Enhancing SARS-CoV-2 variants Research with Blockchain Architecture

Oluwaseyi Ajayi
Engineering Department
Vaughn College of Aeronautics Technology
New York, USA
oluwaseyi.ajayi@vaughn.edu

Tarek Saadawi
Department of Electrical Engineering,
City University of New York, City College
New York, USA
saadawi@ccny.cuny.edu

***Abstract*— The emergence of the novel SARS-CoV-2 (Covid-19) virus in 2019 has led to continuous monitoring of the outbreak attempting to generate accurate reports of people's health information to understand the pandemic's impact. It is likely that more variants will emerge since not all countries and populations have been vaccinated. Thus, with SARS-CoV-2's constant mutation, researchers need to collect individuals' health data to study these variants and vaccine efficacy, especially those who show symptoms. However, researchers have difficulties building comprehensive datasets because people are unwilling to release their health information or have no way to report their health statuses (i.e., at-home testing). This problem stems from a lack of complete control over who assesses their health data. Hence, they cannot guarantee the security, privacy, and integrity of the disclosed health information. As the problem of building secure databases persists, researchers find it challenging to accurately report any evolving variants within a short period. In this work, we propose a blockchain architecture that can guarantee patients' health data integrity, privacy, and security, encouraging individuals to disclose their health information freely. This solution gives patients complete control over who assesses their health information. The framework proposed access management to patients' health data for researchers and contact tracers. This solution classifies patient health information to different sensitivity levels and manages access based on this sensitivity. In case of unauthorized access, the proposed solution detects and prevents such access, thereby ensuring the patient's health information's security, integrity, and privacy.**

Keywords *— Blockchain, Integrity, privacy, SARS-CoV-2 virus, Security, Privacy, Confidentiality, Public Health Information, Access Management.*

I. INTRODUCTION

The outbreak of the SARS-CoV-2 (Covid-19) virus since 2019 has called for an urgent need for effective research and reports to curtail further spreading and deaths from the pandemic. Based on the studies, it is highly contagious and constantly spread around the globe [1]. The Covid-19 virus most often causes respiratory symptoms similar to cold, flu, or pneumonia. Since its discovery, more than 506 million cases have been reported worldwide and have accounted for 6.2 million deaths[2]. 80.7 million cases and more than 989 thousand deaths have been reported in the USA[2]. Currently, about nine virus variants are being monitored, while three of the evolved variants (Delta, Omicron, and Ihu) are of great concern to researchers [3]. Due to its rapid mutation rate, researchers collect patients' health information to study and report new variants. Researchers failed to accurately study the variants despite their effort to collect updated health information. This is due to a lack of willingness from people that have been exposed to disclose health information. The problem stems from an inability of the patients to control who assesses their health data. Hence, they cannot guarantee the security, privacy, and integrity of the disclosed health data. As the problem persists, researchers find it cumbersome to give an updated report of new variants and vaccine efficacy. If no solution is provided, the problem might lead to an outbreak of another variant.

Academia and industrial researchers have put forward diverse blockchain applications to preserve the privacy and confidentiality of the health information collected by contact tracers and researchers. For instance, [3] proposed BeepTrace to bridge the user/patient and authorized solvers to desensitize the user ID and location information. A blockchain architecture that preserves the privacy of contact tracing Covid-19 patients was proposed in [4], while [5] evaluates the benefits of using Big data and blockchain technology to deal with the pandemic and some data quality issues that still present challenges to decision making. The authors in [6] proposed a blockchain architecture that enforces accountability and transparency to bridge the gap between the on-chain and off-chain user information collected by contact tracers.

Despite the numerous researches on privacy-preservation of individual health information, none of the available solutions focus on access management of the health information, hence the motivation to this work.

A. SARS-CoV-2 Virus researchers

These people are dedicated to monitoring the new variants symptoms to make an informed decision and recommendation to the government. These people study the symptoms to i). reports about the new variants, and ii) report the vaccine efficacies. To obtain accurate information based on the new or existing symptoms, they rely on information supplied by contact tracers. They can also request covid related health information from Covid isolation centers and treatment sites or healthcare providers and hospitals.

