International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Digital Medical Passport using Blockchain Technology

Akash Sadamwar

Abstract: ***COVID-19 has emerged as a highly infectious illness that had a worldwide effect, resulting in a significant number of infections and fatalities. Many people are using fake medical certificates for travelling abroad especial for job and for foreign studies. By using Digital medical passports many fraudulent activities may be cult railed and privacy concerns may be minimized. We will look at this issue and contribution in this study by providing a blockchain-based solution that includes self-sovereign identity and decentralized storage. For COVID-19 test takers, proposed system includes digital medical passports. It will demonstrate smart contracts based on the block chain and implemented in Python to preserve a digital medical identity for test-takers, allowing for a quick and trustworthy response from the appropriate medical authorities. Immutable trustworthy blockchain will be used to decrease medical facility response times, relieve the dissemination of incorrect information.***

Keywords: Medical Passport, Blockchain, COVID-19

1. Introduction

1.1 Background

The coronavirus (COVID-19) outbreak in late 2019 comprises a serious threat around the world. The severity of the epidemic was so huge that the World Health Organization (WHO) was compelled to declare it as a pandemic within a month of its wide-scale expansion. The virus spread causes the global economic shock with the massive interruptions of many sectors such as supply chain, industry, insurance, agriculture, transport, and tourism, forcing governments and owners to shut stop operations on a worldwide scale. Coronavirus-2019 (COVID-19) has had unprecedented impact on human life across the world. Being highly contagious, this disease has affected a significant proportion of the world population with a very large number of infections and deaths. With stringent countermeasures, such as lockdown adopted by governments across the world, COVID-19 has not only affected human health but has also caused a significant negative impact on the global economy.

Since the first case was diagnosed in Wuhan, China in late 2019, coronavirus disease 2019 (COVID-19) has spread globally at an unprecedented rate, and was declared a pandemic by the WHO on March 11, 2020. The fatality rate of COVID-19 is 2% – 5%, and the virus has caused many deaths worldwide as it is highly infectious. In addition to COVID-19, a number of other novel infectious diseases have recently been encountered, such as severe acute respiratory syndrome in 2004, novel influenza in 2009, and Middle East respiratory syndrome in 2015, and this is expected to continue in future. Block chain is a recently developed technology that allows transaction designers to make transactions directly through peer-to-peer (P2P) networks, without intermediary organizations, and to store transaction data in a distributed ledger. Because block chain stores data from several individuals simultaneously, in order to amend the data, it is necessary to simultaneously modify the data divided between the individuals. This makes it almost impossible to forge or manipulate the data and ensure their reliability and transparency. The data stored in a block chain are not erased, and so can be easily tracked. In addition, because the participation of intermediaries is minimized, savings in both financial and temporal expenses can be made. There have been attempts to use block chain in various industries, including finance.

COVID-19 has emerged as a highly infectious disease that has had caused the disastrous impact over worldwide resulting in a number of illness and deaths. The pandemic has shown the importance of data and science to build back more stronger health systems so that to avoid the frauds against the fake medical certificates. We propose a cutting edge blockchain based method for preventing the frauds and establishing the trust.

The proposed system will address this issue and contribute in this study by using Blockchain Technology. Purpose of using this technology is its high security. For COVID-19 test takers, proposed system will include digital medical passports and immunity certificates. It will demonstrate smart contracts based on the block chain and implemented in Python to preserve a digital medical identity for test-takers, allowing for a quick and trustworthy responses. Immutable trustworthy blockchain will be used to decrease medical facility response times, relieve the dissemination of incorrect information. Self-sovereign identity,

Relevance
To propose a cutting-edge block chain-based method for establishing trust and preventing fraud. Our system, in particular, makes advantage of programmable smart contracts to do function calls and create events that alert participants to medical information, test changes, and needs.

