. Ahmad, "ARAP-SG: Anonymous and reliable authentication protocol for smart grids," *IEEE Access*, vol. 9, pp. 143366–143377, 2021.
[16] A. A. Khan, V. Kumar, M. Ahmad, B. B. Gupta, M. Ahmad, and A. A. Abd El-Latif, "A secure and efficient key agreement framework for critical energy infrastructure using mobile device," *Telecommun. Syst.*, vol. 78, no. 4, pp. 539–557, Dec. 2021.
[17] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight authenticated key exchange protocol for the internet of drone environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020.
[18] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107731.
[19] T. Maitra, M. S. Obaidat, R. Amin, S. H. Islam, S. A. Chaudhry, and D. Giri, "A robust ElGamal-based password-authentication protocol using smart card for client-server communication," *Int. J. Commun. Syst.*, vol. 30, no. 11, p. e3242, Jul. 2017.
[20] N. Alexopoulos, J. Daubert, M. Muhlhauser, and S. M. Habib, "Beyond the hype: On using blockchains in trust management for authentication," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 546–553.
[21] P. Perera and V. M. Patel, "Face-based multiple user active authentication on mobile devices," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1240–1250, May 2019.
[22] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 136, Aug. 2018.
[23] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, no. 8, p. 141, Aug. 2018.
[24] H. Ma, E. X. Huang, and K.-Y. Lam, "Blockchain-based mechanism for fine-grained authorization in data crowdsourcing," *Future Gener. Comput. Syst.*, vol. 106, pp. 121–134, May 2020.
[25] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019.
[26] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.*, vol. 43, no. 1, p. 5, Jan. 2019.
[27] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 1, pp. 1419–1434, Jan. 2021.
[28] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, "Secure ECC-based three-factor mutual authentication protocol for telecare medical information system," *IEEE Access*, vol. 10, pp. 11511–11526, 2022.
[29] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *J. Med. Syst.*, vol. 44, no. 2, p. 52, Feb. 2020.
[30] S. Itoo, A. A. Khan, V. Kumar, S. Jangirala, and M. Ahmad, "Design flaws and suggested improvement of secure medical data sharing scheme based on blockchain," in *Innovative Data Communication Technologies and Application*. Coimbatore, India: Springer, 2022, pp. 823–832. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-16-7167-8_60
[31] O. O. Olakanmi and K. O. Odeyemi, "Expressible access control scheme for data sharing and collaboration in cloud-centric internet of medical things system," *J. Ambient Intell. Humanized Comput.*, pp. 1–17, 2022, doi: 10.1007/s12652-021-03572-4.
[32] K. Renuka, S. Kumari, and X. Li, "Design of a secure three-factor authentication scheme for smart healthcare," *J. Med. Syst.*, vol. 43, no. 5, p. 133, May 2019.
[33] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of secure protocol for cloud-assisted electronic health record system using blockchain," *Sensors*, vol. 20, no. 10, p. 2913, May 2020.
[34] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in *Decentralized Business Review*. 2008, p. 21260.
[35] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. Khurram Khan, "Proof of X-repute blockchain consensus protocol for IoT systems," *Comput. Secur.*, vol. 95, Aug. 2020, Art. no. 101871.
[36] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[37] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2005.
[38] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *Int. J. Commun. Syst.*, vol. 30, no. 1, p. e2933, Jan. 2017.
[39] A. A. Khan, V. Kumar, M. Ahmad, and S. Rana, "LAKAF: Lightweight authentication and key agreement framework for smart grid network," *J. Syst. Archit.*, vol. 116, Jun. 2021, Art. no. 102053.
[40] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, Mar. 2021.
[41] 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.

SAMIULLA ITOO received the master's degree in mathematics from the Department of Mathematics, Faculty of Natural Science, Jamia Millia Islamia, New Delhi, India, and the M.Phil. degree in mathematics from the Department of Mathematics, Dr. Bhimrao Ambedkar University, Agra. He is currently pursuing the Ph.D. degree with the Department of Applied Sciences and Humanities, Faculty of Engineering and Technology, Jamia Millia Islamia. He has authored or coauthored two research papers in reputed international journals and conferences. His research interests include remote user authentication protocols, design and analysis of authentication protocols using cryptography techniques, information security, and cloud computing.

