IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 20, 2021, accepted June 1, 2021, date of publication June 15, 2021, date of current version July 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3089601

A Transparent and Privacy-Preserving Healthcare Platform With Novel Smart Contract for Smart Cities

ABDULLAH AL OMAR[1], ABU KAISAR JAMIL[1], AMITH KHANDAKAR[2], (Senior Member, IEEE), ABDUR RAZZAK UZZAL[3], RABEYA BOSRI[4], (Student Member, IEEE), NAFEES MANSOOR[5], (Senior Member, IEEE), AND MOHAMMAD SHAHRIAR RAHMAN[6]

[1]Department of Computer Science and Engineering, University of Asia Pacific, Dhaka 1205, Bangladesh
[2]Department of Electrical Engineering, College of Engineering, Qatar University, Doha, Qatar
[3]Shiny Gleam Software, Dhaka, Bangladesh
[4]Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong
[5]Department of Computer Science and Engineering, University of Liberal Arts Bangladesh, Dhaka 1209, Bangladesh
[6]Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh

Corresponding authors: Amith Khandakar (amitk@qu.edu.qa) and Mohammad Shahriar Rahman (msr@ieee.org)

This work was supported by the Qatar National Library.

ABSTRACT A smart city ensures quality maintenance in diverse sectors, namely citizen safety, security, healthcare, transportation, and energy. Besides, data privacy and security have become an uprising concern for Electronic Health Records (EHR) in smart cities. This is because the EHR platforms are constantly getting cyber threats from cybercriminals. On the other hand, health insurance companies offer certain specific policies that require the association of patients' financial data with EHRs. Thus, additional security concern arises as fraudulent entities can alter these insurance policies. An extra challenge is triggered as patients need to validate their identities separately while communicating with different smart healthcare entities. This is because these healthcare facilities and insurance companies ought to ensure authenticity before offering any service for an individual. Hence, we have implemented a blockchain framework to safeguard patients' personal information and insurance policy. In this paper, we propose a solution for the healthcare system that provides data privacy and transparency. Furthermore, in the proposed system, insurance policies are incorporated in blockchain via the Ethereum platform and data privacy is shielded with cryptographic tools.

INDEX TERMS Healthcare data, privacy, smart city, transparency, insurance policy.

I. INTRODUCTION

In order to improve the efficiency of fitness, travel, resources, education, and public infrastructure, smart cities use numerous innovations, resulting in a upper level of comfort for their citizens [7]. The main focus of developing a smart city is to improve the quality of life of its citizens. The components of a smart city are categorized as electronic health monitoring systems, electronic health care, automated traffic management system, intelligent transport, etc. Among them, to achieve the goals of a smart city, smart healthcare plays an important role. The key starting point is likely to have EHR [29] to build smart healthcare. EHR is a collection of a patients' health history in a digital format. The medical history includes diagnostic reports, treatment plans, radiology images, medications, laboratory, test results, insurance policy etc. The doctor has the information of the patients visiting him/her. Doctors require the patient sign a document confirming their understanding of their privacy policy, but they are not concerned about maintaining these data [8]. However, EHR solved the issue as its a digital format of patients' medical history. In recent years, cyber attackers are becoming interested in EHR. EHR, patients' personal informations, and social security numbers are highly valuable, and cyber attackers sell these to counterfeiter on the open market for profit [21]. We have heard of many well-known violations in which patient data has been stolen or lost [9], [23], [30]. Therefore, data privacy and security issues of the EHR system and personal health data are gaining attention day by day in smart cities.

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

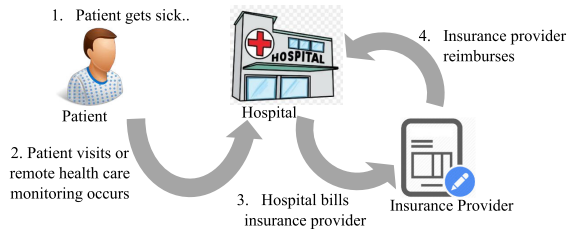

FIGURE 1. Interaction between patient, hospital, and insurance company.

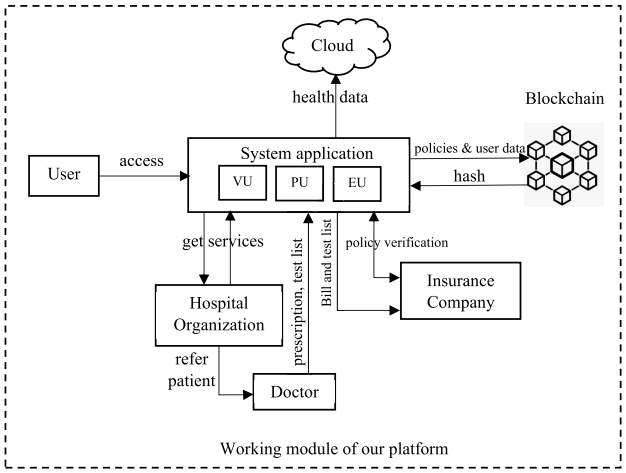

FIGURE 2. An application of our platform.

In healthcare, data is being generated speedily as users are getting interested to smart healthcare for their better living in a smart city. For future analysis or forecast, these personal healthcare data (e.g., diagnostic reports, test lists, prescriptions, etc.) are becoming importance to researchers day by day as these healthcare data can be used in different ways [41]. These healthcare data are something eavesdroppers or intruders look for. Failure to preserve these healthcare data can have serious financial and legal ramifications, and healthcare of smart cities can be affected. Therefore, the challenge is to preserve or store these healthcare data securely for future analysis or forecast and user access. Citizens of a smart city have to pay annually a considerable amount of money to health insurance companies for various forms of insurances, such as medical, dental, and vision [40]. However, if the insurance policies are not transparent to and accessible by the patients, fraud activities can be happened by taking the chances and altering the insurance policies to its advantage.

Integrating blockchain with cloud computing, researchers are working to secure patients' health data. In recent years, the convenience of cloud computing has been getting the importance to the healthcare domain [1]. Cloud computing has shown tremendous potential for enhancing communication between various healthcare entities and meeting common requirements, such as agility, cost efficiency and availability [39]. Patients can preserve their healthcare data (e.g., diagnostic reports, test lists prescriptions, etc.), and even they can share their healthcare data with others (e.g., doctors, researchers, stakeholders, third parties, etc.) with the help of cloud computing [14]. To ensure security in the patients' healthcare data, researchers have proposed several solutions. However, in the previous works, there is no such mechanism to provide transparency in the insurance policy while keeping patients' healthcare data secure. Figure 1 shows the general interaction between a patient, hospital, and insurance company. In recent days, transparency in insurance policy is a very concerning problem, as there is still chances for fraud activities. Even users do not know where their policy data are stored. Therefore, patients are losing their trust in the insurance companies [22]. Reliable insurance companies, on the other hand, are struggling to proof themselves to their patients to gain their trusts. To cover the patient's financial costs, insurance company has to know patients' medical test history. Sometimes insurance company fails to know the actual test history for which any claim can be rejected by the insurance company [18]. Nevertheless, there is no single platform where citizens of a smart city can preserve their diagnostic reports, while keeping their insurance policies transparent.

