**Chapter Four**

**METHODOLOGY**

This chapter provides an overview of the strategies used to attain the study's goals. It describes the study's respondents as well as the research instruments that were used. It then goes on to explain the data collection strategies that contributed in the completion of the study endeavor.



**Figure 4.1 Prototype Model Phases and Process**

Figure xxx illustrates Prototype Model used by the researcher in developing the proposed study entitled “CoviBlock: A Blockchain and Peer-to-peer Platform for Covid-19 Test Results and Vaccine Records” which is under the family of System Development Life Cycle (SDLC). Prototyping was used to ensure faster turnaround time on each phase while addressing client’s requirements and feedbacks. This model also enables the researcher and client to have discussions in between development cycles.

The next sections of this chapter will discuss the phases of the used model.

**4.1 Requirements Modeling**

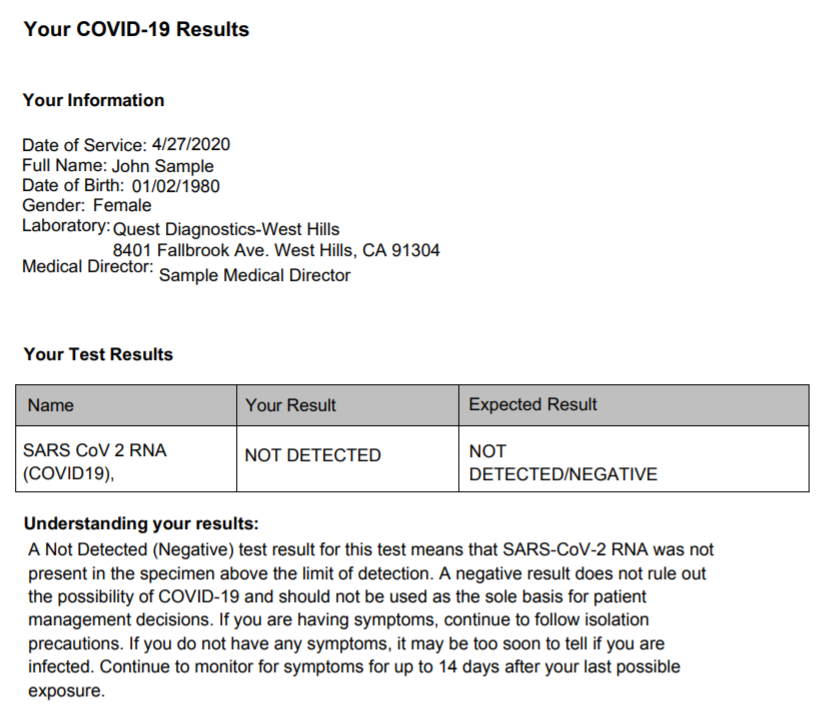
The Prototype Model starts with outlining the requirements. The researcher will conduct an initial investigation to determine the purpose and utilization of the application coupled with the nature and scope of the study. It is also in this stage that the researcher requested permission from medical unit authorities and other parties to conduct the study and all relevant data and information were examined.

Fact-finding was used via interviews and probing of processes to build a logical model of the application. With these interviews, the researcher was able to piece out a picture of transactions involved and analyzed them against the proposed solution. This information will also enable the researcher to identify critical decisions geared toward implementing the application.