AKBER ALI KHAN received the M.Sc.-Tech. degree in industrial mathematics with computer applications from the Department of Mathematics, Jamia Millia Islamia, New Delhi, India, in 2011, and the Ph.D. degree in mathematics from the Department of Applied Sciences and Humanities, Jamia Millia Islamia. He has qualified Faculty Aptitude Test (FATE-2016) in mathematical science with grade A, conducted by AKTU, Uttar Pradesh, India. He has four years five months of teaching experience with the Department of Mathematics, Al-Falah University, Dhouj, Faridabad, Haryana, India, from July 2013 to December 2017, as a Lecturer and an Assistant Professor. He has authored or coauthored of nine research papers in reputed international journals and conferences, like Elsevier/Springer/Taylor & Francis. He has also coauthored books titled *Applied Mathematics-I* and *Applied Mathematics-II* for Diploma engineering courses. His research interests include cryptography, authentication protocols for secure communications, smart grid security and privacy, V2G security and privacy, blockchain, elliptic curve cryptography, optimization, and applied mathematics. He is a Lifetime Member of MathTech Thinking Foundation (MTTF), India. He has served as a Reviewer for reputed journals, such as *Journal of Systems Architecture*, IEEE Access, and *Journal of Electrical Power and Energy Systems*.

VINOD KUMAR received the Master of Philosophy degree in mathematics from Chaudhary Charan Singh University, Meerut, India, the Master of Technology degree in computer science and data processing from IIT Kharagpur, Kharagpur, India, and the Ph.D. degree in elliptic curve cryptography (ECC)-based authentication protocols in cloud computing from the Department of Applied Sciences and Humanities, Jamia Millia Islamia, New Delhi, India. He has qualified CSIR National Eligibility Test (NET) in mathematical sciences, in 2011. In same year, he also qualified Graduate Aptitude Test in Engineering (GATE) in mathematics. He has over more than eight years of experience in teaching, research, and industry in the field of mathematics, information security, and related field. He is currently working as an Assistant Professor with the Department of Mathematics, PGDAV College, University of Delhi, New Delhi. He has supervised five M.Tech. scholars in the area of security and optimization. He has presented 25 research papers/talk in conferences/workshops. He has authored or coauthored of 31 research papers in reputed international journals and conferences, like IEEE/Elsevier/Springer/Wiley/Taylor & Francis. He has also coauthored a book titled *Elementary Real Analysis*. He is a Lifetime Member of Operational Research Society of India (ORSI), India, and MathTech Thinking Foundation (MTTF), India. He has received the Recognition/Reviewer Certificate Award from many reputed journals. He has been associated with many conferences as a TPC member and the session chair. He has served as a reviewer for many renowned journals.

AHMED ALKHAYYAT received the B.Sc. degree in electrical engineering from AL KUFA University, Najaf, Iraq, in 2007, the M.Sc. degree from the Dehradun Institute of Technology, Dehradun, India, in 2010, and the Ph.D. degree from Çankaya University, Ankara, Turkey, in 2015. He is currently the Dean of international relationship and a Manager of the word ranking at Islamic University, Najaf. His research interests include the IoT in the health-care systems, SDN, network coding, cognitive radio, efficient-energy routing algorithms and efficient-energy MAC protocol in cooperative wireless networks and wireless body area networks, as well as cross-layer designing for self-organized networks. He has contributed in organizing a several IEEE conferences, workshop, and special sessions. To serve his community, he has acted as a reviewer for several journals and conferences.

MUSHEER AHMAD received the Ph.D. degree from the Department of Mathematics, Aligarh Muslim University, Aligarh, India. He is currently working as a Professor and the Head of the Department of Applied Sciences and Humanities, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi, India. He has authored or coauthored of more than 50 research papers in reputed international journals and conferences. His research interests include group theory and its applications, graph theory, information security, support vector machine, fuzzy algebra and its applications, and soft computing. He is a reviewer of many reputed journals.

JANGIRALA SRINIVAS (Member, IEEE) received the B.Sc. and M.Sc. degrees from Kakatiya University, Warangal, India, in 2003 and 2008, respectively, the M.Tech. degree from IIT Kharagpur, Kharagpur, India, in 2011, and the Ph.D. degree from the Department of Mathematics, IIT Kharagpur, in 2017. He has worked as a Research Assistant with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He is currently working as an Associate Professor with the Jindal Global Business School, O. P. Jindal Global University, Haryana, India. His research interests include blockchain technology and applications, information security, cryptocurrency, and supplychain. He has authored 34 papers in international journals and conferences in his research areas.