Figure 2 depicts our platform's basic working module which ensures patients' insurance policies transparent to them. Besides, patients can store their healthcare data (e.g., diagnostic reports, test lists prescriptions, etc.) in an encrypted form into cloud. As a result, our platform ensures the privacy of patients' personal health data.

Our Contribution: In this paper, we are presenting a platform incorporating blockchain which attempts to cover most concerning issue of smart cities. The main concept of our work is to keep patients' insurance policy transparent to them. Through the blockchain, our system ensures transparent policy management for EHR in smart cities, and at the same the user can easily store their healthcare data (e.g., diagnostic reports, prescriptions, etc) into the cloud. As the test history of a patient is shared with the insurance company through our platform, insurance company can ensure about the claims for coverage.

Paper Organization: The remainder of the paper is structured as follows: Related work is described in Section II, preliminaries is discussed in Section III. Section IV explains our proposed platform. We describe the protocol construction in Section V. The security analysis of our platform has been briefed in Section VI. In section VII, we evaluate the proposed platform. Section VIII explains property comparison between proposed platform and other related platforms. Lastly, conclusion is included in Section IX.

II. RELATED WORK

To guarantee security with the help of blockchain technology in today's IoT based smart healthcare system, security research communities are developing and making a solution efficient. As blockchain has decentralized characteristic, immutability, and cryptographic security, researchers are trying to guarantee safety in EHR with the advantage

of blockchain. While there are still ways of enhancing the techniques and developing a platform in the EHR platforms to guarantee various safety factors (e.g. insurance policy).

Makhdoom *et al.* [25] addressed the security of Internet-of-Things(IoT) devices in a smart city. They proposed a blockchain-based advanced framework named PrivySharing for handling the privacy and security of IoT data in a smart city area. The proposed system assures that critical user healthcare data is protected and safely stored. They added a reward system called PrivyCoin for data owners sharing their healthcare data with the third parties on the need basis. Moreover, the rules to determine the third parties with whom user wants to share the data through smart contracts depends on users.

A framework named SpeedyChain for a smart city environment is presented in [26]. Their proposed framework is for sharing user data based on blockchain technology. They came up with real-time applications solution to minimize the Transaction (TX) settlement time. In addition, they focused the privacy of its user.

In [33], authors presented a combined network architecture focused on Software Defined Networking (SDN) and blockchain for a smart city. Smart city issues such as high TX latency, security and privacy, bandwidth bottlenecks, and specifications needed for high computing resources have been addressed by the architecture they presented in their paper. They divided their architecture into two categories: the core network and the edge network in order to achieve competency and solve the existing limitations.

Several platforms have been proposed in [3]–[5], [10], [11], [15], [16], [28], [31], to address the privacy and security issues of the healthcare system in a smart city. To handle health issues such as blood pressure (BP), hemoglobin (HB), blood sugar, and abnormal cellular growth, they have proposed an efficient health monitoring system. In their experiments, several researchers have proposed the Body Sensor Network (BSN), and proposed a secured healthcare system, focusing on the various types of technology used for the healthcare system in a smart city. Different strategies have been proposed to interact with various types of needs of patients, suppliers, and third parties in the healthcare system. Dagher *et al.* [15] addressed a blockchain-based solution to focus on ownership and control the EHR of the patients. The proposed platform named Ancile utilized six types of smart contracts for operation such as Classification, Service History, Ownership, Consensus, Permissions, and Re-encryption.

The study conducted in [24] presented an approach to give patients access control to their medical data. They proposed two ethereum smart contracts ensuring the security, immutibility, traceability, and transparency. They mentioned seven types of entities: Regulatory Agency, Hospital, Patient, Doctor, Trusted Re-encryption Oracles, Decentralized Database Storage, Insurance for their proposed solution. The key focus of their work was to ensure decentralized access control over patients' medical records interacting with different entities. They used interplanetary file systems(IPFS) as decentralized database storage and trusted oracles to perform operations related to patients' medical records.

Authors of [37] introduced a conceptual framework named Smart Medical System (SMS) that provides privacy-preserved data collection, storing, and processing for a smart city heathcare system. They used the concept of blockchain technology to protect the medical and personal data from frauds, which are generated continuously from IoT devices and sensors. They connected several hospital organizations to facilitate personal health data sharing incorporating blockchain technology. The proposed architecture ensures real-time monitoring of a patient's health condition and notifies the health status to doctors and healthcare providers.

Chakraborty *et al.* [13] discussed about the security of healthcare data and the maintenance of trust between the citizens and stakeholders of a smart city. In order to share and collaborate healthcare data securely integrating blockchain technology with machine learning, they proposed a solution that communicates with various entities(patient, doctor, healthcare providers, and health insurance companies).

The advantages of blockchain technology to assist the modification of patient data exchange was discussed in [17]. The authors claimed to provide the transparency, the blockchain technology can be used between various third parties over the state of shared data and related transactions. They used permission-based blockchain to share the individual healthcare data of the user, minimizing the cost of authentication of transactions and data integrity compared to conventional systems.

Some of the related studies have been mentioned above. The above-mentioned healthcare data management systems have only attempted to address health data security and privacy issues. However, transparency issue of insurance policy are missing on those studies which is a very concerning issue. Therefore, we are proposing a platform addressing both the issues for EHR platform. The rest of the paper will describe our platform in detail.

A. BLOCKCHAIN SYSTEM

Blockchain is a modern concept to store data and this data stored in blocks. Blockchain is quite innovative because it helps us to keep track of almost everything we can think of (property rights, identities, money balances, health records) while reducing the risk of data tampering. References [19]. Blockchain networks are classified into public blockchain, private blockchain, and consortium blockchain based on user access restrictions. There are various advantages of blockchain:

1) Decentralized: None of the individuals or organizations play as an intermediary role in the transactions. Each connection in the blockchain network has an identical copy of the ledger.
2) Immutability: After a transaction has added to the ledger, no one can alter it with a transaction.