B. Contact Tracing

This is a process of identifying, assessing, and managing people who might have contact with Covid-19 infected person and subsequent collection of further information

about these contacts[7]. The purpose of contact tracing is to minimize the spread of the virus. Contact tracing has been used and proven effective in minimizing the spread of infectious diseases in general. The contact tracing process relied heavily on recalling a list of people they have been in contact with over the previous weeks or locations the confirmed person has been. Letters, phone calls, or emails are being used to inform people who might be exposed. Thus, completeness and accuracy of the list and timeliness and efficiency of the tracing are limited by such a labor-intensive, traditional contact tracing approach. Recently, different digitized contracting through smartphone apps has been deployed to solve the labor-intensive problem. For instance, Singapore TraceTogether[8], GAEN[9], National Health Service (NHS) COVID-19 App [10], and China Health code system [11]. Researchers rely on contact tracing information to study the virus accurately.

C. Contribution

The proposed solution aims to develop a blockchain framework that can guarantee people's health information privacy, security, confidentiality, and integrity so that individuals will be willing to disclose necessary information to study and report new cases of Covid-19 variants. In addition, this framework promotes health equity by often engaging underserved communities. The specific aims of the solution are summarized below:

- **Guarantee PHI privacy, integrity, security, and confidentiality using access management**: One of the significant problems experienced by researchers in obtaining accurate information about the SARS-CoV-2 virus is that there is no way to guarantee privacy or integrity and confidentiality of the health information requested. As a result, individuals find it challenging to trust non-medical practitioners(e.g., Researchers, contact tracers, etc.) requesting their health information. Even if researchers turn to healthcare providers to obtain health information, they are restricted by government policies (e.g., HIPAA) about sharing health records with third parties. Our proposed solution combat this challenge by ensuring that patients have complete control over who accesses health records and that no sensitive health information is disclosed during this process.
- **Classifies individual health information based on its sensitivity**. People find it challenging to share their health information because there is no access control strategy to deter requesters from accessing more than requested information. This means there is no way patients can control the level of access once the health records have been shared. Our approach approached this challenge by classifying the health information based on sensitivity and defining different access levels to enforce restrictions. Apart from creating these access levels, the architecture manages access to health information via verification, authentication, and permission steps.
- **Fosters SARS-CoV-2 virus research:** One of the reasons it is required to study and report the SARS-CoV-2 virus continuously is its constant mutation. This constant mutation has led to a strong need for a prompt and constant collection of health information to generate a dataset for compelling studies and reports. by implementing the proposed solution, people will be willing to release helpful information about their covid status without privacy and integrity breach concerns
- **Reduces the burden on Contact Tracing:** The bulk of the dataset building for effective studying of the variants relies on the information provided by contact tracing. It is often challenging to get accurate health information as people might be unwilling to talk or mispresent their situation. Our architecture allows the individual's health providers (e.g., testing center) to upload accurate information to the blockchain network. Contact tracers can access this information from the blockchain platform by requesting a permit from the health data owner. In this case, both the contact tracer and owner are anonymous, and the contact tracer only accesses the permitted/required information.

This paper's remainder is organized as follows: Section II discusses the background and related works on blockchain applications for healthcare data access. Section III describes the proposed architecture's method. Section IV presents the preliminary results, and finally, section V presents the conclusions of this paper and possible future works.

II. BACKGROUND AND RELATED WORKS

Researchers have applied blockchain in diverse areas, including data security in healthcare, in the past years. The blockchain capabilities make the blockchain technology more secure than other distributed database platforms. Such features are attractive for their secure data collection and management, prompting other researchers to propose blockchain applications in sharing health information. For example, the authors in [1] proposed Gem Health Network, allowing different healthcare specialists to access the same health information from a shared infrastructure. The authors [2] proposed a user-centric health data sharing solution that utilizes a decentralized and permissioned blockchain. In their work, a mobile application is deployed to collect health data from personal wearable devices, manual input, and medical devices, and synchronize data to the cloud for data sharing with healthcare providers and health insurance companies.