Project Undertaken
Object detection is important yet challenging task. It is a critical part of many applications such as image search, image auto-annotation and scene understanding, object tracking. Moving object tracking of video image sequences was one of the most important subject of computer vision. In various fields, there is a necessity to detect the target object and also track them effectively while handling occlusions and other included complexities. In this project the model based on Yolo and the framework as Darknet 53 which consist of 53 Convolutional layers. Yolo takes less time to process the image as compared to R-CNN and Fast R-CNN.

Organization of Project

The next chapter, the Overall Description section, of this document gives an overview of the functionality of the product. It describes the informal requirements and is used to establish a context for the technical requirements specification in the next chapter

2. Design, Implementation & Specifications

2.1 System Block Diagram:

Figure 3.0: Block Diagram of System

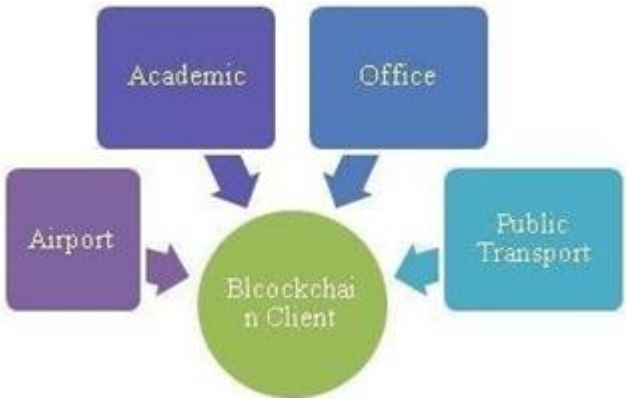

Figure 3.1: Desktop Application Interface

When a person wants to travel as per the security measures to be taken in consideration that he/she has to perform the covid test before travelling. At the authorized covid-19 testing centers the person gets tested if he/she is co-vid positive or negative and the test results are being recorded by the test centers. The test reports, vaccination certificates and other medical history if there any of the patient is uploaded by the authorized testing centers on the block-chain ledger that is on the smart contracts. After successfully uploading the information on the smart contracts, the key that is the hash value of that smart contract will be assigned to the person who is the block-chain client. And the data is securely stored in the decentralized storage where the block-chain client gets the public and the private key. Whenever the block-chain client travels through the airport, public transport or to the office and any academic area client will disclose the public key or the ID number to the invigilator present there. When that ID number is fetched it will show all the information his/her covid-19 test reports, vaccinations done, past travel history about the person

Digital Signature Algorithm using Elliptic Curves

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a Digital Signature Algorithm (DSA) that utilizes elliptic curve cryptography keys to generate signatures (ECC). It's a very efficient public key cryptography-based equation (PKC). ECDSA is utilized in a variety of security systems, is popular in encrypted messaging applications, and is the foundation of Bit coin security (Bit-coin "addresses" serve as public keys). ECDSA is also used to encrypt connections between web browsers and online applications using Transport Layer Security (TLS), the successor to Secure Sockets Layer (SSL). The encrypted connection of an HTTPS website is established via signed certificates utilizing ECDSA, as indicated by a picture of a physical padlock in the browser.

ECDSA has the advantage of providing a better level of security with lower key lengths than another popular method, RSA. ECDSA utilizes less computer resources than RSA, a less secure competing equation, which improves its ROI even further.

2.2 Data Flow Diagrams

A **data flow diagram (DFD**) is a graphical representation of the "flow" of data through an information system, modeling its *process* aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design).

A DFD shows what kind of information will be input to and output from the system, how the data will advance through the system, and where the data will be stored. It does not show information about process timing or whether processes will operate in sequence or in parallel, unlike a traditional structured flowchart which focuses on control flow, or a UML activity workflow diagram, which presents both control and data, flows as a unified model.