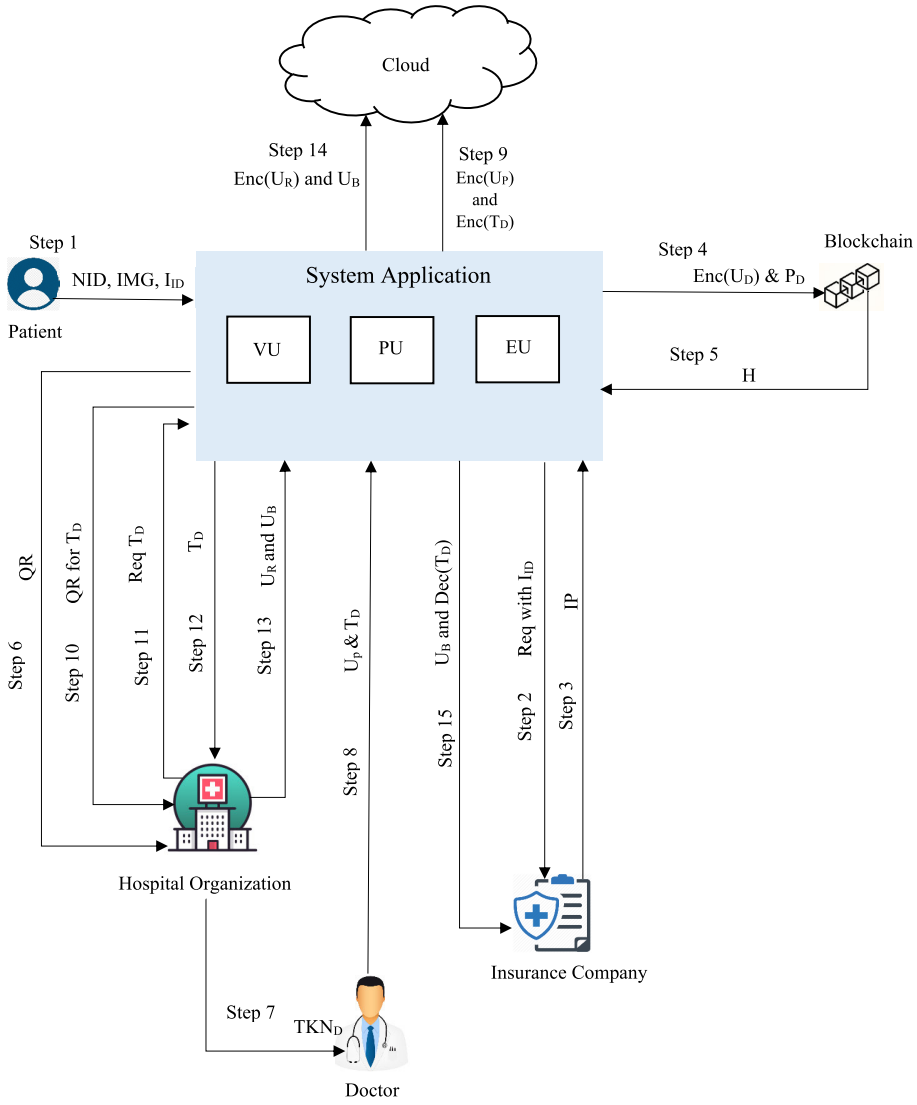

FIGURE 3. A healthcare platform for smart cities.

3) Transparency: Blockchain is basically a transparency machine in which any one can access the network and therefore view all of the records on it.

Therefore, several platforms [6], [12], [36] are using blockchain as a backbone in their works. We are also using blockchain in our platform to store our user's personal data and insurance policy. Figure 4 shows the structural view of blocks in blockchain. In the figure, each block contains timestamp, previous block hash, current block hash and block data. Each block is chained with its previous block as it contains the hash of previous block in itself. Satoshi Nakamoto developed the first blockchain Nakamoto and Bitcoin [27]. The success of blockchain is due to its decentralised characteristics in storing transactions without any third parties [34]. These transactions are stored on the blockchain with the help of smart contract [4]. Smart contract is a contract of rules that regulates transactions, and it is preserved on the blockchain

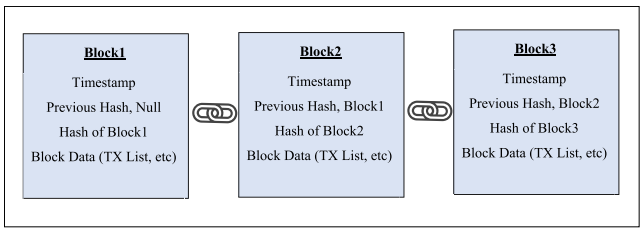

FIGURE 4. Structural view of Blocks in Blockchain.

and executed as part of the transaction. To validate transactions on a blockchain, Proof-of-Work (PoW) and Proof-of-Stake (PoS) are used as key methods [10].

B. SMART CONTRACT

In 1994, Szabo [35] first proposed smart contracts as a digital transaction that carry out the terms of a contract. Smart

contract is considered as a self-executing contract that can be used to execute any task through a blockchain network. Smart contracts remove the need for a central authority or an external regulatory mechanism to carry out trustworthy transactions and agreements between disparate, anonymous parties. In smart contract, all the terms and conditions of an agreement are written into code. When users go through any transaction, this code is executed [32]. Programmers write this code using Solidity programming language to implement the smart contract on the Ethereum blockchain platform. After writing the code, programmers use the EVM(Ethereum virtual machine) bytecode to compile the contract. EVM bytecode is a low-level programming language generated by compiling a high-level programming language like Solidity. Once compiled, it will be executed and deployed on the ethereum blockchain [38].

C. ETHEREUM

Ethereum is a public blockchain-based computing platform that allows programmers to develop decentralized applications through smart contracts [24]. Ethereum and bitcoin are close in that they are both decentralized permissionless blockchain networks [2]. However, there exist few differences according to their purpose and capacities. To use the ethereum network, users need to pay a fee. The amount of fees that must be charged to the network in order to execute a smart contract is measured using Gas. Gas costs are expressed in gwei, which are small fractions of ether. On the ethereum blockchain, Ether or ETH is used as its own cryptocurrency. Moreover, there are two type of accounts available on ethereum: an externally owned account (EOA) and a contract account (CA). These two types account are identified by 20-bytes addresses. An EOA can initiate any change regarding the state of the Ethereum blockchain. To interact with the code of any given CA, a transaction from an EOA is has to be initiated with the input parameters required for the CA code execution.

III. PRELIMINARIES

In this, we first briefly discussed each properties (e.g., privacy, security and integrity) that our protocol achieved. After that, we introduced the cryptographic tools of our protocol.

The notations used in this paper are listed in table 1.

A. PROPERTIES

1) SECURITY AND PRIVACY

This system's key points are integrity, stability, and privacy. Key points of security and privacy are brie?y described below:

1) Integrity: Only authenticated users are able to store their personal health data to our platform.
2) Privacy: Verification Unit of our platform will guarantee the privacy of users, and Encryption Unit will provide the privacy too.

TABLE 1. Terminology table.

Notation	Description
ID	ID of the patient
PW_{D}	Password of the patient
IMG	An instant image of the patient
U_{D}	Patient info data
P_{D}	Insurance Policy data
H	Hash of stored patient data
U_{R}	Diagnostic report of patient
U_{P}	Prescription of patient
T_{D}	Test list data
TKN_{D}	Token Data
U_{B}	Patient's bill
I_{ID}	Patients' insurance card
IP	Insurance Policy
VU	Verification unit
EU	Encryption and decryption unit
PU	Policy management unit
BC	Blockchain
EC	Election Commission
HO	Health Organization

3) Security: User will store their healthcare data as encrypted form in the system which assures secured environment for them.

