2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) |978-1-6654-0392-4/20/$31.00 ©2020 IEEE | DOI: 10.1109/TRUSTCOM50675.2020.00173

Towards A Transparent and Privacy-preserving Healthcare Platform with Blockchain for Smart Cities

Abdullah Al Omar*, Abu Kaisar Jamil†, Md. Shakhawath Hossain Nur‡, Md Mahamudul Hasan‡, Rabeya Bosri¶,
Md Zakirul Alam Bhuiyan‖, and Mohammad Shahriar Rahman**
*†‡ § *Department of Computer Science and Engineering, University of Asia Pacific, Dhaka, Bangladesh*
¶ *Department of Computer and Information Sciences, Fordham University, New York, NY 10458, USA*
‖ *Department of Computer Science and Engineering, University of Liberal Arts Bangladesh, Dhaka, Bangladesh*
**omar.cs.bd@gmail.com,* †*kaisarjamil.cse@gmail.com,* ‡*shakhawathnur.cse@gmail.com,*
§*mahamudulhasan6478@gmail.com,* ¶*rabeyabosri.cse@gmail.com,* ‖*bhuiyan3@fordham.edu,* ***shahriar.rahman@ulab.edu.bd*

***Abstract*—In smart cities, data privacy and security issues of Electronic Health Record(EHR) are grabbing importance day by day as cyber attackers have identified the weaknesses of EHR platforms. Besides, health insurance companies interacting with the EHRs play a vital role in covering the whole or a part of the financial risks of a patient. Insurance companies have specific policies for which patients have to pay them. Sometimes the insurance policies can be altered by fraudulent entities. Another problem that patients face in smart cities is when they interact with a health organization, insurance company, or others, they have to prove their identity to each of the organizations/companies separately. Health organizations or insurance companies have to ensure they know with whom they are interacting. To build a platform where a patient's personal information and insurance policy are handled securely, we introduce an application of blockchain to solve the above-mentioned issues. In this paper, we present a solution for the healthcare system that will provide patient privacy and transparency towards the insurance policies incorporating blockchain. Privacy of the patient information will be provided using cryptographic tools.**

***Keywords*-Healthcare data, Privacy, Smart City, Transparency, Insurance policy.**

I. Introduction

The goal of developing a smart city is to ease the lives of its citizens. A smart city has several components such as electronic health monitoring systems, electronic health care, automatic traffic management system, smart transportation, and so on. Among them, smart healthcare plays a significant role to achieve the goals of a smart city. To establish smart healthcare, Electronic Health Records (EHR) [1] is probably the main initiating point. EHR is a collection of patient's medical information in a systematic way and digital format. The medical information includes diagnostic reports, treatment plans, radiology images, medications, laboratory, test results, insurance policy etc. In recent years, cyber attackers are becoming interested in EHR. Therefore, data privacy and security issues of the EHR system and personal health data are gaining attention in smart cities day by day.

Healthcare data are being generated rapidly as users are moving to smart healthcare for their better experiences in a smart city. These personal healthcare data (e.g., diagnostic reports, prescriptions, etc.) are getting importance to researchers as these healthcare data can be used for analysis or forecast in the future [2]. These personal health data are getting leaked by eavesdroppers as well as by the intruders. Therefore, the challenge is to preserve or store those data for future work and user access. The citizens of a smart city have to pay yearly a considerable amount of money to health insurance companies for covering the whole or a part of the risk. However, if the insurance policies are not transparent to and accessible by the patients, a fraudulent insurance company may wish to take chances and alter the insurance policy to its advantage.

Researchers are working on cloud computing and EHR, incorporating blockchain to secure patient's health data. In recent years, the advantage of cloud computing has been grabbing the attention of the healthcare domain [3]. With the help of cloud computing, patients can store their healthcare data (e.g., diagnostic reports, prescriptions, etc.), and even they can share their healthcare data with others (e.g., doctors, researchers, stakeholders, third parties, etc.) for future usage [4]. To provide security in the patient's healthcare data, researchers have proposed several solutions. However, in the previous efforts, there is no such mechanism to provide transparency in the insurance policy while keeping patient's healthcare data secure. Transparency in the insurance policy is a very concerning issue in recent days as there remains a chance for fraud activities. Even users do not know where their policy data are stored. Therefore, patients are losing their trust in the insurance companies [5]. On the other hand, reliable insurance companies are struggling to gain patients' trust. There is no single platform where citizens of a smart city can preserve their diagnostic reports, and at the same, their insurance policies are kept transparent to them.