The authors in [3] proposed a conceptual design for sharing personal continuous dynamic health data using blockchain technology supplemented by cloud storage to share the health-related information in a secure and transparent manner. The primary goal of their proposed system is to enable users to own, control and share their personal health data securely. The solution also provides an efficient way for researchers and commercial data consumers to collect high quality personal health data for research and commercial purposes. A blockchain-supported architectural framework for secure control of personal data in a health information exchange by pairing user-generated acceptable use policies with smart contracts was proposed in [4]. In [5], the authors proposed blockchain-enabled IoMT to address the security and privacy concerns of IoMT systems to combat COVID-19. The authors in [6] presented a blockchain-enabled privacy-preserving contact tracing scheme, BeepTrace. Their work proposed adopting blockchain bridging the user/patient and the authorized solvers to desensitize the user ID and location information.

Our proposed application is unique from previous proposals in that it ensures data security with additional steps Although the available solutions utilized the same blockchain platform to share personal health information, our approach introduced two specific, novel steps: i. our proposed solution classifies health information based on sensitivity for easy access management. ii. our application mounted an extra verification step on the existing blockchain framework to ensure that no unauthorized access is permitted. This mode of operations makes our approach different from existing blockchain applications in healthcare. The proposed architecture classifies and stores people's health information (PHI) then manages access based on the sensitivity and class of the requester, thereby guaranteeing the privacy, integrity, and security of an individual's health information. The requesters are classified (e.g., Researcher, Contact tracer, Physician, Nurse), and access to sensitive information is defined based on each class. Any entity that submits a request to access health data goes through verification steps. If the verification fails, the access is denied, and no health information is returned to the sender. Although the proposed framework can manage access from different requester classes, this work focuses on SARS-CoV-2 virus studies and reports.

III. Methodology

This approach aims to build a distributed database that guarantees health information security, privacy, and integrity by providing access management. The novel access management strategy encourages individuals to disclose their health information, enhancing covid-19 studies and vaccine efficacies testing. Figure 1 describes the high-level mode of operation. The key actors involved in the proposed approach are:

- **PHI generators**: These are health professionals that generate patient health information. An example is a Covid testing center, a healthcare provider etc. These entities send the PHI into the blockchain network[1] via a classification module(described below).
- **Owner**: The individual that owns the health information uploaded to the blockchain network. The owner approves whenever there is a request to access the stored health records. The owner grants or denies the access based on the request and sender's information. The request pushed to the owner is a successfully verified request.
- **Requesters**: These entities need health records for different purposes, e.g., research. They request health information relating to the Covid-19 virus to conduct better studies, make accurate reports, adjust the vaccines, evaluate the performance, advise government agencies like CDC, task-force on the pandemic, etc. Examples are SARS-CoV-2 virus researchers and contact tracers.

Apart from the above descriptions, the architecture can enable the inclusion of underrepresented populations, especially those whose health issues have been neglected in research