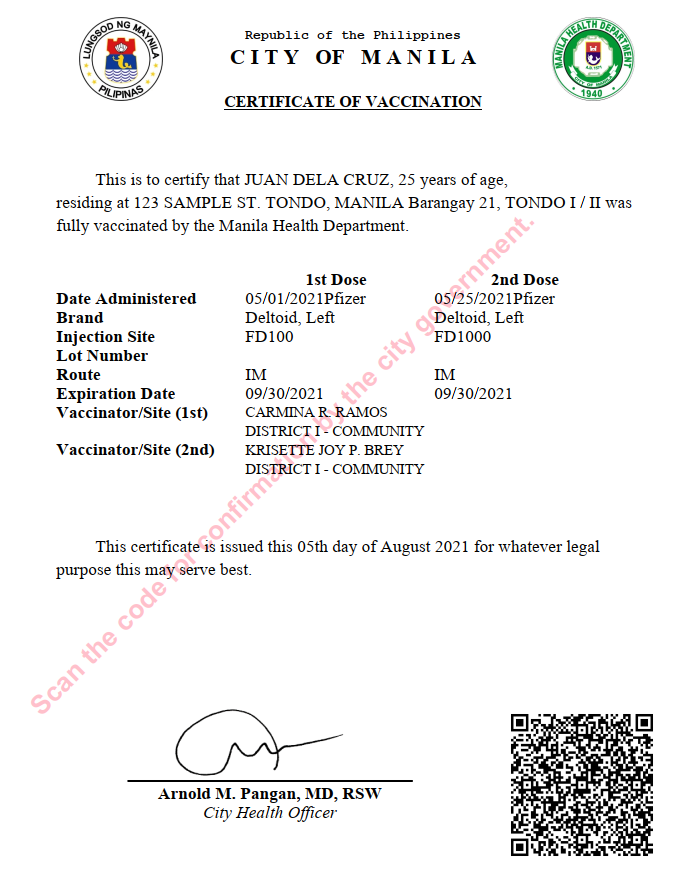
At present time, Ospital ng Makati have a hybrid setup in executing test results. They have an independent laboratory and have partnerships to third-party laboratories to accommodate influx of patients. Once requested by the patient from the hospital, they will either execute the tests in-house or hand-over the execution to the third-party lab. After results comes out, the hospital will furnish a physical copy to the patient whilst maintaining a softcopy in their archive.

For vaccination records, Makati citizens are encouraged to register online via the web portal. This will ensure a scheduled slot on a specified date. On the day of vaccination, patient will be checked up by a physician to ensure he is fit for vaccination. The physician’s findings are logged on the system. Upon issuing a go signal, patient can now be vaccinated. After vaccination, vaccination site will sign a vaccination card while tagging the patient in their system as fully vaccinated.

The study will be focused on two Covid-related records: Test Results and Vaccine Certificate. Mocked test data will be used and will only be for the purpose of this research. This is due to various privacy regulation such as Health Insurance Portability and Accountability Act (HIPAA). This is a United States created health law adopted by medical facilities in the Philippines.



**Figure 4.2 - Sample Covid-19 Test Result**



**Figure 4.3 - Sample Covid Vaccination Certificate**

Once above files are generated from existing system or printed by medical volunteers or workers, it is now ready to be consumed by the application.

Below are requirements grouped by specific role:

Patient

* Register and Login – register to gain access to the system
* Grant and Revoke Access – Grant and remove access from physicians or third party.
* View Own Record – Get access to own results/certificate

Verifying Third Party

* Register and Login – register to gain access to the system
* View Patient Record – retrieve and view patient record if was given access

Physician/Medical Unit

* Register and Login – register to gain access to the system
* Create record – create a record for the patient
* View Patient Record – retrieve and view patient record if was given access

**4.1.1 Data Storage Scheme**

Since the study is primarily concerned on how medical records will be stored, this section will discuss the different schemes that will be used in the application. This will involve simulation, graphical visualizations and detailed discussions.

**4.1.1.1 IPFS – Merkle DAG**

The algorithm used in IPFS to manage content and assets is Merkle DAG. Suppose we want to upload 2 vaccine certificates. For brevity, we will use a small size text file to better illustrate the process. The default chunk size of IPFS is 256Kb but in this example we will reduce it to 32Kb to have appropriate representation using small sample files.

File 1

Name: cert\_allen\_smith.txt

Size: 86 bytes

Content:



File 2

Name: cert\_john\_doe.txt.txt

Size: 83 bytes

Content:



Generated Details for cert\_allen\_smith.txt:

|  |  |  |
| --- | --- | --- |
| Node Type | Size  (Bytes) | Hash |
| Root | 0 | [QmZkJLp7PJGMc3mMSxTeLtyQCRqZ5CudGdjPB3jjTSFaoX](https://cid.ipfs.io/#QmZkJLp7PJGMc3mMSxTeLtyQCRqZ5CudGdjPB3jjTSFaoX) |
| Link | 32 | [QmdsyzBk5nWmC7a92gaAuRHxWTQu6e4wwyv2bVmZtF7mcq](https://cid.ipfs.io/#QmdsyzBk5nWmC7a92gaAuRHxWTQu6e4wwyv2bVmZtF7mcq) |
| Link | 32 | [QmPsFk9hcP4WmN96r8mXYjV5rKCNNb94c95jfqLBNZvigT](https://cid.ipfs.io/#QmPsFk9hcP4WmN96r8mXYjV5rKCNNb94c95jfqLBNZvigT) |
| Link | 22 | [QmVVrfBPAnF5DC1DXDZH2yftW6MEoCSKXEQEbY5LKfFzAt](https://cid.ipfs.io/#QmVVrfBPAnF5DC1DXDZH2yftW6MEoCSKXEQEbY5LKfFzAt) |

Generated Details for cert\_john\_doe.txt:

|  |  |  |
| --- | --- | --- |
| Node  Type | Size (Bytes) | Hash |
| Root | 0 | [QmanmTVLostTHeeLiz8vr99QDWmVbmbd53rSA2iFoDcmXu](https://cid.ipfs.io/#QmanmTVLostTHeeLiz8vr99QDWmVbmbd53rSA2iFoDcmXu) |
| Link | 32 | [QmdsyzBk5nWmC7a92gaAuRHxWTQu6e4wwyv2bVmZtF7mcq](https://cid.ipfs.io/#QmdsyzBk5nWmC7a92gaAuRHxWTQu6e4wwyv2bVmZtF7mcq) |
| Link | 32 | [QmTfDsTDe3nVu7b3hij43R3mBzyhJZgVm9eFBewVb5FfKV](https://cid.ipfs.io/#QmTfDsTDe3nVu7b3hij43R3mBzyhJZgVm9eFBewVb5FfKV) |
| Link | 19 | [QmRF3DNTkA43a7AG26uva4n7pgR22ctz6PjZW4KMuN5Cvu](https://cid.ipfs.io/#QmRF3DNTkA43a7AG26uva4n7pgR22ctz6PjZW4KMuN5Cvu) |

We can now map out the links with their respective roots. Notice that link “Qmdsy” is referenced by both root objects.



**Figure 4.4 – Merkle DAG representing sample records**

**4.1.1.2 Blockchain**

The main purpose of using a blockchain is to validate whether a given or requested CID is authentic in the context of the system. After a doctor uploads a record in IPFS, the generated IPFS CID will then be logged to the blockchain. Blockchain validation will then be used as a proof that a CID exists in the context of CoviBlock. This will prevent illegal tampering or modification of records.

Taking our sample files from 4.1.1.1, we will create a blockchain of transactions given the files were already uploaded to IPFS and CIDs are generated. JSON Objects will be used as format of the payload.

Object for cert\_allen\_smith.txt:

{

“CID”: “[QmZkJLp7PJGMc3mMSxTeLtyQCRqZ5CudGdjPB3jjTSFaoX](https://cid.ipfs.io/#QmZkJLp7PJGMc3mMSxTeLtyQCRqZ5CudGdjPB3jjTSFaoX)”,

“MedPerson”: “Dr. Ramon Cruz”,

“LicenseNum”: “123-456”,

“DateTime”: “23/07/2021 14:00:00”

}

Object for cert\_john\_doe.txt:

{

“CID”: “[QmanmTVLostTHeeLiz8vr99QDWmVbmbd53rSA2iFoDcmXu](https://cid.ipfs.io/#QmanmTVLostTHeeLiz8vr99QDWmVbmbd53rSA2iFoDcmXu)”,

“MedPerson”: “Dr. Erik Lim”,

“LicenseNum”: “122-322”,

“DateTime”: “23/07/2021 09:00:00”