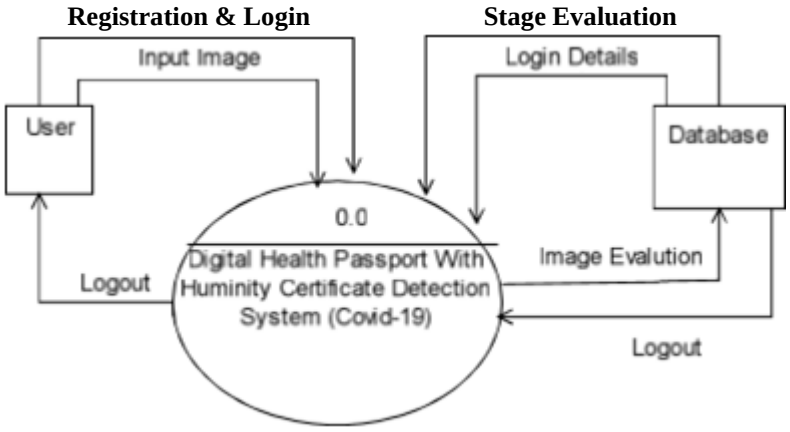

Figure 3.2: DFD level 0

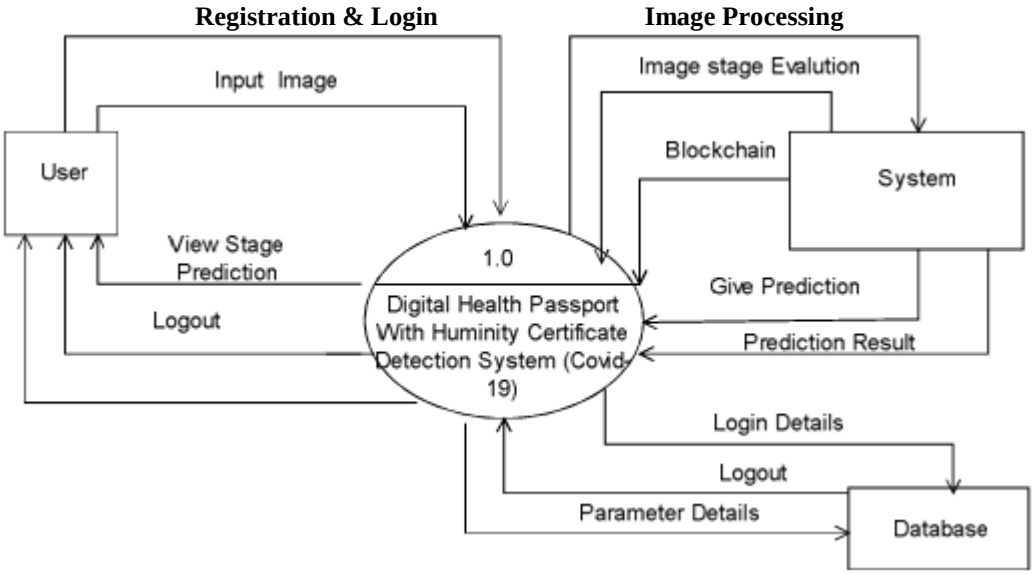

Figure 3.2.1: DFD level 1

2.3 Entity Relationship Diagrams

An entity–relationship model (ER model for short) describes interrelated things of interest in a specific domain of knowledge. A basic ER model is composed of entity types (which classify the things of interest) and specifies relationships that can exist between instances of those entity types.

In software engineering, an ER model is commonly formed to represent things that a business needs to remember in order to perform business processes. Consequently, the ER model becomes an abstract data model that defines a data or information structure which can be implemented in a database, typically a relational database.