Our Contribution: In this work in progress paper, we are proposing a platform incorporating blockchain which guarantees the privacy of a user's healthcare data. The main idea of our work is to keep patient's insurance policy transparent to them. Through the blockchain, our system ensures transparent

978-1-6654-0392-4/20/$31.00 ©2020 IEEE
DOI 10.1109/TrustCom50675.2020.00173

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.

Paper Organization: The remainder of the paper is organized as follows: Related work is described in Section II, preliminaries is discussed in Section III. Section IV explains our proposed platform. The security analysis of our architecture has been described in Section V. Section VI explains property comparison between proposed architecture and different related systems. Conclusion is included in Section VII.

II. Related Work

To ensure security using blockchain technology in today's IoT based smart healthcare system, security research experts are improving and making a solution efficient. Researchers are trying to ensure security in EHR with the benefit of blockchain as blockchain has decentralized control, immutability, and cryptographic security. Though there are still ways to improve the techniques and design a platform to ensure different factors (e.g., insurance policy) of security in the EHR platforms.

Recently, authors in [6] discussed the security of IoT devices in a smart city. They presented a platform named PrivySharing, a blockchain-based innovative framework for privacy-preserving and secure IoT data sharing in a smart city environment. The strategy they proposed ensures that personal user record data is preserved in top-secret, securely processed and is shared with the third parties on the need basis.A user can establish some rules to determine the entities with whom user wants to share the data through smart contracts.

In [7], the authors proposed a framework for a smart city environment, which is based on blockchain technology for sharing user data. The framework they proposed is called SpeedyChain. They found a solution for real-time applications to reduce the Transaction (TX) settlement time and they were focused to ensure the privacy of it's user.

Authors of [8] presented a Software Defined Networking (SDN) and blockchain-based hybrid network architecture for a smart city. The architecture they presented in their paper has addressed smart city issues such as high TX latency, security and privacy, bandwidth bottlenecks, and requirements that are needed for high computational resources. They divided the smart city network into a distributed core network and the centralized edge network constituting inexperienced devices.

A framework called Smart Medical System (SMS) for the smart city was proposed in [9] that ensures the privacy of the healthcare system. They used blockchain technology to protect the medical and personal data from hackers, which are generated continuously from IoT devices and sensors. They connected several hospital organizations for sharing personal health data with the help of blockchain technology. The framework they proposed ensures real-time monitoring of a patient's health condition and notify the health condition to doctors and healthcare providers.

Several platforms have been proposed in [10]–[17], to address the security threats in the healthcare system. They have proposed a proficient health monitoring system to manage health issues such as blood pressure (BP), hemoglobin (HB), blood sugar, and abnormal cellular growth. In their research, many researchers have presented the Sensor Network (BSN), and presented a secured healthcare system, and focused on the different types of technology used in a smart city for the healthcare system. To focus on ownership and control the EHR of the patients, researchers proposed a blockchain-based solution in [13]. The proposed framework Ancile utilized six types of smart contracts for operation such as Consensus, Classification, Service History, Ownership, Permissions, and Re-encryption.

Authors of [18] discussed about the security of healthcare data and the maintenance of trust between the citizens and stakeholders of a smart city. They proposed a solution interacting with different entities (patient, doctor, healthcare providers, and health insurance companies) to share and collaborate healthcare data securely with the help of blockchain and machine learning.

In [19], authors presented the advantages of blockchain technology to simplify the transformation of the exchange of data for the patients. The researchers claimed to provide the transparency, the blockchain technology can be used over the state of shared data and related transactions among different third parties. For sharing the user's private health data, they used permission-based blockchain which reduces the cost of transactions verification and data integrity as compared with the traditional systems.

Some of the relevant researches have been discussed above. The above-discussed healthcare data management systems have tried to solve only the security and privacy issues of health data. However, transparency issue of insurance policy are missing on those platforms. Hence, we are proposing a platform addressing both the issues for EHR platform. The rest of the paper will describe our platform in detail.

III. Preliminaries

Table I shows the notations that are used in this paper. I.