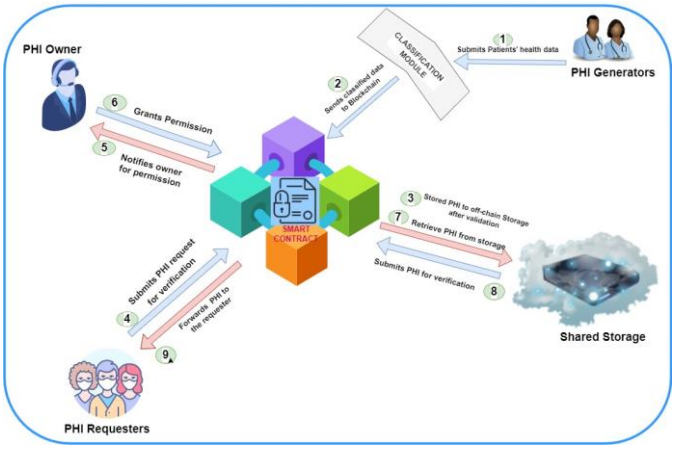

Fig. 1. The Proposed architecture

The architecture comprises a blockchain network that features a programmable smart contract and an off-chain storage system, e.g., IPFS. The main building blocks of the proposed architecture are shown in Fig. 2. The building blocks comprise a classification module, access management module, and storage system.

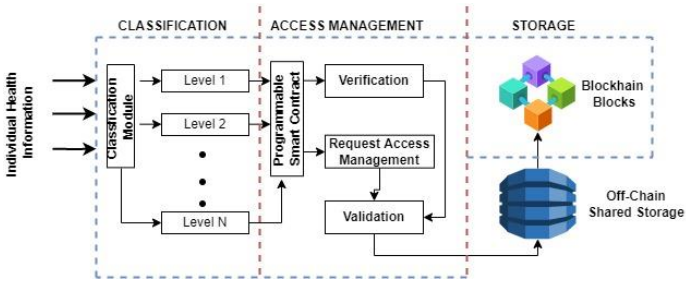

Fig. 2. Building blocks of the proposed architecture

Algorithm 1: Classification Module

```
Require:
    Mapping(Incoming IHI ->struct) private Sensitivity;

Procedure: ReadIncomingIHI (Individual Health Information)
    For ihi in IHI:
        If ihi ∈ basic information
            basic information ← ihi
            Sensitivity =>1
        else
            If ihi ∈ covid-19 related information
            covid-19 information ← ihi
            Sensitivity => 2
        else
            other health information ← ihi
            Sensitivity => 3
        end If
    end For loop
end procedure
```

1. *Classification module*

The classification module is an interactive script developed in a python programming language that identifies sensitive health information and groups them according to the sensitivity level. This module reformats the health record according to sensitivity features written in the smart contract. For the script to effectively classify ingress health records, it is required that the health record be sent in a particular format. Based on this format, the script interacts, extracts, and separates the information according to sensitivity. For proof-of-concept evaluated in this work, we defined three sensitivity levels:

- *Basic information:* The general or basic information about the individual is extracted here. An example of the information extracted includes name, age, date of birth, gender, weight, height, race, origin, etc. The basic information is accompanied by a tag that defines the sensitivity and access level.
- *Covid-19 information:* The health records here are Covid-19 and vaccines-related information. Individual Covid-19 related information is obtained and registered here. An example of the information extracted includes underlining health problems, age, gender, race, origin, vaccine status, Covid-19 symptoms, etc. The Covid-19 information is accompanied by a tag that defines who can access the information and the level of sensitivity
- *Other Health information*. The health information here is other health records not covid-related. Examples include health history from PCP, list of drugs, previous tests, etc. This information is not to be accessed by Covid-19 researchers or contact tracers. The health information is accompanied by a tag that defines the sensitivity and access level

Algorithm 1 below illustrates how the classification module script reads the incoming individual health information (IHI), classifies it, and sets the sensitivity level. To achieve this classification, the module matches the field of the received IHI to what it runs then retrieves the features.

Based on these classifications, the module prepares separate transactions. These transactions are digitally signed and submitted to the blockchain network for verification and validation. In addition to the information, the sending blockchain node submits its information for sender authentication.