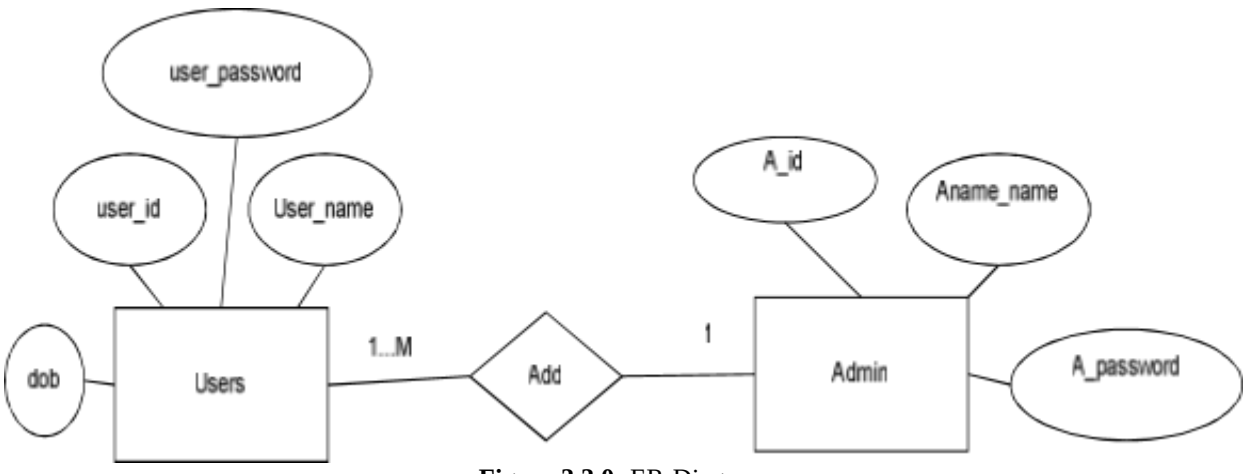

Figure 3.3.0: ER-Diagram

2.4 UML Diagrams

2.4.1 Use case diagram:

A use case diagram is a graphical representation of a user's interaction with the system and depicting the specifications of a use case. A use case diagram can show the different types of users of a system and the various ways in which they interact with the system. Use case diagrams are used to gather the requirements of a system including internal and external influences. These requirements are mostly design requirements. So when a system is analyzed to gather its functionality use cases are prepared and actors are identified. The purposes of use case diagrams can be as follows:

2.4.1.1 Used to gather requirements of a system.
2.4.1.2 Used to get an outside view of a system.
2.4.1.3 Identify external and internal factors influencing the system.
2.4.1.4 Show the interaction among the actors.