A. Cryptographic tools

Here, we describe Elliptic Curve Cryptography (ECC) encryption algorithm which has been used as the cryptographic tool to provide proper cryptographic functionality to the patients. Formal definition of ECC is given here.

Definition 1: Elliptical curve cryptography (ECC) is a public key encryption algorithm. ECC is based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. An elliptical curve can be simply created as a set of points defined by the following equation:

$$y^2 = x^3 + ax + b$$

The shape of the curve will be determined based on the values of a and b. These curves are used over finite fields to create 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

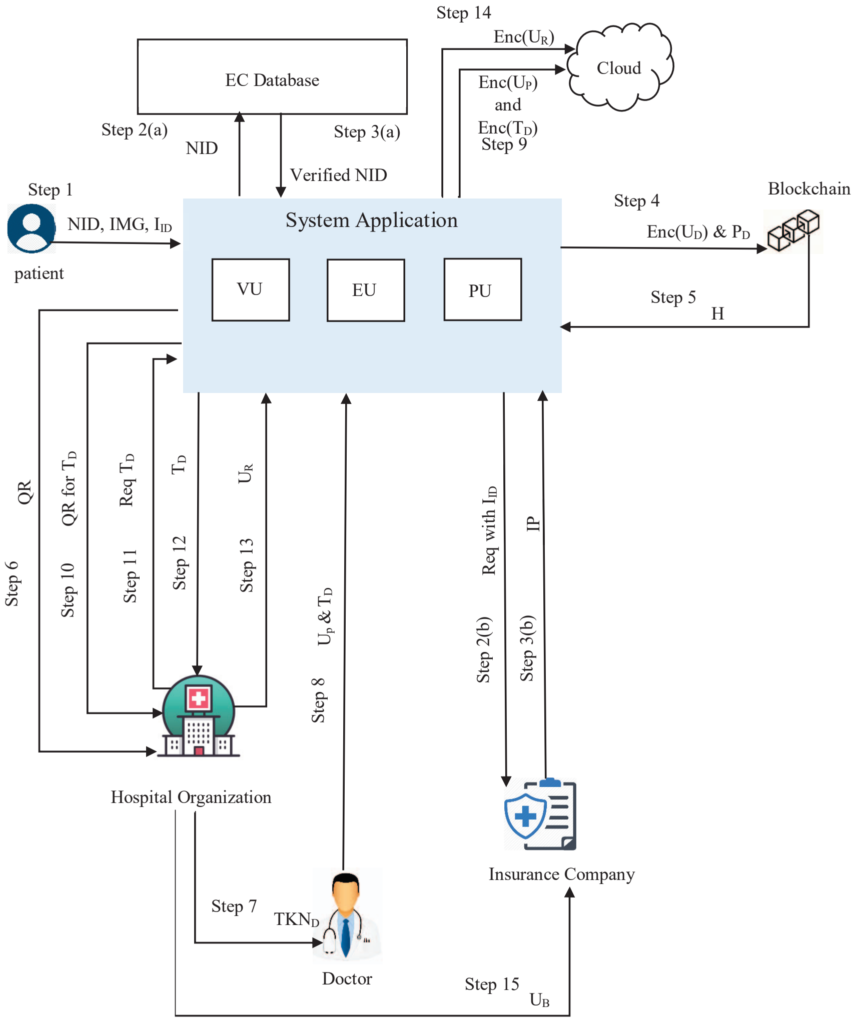

Figure 1: A healthcare platform for smart cities

problem is to solve.

Encryption Scheme Encryption function Enc(Key, Data) is used to encrypt the data. Below we will see how this function works for our U_{R}, U_{P}, T_{D}, U_{D}

$$Enc(Key, Data) = U_{\mathrm{R}}, Enc(Key, Data) = U_{\mathrm{P}}$$

$$Enc(Key, Data) = T_{\mathrm{D}}, Enc(Key, Data) = U_{\mathrm{D}}$$

By providing key and the diagnostic report data to this function,U_{R}, U_{P}, T_{D}, U_{D} will be formed and will be stored into cloud.