2. *Access Management Module*

This module describes the verification, validation, and request access management of health information. The transaction sensitivity level, public keys, and authorized nodes' information are stored in the smart contract. The transaction owner is authenticated, and the submitted transactions are verified. Verification and request access control are managed on the server-side of the architecture, i.e., smart contract, while transaction validation is handled by blockchain consensus protocol. Thus, smart contract handles the following functions:

i. Node Authentication

The smart contract handles nodes authentication. The purpose of authenticating a node is to ensure that all transactions are sent from authorized nodes only. The smart contract retrieves the sender's information that accompanies the transaction and invokes a code that compares it with stored information. The information confirmed includes the transaction account, MAC and IP addresses, and the digital signature. We recognized that hackers could easily spoof the MAC and IP addresses in a highly unsecured environment; hence, we added a multifactor authentication process that involves verifying the sender's transaction account and digital signature in addition to the verified MAC and IP addresses. The pseudocode in Algorithm 2 describes the snippet of the smart contract that handles the node's authentication. The smart contract invokes the code that reads the sender's information. It verifies the digital signature using the owner's public key (o.pk) and confirms the transaction account, MAC,

and IP addresses. The algorithm invokes the transaction verification code if the node authentication is successful. For a node to be successfully authenticated, the sender must be an authorized node i.e., the digital signature and other information must be verified. If any of these fail, the node's transaction is dropped.

Algorithm 2: Node Authentication

```
1   Require:
2     Mapping (pubkey=>bytes32) public Keys;
3     Mapping (account => bytes32) public Account;
4     Mapping (ip_addr=>bytes32) public IP;
5     Mapping (mac_addr => bytes32) public MAC;
6
7     procedure: ReadOwnerData (Transaction tag)
8           Transaction.owner ←msg.sender
9           Transaction.account ← account
10          Transaction.pubkey ← o.pk
11          Transaction.ip ← ip_addr
12          Transaction.mac ←mac_addr
13          Return TRUE
14    end procedure
15
16    procedure: NodeAuthentication (OwnerData)
17          require (ip_addr ∈ IP)
18          require (mac_addr ∈ MAC)
19          require (pubkey ∈ Keys)
20          require (account ∈ Account)
21          require (o.pk verifies digital signature)
22          return successful authentication with timestamp
23    end procedure
```

ii. Transaction verification

One of the novelties of the proposed solution is the implementation of the verification stage. The verification stage ensures that any submitted transaction conforms with the agreed-upon format and contains the correct information. The verification step also ensures no leakage of sensitive information due to incorrect classification—the smart contract reviews and matches tags accompanying each transaction to its sensitivity level. A snippet from the smart contract runs through the submitted transaction to ensure no features are missing. Every authorized node sign its transaction with the private key, and a smart contract code verifies the digital signature using the known public keys whenever a transaction is submitted to the blockchain. For digital signature implementation, we generate key pairs with Digital Signature Algorithm (DSA) with 1024 bit-length using the command "*ssh-keygen -t dsa -b 1024"* and store the public key in the smart contract. The smart contract also stores the tag information accompanying each transaction to manage access. A snippet from the smart contract shows algorithm 3 pseudocode describing the transaction verification process. For transaction verification to be successful, the transaction must agree with the defined format, and the sensitivity level must match the information. If the sensitivity level does not match the information, the sender is notified, and the transaction is dropped.

Algorithm 3: Transaction Verification

```
1   Require:
2     Mapping (transaction=>struct) public Sensitivity;
3     Mapping (transaction => struct) public Format;
4
5     procedure: ReadTransaction (format, tag)
6           Transaction.field ←format
7           Transaction.tag ← level
8           Return TRUE
9     end procedure
10
11    procedure: NodeAuthentication (OwnerData)
12          require (format ! = NULL)
13          require (level == tag[level])
14          return successful verification with timestamp
15    end procedure
```