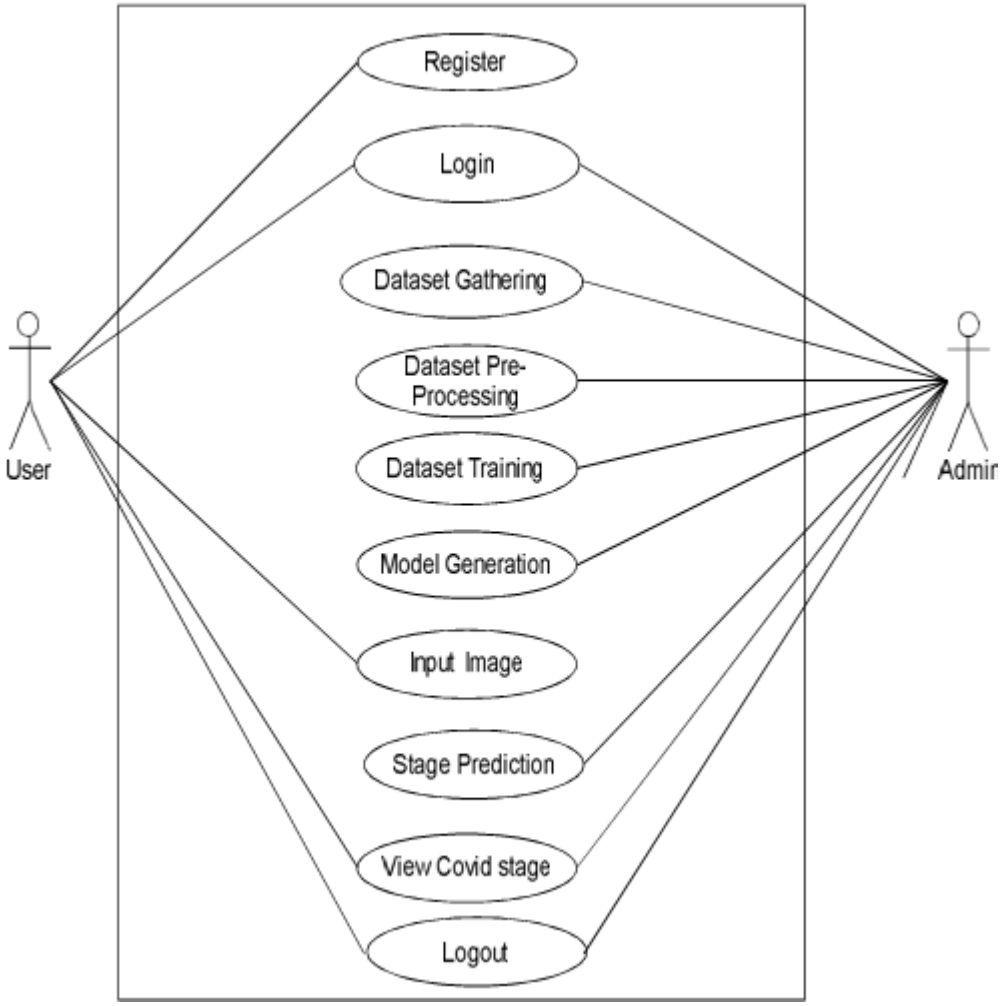

Figure 3.3.1: Use Case Diagram

2.4.2 Activity diagrams

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes (i. e. workflows). Activity diagrams show the overall flow of control. Activity diagrams are constructed from a limited number of shapes, connected with arrows. The most important shape types:

1) Rounded rectangles represent actions;
2) Diamonds represent decisions;
3) Bars represent the start (split) or end (join) of concurrent activities;
4) A black circle represents the start (initial state) of the workflow;
5) An encircled black circle represents the end (final state).

Arrows run from the start towards the end and represent the order in which activities happen. Hence, they can be regarded as a form of flowchart. Typical flowchart techniques lack constructs for ex-pressing concurrency. However, the join and split symbols in activity diagrams only resolve this for simple cases; the meaning of the model is not clear when they are arbitrarily combined with decisions or loops.

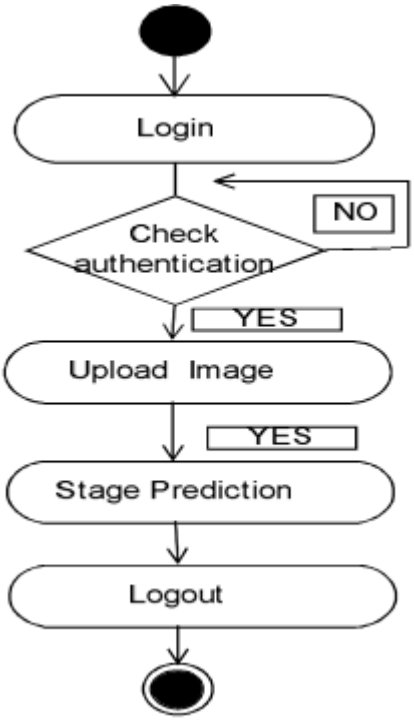

Figure 3.4.1: Activity Diagram

2.4.3 Class Diagram

The class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing and documenting different aspects of a system but also for constructing executable code of the software application. The class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modeling of object oriented systems because they are the only UML diagrams which can be mapped directly with object oriented languages. The class diagram shows a collection of classes, interfaces, associations, collaborations and constraints. It is also known as a structural diagram. The purpose of the class diagram is to model the static view of an application.