}

**4.2 Quick Design**

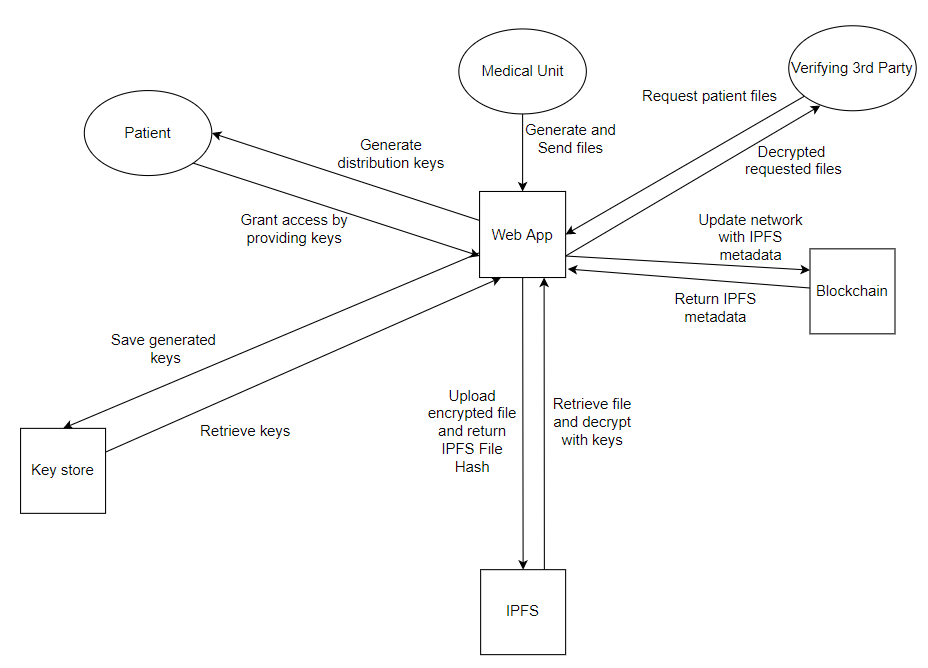
After identifying the requirements, a design of the proposed application is created. This is not a detailed design with complete technical specifications but a simplified one with critical aspects of the solution. This phase will give a bird’s eye view to the client of the application.

**4.2.1 Context Diagram**



The context diagram above summarizes the application on inputs and outputs of the system and targeted users. In general, all the users will be required to put in distribution keys and in return the system will generate files or sets of keys (for upload functionality).