iii. Request Access Management

Another novelty of this proposed work is its ability to enforce access control on the stored health information. The purpose of managing the requester's access is to ensure that a requester is assessing only the required information. We implement the access control function by defining a transaction retrieval policy that uses the transaction's sensitivity. We defined each class of requesters' information and wrote it into the smart contract. Every requester must submit the required information according to the access level requested. If a requester fails to provide the required information, access is denied. After the smart contract has successfully verified the requester, an access request is pushed to the owner for approval. If approved, the requester can access the information; else, access is denied. Algorithm 4 shows that for a request to be granted, a smart contract must verify the requester's information, the owner must approve the request, access level must match the requester level (e.g., a researcher requesting covid-19 related health information), and a sender cannot request multiple information (i.e., no cross-level request).

```
Algorithm 4: Access Management
Require:
    Mapping(request => struct) public Request;
    Mapping (requester_sender => struct) public Information

    procedure: ReadRequest(,requester )
        Requester_info ← info
        Requester_request ←health_info
        Requester_level ← access_level
        Return True
    end procedure

    procedure: RetrieveTransaction (Transaction)
        require (access_level ∈ Tag[level])
        require (info must be correct)
        require(health.owner must approve)
        require (request_info == 1)
        Allow Access to Specified Information
    end procedure
end procedure
```

3. *Storage Module*

i. Off-chain shared Storage

Owning to the massive amount of data accompanying patient health records, we introduce a decentralized off-chain shared storage medium called interplanetary File System(IPFS). One of the features of IPFS is that each stored file can be allocated a unique hash according to its content to identify it uniquely. So, if somebody uploads two files with the same hash value, IPFS pins them to the server and creates only one entry in the content addressed storage block. Due to this feature, IPFS has no access control, and files over IPFS can be directly accessed by their respective hash value [14]. Unlike [14], access to the IPFS is limited to the blockchain network. Blockchain network offloads health records to the IPFS after successful verification and authentication. A successfully verified transaction is pushed to the off-chain Storage, and reference to the location of this information is sent to the blockchain network for validation and Storage. The reference location of the newly added information undergoes a validation process and is added to the blockchain network blocks. Our previous works have extensively described the validation process [15-17].

ii. Blockchain Blocks

After successfully validating the location reference, the newly added block reflects on the ledger of all blockchain nodes, and the transaction is ready to be retrieved. All blockchain nodes receive the newly added block notification but do not access the block's content. The smart contract retrieves the transaction address after the requester has been successfully verified and the owner approves the request.

IV. RESULT

The on-going work is implemented on an Ethereum blockchain platform. We use *Solidity v 0.8.11* implementation for smart contracts and *geth v 1.10.13* for Ethereum. For initial testing of the proof-of-concept, the private blockchain network is set up in the laboratory with five computers serving as blockchain nodes (Fig. 1) to evaluate the performance. We evaluated access management on the stored information, and the preliminary result was as described below. We also present the further work to be carried out.

A. Access Control/Management

We evaluate the access control function by implementing a node attempt to retrieve an unauthorized transaction. We submit a transaction using one of the blockchains. The submitted information was successfully verified and pushed to the off-chain Storage. The reference to the location was successfully verified and added to blocks. Another random node was used to query this stored information. The smart contract handles each transaction's access control by comparing the information of the requesting node to the authorized requester. The node queries the blockchain for the content of a newly added block that it is not privileged to download. We investigate further by querying the blockchain using a node that can retrieve the data. The node successfully downloads the block's content from the blockchain. No information was returned to the requester because the node is not privileged to retrieve the data.

V. CONCLUSION

We proposed a blockchain framework that can guarantee the privacy and integrity of shared patient's health information, thereby encouraging people to disclose more helpful health information to enhance the SARS-CoV-2 (Covid-19) virus study and monitor vaccine efficacies. Implementing the proposed architecture will foster the study and reporting of new SARS-CoV-2 variants. Due to its distributed database implementation, the proposed solution can enhance the inclusion of underrepresented populations, especially those whose health issues have been neglected in research.