Decryption Scheme: To decrypt the diagnostic report data, Dec(Key, Enc(Data)) function will be used.

$$Dec(key, U_{\mathrm{R}}) = plaintext, Dec(key, U_{\mathrm{P}}) = plaintext$$

$$Dec(key, T_{\mathrm{D}}) = plaintext, Dec(key, U_{\mathrm{D}}) = plaintext$$

IV. Proposed Platform

A. Overview of Our System

The proposed platform for smart cities is a blockchain-based solution in which user's IP is kept transparent to her and at the same time user can store her U_{R}, U_{P}, and U_{D} into the cloud for further access. In our platform, there are seven entities, namely users, EC database, system application, HO, the insurance company, cloud, and blockchain.

In this, System Application interacts with patients, EC database, HO, Doctors, Health Insurance Company, Cloud, and Blockchain. A new user needs to submit the required information to register in our system. VU performs the user registration by verifying the provided data from EC database and insurance company, and authenticates the user by taking IMG. Another entity HO will be authenticated from the government health service database by verifying whether it is registered or not. This verification ensures that only the

Table I: Terminology table

Notation	Description
ID	Patient's ID
PW_{D}	Patient's password
IMG	An instant image of patient
U_{D}	Patient info data
P_{D}	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}	Patient's insurance card
IP	Insurance Policy
VU	Verification unit
EU	Encryption unit
PU	Policy management unit
BC	Blockchain
EC	Election Commission
HO	Health Organization

authenticated HO is allowed to our platform. U_{P}, T_{D}, and U_{R} will be stored in encrypted form in cloud. The records of the patient's personal information and insurance policy are stored on blockchain where the possibility of data tampering is negligible as the patient's personal information will be kept as an encrypted form. As insurance policy is a public data it will be kept as plaintext in the blockchain.

Figure 1 shows the high level view of our proposed platform and their interactions. The entities and their roles are described briefly below.

- **Patient:** The patient is the person who will use our system to get the service from any hospital organization within the smart city. Patients can store diagnostic reports in the cloud. To connect, a patient must go through a registration process for proving her authenticity.
- **System Application:** System Application acts as an intermediary of our platform through which our patients will interact with other entities such as the EC database, HO, cloud, BC, health insurance company. System Application is formed up with three-units: VU, PU, and EU. VU performs patient's information verification interacting with EC database. PU manages the IP of the user interacting with the insurance company. VU performs the encryption mechanism of the stored data in the cloud. Here Elliptic Curve Cryptography (ECC) encryption is used as the cryptographic tool to provide proper cryptographic functionality to the users.
- **EC Database:** We use the EC Database to verify the patient's NID information that is provided by the patient.
- **Inurance Company:** Insurance company is used to verify I_{ID} information and to retrieve the IP of the patient. A lot of reliable insurance companies are losing their patients' trust for a few fraud companies. If insurance companies join our platform, they will be able to get their user's trust again.
- **Blockchain:** BC is an entity of this system, and we are using the ethereum network in this platform. BC stores the U_{NID} of a patient and the IP of a patient. Our system will have one node, which will operate all the BC transactions. In this platform, BC will store two kinds of data. First, the U_{NID} that will come after the verification by the VU. Second, the IP, which will be verified by the PU before storing it. After every transaction, the BC will return the transaction ID that will be provided to the patient by this platform. A patient can view her IP by using the transaction ID.
- **Hospital Organization:** HO is an entity from where our user gets the services through visit. HO is connected with system application and health insurance company. HO gets the information of a patient by scanning the patient's QR code. After the consultancy, HO sends T_{D}, U_{P}, and U_{R} to the system application. It also sends U_{B} of patients to the health insurance company.
- **Cloud:** Cloud works as the off-chain storage of our system. It stores T_{D}, U_{P}, and U_{R} for further access.

1) Steps in our system: Steps that are involved in our proposed system from Figure 1 are given below.

- Step 1: User creates account with NID, IMG, and I_{ID} information and accesses our system with ID, PW_{D} and H.
- Step 2(a): NID information is sent to EC database for verification.
- Step 2(b): I_{ID} information is sent to insurance company for verification.
- Step 3(a): Verified NID information is received.
- Step 3(b): IP is retrieved from insurance company.
- Step 4: $Enc(U_{\mathrm{D}})$ & 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.
- Step 8: Doctor sends patient's U_{P} & T_{D} to System Application.
- Step 9: $Enc(U_{\mathrm{P}})$ & $Enc(T_{\mathrm{D}})$ are stored into 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} is sent to System Application.
- Step 14: U_{R} is stored to cloud in an encrypted form.
- Step 15. U_{B} is sent to insurance company.

