Privacy-preserving COVID-19 Contact Tracing using Blockchain

Shahzaib Tahir, Hasan Tahir, Ali Sajjad, Muttukrishnan Rajarajan, and Fawad Khan

***Abstract*—The outbreak of the COVID-19 virus has caused widespread panic and global initiatives are geared towards treatment and limiting its spread. With technological advancements, several mechanisms and mobile applications have been developed that attempt to trace the physical contact made by a person with someone who has been tested COVID-19 positive. While designing these apps, user's privacy has been an afterthought and has resulted in mass violations of privacy of the public and the patients. A total of 32 countries have designed apps and rely on them as a strategy to flatten the pandemic curve. Along with lack of privacy, these methodologies are centralized, where they are fully controlled by the government and the healthcare providers. Owing to these and many other concerns, people are hesitant in the adoption of these technologies. This paper presents a detailed analysis of user tracking apps belonging to 32 countries, thus demonstrating that they collect personal data and are a gross violation of user privacy. This paper presents a novel architecture for the efficient, effective and privacy-preserving contact tracing of COVID-19 patients using blockchain. The proposed architecture preserves the privacy of individuals and their contact history by encrypting all the data specific to an individual using a privacy-preserving Homomorphic encryption scheme and storing it on a permissioned blockchain network. The contacts made with a COVID-19 positive patient are identified by performing search queries directly over the Homomorphic encrypted data stored in the blocks. Therefore, only those contacts that are suspected to be COVID-19 positive may be decrypted by the healthcare professional or government for further contact tracing/ diagnosis and COVID-19 testing; thereby leading to enhanced privacy.**

***Index Terms*—Coronavirus, Hyperledger Fabric, pandemic, searchable encryption.**

I. INTRODUCTION

ONE of the biggest challenge being faced by the world in the 21st century is dealing with the COVID-19 pandemic [1]. The virus originated on the 20th Oct, 2020, it has spread across every country, claimed more than 4.2 million lives and more than 200 Million positive cases have been reported worldwide [2]. The pandemic has widely effected all and its impact has been seen in both emerging and developed economies as industrial production and trade is adversely effected, leaving millions jobless resulting in global poverty. These unprecedented times have also put the healthcare systems of the world leading countries under stress. All countries have their own national healthcare systems which are considered mature enough to deal with any epidemic, pandemic or emergent situations. To name a few systems, the UK relies on the national health service (NHS), US has health and human services (HHS) while the Italian public health service is known as servizio asnitario nazionale (SSN). However, these system have struggled to cope with the pandemic and failed to offer healthcare services to the influx of patients suffering with COVID-19. The world leading hospitals grossly failed to provide the essential patient care materials and equipments including ventilators and intravenous pumps. Therefore, a mechanism was required to systematically control the community transmission of the virus in an attempt to reduce the number of patients seeking medical help.

The primary reason behind the spread of the Coronavirus is when an individual comes in contact with someone who is infected (COVID-19 positive). The world health organization (WHO) defines a contact as [3]:

- Being within 1 metre of a COVID-19 positive for more than 15 minutes;
- Coming in direct/physical contact with a COVID-19 positive case;
- Someone or a healthcare professional providing direct care for COVID-19 positive patients without following the defined SOPs and without using personal protective equipment (PPE).

According to the WHO, this virus can be contained by wearing PPE, maintaining social distance, self-isolating, and by concentrating on personal hygiene [4]. While all these methods have proven to be effective in prevention; the dominant method adopted internationally has been the enforcement of lock-down protocols through social distancing and self isolation. This gave rise to the dire need of having a mechanism to trace the community contacts made by a COVID-19 positive to contain the spread of the virus. In regard to this, many countries have been working on developing their own contact tracing apps, for example, UK has developed an NHS coronavirus app, US is planning to use the Exposure Notification API developed by Apple and Google, and Italy has already launched its version of contact tracing app called "Immuni".

The existing healthcare systems were governed by strict

Manuscript received March 25, 2021; revised August 7, 2021; approved for publication by Zhu Han, Guest Editor, August 26, 2021.

S. Tahir and F. Khan are with the Department of Information Security, College of Signals, National University of Sciences and Technology (NUST), Islamabad, Pakistan, email: {shahzaib.tahir, fawadkhan}@mcs.edu.pk.

H. Tahir is with the Department of Information Security, School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad, Pakistan, email: hasan.tahir@seecs.edu.pk.

A. Sajjad is with British Telecommunications Plc, UK, email: ali.sajjad@bt.com.

M. Rajarajan is with the School of Mathematics, Computer Science and Engineering, City, University of London, UK, email: r.muttukrishnan@city.ac.uk.

S. Tahir is the corresponding author.

Digital Object Identifier: 10.23919/JCN.2021.000031

1229-2370/21/$10.00 © 2021 KICS

rules and regulations such as the latest EU general data protection regulation (GDPR) [5], [6], applicable to all EU member states, and the health insurance portability accountability act (HIPAA) [7] enacted by the United States congress, lead to a compelling case to demonstrate accountability and compliance to these regulations. These regulations increased the patient's trust in the system that resulted in the patient willingly providing access to critical health data to enhance the quality, safety, and outcome of care. Thus, it was important to ensure that healthcare systems and devices process user data while maintaining privacy, security, and scalability. However, to deal with the pandemic and to perform effective contact tracing, many EU member states have flexed the existing regulations. For example, the Article 9(1) of the GDPR states [5]:

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

The above mentioned clause has now been suspended in the face of civil crisis and is supported by the following clause already part of the GDPR, Article 9(2-i) [5]:

> "Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;"

Similarly, Italian civil protection department during the early stage of the COVID-19 outbreak on February 3, 2020 adopted civil protection ordinance No.630 [8]. This ordinance allows the civil protection personnel to analyze the sensitive data restricted access to in the GDPR Article 9(1). HIPAA has been widely adopted by the US. The HIPAA regulation has not been suspended, rather the fines as a result of the violations have been removed for the time being to facilitate and encourage data analytics by the civil protection personnel in these unprecedented times and mainly for contact tracing. Similarly, France and Germany have also issued advisory notes that relax the existing regulations to facilitate contact tracing. Having said this, it would not be wrong to say that in the challenging times, in regards to contact tracing, security and privacy is being treated as an after thought. While the intention behind contact tracing was commendable and justified; its outcomes and implications were perhaps not given enough thought. Reliance on a policy does not give ground to a purpose that is questionable and does not make it justified. Due to the reduced regulatory influence on the contact tracing app, people often link this tracing capability as "lack of freedom" and hence it is being politicized. In [9] authors study public attitudes towards contact tracing apps within the UK. The main concerns highlighted by the people included; *a)* lack of privacy, *b)* social stigma, and *c)* lack of uptake.

Since the existing contact tracing services have suffered from weaknesses such as lack of privacy in sharing sensitive data with the third parties [10], [11]. As a result, the entire data can be disclosed to the third parties involved during the tracing process. Third parties such as healthcare providers, insurance companies, pharmacies, researchers, etc., should have different access privileges/views of the patient data so that security and privacy related issues can be addressed efficiently and effectively. Therefore, this leads to the requirement of an architecture that solves the following inherent problems related to contact tracing:

- Security and privacy
- Authentication and access control
- Flexibility and scalability
- Interoperability and efficiency

This paper explores a novel privacy preserving COVID-19 contact tracing (PPCCT) architecture that enables contact tracing, thereby addressing the problems enlisted above and refers to them as the design principles further discussed in the Section III. The PPCCT architecture primarily focuses on securely handling contact data including; the patient data held by the hospital to uniquely identify an individual found COVID-19 positive. The proposed architecture also takes care of the sensitive data related to other individuals with whom contact was made by a COVID-19 positive. PPCCT enables efficient contact management and tracing over a permissioned blockchain infrastructure. This enables the possibility of maintaining/inferring immutable contact records related to the users/ entities involved in the application. PPCCT architecture ensures a higher level of security and privacy preservation as it is based on privacy-preserving homomorphic-based searchable encryption (HSE) and the concept of permissioned Blockchain. These technologies jointly enhance the usability, security, efficiency, scalability, and immutability in a privacy-preserving manner.

A. Contributions

This research makes the following contributions to the field of healthcare:

- This paper analyzes the different COVID-19 tracing applications used worldwide by 32 countries and highlights their shortcomings in terms of security and privacy.
- The paper proposes a novel privacy-preserving COVID-19 contact tracing (CCT) architecture based on permissioned blockchain. The permissioned blockchain in effect helps to achieve immutability, provenance, traceability, transparency, enhanced security, and restricted access. The architecture is based on the use of state-of-the-art homomorphic-based privacy-preserving searchable encryption scheme.
- We design and develop a COVID-19 contact tracing solution to demonstrate the feasibility of the proposed PPCCT architecture. The developed solution highlights the functionality of the PPCCT architecture and the advantages it has to offer.