Further works

As part of the further work, we plan to implement the following

- Add Off-chain shared storage medium to offload the Storage of health information from the blockchain
- Evaluate the effectiveness of the classification with real data
- Evaluate and present the results of the architecture's effectiveness towards guaranteeing privacy, integrity, confidentiality, and security of Individuals' public health information.
- Describes how the architecture achieves the user training module and inclusion of underserved populations

REFERENCES

[1] https://www.yalemedicine.org/news accessed 4/20/2022

[2] https://coronavirus.jhu.edu/map.html accessed 4/20/2022

[3] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan and M. A. Imran, "BeepTrace: Blockchain-Enabled Privacy-Preserving Contact Tracing for COVID-19 Pandemic and Beyond," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3915-3929, 1 March1, 2021, doi: 10.1109/JIOT.2020.3025953.

[4] S. Tahir, H. Tahir, A. Sajjad, M. Rajarajan and F. Khan, "Privacy-preserving COVID-19 contact tracing using blockchain," in Journal of Communications and Networks, vol. 23, no. 5, pp. 360-373, Oct. 2021, doi: 10.23919/JCN.2021.000031.

[5] I. Ezzine and L. Benhlima, "Technology against COVID-19 A Blockchain-based framework for Data Quality," 2020 6th IEEE Congress on Information Science and Technology (CiSt), 2020, pp. 84-89, doi: 10.1109/CiSt49399.2021.9357200.

[6] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar and S. Ellahham, "COVID-19 Contact Tracing Using Blockchain," in IEEE Access, vol. 9, pp. 62956-62971, 2021, doi: 10.1109/ACCESS.2021.3074753.

[7] Ferretti et al., "Quantifying SARS-CoV-2 transmission sug gests epidemic control with digital contact tracing," Science, vol. 368, no. 6491, 2020, Art. no. eabb6936. [Online]. Available: https://science.sciencemag.org/content/368/6491/eabb6936

[8] J. Bay et al., "BlueTrace: A privacy-preserving protocol for community driven contact tracing across borders," SingaporeŠs Government Technol. Agency, Singapore, White Paper, p. 9, 2020.

[9] Exposure Notification, Apple Inc., Cupertino, CA, USA and Google LLC., Mountain View, CA, USA, May 2020.

[10] I. Levy. (2020). The Security Behind the NHS Contact Tracing App. Accessed: May 8, 2020. [Online]. Available: https://www.ncsc.gov.uk/ blog-post/security-behind-nhs-contact-tracing-app

[11] P. Mozur, R. Zhong, and A. Krolik, In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, New York, NY, USA, 2020. [Online]. Available: https://www.nytimes.com /2020/03/01/business/china-coronavirus-surveillance.html

[12] O. Ajayi, M. Abouali and T. Saadawi, "Secure Architecture for Inter-Healthcare Electronic Health Records Exchange," 2020 IEEE International IoT, Electronics, and Mechatronics Conference (IEMTRONICS), 2020, pp. 1-6, doi: 10.1109/IEMTRONICS51293.2020.9216336.

[13] O. Ajayi and T. Saadawi, "Detecting Insider Attacks in Blockchain Networks," 2021 International Symposium on Networks, Computers, and Communications (ISNCC), 2021, pp. 1-7, doi: 10.1109/ISNCC52172.2021.9615799.

[14] Meryem Abouali, Kartikeya Sharma, Oluwaseyi Ajayi, Tarek Saadawi, "Blockchain Framework for Secured On-Demand Patient Health Records Sharing" 2021 IEEE 12th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON 2021) December 1-4, 2021, New York, USA.

[15] O. Ajayi, M. Cherian and T. Saadawi, "Secured Cyber-Attack Signatures Distribution using Blockchain Technology." 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 2019, pp. 482-488.

[16] O. Ajayi and T. Saadawi, "Blockchain-Based Architecture for Secured Cyber-Attack Features Exchange," 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), New York, NY, USA, 2020, pp. 100-107, doi: 10.1109/CSCloud-EdgeCom49738.2020.00025.

[17] O. Ajayi, O. Igbe and T. Saadawi, 2019. Consortium Blockchain-Based Architecture for Cyber-attack Signatures and Features Distribution, 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 2019, pp. 0541-0549, doi: 10.1109/UEMCON47517.2019.8993036.