B. Platform Analysis

1) Patient Verification and Policy Management: Figure 2 shows a low-level view of patient verification and insurance policy management. The patient performs a registration with this system through the VU. At the very first of the patient verification process starts with submitting required information (NID number, Insurance Card Number, Insurance Policy Document) to VU. VU sends the patient's IP to the PU for generating a hash from the policy document. Next, the patient verification will be done in two ways. Firstly, the VU sends the NID to the EC for verifying the authenticity of the patient. Secondly, a request is sent to the insurance company along with the I_{ID} information. EC sends the patient information, and the insurance company sends the policy document. Now, PU generates the hash again from the policy document given by the insurance company. If the two hashes are matched that ensures, the insurance company did not change the IP. If any single bit of the policy has changed then it will produce a different hash, which will not match with the previous hash (generated from the IP given by the patient). When the hash matches, VU sends the IP into BC along with the NID information.

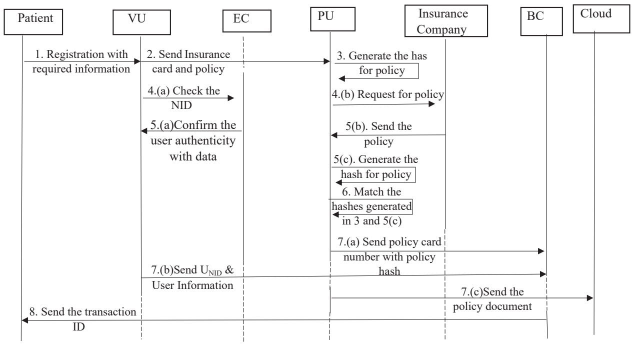
Patient
VU
EC
PU
Insurance Company
BC
Cloud
1. Registration with required information
2. Send Insurance card and policy
3. Generate the has for policy
4.(a) Check the NID
4.(b) Request for policy
5.(a)Confirm the user authenticity with data
5(b). Send the policy
5(c). Generate the hash for policy
6. Match the hashes generated in 3 and 5(c)
7.(a) Send policy card number with policy hash
7.(b)Send U_{NID} & User Information
7.(c)Send the policy document
8. Send the transaction ID

Figure 2: Patient verification and insurance policy management (On-chain storage)

2) Data transaction in our platform: Figure 3 shows the low-level view of how a patient gets services from this system and how cloud stores patient data. A registered patient can send a service request from a HO (HO is also connected with this system). A patient sends the request by providing her QR code and H to the HO. After retrieving data by scanning the QR code, HO creates a TKN_{D} for patient and sends to the doctor. Doctor interacts with the system application by giving the U_{P} and T_{D}. The system application verify the HO and allow the data to store. The data is stored in the cloud after the encryption process. Then the system application generates a QR code for the T_{D} and provides it to the patient. Now, a patient can go to the HO for testing with the QR code. Whenever patient sends the QR code of T_{D}, the HO retrieves T_{D} by requesting to System Application. System application verifies the request and sends the data to HO after a decryption process. When the U_{R} is ready, the HO sends the data to system application. System application stores the data in the cloud after the encryption process.

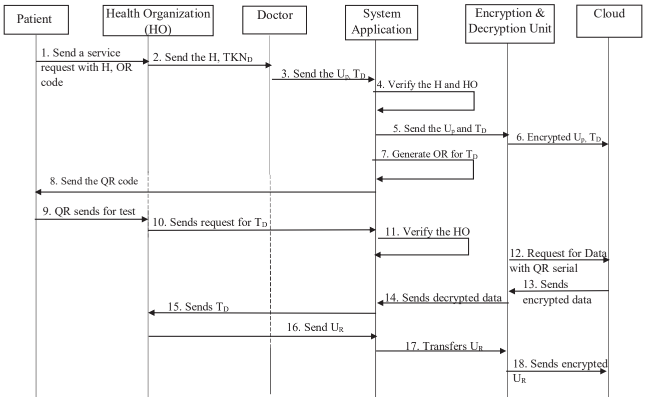

Figure 3: User interaction and off-chain storage

V. Security Analysis

Authorization: Patient authorization is performed by BC. BC generates H for each patient after storing U_{D} to BC. When patient login to access our system, she will have to submit the H along with ID, PW_{D}. H is generated by BC from the patient's stored data. If the submitted H belongs to our all generated hashes, then the patient is allowed to access our system.