B. CRYPTOGRAPHIC TOOLS

In this section, we discuss about Elliptic Curve Cryptography (ECC) [20] encryption scheme. We used ECC as the cryptographic tool to ensure proper cryptographic functionality of our platform. Definition of ECC is given below.

Definition 1: Elliptical Curve Cryptography (ECC) is a public key encryption algorithm. It uses trapdoor function for encryption. Trapdoor means if we compute Y from X then it is impossible to generate X from Y.

$$X \xrightarrow{trapdoor} Y \tag{1}$$

$$X \nleftarrow Y \tag{2}$$

ECC is focused on elliptic curve concept which is used to generate smaller, faster and more efficient cryptographic keys. An elliptical curve can be simply created as a set of points defined by the following equation:

$$y^2 = x^3 + ax + b \tag{3}$$

Here, the values of a and b will determine the shape of the curve. These curves are used over finite fields to generate a secret that only the private key holder is able to unlock. The larger the key size, the larger the curve, and the harder the problem is to solve.

1) ENCRYPTION SCHEME

Let, $\mathbb{E}_{\mathrm{p}}$(a,b) be the elliptic curve with parameters a, b and p, where p is a prime or an integer of the form 2^m. $\mathbb{G}$ is a point whose order is large value n.

Let, the Message be $\mathcal{M}$. First, encode this $\mathcal{M}$ into a point $\mathrm{P_m}$ on the elliptic curve.

Sender A and receiver B select a private key respectively $n_A < n$ and $n_B < n$. Therefore, public key respectively $P_A = n_A\mathbb{G}$ and $P_B = n_B\mathbb{G}$.

Ciphertext point, $C_m = \{ \mathcal{K}\mathbb{G}, P_m + \mathcal{K}P_B \}$

Here, $\mathcal{K}$ is a random positive integer number.

2) DECRYPTION SCHEME

To decrypt the cipher text, receiver B multiplies the first point by private key n_B and then subtracts the result from the second point.

Plaintext point $= P_m + \mathcal{K}n_B\mathbb{G}$ - $n_B\mathcal{K}\mathbb{G} = P_m$

IV. PROPOSED PLATFORM

A. OVERVIEW OF OUR PLATFORM

Our proposed platform provides a blockchain-based solution for smart cities that keeps user's *IP* transparent to her while also allowing to store her U_R, U_P, and U_D into the cloud for future access. We introduce seven entities in our platform, named patient, system application, *HO*, doctor, insurance company, cloud, and *BC*.

In this, the whole system application is devided into three units: *VU*, *PU*, *EU* which interact with patient, *HO*, doctor, insurance company, cloud, and *BC*. Initially, a new user have to share the required credentials to get registered in our system. Here, user registration process is performed by *VU*. *VU* verifies all the provided credentials from *EC* database and insurance company, and takes *IMG* to authenticate the user. By checking whether it is licensed or not, another entity *HO* will be authenticated from the government health service database. This verification process makes sure that only the authenticated *HO* is allowed to interact with our system. *EU* performs the encryption and decryption process for our system. U_P, T_D, and U_R will be stored in an encrypted form into cloud. All the personal information of user including *IP* are stored into *BC*. As the user's confidential details will be kept in an encrypted form, the risk of data tampering is ignorable. *IP* will be kept in plaintext form as it is a public data.

As shown in Figure 3, we have designed the high level view of our proposed platform and interactions with different entities. All the entities and their functions are brie?y described below.

- **Patient:** Patient is the user who will use our platform to receive care from any *HO* in the smart city. Patient shares her *IP* with our platform to make it transparent to all after proper verification. Patient can interact with *HO* and after that store her U_R into cloud. To connect, a patient have to go through a registration process for ensuring her authenticity.
- **System Application:** System Application plays an intermediary role of our platform. Patient will interact with other entities such as *HO*, health insurance company, cloud, *BC* through the system application. We divided the whole system application into three-units: *VU*, *PU*, and *EU*. All the provided credentials of patient will be verified through *VU* interacting with *EC* database. User's *IP* is managed by *PU* interacting with the insurance company. All the encryption and decryption mechanism of our platform are performed by *EU*. We are using Elliptic Curve Cryptography (ECC) as the cryptographic tool to ensure proper cryptographic functionality for our user.
- **EC Database:** Interacting with *EC* Database, we verfify the NID information that patient shares while registering into our platform.
- **Insurance Company:** To make the *IP* transparent, user's *IP* needs to be retrieved from the insurance company only after verifying I_{ID} information. A large number of trusted insurance companies lose the confidence of their patients for a few fraudulent companies. By joining our platform, insurance companies can regain user confidence.
- **Hospital Organization:** *HO* is an entity of our platform where user visits for her treatment. *HO* interacts with system application after the registration process is done. When a patient will visit *HO*, U_D of the patient will be shared with *HO* simply by scanning the patients' QR code. After the treatment, *HO* sends T_D, U_P, U_R and U_B to the system application.
- **Blockchain:** *BC* is the main entity in this platform, and we are using the ethereum network. Our platform will have one node, which will perform all the *BC* transactions. In this platform, we are keeping two kinds of data into *BC*. First, the U_D which will be stored as encrypted data after the verification by the *VU*. Second, the P_D will be stored into *BC*. *PU* verifies the *IP* from insurance company before storing it. After every transaction, our platform will provide the transaction ID to the user which will be returned from *BC*. By using the transaction ID, patient can check her P_D.
- **Cloud:** In this platform, cloud acts as the off-chain storage. U_R, U_P and T_D will be kept into cloud in encrypted form for further access. Another data of user U_B will also be stored on the cloud which will be shared with the insurance company in future.

1) STEPS IN OUR PLATFORM

Steps that are involved in our proposed platform from Figure 3 are given below.

- Step 1: User gets registered with NID, *IMG*, and I_{ID} information and accesses the platform with *ID*, PW_D and *H*.
- Step 2: I_{ID} information is sent to insurance company for verification.
- Step 3: *IP* is retrieved from insurance company.
- Step 4: $Enc(U_D)$ & P_D are stored into blockchain.
- Step 5: *H* is sent to system application.
- Step 6: QR code is sent to the *HO* for sharing user's information.
- Step 7: *HO* sends TKN_D to doctor.

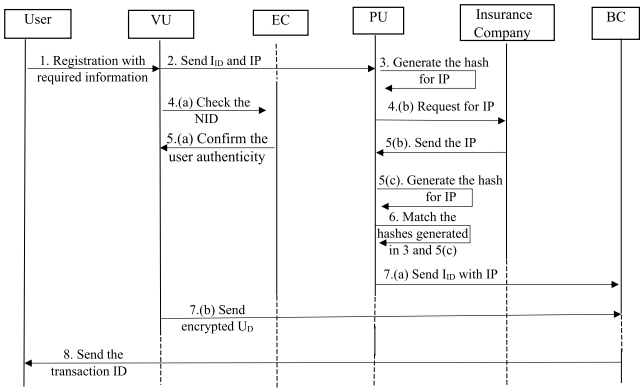

FIGURE 5. User verification and insurance policy management (On-chain storage).