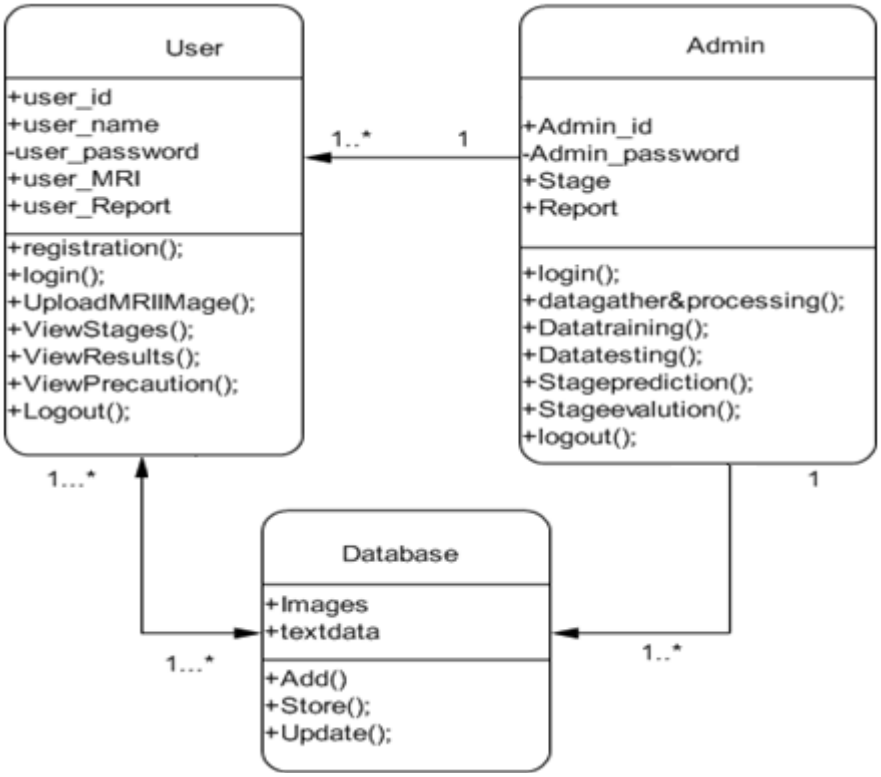

Figure 3.4.2: Class Diagram

2.4.4 Sequence Diagram

A Sequence diagram is an interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