Integrity: The integrity of IP is performed by BC. As the IP is stored into the BC, the IP is transparent to all. No one can alter the patient's IP as BC has the properties such as immutability, transparent etc.

Security: Our system provides the security by keeping the U_{R} into the Cloud. As U_{R} is stored in an encrypted form, U_{R} cannot be accessed without the encryption key. In our platform RU performs the patient authentication. The authentication starts when patient submits the required information (NID information, IMG, I_{ID}) to VU. Firstly, VU sends the I_{ID} to PU for confirming the information provided by patient and to retrieve the IP. After that insurance company sends the confirmation with the IP of that patient. At the same time VU verifies the NID information from the EC database and matches IMG with the image from NID with the help of machine learning. By verifying the provided information, only the authenticated patients are allowed to use our platform.

Another entity of our platform which is HO have to submit the required information for validation. The provided data will be sent to the government health service database and verifies whether it is registered by the government or not. If the HO is registered by the government then the HO will be allowed to our platform for registration. By doing this, only the authenticated HO is allowed to interact with our platform.

VI. Comparison between our architecture and the related works

In this section, we show the results in the six properties/metrics of the architectures. If a particular architecture has the property in it then we marked it with 'Y' otherwise marked with 'N'. Here, Table II compares our architecture with other existing architectures. With the careful analogy of the systems and in account of the important six properties/metrics of blockchain based transparent healthcare systems, a conclusion can be drawn that our architecture has greater advantages than the other systems in this table.

Table II: Comparison table

Metric	[13]	[9]	[2]	Our architecture
User Authentication	N	N	N	Y
User Centric	N	N	Y	Y
Data Encryption	N	Y	Y	Y
Privacy of data owner	Y	Y	Y	Y
Transparent insurance policy	N	N	N	Y
Blockchain based	Y	Y	Y	Y

VII. Conclusion

In this work in progress paper, we proposed a transparent healthcare system where user's insurance policy will be stored into the blockchain for making the user's insurance policy transparent to them. User can also store healthcare data (i.e., diagnostic report, prescription, and test list) securely in the cloud, and their personal information in the blockchain. In our future research we will implement this whole system.

References

[1] 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 Generation Computer Systems*, vol. 108, pp. 935–949, 2020.

[2] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE, 2018, pp. 1–6.

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

[4] L. da Costa, B. Pinheiro, R. Araújo, and A. Abelém, "A decentralized protocol for securely storing and sharing health records," in *2019 IEEE International Conference on E-health Networking, Application & Services (HealthCom)*. IEEE, 2019, pp. 1–6.

[5] P. Littlejohns, "Lack of trust in insurance companies driven by poor customer engagement," https://www.nsinsurance.com/news/low-trust-in-insurance-customer-engagement/, 2019, [Online; accessed 10-June-2020].

[6] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Computers & Security*, vol. 88, p. 101653, 2020.

[7] 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 *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2018, pp. 145–154.

[8] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650–655, 2018.

[9] G. Tripathi, M. Abdul Ahad, and S. Paiva, "Sms: A secure healthcare model for smart cities," *Electronics*, vol. 9, no. 7, p. 1135, 2020.

[10] P. Gope and T. Hwang, "Bsn-care: A secure iot-based modern healthcare system using body sensor network," *IEEE sensors journal*, vol. 16, no. 5, pp. 1368–1376, 2015.

[11] V. M. Rohokale, N. R. Prasad, and R. Prasad, "A cooperative internet of things (iot) for rural healthcare monitoring and control," in *2011 2nd international conference on wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (Wireless VITAE)*. IEEE, 2011, pp. 1–6.

[12] N. Pacheco 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, 2019.

[13] 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," *Sustainable cities and society*, vol. 39, pp. 283–297, 2018.

[14] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2017, pp. 534–543.

[15] A. Al 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 generation computer systems*, vol. 95, pp. 511–521, 2019.

[16] 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 *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 376–381.

[17] 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 Transactions on Network Science and Engineering*, pp. 1–1, 2020.

[18] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2019, pp. 260–264.

[19] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability," *Computational and structural biotechnology journal*, vol. 16, pp. 224–230, 2018.