B. Organization

Section II discusses the existing contact tracing apps that are being used by 32 countries across the globe. Section III presents the proposed privacy preserving COVID-19 Contact Tracing architecture by highlighting the design principles. Section IV presents a discussion on the proposed architecture against the design principles presented in the Section III. Section V presents the COVID-19 contact tracing solution in the form of a proof of concept prototype after implementing the PPCCT architecture. The conclusions are drawn towards the end of the paper in Section VI.

II. PREVIOUS WORK

Countries around the globe are developing COVID-19 smartphone apps to help their respective health services with contact tracing and instantaneous notification to their citizens when and if their COVID-19 infection has been confirmed. The hope is that the wide deployment of these apps will help limit the spread of the coronavirus and enable the countries to relax their lockdown restrictions more quickly. Most of these apps are utilising Bluetooth LE [12] radio signals to check and log the proximity of smartphone users to each other, and then using either "centralised" or "decentralised" models to process the data gathered in this process. Similarly, a technique [13] has been proposed aiming to limit the outbreak of COVID-19 by determining a safe movement distance from a Bluetooth PAN creator. The authors have created an effective method that uses Bluetooth to measure distances with a high reliability.

In the centralised model, the data gathered from a user is uploaded to a central server, often managed by a national health service, where it is analysed with similar data gathered from other users. The centralised model gives better data analysis related insights to epidemiologists of the verified health authority. Various protocols have been designed around this model to facilitate logging of a user when in close proximity of other users, uploading and processing these contact logs on a centralized server and then individually notifying users of potential contact with an infected user. Pan-European privacy-preserving proximity tracing (PEPP-PT/PEPP) [14] and BlueTrace [15] are examples of protocols following the centralised model. These and similar protocols have been implemented as smartphone apps by many countries around the globe, e.g., the contact-tracing app deployed in China [16] collects data on a user's movements and uploads it to a central database. An AI system analyses this database and returns a colour code (green, amber or red), which is used to enforce restrictions on the user's movement. Similar apps have been deployed by South Korea [17], Singapore [18], India [19], Australia [20], etc. The main disadvantage of centralised contact-tracing apps is potential of privacy invasion [21], as all data shared by the users is fully visible to the central diagnostic and analysis service by design. This design also introduces a single point of data vulnerability and exposure in case of a successful attack on the service.

On the other hand, in the decentralised model, the data gathered from a user remains on his/her smartphone and not shared with a central server. Different protocols have been designed around this model to facilitate the tracking and logging of a user when in close proximity of other users, however all contact logs are not uploaded to a central server. Only once a user tests positive for an infection, a report containing their last 14 days' proximity data is sent to a central repository managed by a verified health authority. Other users can download reports of last 14 days from the repository and independently check them against their local contact logs for possible recent contacts with any infected person. Examples of protocols implementing this model are temporary contact number (TCN) protocol [22], decentralized privacy-preserving proximity tracing (DP3T) [23] and the Google/Apple exposure notification framework for contact-tracing [24]. This model has also been taken up and implemented by many countries like Italy [25], Germany [26], Poland [27], Switzerland [28], United Kingdom [29], etc. The decentralised model gives better privacy guarantees than the centralised model, but only with regard to location tracking of the users. A sophisticated attacker can still gain information about at-risk individuals and infected individuals by eavesdropping the Bluetooth signals and de-anonymising the contact logs of known reported users [30]. False alert injection attack is also a possibility where a malicious adversary can target a victim's app to raise false infection alerts. This model also requires more computing power on the client side to process the infection reports, which can be problematic on power-constrained smartphones. Similarly, [31] proposes a blockchain-based solution for the sharing of healthcare data. The authors present a blockchain solution that attains security and privacy while sharing the data globally. Although this research may be termed as a breakthrough, the granular data secrecy cannot be attained as all the peers part of the network will be authenticated and will share the same ledger.

Table I presents a detailed analysis of the COVID-19 contact tracing apps used by 32 countries. The table discusses the Country where the app is being used, app name, status (public/private/state), usage (mandatory/voluntary), data collected, and architecture (centralized/decentralized). The concerns are also highlighted that mainly focus on the security and privacy breeches. The column "Data Collected" is populated after analyzing the individual app and categorizing the data according to the guidelines of the WHO. Table II, highlights these categories and discusses the type of data collected. It is observed that the apps that are available to download from the play store are mostly centralised and most of them lead to security and privacy breech. Some of the apps take consent from the user before disclosing the data to the government officials or trusted third parities. Such apps are identified as "No known privacy concern prior to user's explicit permission". We also refer readers to [32]–[36] that present a survey of the existing contact tracing apps.

Research [37] has also studied the use of popular smartphone based non-cooperative game where the dominating strategy for all the players is to maintain home isolation. The proposed game maintains the Nash equilibrium and also allows the authors to assess the sustainability of a lockdown protocol with the proposed model. The proposed model allows one to determine the extent of effectiveness of the lock-down protocol

TABLE I
A COMPARISON OF COVID-19 CONTACT TRACING APPS USED IN DIFFERENT COUNTRIES.

Sr. No.	Country	App name	Status (public/private/state)	Usage (mandatory/voluntary)	Data collected	Architecture (centralised/decentralised)	Concerns
1.	Austria	Stopp Corona	State	Voluntary	Type of contact	Centralized	Inaccuracy
2.	Australia	COVIDSafe	State	Voluntary	Contact identification, type of contact	Centralized	Trusted third party, lack of data control, privacy breech
3.	Bahrain	BeAware Bahrain	Public	Voluntary	Contact identification	Centralized	Trusted third party, lack of data control, privacy breech
4.	Bulagria	ViruSafe	State	Voluntary	Contact identifications, symptoms	Centralized	Trusted third party, lack of data control, privacy breech
5.	Canada	ABTraceTogether	Public	Voluntary	Contact identifications	Centralized	Inaccuracy, trusted third party, lack of data control, privacy breech
6.	China	Alipay & WeChat	Private	Mandatory	Contact identifications	Centralized	Trusted third party, lack of data control, privacy breech
7.	Colombia	CoronApp	Public	Voluntary	Contact identification, demographics, symptoms, actions taken	Centralized	Trusted third party, lack of data control, privacy breech
8.	Cyprus	CovTracer	Public/private	Voluntary	Contact identification	Centralized	No known privacy concerns prior to the user's explicit permission.
9.	Czech Republic	eRouška & Mapy.cz	Public/private	Voluntary	Contact identification	Centralized	Trusted third party, lack of data control, privacy breech
10.	Ghana	GH COVID-19 Tracker	Public	Voluntary	Contact identification, type of contact, actions taken	Centralized	Trusted third party, lack of data control, privacy breech
11.	Iceland	Rakning C-19	State	Voluntary	Contact identification	Centralized	No known privacy concerns prior to the user's explicit permission.
12.	India	Aarogya Setu, Saiyam, COVA Punjab & Corona Watch	Public/private/state	Mandatory/Voluntary	Contact identification, actions taken	Centralized	Trusted third party, lack of data control, privacy breech
13.	Indonesia	Care Protect	State	Voluntary	Contact identification	Centralized	Trusted third party
14.	Israel	HaMagen & Track Virus	Public/private	-	Contact identification, type of contact,	Centralized	Trusted third party, lack of data control, privacy breech
15.	Italy	SM_COVID19	Private	Voluntary	Contact identification, type of contact	Decentralized	Trusted third party, lack of data control, privacy breech
16.	Kyrgyzstan	Stop COVID-19 KG	Public	-	Contact identification	Centralized	Trusted third party, lack of data control, privacy breech
17.	North Macedonia	StopKorona!	Private	-	Contact identification, type of contact	Centralized	No known privacy concerns prior to the user's explicit permission.
18.	Norway	Smittestopp	Public/private	Voluntary	Contact identification	Centralized	Trusted third party, privacy breech
19.	Pakistan	COVID-19 Gov PK	State	Voluntary	Contact identification, type of contact	Centralized	Trusted third party, lack of data control, privacy breech
20.	Philippines(Cebu)	WeTrace	Public/private	-	Contact identification, type of contact	Centralized	Trusted third party, lack of data control, privacy breech
21.	Poland	Home Quarantine & ProteGO-Safe	Public/private	Mandatory/Voluntary	Contact identification, type of contact, symptoms, actions taken	Decentralized	Trusted third party, lack of data control, privacy breech
22.	KSA	Rest Assured & Tawakkalna	Public	Mandatory/Voluntary	Contact identification, symptoms, actions taken	Centralized	Trusted third party, lack of data control, privacy breech
23.	Singapore	TraceTogether	Public	Voluntary	Contact identification	Centralized	No known privacy concerns prior to the user's explicit permission.
24.	Slovak Republic	ZostanZdravy	Private	-	Contact identification, actions taken	Centralized	No known privacy concerns prior to the user's explicit permission.
25.	South Korea	Corona 100m	Private	Voluntary	Contact identification, demographics	Centralized	Trusted third party, lack of data control, privacy breech
26.	Spain	CoronaMadrid	Public	Voluntary	Contact identification, symptoms,	Centralized	Trusted third party, lack of data control, privacy breech
27.	Sri Lanka	MyHealth Sri Lanka	Public	Voluntary	Contact identification	Centralized	Trusted third party
28.	Thailand	MorChana	Public/private	Voluntary	Contact identification, type of contact	Centralized	Trusted third party, lack of data control, privacy breech
29.	Turkey	Korona Önlem	Public	Mandatory	Contact identification, symptoms	Centralized	Unclear
30.	Ukraine	Act at home	Public	Voluntary	Contact identification	Centralized	Trusted third party, lack of data control, privacy breech
31.	USA	Private kit: SafePaths	Private	Voluntary	Contact identification	Centralized	No known privacy concerns prior to the user's explicit permission.
32.	UK	NHS COVID-19	State	Voluntary	Contact identification	Decentralized	No known privacy concerns prior to the user's explicit permission.