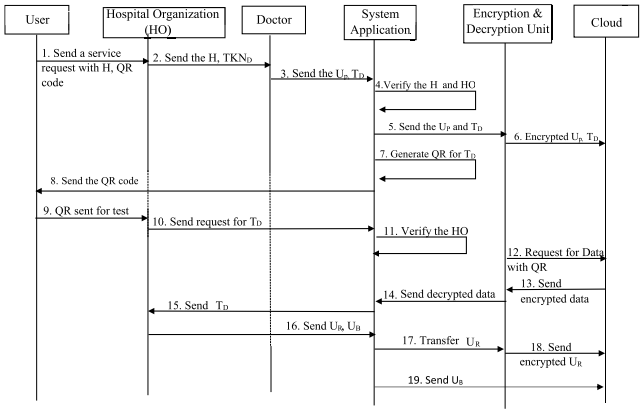

FIGURE 6. User interaction and off-chain storage.

- Step 8: Doctor sends patient's U_P & T_D to System Application.
- Step 9: $Enc(U_P)$ & $Enc(T_D)$ are stored on the cloud and a QR code is generated for T_D.
- Step 10: QR code is sent to the *HO* to get the T_D.
- Step 11: *HO* sends request for retrieving T_D.
- Step 12: T_D is retrieved.
- Step 13: When U_R is ready, the U_R & U_B are sent to System Application.
- Step 14: $Enc(U_R)$ & U_B are stored on the cloud.
- Step 15. $Dec(T_D)$ & U_B is sent to insurance company.

B. PLATFORM ANALYSIS

1) USER VERIFICATION AND POLICY MANAGEMENT

Figure 5 demonstrates the low-level view of user verification and insurance policy management of our platform. The user registers with the system through the *VU*. First, the user verification process begins with submitting the required credentials (NID number, *IMG*, insurance card number, insurance Policy document) to *VU*. *VU* transfers the user's I_{ID} and *IP* to the *PU* for generating a hash from the insurance policy document. Basically, our platform handles the patient verification in two ways. Firstly, the *VU* checks the NID from the *EC* to verify the authenticity of the user. Secondly, *PU* sends a request for *IP* to the insurance company along with the user's I_{ID} information. *EC* ensures the user information, and the insurance company sends the policy document. Now, *PU* generates another hash from the provided policy document by the insurance company. If the two hashes are found same that ensures, the insurance company did not alter the user's *IP*. If a single bit of the policy document has changed then it will generate a different hash for that, which will not match with the previous generated hash (generated from the user provided *IP*). *VU* stores the *IP* into *BC* along with the encrypted U_D, when the hash matches.

2) DATA TRANSACTION IN OUR PLATFORM

Figure 6 demonstrates the low-level view of how a user uses services from our platform and how user data is stored on the cloud. A patient who is a registered user of our platform, can visit *HO* (*HO* is also connected with this system) to get services. To get the services from *HO*, user shares her U_D with *HO* by providing her QR code and *H*. By scanning the QR code, *HO* retrieves the data and creates a TKN_D for patient and transfers it to the doctor. Doctor interacts with the system application by sending the U_P and T_D. The system application verifies the *HO* and allows the data to be stored after the encryption process. For future uses, the system application generates a QR code from the T_D data and sends it to the user. Now, a user can go to the *HO* for testing with the QR code. *HO* retrieves T_D from system application, whenever user sends the QR code of T_D. System application verifies the request and sends the data to *HO* in decrypted form. When the U_R and U_B are ready, the *HO* sends the data to system application. After that, system application stores encrypted U_R into cloud. As the U_B will be shared later with insurance company, it is stored as plaintext into cloud.

V. PROTOCOL CONSTRUCTION

A. USER VERIFICATION

Algorithm-1 is essential for user verification. To use our platform, patient needs to be verified with the help of National Identification Number. If the N_{id} and *IMG* which are provided by the user don't belong to D_{ec} then the algorithm will return verification failed. If the system operator has the Ethereum Wallet then the system operator will able to send δ to Blockchain. By using *block.Number()* function, the B_{id} will be retrieved which will be used in next step to retrieve *H*. This *H* will be used in future when patient will login to the system.

B. PRESCRIPTION AND TEST DATA UPLOAD

Algorithm-2 is used for uploading data. This algorithm will be executed after fulfilling few conditions. If H_m and H_i are same and β_i and β_m are same then it will be allowed to upload the prescription and test list data to cloud.

There will be two data sets, one is for prescription data(γ_1) and another one is for test list data(γ_2). The data will be stored

Algorithm 1 User Verification

Input: $N_{id}, IMG, B_{id}, D_{ec}, H$
Output: H
$N_{id} = National\ identification\ number$
$IMG = An\ instant\ image\ of\ user$
$B_{id} = Blocknumber$
$D_{ec} = Database\ of\ Election\ Commission$
$H = Hash\ of\ the\ block$
$W_{operator} = Ethereum\ Wallet\ of\ system\ Operator$
$\delta = User\ information\ and\ insurance\ policy$
1: **if** N_{id} && $IMG \in D_{ec}$ **then**
2: $W_{operator} \xrightarrow{\delta} BC$
{ User data is sent to the blockchain }
3: $B_{id} \longleftarrow block.Number()$
{ Retrieve the block number }
4: $H \longleftarrow block.hash(B_{id})$
{ Retrieve the hash of the block }
5: **return** H
6: **else**
7: **return** Verification failed
8: **end if**

in the following way:

$$data = \sum_{n=1}^{2} \gamma_n \tag{4}$$

Line-3 shows that n=2 number of individual dataset from an individual patient simultaneously.

In the loop, data will be assigned to its corresponding dataset in line- 5 and then the data will be stored into the cloud.

VI. SECURITY ANALYSIS

Our protocols are described in this section in terms of security parameters.

Authentication: In our platform, we handle authentication for our user and stakeholders(*HO*, Insurance company). User authentication starts when she provides respective registration details(NID information, *IMG*, I_{ID}) to *VU*. Primarily, *VU* transfers the I_{ID} to *PU* to validate the provided information and to retrieve the *IP* from insurance company. After that insurance company sends the confirmation with the *IP* of that user. Besides, *VU* verifies the NID information from the *EC* database and matches *IMG* with the user's NID image using machine learning technology which operates the highest security. By verifying the provided data, only authenticated users are permitted to use our platform.

HO, which is an another entity of our platform, must provide the information required for validation. The information provided will be sent to the government's health services database and will check whether it is recorded by the government or not. Only the authenticated *HO* is allowed to interact with our platform after this verification.