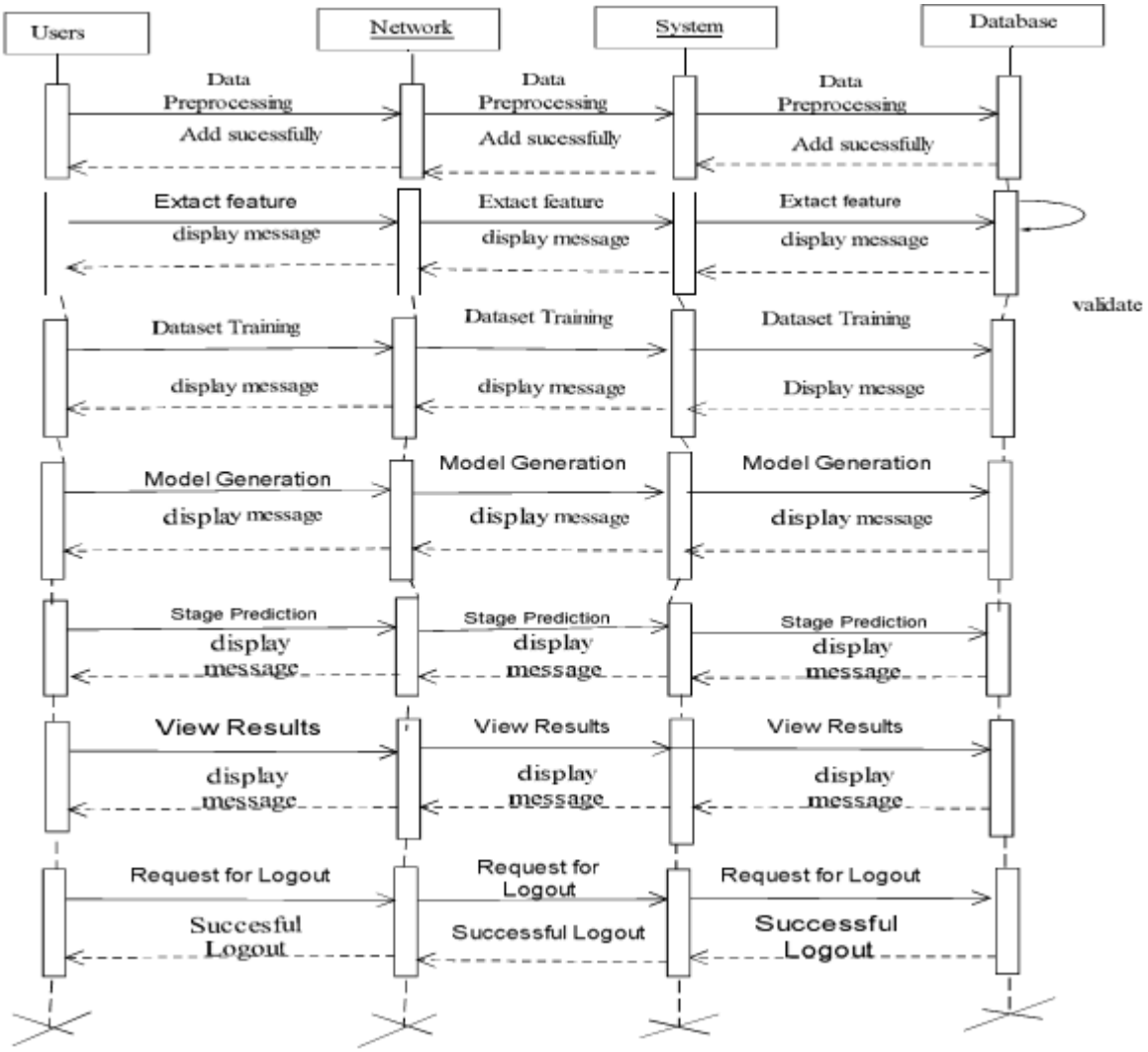

Figure 3.4.3: Sequence Diagram

2.4.5 Component Diagram

A Component Diagram displays the structural relationship of components of a software system. These are mostly used when working with complex systems that have many components. Components communicate with each other using interfaces. The interfaces are linked using connectors.

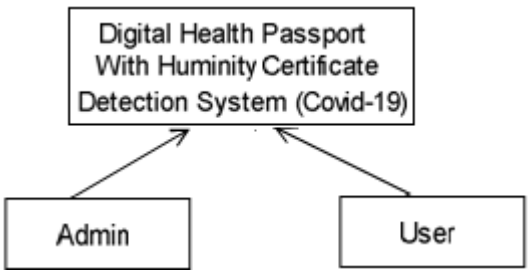

Figure 3.4.4: Component Diagram

Deployment Diagram

Deployment diagrams are used to visualize the topology of the physical components of a system where the software components are deployed. So, deployment diagrams are used to describe the static deployment view of a system. Deployment diagrams consist of nodes and their relationships.

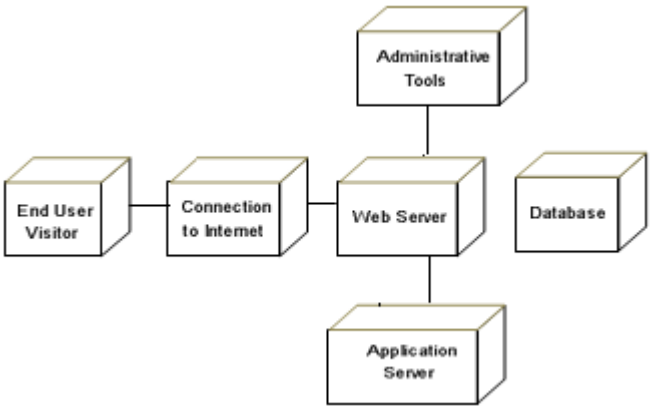

Figure 3.4.5: Deployment Diagram

State Diagram:

A state diagram is a type of diagram used in computer science and related fields to describe the behavior of systems. State diagrams require that the system described is composed of a finite number of state sometime.