TABLE II
TYPE OF DATA COLLECTED BY A COVID-19 CONTACT TRACING APP.

Information category	Description
Contact identification	• Contact ID • Full name • Address/GPS location/proximity • Phone number • National identification number/passport number
Demographics	• Age • Gender • Relationship with the source contact • Occupation
Type of contact	• Type of contact • Date of contact • Duration of contact
Symptoms	• Fever • Sore throat • Cough • Shortness of breath • Diarrhoea • Loss of taste or smell • Others
Actions taken	• Date of sample collection • Contact's new location and contact details

with reference to its practicality and adherence by the people.

III. THE PROPOSED PPCCT ARCHITECTURE

A detailed study of the existing COVID-19 contact tracing apps (presented in the Section II) brings to light the need for a comprehensive system that provides security and privacy, authentication and access control, flexibility, scalability, interoperability and efficiency. The existing apps cannot be widely used due to major security concerns, and a novel privacy-preserving COVID-19 contact tracing architecture is therefore required. The contact tracing is influenced by a range of attacks that are possible on the data while being transmitted or at rest. These attacks include eavesdropping sensitive information and patient's privacy breach when they come in contact with a COVID-19 positive. The attackers can be insiders, outsiders, or both. The main asset that needs to be secured is the user's data. The confidentiality of the data should remain intact while at rest or during transmission. The identity of the user should be preserved until he/she comes in close contact with a COVID-19 positive. A major assumption made by the existing contact tracing architectures is that all stakeholders that are part of the process are fully trusted and only the outsiders are marked as a potential threat to the system. Therefore there is a need for an architecture that can also counter insider threats in contact tracing. Furthermore, the blockchain technology is widely being used for the provision of immutability and provenance. Blockchain is a peer-to-peer distributed ledger technology that efficiently records transactions in a sequential tamperproof manner while placing the app user/ patient at the center of the healthcare ecosystem. The transactions recorded on blockchains can be shared between individuals that are part of the network. Every transaction is immutable since it is timestamped when added to the ledger.

From the perspective of the application scenario in question; blockchains can be permissionless or permissioned. Permissionless blockchains are very open and enable pseudonyms/anonymous participants to append new blocks to the existing distributed ledger. This is a major disadvantage of permissionless blockchains which supports a very weak notion of security. In contrast to permissionless blockchains, permissioned blockchains are based on permissioned networks that allow only specific entities to participate in the ledger and thereby add transactions to the blockchain. Each entity is assigned a digital identity for identification by a trusted identity provider and access to the blockchain is granted based on the access rights governed by the identity provider. This enables different entities to participate in the permissioned blockchain based on the access rights assigned. Having said this, typical blockchains create a distributed peer-to-peer network where non-confident members can interact with each other without a trusted intermediary [38].

This paper explores the utilization of a distributed ledger technology (blockchain) as the underlying infrastructure. Table III shows a comparison between two well-known permissionless and permissioned blockchain implementations formally referred to as Ethereum and Hyperledger, respectively. The reader is referred to [39] where a comprehensive comparison of various blockchains is presented.

To design a state-of-the-art COVID-19 contact tracing architecture there are several aspects that need to be taken into account. We firstly elaborate the threat model and design principles that lead to the overview of the PPCCT architecture.

A. Design Principles for PPCCT

The PPCCT architecture requires adherence to certain design goals for secure and reliable contact monitoring and inference. Depending on the analysis presented in the Section II, we identify the security and access control requirements that give rise to the inter-related design principles as follows:

1) **Security and privacy** is the primary objective of the PPCCT architecture to preserve people's privacy, in accordance with the CIA (confidentiality, integrity, and availability) triad.
2) **Authentication and access control** in the proposed PPCCT architecture should enable only authenticated entities to become part of the COVID-19 contact tracing application. This will also ensure non-repudiation and accountability based on secure credentials associated with people.
3) **Flexibility and scalability** in the PPCCT should withstand bottlenecks and single point of failures. This requires a distributed architecture scalable across different entities involved in the contact tracing application. At the same time, the PPCCT architecture should be flexible enough to meet the requirements of the entities that are part of contact tracing architecture.

TABLE III
A COMPARISON OF ETHEREUM AND HYPERLEDGER.

Feature	Ethereum	Hyperledger
Architecture type	Generic blockchain platform	Modular blockchain platform
Model type	Permissionless	Permissioned
Consensus	Proof of work	Pluggable consensus
Governance	Ethereum	LINUX foundation
Smart contract implementation	Smart contracts	Chaincode
Currency	Ether and tokens based on smart contracts	Tokens based on chaincode

4) **Interoperability and efficiency** is an objective in the PPCCT architecture that should enable monitoring, identification and the contact data management. This goal can be achieved by designing a architecture that allows interoperability among different technologies, entities and components involved. This would result in the availability-on-demand, effective and efficient reporting activities between the entities.

B. PPCCT Reference Architecture

Fig. 1 presents the reference architecture for the proposed COVID-19 contact tracing application based on blockchain. The architecture is focused on Hyperledger Fabric and is an extension of the reference architecture presented by IBM in [40]. Table IV highlights the events that occur when the architecture is in place. It may be observed that the PPCCT architecture does not rely on a particular variant of the primitive technologies including encryption, access control, inference that are part of the PPCCT architecture. Therefore, the architecture can be tuned and integrated according to the application requirements.

IV. ANALYSIS OF THE PROPOSED PPCCT ARCHITECTURE

The following section discusses the provisioned security advantages of the PPCCT architecture with reference to the incorporated technologies and the design goals mentioned in Section III. The incorporated technologies have been carefully chosen as a consequence of which the desired security goals are achieved.

A. Security and Privacy

In the proposed PPCCT architecture, access can be gained only by those who are using the COVID-19 contact tracing App and have been granted access to a specific action on the PPCCT network. Privacy in PPCCT is maintained by agreement about which entity has access/permission to what resource. As PPCCT is a permissioned blockchain architecture, data stored on the blockchain can be shared securely with only pre-approved and trusted group of entities. Furthermore, since the data is homomorphically encrypted at the source, this maintains the confidentiality of the data at rest and during transmission. Each trusted entity has a private key and a public key that acts as an open identifier. A person's private key is required to access the relevant information from the blockchain. This public/private key encryption scheme allows patients to share unique information with different contact tracing data providers on an as-needed-basis. Even if a patient's private key is exposed, the damage is contained and other records remain secure. The PPCCT architecture makes use of a privacy-preserving homomorphic-based searchable encryption (HSE) that provides confidentiality of the data while preserving the privacy of the contact data. Hence, the merger of these technologies in the PPCCT architecture helps to achieve the security and privacy goals. The proposed PPCCT architecture thwarts the possible attacks as the data is encrypted at the source, therefore, eavesdropping, spoofing, or any type of meaningful manipulation of source data is not possible. Furthermore, since the architecture is based on permissioned blockchain, only an authorized person can gain access to the network hence reducing the attack surface associated with unauthorized access.