Algorithm 2 Prescription and Test Data Upload

Input: $H_m, H_i, \beta_m, \beta_i, \gamma_1, \gamma_2,$
Output: *Prescription and Test Data Upload*
$H_m = Set\ of\ all\ identical\ hashes$
$H_i = Hash\ of\ the\ patient$
$\beta_m = Set\ of\ all\ hospital\ address$
$\beta_i = Address\ of\ Doctor's\ hospital$
$\gamma_1 = Prescription\ Data$
$\gamma_2 = Test\ List\ Data$
1: *Data* [] *data*
2: *bool* $\longleftarrow$ 0
3: **while** $\underline{n}$ **do**
4: **if** $H_i \in H_m$ && $\beta_i \in \beta_m$ **then**
5: $data = \sum_{n=1}^{2} \gamma_n$
6: *bool* $\longleftarrow$ 1
7: **return** bool
8: **else**
9: **return** bool
10: **end if**
11: **end while**
12: **if** *bool* == 1 **then**
13: **return** "Data is uploaded successfully"
14: **else**
15: **return** "Failed to upload data"
16: **end if**

Authorization: BC performs the patient authorization. *BC* generates *H* for each user after storing U_D and P_D to *BC*. When user tries to access our platform, she will have to submit the *H* along with *ID*, PW_D. User is granted to access our platform if only the submitted *H* belongs to our all generated hashes. Therefore, our proposed architecture ensures that no unregistered patients can be connected to our architecture.

Privacy: In this platform, *VU* will ensure the privacy of the user. We are using cryptographic tools to encrypt data which will provide the privacy too.

Integrity:

- **Access data integrity:** User who wants to access our platform, she has to authenticate herself primarily. This access request will need correct *ID*, PW_D and *H* which will be generated in the registration process and will be kept to our system. Therefore, no one can access our platform without the correct *ID*, PW_D and *H*. By which our platform ensures the access data integrity.
- **User Data integrity:** User's Enc(U_D) and P_D are stored into *BC* which ensure the data integrity. As the *IP* is stored into the *BC*, the *IP* is transparent to all. No one can alter the user's *IP* as *BC* has the properties such as immutability, transparency etc. With the use of encryption function below, U_R, U_P and T_D are stored in encrypted form into cloud.

$$Enc(Key, Data) = Enc(U_R)$$
$$Enc(Key, Data) = Enc(U_P)$$

$$Enc(Key, Data) = Enc(T_D)$$
$$Enc(Key, Data) = Enc(U_D)$$

In case to share data, system applications retrieves data from cloud and performs decryption operation using the following function.

$$Dec(key, Enc(U_R)) = plaintext$$
$$Dec(key, Enc(U_P)) = plaintext$$
$$Dec(key, Enc(T_D)) = plaintext$$
$$Dec(key, Enc(U_D)) = plaintext$$

To breach this integrity standard, attackers must breach the protection of the underlying encryption scheme, ECC.

Security: Our platform provides the security by keeping the U_R, U_P, T_D into the cloud. As EU performs the encryption process and stores U_R, U_P, T_D into cloud in encrypted form, these cannot be accessed without the encryption key.

VII. EMPIRICAL STUDY

We simulate our proposed platform in this section to assess the feasibility through graph and description.

Experimental Setup: To evaluate the effectiveness and performance efficiency of our protocol, we setup an environment by using the following configurations:

- Intel(R) Core(TM) i5-7200U 2.50GHz
- 8.00GB of RAM, Windows 10 (64-bit) OS

In our evaluation, we have written the programs by using languages: Solidity, Web3.js, HTML and CSS. Software: atom, browser, Remix-Ethereum IDE to write the smart contract using solidity language to form a simulated Ethereum network locally. Wi-Fi connection is required in the setup.

A. Gas CONSUMED FOR TRANSACTION

Gas refers to the amount of computational effort required to perform such operations in ethereum blockchain network. Here, we have measured the Gas consumed to execute transactions of varying input sizes. Figure 7 shows an overview of the Gas used for each transaction occurs in our system. The time has been measured in milliseconds while the input size has been measured in kilobytes (KB). From the resultant graph, we notice a linear pattern from 2kb to 13kb input data. As a result, with the increase size of input data, Gas increases.

B. LATENCY TIME OF OUR PLATFORM

In terms of time, latency is the difference between the time it takes to deploy a transaction and the time it takes to complete it. To determine the performance of our proposed system, we have evaluated the latency (speed) in our empirical study. Here, we have considered the latency to be the total time taken for making a transaction successful. Figure 8 shows the results of the latency observations of our proposed system. The time has been measured in milliseconds while the input size has been taken in kilobytes (KB). We have noticed that the time increases with the input data from 2kb to 11kb but suddenly decreases for input 13kb. For 11kb input data, it has taken the highest time due to inconsistencies in the testing environment.

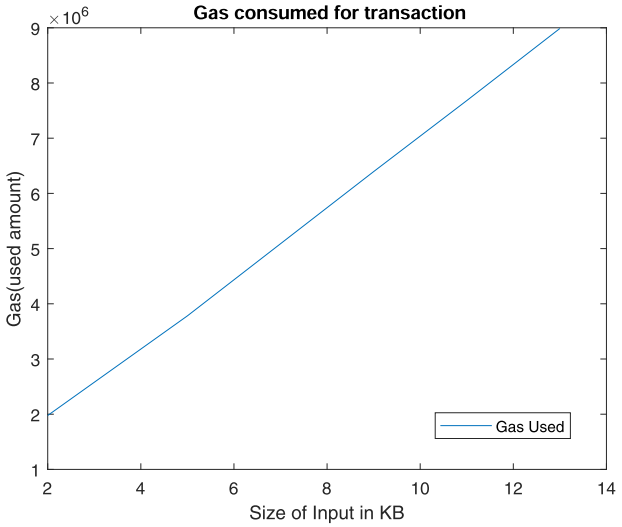

FIGURE 7. Gas used during transaction in blockchain.

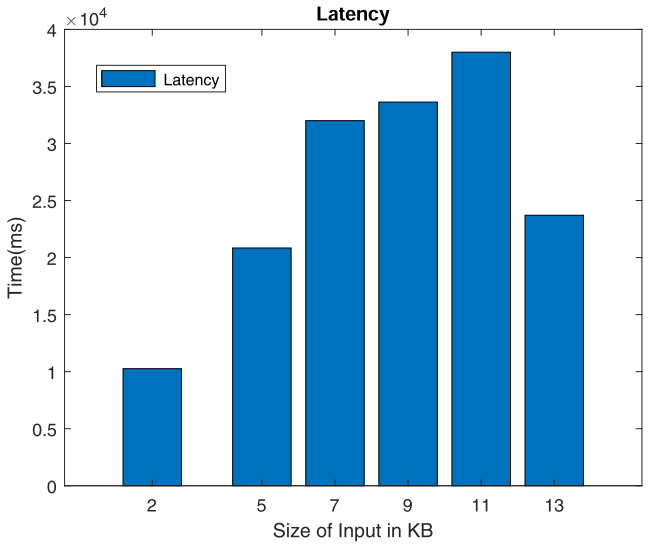

FIGURE 8. Latency time of our platform.