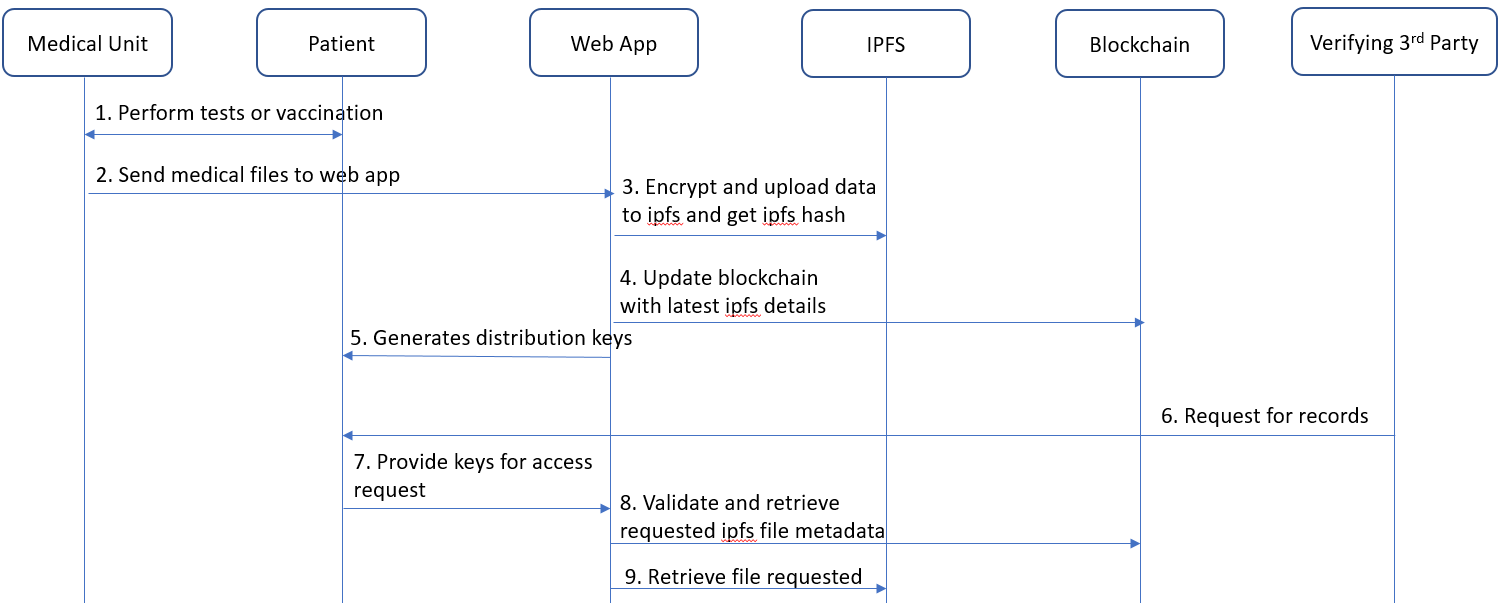
**4.2.2 Data Flow Diagram**

****

**4.2.3 Use Case Diagram**

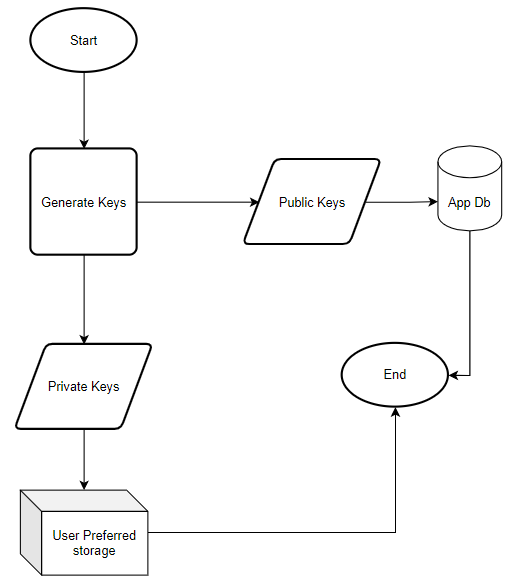
****

**4.2.4 Transactional Operation Diagram**

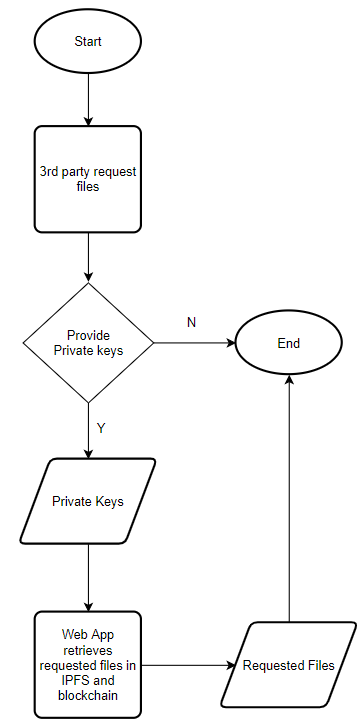


**4.2.5 System Flowcharts**

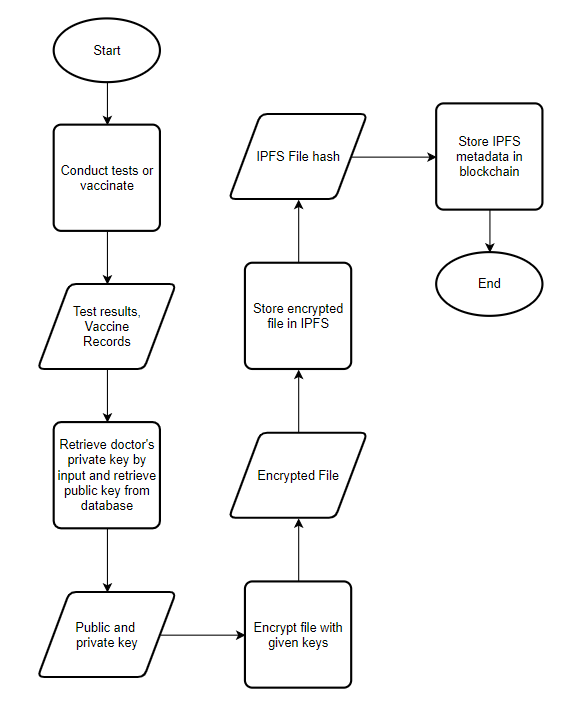
Key Generation Process



Grant Access Process



Store files in blockchain and IPFS



Retrieve Files from IPFS and Blockchain