B. Authentication and Access Control

The PPCCT architecture integrates technologies specifically designed for enforcing authentication and access control. The PPCCT architecture utilizes the services of a permissioned blockchain that fully govern all the access control policies involved in the architecture. The access management module is able to manage security objects like X.509 certificates and tokens, as well as provide ABAC services based on the XACML standard. For authentication, token-based authentication [41] has been used, which authenticates users with their usernames and password, and obtains a time-limited cryptographically secure token upon successful authentication. They are now able to use that token for further authentication for a session of limited duration. Access control is provided through a XACML policy decision point (PDP), which is a decision engine that evaluates user or administrator defined access control policies to provide fine-grained access control to the available resources. An advantage of this authentication and access control approach is that the users can share their tokens with some trusted entities not only for a limited time but also a limited set of resources, without having to share their usernames, passwords or other sensitive security credentials. This approach is also useful for security evaluation and auditing purposes.

By virtue of the incorporated technologies; the PPCCT environment enables people/ patient to maintain full access and control of their own data, providing access to the government officials they would like to share their data with. This enables government officials, hospitals, doctors and patient to connect and share information instantly and seamlessly, in a secured way. This is also ideal for medical research, facilitating studies that can help to better understand COVID-19.

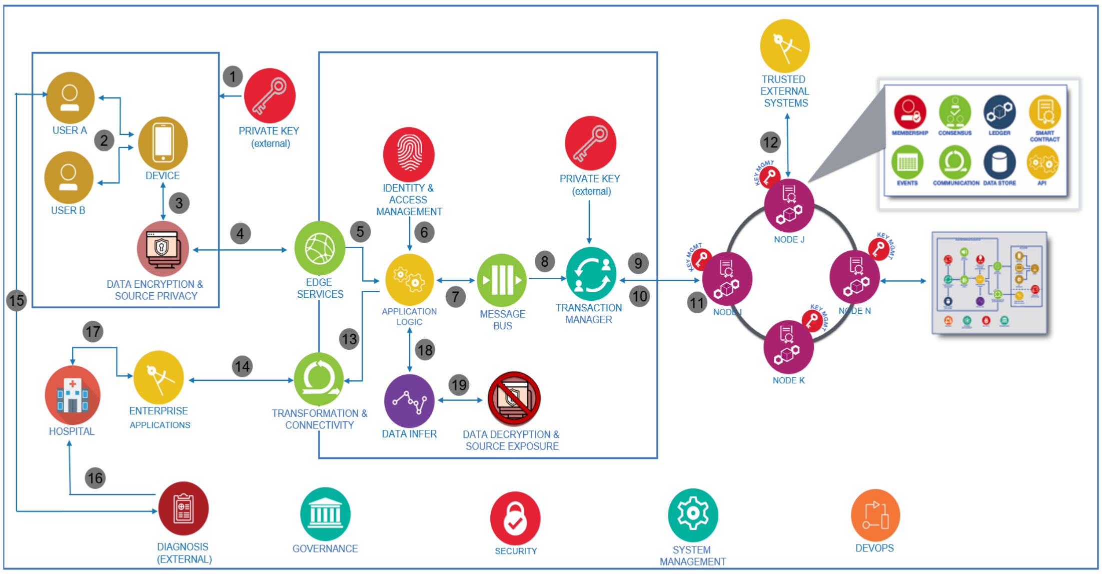
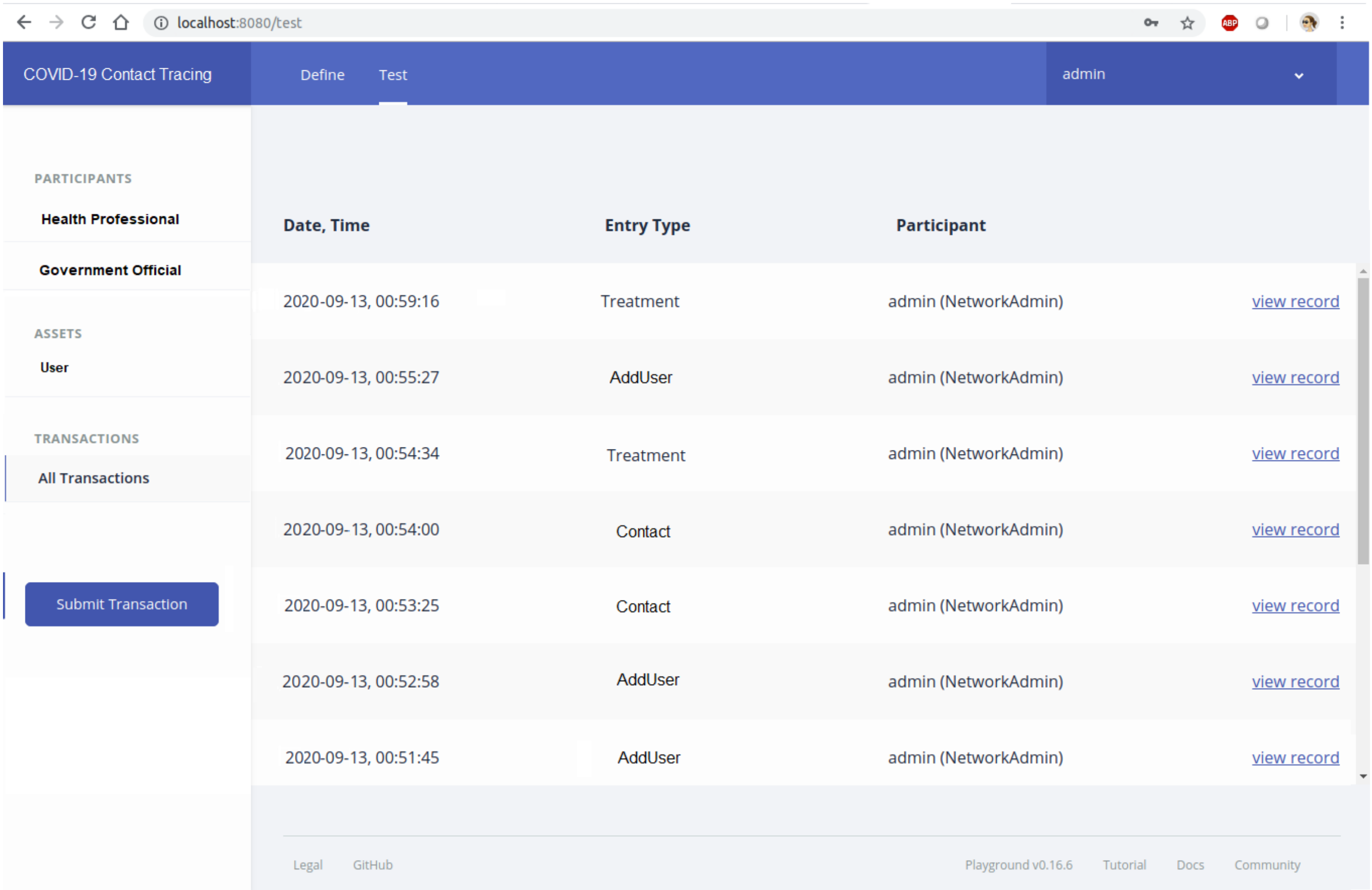


Fig. 1. Proposed reference architecture.

TABLE IV
DESCRIPTION ON THE STEPS INVOLVED IN THE PPCCT ARCHITECTURE.