C. INPUT GENERATION VS OUTPUT RETRIEVAL TIME OF SYSTEM

In Figure 9, we perform a comparative evaluation of the time taken by the system to encrypt and decrypt user data. The size of the data can vary for different users. The input size has been measured in kilobytes (KB) while the time has been measured in milliseconds. From the resultant graph, we have noticed both curves showed a similar pattern. The time required to generate input data and to retrieve output data of size 2kb to 7kb have increased similarly. Suddenly, both curves have been found to be low for 9kb data. The highest time taken to generate input data has been found almost 1930ms where it

TABLE 2. Comparison table.

Metric	Gaby G Dagher et al. [15]	Gautami et al. [37]	Xiaochen et al. [41]	William et al. [17]	Our architecture
User Centric	Y	N	Y	Y	Y
User Authentication	N	N	N	N	Y
Privacy of data owner	Y	Y	Y	Y	Y
Store personal data into blockchain	N	N	N	N	Y
Transparent policy	N	N	N	N	Y
Use of cryptographic functions	N	Y	Y	N	Y
Blockchain based	Y	Y	Y	Y	Y

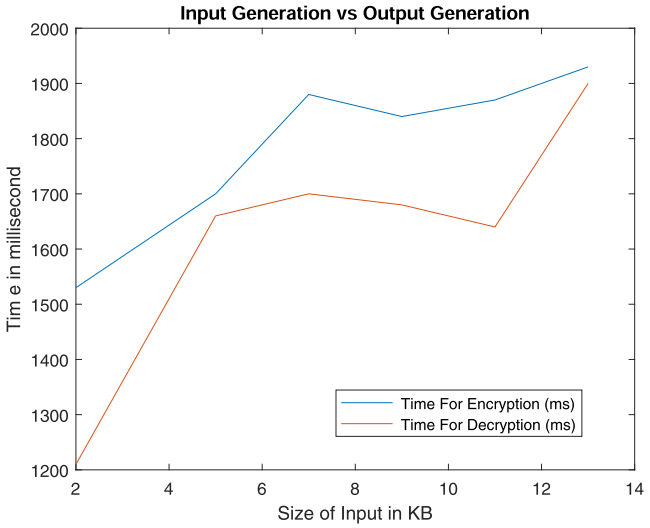

FIGURE 9. Input vs Output generation time of our platform.

has taken 1900ms for output generation. With the increase of input size both time increase where encryption requires more time than decryption.

VIII. COMPARISON BETWEEN OUR ARCHITECTURE AND THE RELATED WORKS

This section shows the results in all seven properties/metrics of the architecture. We marked it with 'Y' if a particular architecture holds the property, if not marked with 'N'. At this point, we compares our architecture with other existing architectures in table 2. With the careful comparison of the proposed systems and in account of the important seven properties/metrics of blockchain based transparent healthcare systems, it can be concluded that our proposed architecture has more advantages than the other systems in this table.

IX. CONCLUSION

In this paper, we presented a transparent and privacy preserving healthcare platform for smart cities. Every year citizens of smart cities pay a considerable amount of fee to insurance company against specific insurance policies for their health safety. The proposed platform ensures the transparency of insurance policy to the patients by preserving the insurance policies into the blockchain. We presented seven entities: patient, system application, EC database, insurance company, hospital organization, blockchain, and cloud for our proposed platform. Patients can share their test lists to claim for coverage to insurance company through our platform. Patients can also preserve healthcare data (i.e., diagnostic report, prescription, user bill and test list) securely in the cloud, and their identity information in the blockchain. We also presented algorithms along with their implementation and details. Finally, the implementation and evaluation indicate the practicability and effectiveness of our proposed platform.

In future, we plan to perform data aggregation on the stored user prescription. This is very useful this time as from the result of data aggregation, any prediction can be given regarding the health condition of a population. During this COVID-19 situation, it can put a value to give any prediction about the affected area.

ACKNOWLEDGMENT

The authors would like to thank the University of Asia Pacific, Bangladesh for technical resource-related assistance. This article was presented at the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020). *(Abdullah Al Omar and Abu Kaisar Jamil contributed equally to this work.)*

REFERENCES

[1] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 4, pp. 1431–1441, Jul. 2014.

[2] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.

[3] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Guangzhou, China: Springer, 2017, pp. 534–543.

[4] A. A. Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.

[5] A. Al Omar, A. K. Jamil, M. S. H. Nur, M. M. Hasan, R. Bosri, M. Z. A. Bhuiyan, and M. S. Rahman, "Towards a transparent and privacy-preserving healthcare platform with blockchain for smart cities," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1291–1296.

[6] A. Al Omar, R. Bosri, M. S. Rahman, N. Begum, and M. Z. A. Bhuiyan, "Towards privacy-preserving recommender system with blockchains," in *Proc. Int. Conf. Dependability Sensor, Cloud, Big Data Syst. Appl.* Guangzhou, China: Springer, 2019, pp. 106–118.