Steps	Description
1	A user has already registered with an application encryption server and fetches his private key. This key will be used for verification purposes and will be used to access the contact tracing application.
2	A user gains access to the blockchain network through his mobile device that runs a contact tracing application.
3	The mobile application encrypts the data at source before sharing it across the peers. The data is encrypted using homomorphic encryption
4	The edge services convert the homomorphically encrypted data into the blockchain-specific format.
5	The request along with the data specifics are forwarded to the blockchain application and forwarded to the peers.
6	Since, the blockchain application is a private network; it uses the identity and access management to authenticate and authorize a user access/modification to the ledger.
7	The application logic invokes the smart contract by forwarding/ routing user requests to the transaction manager via an optional message bus.
8	The transaction manager processes the requests received from the application logic via the message bus.
9	The transaction manager invokes the smart contract depending upon the request received from the application logic and in relation to the user credentials. The request can primarily include, put, get or query a transaction. Put transaction will be triggered to make note of the contacts made by a user. Get may be triggered to uncover the identity of the user once tested positive for COVID-19. A query may be triggered to reveal the contacts made with a COVID-19 positive patient.
10	The transaction manager invokes the smart contract and the payload depending upon the type of request made, the transaction is added to the ledger of the appropriate nodes.
11	The blockchain network relies on a consensus algorithm. The permissioned blockchain will use endorsing peers that will endorse a transaction based on byzantine fault tolerance and ordering service. This will govern that only correct information is added to the ledger.
12	In some cases, the blokchcain will need to be accessed by external systems such as insurance companies, WHO, pharmacists, etc. This would essentially disclose anonymized data such as the total number of positive cases.
13	The application interfaces with the external enterprise applications for further analytics of the data store on the blockchain network.
14	The user identification information is stored on the enterprise application.
15	An external COVID-19 test is performed that may be a PCR test, RNA test or antibody test.
16	The COVID-19 test result is shared with the hospital.
17	The hospital may send the report to the enterprise application, that is further sent to the application logic via the transformation and connectivity
18	For positive cases reported, the data will be inferred to uncover the contacts made with a COVID-19 positive patient.
19	Upon the successful identification of the relevant blocks containing data regarding the contact made with a COVID-19 positive patient, the data will be decrypted and the identities will be revealed for further testing by the hospital.
Note:	During the entire process, the data is not decrypted or revealed to the unauthorized entities. Get commands can be triggered only over the transactions that have been identified to contain information regarding the contact with the COVID positive. This would then disclose a subset of the anonymized data to only authorized personnel. The authorized person would further perform some diagnosis or share the data with the healthcare department.



Date, Time	Entry Type	Participant	
2020-09-13, 00:59:16	Treatment	admin (NetworkAdmin)	view record
2020-09-13, 00:55:27	AddUser	admin (NetworkAdmin)	view record
2020-09-13, 00:54:34	Treatment	admin (NetworkAdmin)	view record
2020-09-13, 00:54:00	Contact	admin (NetworkAdmin)	view record
2020-09-13, 00:53:25	Contact	admin (NetworkAdmin)	view record
2020-09-13, 00:52:58	AddUser	admin (NetworkAdmin)	view record
2020-09-13, 00:51:45	AddUser	admin (NetworkAdmin)	view record

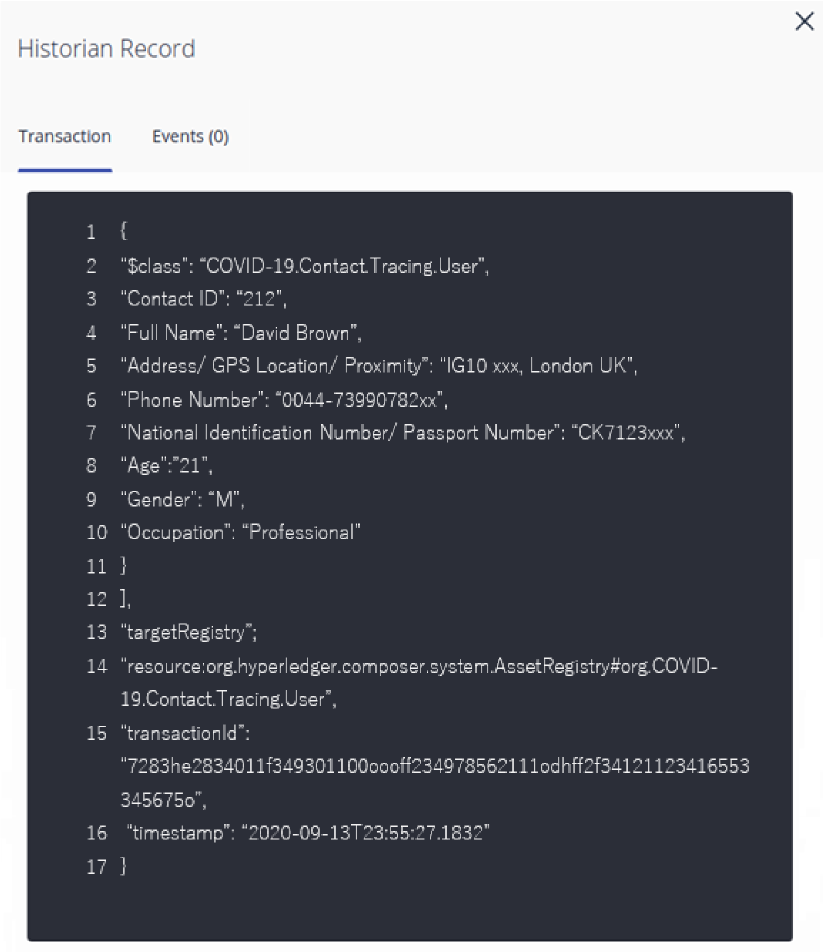
Fig. 2. COVID-19 contact tracing Hyperledger Fabric network-ledger overview.

C. *Flexibility and Scalability*

PPCCT is based on a distributed ledger technology, thus preventing bottle-necks and single point of failures in the COVID-19 contact tracing. The distributed nature of the ledger also ensures that no permissioned member or a group of members can modify or control the entries in the ledger. This is of great importance in types of applications where the participating members do not fully trust each other. To manage the work load created by the users on the distributed ledger, its members can dynamically increase or decrease the number of nodes participating in the ledger. Every node in the distributed ledger is considered equal to other nodes, however, some nodes can have different roles in the manner in which they participate in the blockchain network. For example, some nodes may store partial copies of the blockchain, some may store a full copy of the blockchain and some may only validate transactions. Thus members are flexible to choose which kind of role they want to play in the architecture by focusing on the types of nodes they include in the blockchain, and also to manage how they want to scale their participation in the architecture by increasing or decreasing the number of nodes they include in the blockchain. Furthermore, in the real world setting the application would be extended to a cloud-based solution, thereby benefiting from the extensive benefits the cloud has to offer including but not limited to scalability, elasticity, remote processing and availability. The usage of the cloud would further compliment the features of the the PPPCCT solution.

D. *Interoperability and Efficiency*

PPCCT for effective monitoring and COVID-19 record management could help government organizations bridge traditional data management problems, thereby considerably increasing the efficiency. PPCCT's transparent architecture eliminates the need for time-consuming reporting activities that may also lead to single point of failure between the entities part of the COVID-19 contact tracing application. Hence, this improves the coordination between the healthcare entities, thereby increasing the quality and timeliness of contact tracing. PPCCT also reduces the business costs whereby the costs of transferring contact records between entities will be reduced, compliance costs will go down, and auditing will be much easier. Hyperledger by default supports offerings from different vendors, which ensures the interoperability of the different solutions developed using Hyperledger Fabric. The proposed PPCCT architecture can be extended to a software development toolkit (SDK) that would allow integration with an existing COVID-19 bulletin framework, therefore allowing on-go integration and interoperability.



```
{
"$class": "COVID-19.Contact.Tracing.User",
"Contact ID": "212",
"Full Name": "David Brown",
"Address/ GPS Location/ Proximity": "IG10 xxx, London UK",
"Phone Number": "0044-73990782xx",
"National Identification Number/ Passport Number": "CK7123xxx",
"Age":"21",
"Gender": "M",
"Occupation": "Professional"
}
],
"targetRegistry";
"resource:org.hyperledger.composer.system.AssetRegistry#org.COVID-
19.Contact.Tracing.User",
"transactionId":
"7283he2834011f349301100oooff234978562111odhff2f34121123416553
345675o",
 "timestamp": "2020-09-13T23:55:27.1832"
}
```

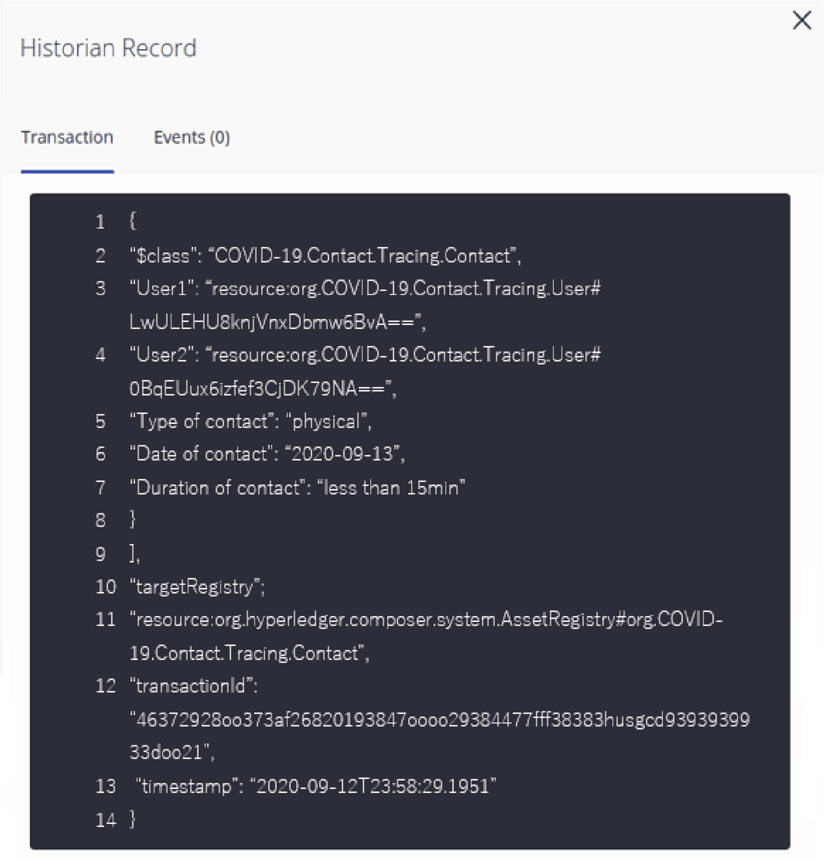
Fig. 3. COVID-19 contact tracing Hyperledger Fabric network-user record.

V. COVID-19 Contact Tracing Solution

We use Hyperledger Fabric (HLF) [42] for the implementation of the COVID-19 contact tracing (CCT) solution. Hyperledger Fabric is an open-source solution for deploying and running distributed applications on permissioned blockchains. Permissioned blockchains are setup among a group of known and identified users or organisation. Permissioned blockchains provide a way to insure integrity of the transactions among a group that have a common goal but which may not fully trust each other. The distributed applications in Hyperledger Fabric can be written in standard, general-purpose programming languages like Java, Go or Node.js, etc. which makes it easier to be integrated with existing code-bases. The CCT blockchain solution instantiates and uses the following components provided by HLF:

- An orderer service, which atomically broadcasts state updates to peers and establishes consensus on the order of transactions;
- A membership service provider (MSP), which associates peers with cryptographic identities;
- Peers, which maintain the ledger locally in form of an append-only blockchain and as a snapshot of the most recent state in a key-value store.

The CCT blockchain solution consists of a HLF network comprising of 4 peers representing two different organizations, the Hospital and the user, and an orderer node. At the initial bootstrapping time of our HLF network, the prototype generates all of the certificates and keys for our various network entities, the genesis block for the ordering service, and a collection of configuration transactions required to configure the blockchain. After this step, our prototype sets up the blockchain infrastructure using docker and docker-compose [43], such that each peer node, as well as the orderer service, is instantiated as a docker container. After the blockchain network has been started and provisioned, the main operation is to ensure that the transactions conducted by the participants of the blockchain are validated according to a common policy, that is agreed between the designated participants of the blockchain network. This common policy is also referred to as the consensus protocol or chaincode of the HLF network. In the context of the CCT blockchain solution, the consensus is reached by creating a model in terms of assets, participants, and transactions. Assets are tangible or intangible goods, services, or property; participants are uniquely identifiable entities that can own assets and submit transactions; and transactions are functions or rules that govern how participants



```
{
"$class": “COVID-19.Contact.Tracing.Contact”,
"User1": “resource:org.COVID-19.Contact.Tracing.User#
LwULEHU8knjVnxDbmw6BvA==”,
"User2": “resource:org.COVID-19.Contact.Tracing.User#
0BqEUux6izfef3CjDK79NA==”,
“Type of contact”: “physical”,
“Date of contact”: “2020-09-13”,
“Duration of contact”: “less than 15min”
}
],
“targetRegistry”;
“resource:org.hyperledger.composer.system.AssetRegistry#org.COVID-
19.Contact.Tracing.Contact”,
“transactionId”:
“46372928oo373af26820193847oooo29384477fff38383husgcd93939399
33doo21”,
 “timestamp”: “2020-09-12T23:58:29.1951”
}
```

Fig. 4. COVID-19 contact tracing Hyperledger Fabric network ledger-contact record.

interact with the assets. We created the model for the CCT blockchain solution using Hyperledger composer [42], which is a development toolset that can work with HLF.

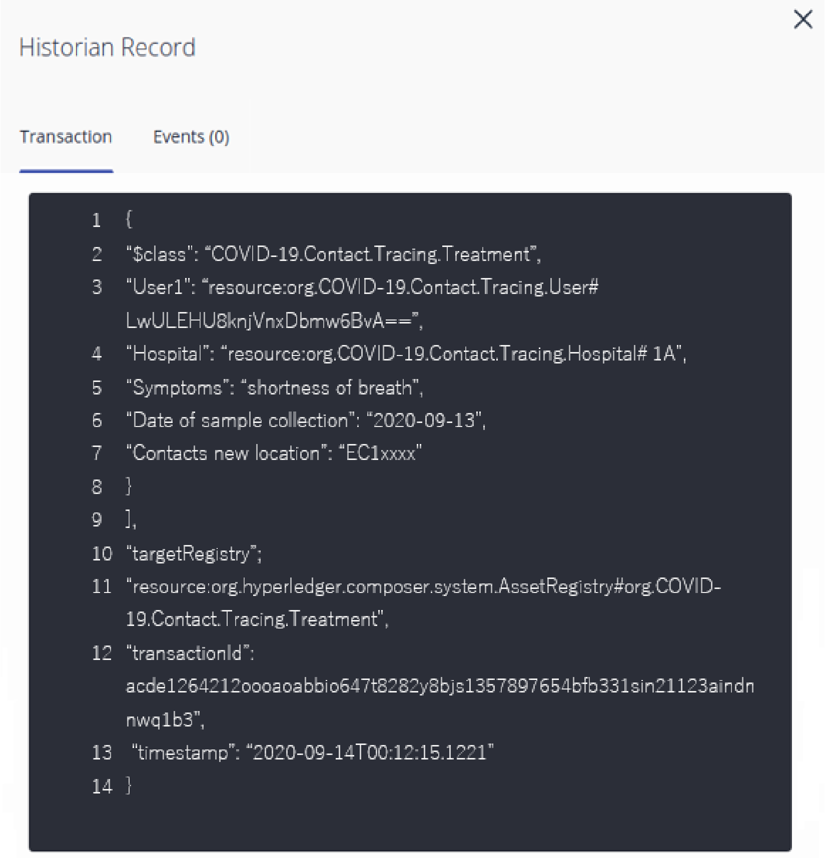
A. *Proof-of-Concept Demonstration*

To model the proposed PPCCT architecture, a COVID-19 contact tracing (CCT) Blockchain solution has been developed in Hyperledger. The developed CCT Blockchain solution is based on government officials and hospitals being the participants and the users/ patients being the assets in the COVID-19 registry. The government officials are added to the COVID-19 registry based on their attributes such as ID, first name, and last name. The users are added to the COVID-19 registry based on their contact identification. The hospital and goverment official can submit and retrieve transactions associated with a user. This section depicts the full working of the CCT blockchain solution. It is worth mentioning that the CCT blockchain solution is implemented as a coherent application. The components involved in the PPCCT architecture run in the back end of the CCT solution and cannot be demonstrated. For this reason, a comprehensive discussion and analysis of the underlying architecture is presented in the earlier sections and thereby finally demonstrating the front end of the system in this section. Hence, this entire paper covers the front end and back end aspects of a fully functional CCT solution.

Fig. 2 shows the record of all transactions that are part of the ledger. This record of transactions can be accessed and retrieved by the health professional or government officials.

All activity that is carried out by the participants as part of the CCT blockchain solution is logged and the ledger in Fig. 2 showcases the log of all these transactions. As mentioned in the Section III, all the data records related to the contact are encrypted before being stored on the ledger. Therefore, the system allows a range of queries over the encrypted data to identify the connections and accordingly stores the data as a transaction. The record of all transactions can be retrieved by the health professional or government official by selecting all transactions; thereby viewing all the transactions that have been carried out. Each transaction in the ledger has a timestamp and a type associated with the transaction. The type associated with the transaction is an attribute that is assigned at the time of participant creation, asset creation or creation of a new transaction. The AddUse type signifies the addition of a new user to the COVID-19 contact tracing Hyperledger Fabric network, the contact signifies the type of contact made to a user already part of the network and the treatment is triggered by the hospital to treat a COVID-19 positive patient.