[7] T. Alam, M. A. Khan, N. K. Gharaibeh, and M. K. Gharaibeh, "Big data for smart cities: A case study of Neom City, Saudi Arabia," in *Smart Cities: A Data Analytics Perspective*. Saudi Arabia: Springer, 2021, pp. 215–230.
[8] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and big data to transform the healthcare," in *Proc. Int. Conf. Data Process. Appl. (ICDPA)*, 2018, pp. 62–68.
[9] M. Z. A. Bhuiyan, M. Zaman, G. Wang, T. Wang, and J. Wu, "Privacy-protected data collection in wireless medical sensor networks," in *Proc. Int. Conf. Netw., Archit., Storage (NAS)*, Aug. 2017, pp. 1–2.
[10] R. Bosri, M. S. Rahman, M. Z. A. Bhuiyan, and A. A. Omar, "Integrating blockchain with artificial intelligence for privacy-preserving in recommender systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Oct. 14, 2020, doi: 10.1109/TNSE.2020.3031179.
[11] R. Bosri, A. R. Uzzal, A. Al Omar, M. Z. A. Bhuiyan, and M. S. Rahman, "HIDEchain: A user-centric secure edge computing architecture for healthcare IoT devices," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 376–381.
[12] R. Bosri, A. R. Uzzal, A. A. Omar, A. S. M. T. Hasan, and M. Z. A. Bhuiyan, "Towards a privacy-preserving voting system through blockchain technologies," in *Proc. IEEE Intl Conf Dependable, Autonomic Secure Comput., Intl Conf Pervas. Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber. Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 602–608.
[13] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 260–264.
[14] L. da Costa, B. Pinheiro, R. Araujo, and A. Abelem, "A decentralized protocol for securely storing and sharing health records," in *Proc. IEEE Int. Conf. E-health Netw., Appl. Services (HealthCom)*, Oct. 2019, pp. 1–6.
[15] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.
[16] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.
[17] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, Jan. -2018.
[18] *Health Insurance Claim Rejected? These Could be the Reasons*. Accessed: Oct. 2, 2021. [Online]. Available: https://www.hdfcergo.com/blogs/health-insurance/health-insurance-claim-%rejected-these-could-be-the-reasons
[19] S. Jimi. (2019). *How Does Blockchain Work in 7 Steps-a Clear and Simple Explanation, 2018*. Dostupno na. [Online]. Available: https://blog.goodaudience.com/blockchain-for-beginners-what-isblockchain-519db8c6677aDatumpristupa
[20] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[21] V. Kumar, "Cyber-attacks: Rising threat to healthcare," Vascular Disease Manage., HMP Global, Malvern, PA, USA, Tech. Rep., 2017.
[22] P. Littlejohns. (2019). *Lack of Trust in Insurance Companies Driven by Poor Customer Engagement*. Accessed: Jun. 10, 2020. [Online]. Available: https://www.nsinsurance.com/news/low-trust-in-insurance-customer-engage%ment/
[23] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.
[24] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.
[25] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivyShare: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101653.
[26] R. A. Michelin, A. Dorri, M. Steger, R. C. Lunardi, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "SpeedyChain: A framework for decoupling data from blockchain for smart cities," in *Proc. 15th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, Nov. 2018, pp. 145–154.
[27] S. Nakamoto and A. Bitcoin. (Apr. 2008). *A Peer-to-Peer Electronic Cash System*. Bitcoin. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[28] N. P. Rocha, A. Dias, G. Santinha, M. Rodrigues, A. Queirós, and C. Rodrigues, "Smart cities and healthcare: A systematic review," *Technologies*, vol. 7, no. 3, p. 58, Aug. 2019.
[29] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic health record hiding in images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Future Gener. Comput. Syst.*, vol. 108, pp. 935–949, Jul. 2020.
[30] F. Rahman, M. Z. A. Bhuiyan, and S. I. Ahamed, "A privacy preserving framework for RFID based healthcare systems," *Future Gener. Comput. Syst.*, vol. 72, pp. 339–352, Jul. 2017.
[31] V. M. Rohokale, N. R. Prasad, and R. Prasad, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," in *Proc. 2nd Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol. (Wireless VITAE)*, Feb. 2011, pp. 1–6.
[32] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.
[33] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Gener. Comput. Syst.*, vol. 86, pp. 650–655, Sep. 2018.
[34] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
[35] N. Szabo, "The idea of smart contracts," in *Nick Szabo's Papers and Concise Tutorials*, vol. 6, no. 1. Chicago, IL, USA: First Monday, 1997.
[36] M. A. Tasnim, A. Al Omar, M. S. Rahman, and M. Z. A. Bhuiyan, "Crab: Blockchain based criminal record management system," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Melbourne, VIC, Australia: Springer, 2018, pp. 294–303.
[37] G. Tripathi, M. A. Ahad, and S. Paiva, "SMS: A secure healthcare model for smart cities," *Electronics*, vol. 9, no. 7, p. 1135, Jul. 2020.
[38] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and Ethereum: A brief overview," in *Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, Mar. 2018, pp. 1–6.
[39] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," in *Proc. 8th IEEE Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*, Oct. 2012, pp. 711–718.
[40] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Proc. IEEE 3rd Int. Conf. Cloud Comput.*, Jul. 2010, pp. 268–275.
[41] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2018, pp. 1–6.

ABDULLAH AL OMAR received the B.Sc. degree from the Department of Computer Science and Engineering (CSE), University of Asia Pacific (UAP), in 2016. He is currently working as a Lecturer with the Department of Computer Science and Engineering (CSE), University of Asia Pacific (UAP). His research interests include applied cryptography, protocol construction, privacy-preserving and secured platform design, and blockchain. His work in these areas published in top-tier venues, including *FGCS*, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING (TNSE), IEEE TEMS, IEEE INFOCOM, IEEE TrustCom, DASC, and SpaCCS. He has served as a reviewer in IEEE ACCESS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII), IEEE TRANSACTIONS ON SERVICES COMPUTING (TSC), IEEE INTERNET OF THINGS JOURNAL (IoTJ), *CSBJ*, *JMIR*, and *TJCA* and also in different international conferences.

ABU KAISAR JAMIL is currently pursuing the B.Sc. degree with the Department of Computer Science and Engineering (CSE), University of Asia Pacific (UAP). Recently, he has joined as an Intern with Mistri Solution (Techstack Company). His research interests include privacy-preserving, security, and blockchain.

AMITH KHANDAKAR (Senior Member, IEEE) received the B.Sc. degree in electronics and telecommunication engineering from North South University, Bangladesh, and the master's degree in computing (networking concentration) from Qatar University, in 2014. He graduated as the Valedictorian (President Gold Medal Recipient) with North South University. He is currently the General Secretary of the IEEE Qatar Section and Qatar University IEEE Student Branch Coordinator and an Adviser (Faculty). He is also a certified Project Management Professional and the Cisco Certified Network Administrator. He was a Teaching Assistant and the Laboratory Instructor for two years for courses, such as mobile and wireless communication systems, principle of digital communications, introduction to communication, calculus and analytical geometry, and Verilog HDL, such as modeling, simulation, and synthesis. Simultaneously, he was a Laboratory Instructor for the following courses such as, programming course "C," Verilog HDL, and general physics course. He has been with Qatar University, since 2010. After graduation, he was a consultant in a reputed insurance company in Qatar and in a private company that is a sub-contractor to National Telecom Service Provider, Qatar.

ABDUR RAZZAK UZZAL received the B.Sc. degree in computer science and engineering (CSE) from the University of Asia Pacific, Bangladesh. He is currently a Full Stack Web Developer with Shiny Gleam Software. His research interests include blockchain, cryptography, and data privacy.

RABEYA BOSRI (Student Member, IEEE) received the B.Sc. degree in computer science and engineering (CSE) from the University of Asia Pacific (UAP), in 2020. She is currently a Research Assistant with the City University of Hong Kong. Her research interests include security, privacy, and blockchain.

NAFEES MANSOOR (Senior Member, IEEE) received the Ph.D. degree from Universiti Teknologi Malaysia (UTM), in 2016, with a focus on communication systems and networks. He is currently an Assistant Professor with the Computer Science and Engineering Department and the Coordinator of Faculty Research with the University of Liberal Arts Bangladesh (ULAB). His research interests include cognitive radio networks, vehicular *ad hoc* networks, and graph theory. He was a recipient of multiple best paper awards from various conferences that includes the ICED'20, ICAICT'16, RISP-NCCP'15, ICEEE'14, and MJJIS'13. He is also an Associate Editor of IEEE Access Journal.

MOHAMMAD SHAHRIAR RAHMAN received the B.Sc. degree in computer science and engineering from the University of Dhaka, Bangladesh, in 2006, and the M.S. and Ph.D. degrees in information science from the Japan Advanced Institute of Science and Technology (JAIST), in 2009 and 2012, respectively. He worked as a Research Engineer with the Information Security Group of KDDI Research, Japan. He is currently an Associate Professor with the United International University, Bangladesh. He has coauthored more than 50 research articles and submitted eight coauthored Japanese patent applications. His research interests include secure protocol construction, privacy-preserving computation, and security modeling. He is a member of International Association for Cryptologic Research (IACR).