A detailed record of each transaction can be retrieved by the participant by clicking view record. Fig. 3 depicts a health professional viewing detailed historian record of a user. As per the guidelines of the WHO (presented in Table I), the historian record for the user shows that a unique id is assigned to a



```
{
"$class": “COVID-19.Contact.Tracing.Treatment”,
“User1”: “resource:org.COVID-19.Contact.Tracing.User#
LwULEHU8knjVnxDbmw6BvA==”,
“Hospital”: “resource:org.COVID-19.Contact.Tracing.Hospital# 1A”,
“Symptoms”: “shortness of breath”,
“Date of sample collection”: “2020-09-13”,
“Contacts new location”: “EC1xxxx”
}
],
“targetRegistry”;
“resource:org.hyperledger.composer.system.AssetRegistry#org.COVID-
19.Contact.Tracing.Treatment”,
“transactionId”:
acde1264212oooaoabbio647t8282y8bjs1357897654bfb331sin21123aindn
nwq1b3”,
 “timestamp”: “2020-09-14T00:12:15.1221”
}
```

Fig. 5. COVID-19 contact tracing Hyperledger Fabric network ledger-treatment record.

user and the application records the full name, address, phone number, passport number, age, gender, and occupation of the user. The timestamp and transaction id are parameters that are maintained by the CCT blockchain solution but can be used by the health professional or government official to see the timestamp of a certain event/activity.

Fig. 4 shows health professional or government official of the specifics of the contact that was made between two users. The user id’s are encrypted to achieve confidentiality. Whereas, the type of contact, date of contact, and contact duration is recorded. Fig. 5 shows the treatments that were recommended/carried out associated with a COVID-19 positive. The symptoms are recorded, samples are collected, and the patient is isolated. From this point onwards, the government official will perform search across the encrypted user ids to identify the contacts made with other users and the COVID-19 sample collection will carry on to be conducted.

B. Computational Complexity

The most resource intensive task of the proposed CCT blockchain solution is the computations required to homomorphically encrypt the data segments. Although the proposed PPCCT architecture is not dependent on a particular variant of homomorphic encryption and has the ability to adapt any variant, to demonstrate this capability and its feasibility, the homomorphic encryption library (HElib-BGV) [44] has been implemented on a stand alone system. The system specifications include Ubuntu 18.04 running over an Intel Core i7 processor having 8GB RAM. The CCT blockchain solution is mainly based on the encryption, search and the decryption operations supported by homomorphic encryption. For illustration of the results, we have taken a total of 100 data segments that are encrypted gradually with an increment of 10 segments on each iteration. Figs. 6, 7, and 8 demonstrate the time required to encrypt, search, and decrypt those 100 data segments. It can be observed that these operations generally

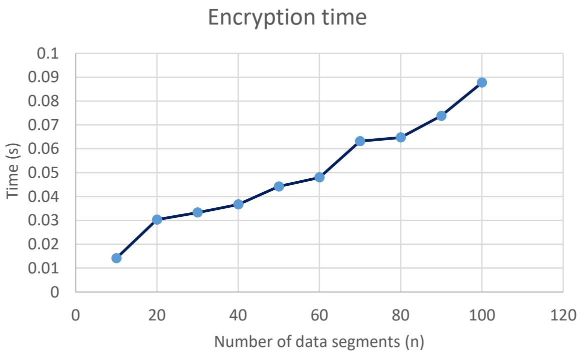


Fig. 6. Homomorphic encryption-time required to encrypt.

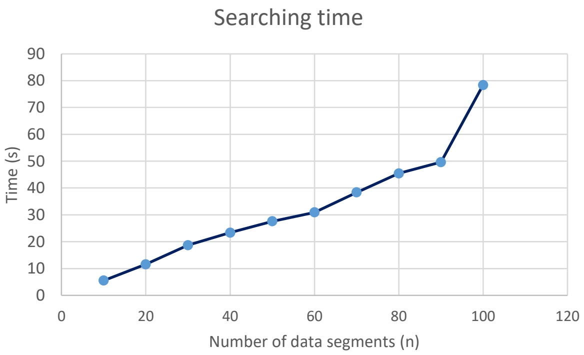


Fig. 7. Homomorphic encryption-time required to search.

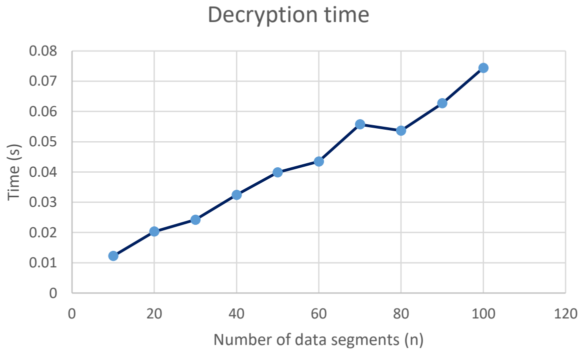


Fig. 8. Homomorphic encryption-time required to decrypt.

show a linear growth with the increase in the data segments. The total time required to encrypt the 100 data segments is 0.088 s. Whereas, for the search and decryption the total time required is 77.3 s and 0.074 s, respectively.

As apparent from the demonstration of the CCT blockchain solution, the proposed PPCCT architecture is a more secure, privacy preserving, reliable, effective and efficient solution for the COVID-19 contact tracing.

VI. Conclusion

The COVID-19 pandemic has stunned the world due to its impact on human health. The pandemic has spread so rapidly that many nations were ill prepared to combat its spread which led to unnecessary deaths. Once the healthcare system started to show signs of being overwhelmed governments followed the recommendations of the WHO and enforced lock down protocols of various stringency to limit the community spread of the pandemic. To track the movement of individuals in lock down and monitor interactions at the community level, a total of 32 countries put effort to launch smartphone apps that collect data of various nature. This paper presents a detailed study of the apps introduced by 32 countries and shows that the apps collect personal data on a vast level which is a gross violation of user privacy. Analysis has shown that the applications collected data related to demographics, contact identification, type of contact made with COVID positive individual, user symptoms, etc. Owing to this the apps were not well received by the users and concerns were expressed over their privacy. This paper proposes a novel privacy-preserving COVID-19 contact tracing (PPCCT) architecture. The PPCCT architecture is based on blockchain Hyperledger Fabric and offers enhanced security, privacy, authentication, access control, flexibility, scalability, interoperability and efficiency thanks to the state-of-the-art technologies including searchable encryption and inference over the encrypted blockchain data. The proposed architecture has the potential to resolve all the prevalent issues in the existing application and if deployed could effectively and efficiently flatten the COVID-19 curve by limiting the proliferation of community spread cases.

Acknowledgment

This work was done collaboratively by the Information Security and Privacy Lab, NUST supported by the National Centre for Cyber Security, Pakistan, under the project titled “Privacy Preserving Search over Sensitive Data Stored in the Cloud” and the City, University of London, UK.

References

[1] A. A. Balkhair, “COVID-19 pandemic: A new chapter in the history of infectious diseases,” *Oman Medical J.*, vol. 35, no. 2, p. e123, 2020.

[2] “COVID-19 dashboard by the center for systems science and engineering (CSSE) at johns hopkins university (JHU).” [Online]. Available: https://coronavirus.jhu.edu/map.html

[3] World health organization *et al.*, “Contact tracing in the context of covid-19: interim guidance, 10 may 2020,” Tech. Rep., 2020.

[4] L. Cirrincione *et al.*, “COVID-19 pandemic: Prevention and protection measures to be adopted at the workplace,” *Sustainability*, vol. 12, no. 9, p. 3603, 2020.

[5] European commission. 2018 reform of EU data protection rules. [Online]. Available: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

[6] C. J. Hoofnagle, B. van der Sloot, and F. Z. Borgesius, “The european union general data protection regulation: What it is and what it means,” *Inf. Commun. Technology Law*, vol. 28, no. 1, pp. 65–98, 2019.

[7] P. Edemekong, P. Annamaraju, and M. Haydel, “Health insurance portability and accountability act,” *StatPearls*, vol. 72, no. 2, pp. 9–18, 2020.

[8] S. Ikeda, “Coronavirus adds an extra layer of challenge to collection and handling of health data under the GDPR,” Apr. 2020. [Online]. Available: https://www.cpomagazine.com/data-protection/coronavirus-adds-an-extra-layer-of-challenge-to-collection-and-handling/

[9] S. N. Williams, C. J. Armitage, T. Tampe, and K. Dienes, “Public attitudes towards COVID-19 contact tracing apps: A uk-based focus group study,” *Health Expectations*, vol. 24, no. 2, pp. 377–385, 2021.

[10] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure and trustable electronic medical records sharing using blockchain,” in *AMIA annual symposium proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 650.

[11] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” *Information*, vol. 8, no. 2, p. 44, 2017.

[12] R. Faragher and R. Harle, “Location fingerprinting with bluetooth low energy beacons,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 11, pp. 2418–2428, 2015.

[13] M. S. Munir, D. H. Kim, A. K. Bairagi, and C. S. Hong, “When cvar meets with bluetooth pan: A physical distancing system for COVID-19 proactive safety,” *IEEE Sensors J.*, vol. 21, no. 12, pp. 13 858–13 869, 2021.

[14] PEPP-PT Team. Pan-European privacy-preserving proximity tracing. [Online]. Available: https://github.com/pepp-pt/pepp-pt-documentation/blob/master/PEPP-PT-high-level-overview.pdf

[15] J. Bay *et al.*, “Bluetrace: A privacy-preserving protocol for community-driven contact tracing across borders,” *Government Technology Agency-Singapore, Tech. Rep*, 2020.

[16] S. Chen, J. Yang, W. Yang, C. Wang, and T. Bärnighausen, "COVID-19 control in China during mass population movements at new year," *The Lancet*, vol. 395, no. 10226, pp. 764–766, 2020.

[17] Ministry of the interior and safety. South korea-self-quarantine safety protection app. [Online]. Available: https://play.google.com/store/apps/details?id=kr.go.safekorea.sqsm

[18] Singapore Government agency. "tracetogether". [Online]. Available: https://www.tracetogether.gov.sg/

[19] Government of India. "aarogya setu". [Online]. Available: https: //play.google.com/store/apps/details?id=nic.goi.aarogyasetu

[20] Government of Australia. The COVIDSafe app. [Online]. Available: https://www.australia.gov.au/app

[21] H. Coffey, "Coronavirus tracking app exposes cheating partners in South Korea," May 2020. [Online]. Available: https://www.independent.co.uk/life-style/love-sex/coronavirus-tracking-app-cheating-partners-married-south-korea-affair

[22] E. Daw, "Component-based comparison of privacy-first exposure notification," May 2020. [Online]. Available: https://tcncoalition.files.wordpress.com/2020/05/tcn_component_based_comparison_between_privacy_first_exposure_notification_protocols.pdf

[23] C. Troncoso *et al.*, "Decentralized privacy-preserving proximity tracing," *arXiv preprint arXiv:2005.12273*, 2020.

[24] Privacy-preserving contact tracing. [Online]. Available: https://www.apple.com/covid19/contacttracing/

[25] Governo Italiano Presidenza del Consiglio dei Ministri. Immuni. [Online]. Available: https://www.immuni.italia.it/download.html

[26] Corona-Warn-App open source project. Corona-Warn-App. [Online]. Available: https://www.coronawarn.app/en/

[27] Republic of Poland. ProteGo Safe. [Online]. Available: https: //www.gov.pl/web/protegosafe

[28] Swiss Federal office of public health. Swisscovid. [Online]. Available: https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html

[29] NHS COVID-19 app. [Online]. Available: https://www.nhsx.nhs.uk/covid-19-response/nhs-covid-19-app/

[30] S. Vaudenay, "Analysis of DP3T between Scylla and Charybdis," Apr. 2020. [Online]. Available: https://eprint.iacr.org/2020/399.pdf

[31] S. Biswas *et al.*, "GlobeChain: An interoperable blockchain for global sharing of healthcare data - a COVID-19 perspective," *IEEE Consumer Electron. Mag.*, vol. 10, no. 5, pp. 64–69, Sept. 2021.

[32] J. Li and X. Guo, "COVID-19 contact-tracing apps: A survey on the global deployment and challenges," *arXiv preprint arXiv:2005.03599*, 2020.

[33] L. Simko, R. Calo, F. Roesner, and T. Kohno, "COVID-19 contact tracing and privacy: Studying opinion and preferences," *arXiv preprint arXiv:2005.06056*, 2020.

[34] L. Reichert, S. Brack, and B. Scheuermann, "A survey of automatic contact tracing approaches," *ACM Trans. Comput. Healthcare*, vol. 2, no. 2, pp. 1–33, 2021.

[35] A. Aravindan and S. Phartiyal, "Bluetooth phone apps for tracking COVID-19 show modest early results," *Reuters, April*, vol. 21, 2020.

[36] "Office of the privacy commissioner: Overview of COVID-19 contact tracing apps," 12 May 2020. [Online]. Available: https://privacy.org.nz/assets/2020-05-12-OPC-Comparison-of-COVID-19-Apps-colours.pdf

[37] A. K. Bairagi *et al.*, "Controlling the outbreak of COVID-19: A noncooperative game perspective," *IEEE Access*, vol. 8, pp. 215 570–215 581, 2020.

[38] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, 2017.

[39] Z. Hintzman, "Comparing blockchain implementations," in *2017 Fall Technical Forum*. SCTE/ISBE, 2017, pp. 1–29.

[40] IBM-blockchain architecture for trusted transactions. [Online]. Available: https://www.ibm.com/cloud/architecture/architectures/blockchainArchitecture/reference-architecture

[41] R. Winch, *Spring Security 3.1*. Packt Publishing Ltd, 2012.

[42] E. Androulaki *et al.*, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. ACM EuroSys*, 2018.

[43] J. Turnbull, *The docker book*. Lulu. com, 2014.

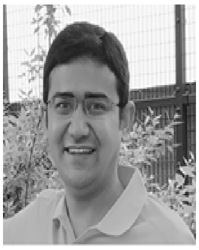
[44] Helib documentation. [Online]. Available: https://homenc.github.io/HElib/

Shahzaib Tahir received his Ph.D. in Information Engineering from City, University of London, UK in January 2019. He received his B.E. degree in Software Engineering from Bahria University, Islamabad, Pakistan, in 2013. In 2015, he received his M.S. degree in Information Security from NUST, Islamabad, Pakistan. Currently, he is an Assistant Professor in the Department of Information Security, NUST. He is also the Founder and the Chief Technical Officer of CityDefend Limited, UK. His research interest include applied cryptography and cloud security. He is a Senior Member of IEEE. He is a Reviewer of many high impact journals including IEEE Transactions on Dependable and Secure Computing, IEEE Journal of Biomedical and Health Informatics, IEEE ICC, Elsevier FGCS, Springer Cluster Computing, Springer Sadhna, Springer Science China Information Sciences, Springer Neural Computing and Applications. He has been a TPC Member of many international IEEE conferences. Dr. Shahzaib Tahir is also an alumni of InnovateUK CyberASAP.

Hasan Tahir is an Assistant Professor and Head of Department Information Security at School of Electrical Engineering and Computer Science (SEECS), NUST. He holds a Ph.D. in Information Security from the University of Essex UK. He obtained his B.E. in Software Engineering from Bahria University, Islamabad, Pakistan and MS in Software Engineering from College of E&ME, NUST. He was the recipient of the University of Essex Doctoral Scholarship award. He specializes in Computer Security and IoT. He actively researches applications of cryptography in one to one and group settings. His primary area of research is the use of Physically Unclonable Functions for securing group of devices. He teaches courses related to applied cryptography, cyber security, information security management, cloud computing security, software engineering, software requirements analysis and design. He has served as a committee member in many renowned IEEE conferences. He is a Senior Member of IEEE.

Ali Sajjad is a Senior Security Researcher in British Telecom UK, where he contributes to internal research and innovation programmes and international research collaboration activities in the areas of Secure Cloud Storage, Cyber Security and Cloud-based Managed Security Services. He has over 10 years' academic and industrial experience in Data and Network Security. He holds a Ph.D. in Information Engineering from City University London, UK and Masters degree in Computer Engineering from Kyung Hee University, Seoul, South Korea.

Muttukrishnan Rajarajan is Professor of Security Engineering at the City, University of London, UK. He obtained his Ph.D. from City University London in 2001. His research expertise are in the areas of mobile security, intrusion detection and privacy techniques. He has chaired several international conferences in the area of information security and involved in the editorial boards of several security and network journals. He is also a visiting fellow at the British Telecommunications (BT) UK and is currently actively engaged in the UK Governments Identity Assurance programme (Verify UK). He is a Senior Member of IEEE, Member of ACM and Advisory board member of the Institute of Information Security Professionals UK.



F. Khan received his Ph.D. degree from the School of Cyber Engineering, Xidian University in 2018. Currently he works at the National University of Science and Technology, Pakistan. His research interests includes but not limited to outsourced data access control, blockchain, and privacy preserving techniques. His professional services include Technical Program Committee Member and reviewer for several international journals and conferences.