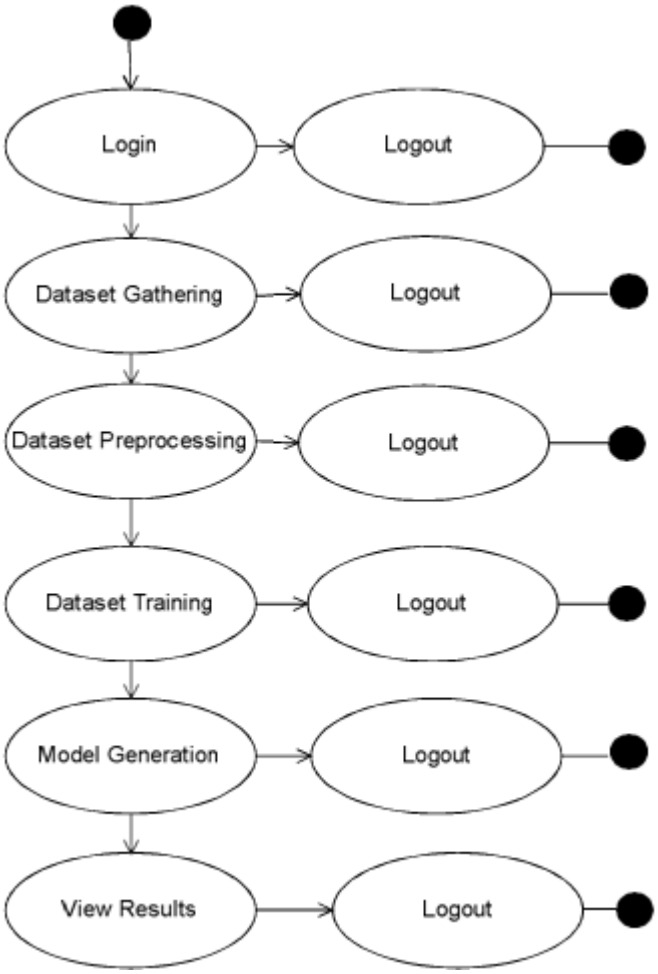

Figure 3.4.6 Admin State Diagram

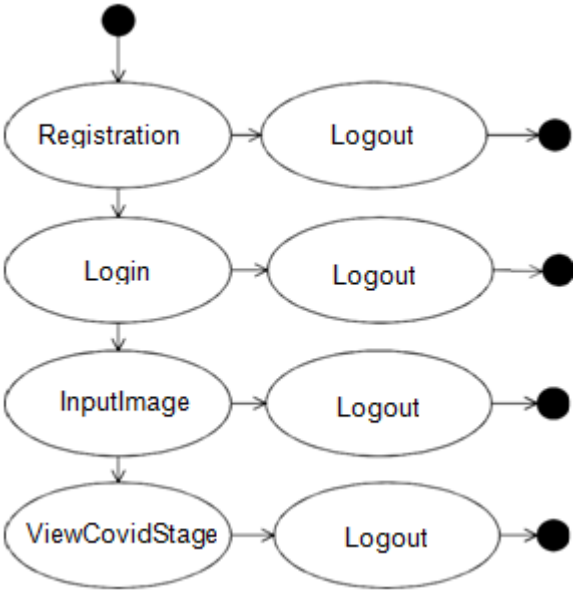

Figure 3.4.7: User State Diagram

3. Implementation

Overview of Project Modules

The proposed block chain-based solution presents the on-chain participating entities with different smart contracts, distributed storage, block chain clients, and interested stakeholders. There are four main types of smart contracts used in our proposed solution i.e. i) the MoFA smart contract, ii) the MoH smart contract, iii) the COVID-19 Testing Center smart contract, and iv) the Patient smart contract Digital health passports are a crucial mode of identification which can help mitigate the spread of contagious diseases. The patient smart contract is envisaged to address this objective. It is an immutable record that is authenticated by the MoH and the MoFA for international usage. The patient smart contract holds the IPFS hash of the vaccination and immunization records as well as the medical and travel history of an individual. In the context of the personally identifiable information used in this structure, the disclosure of the information is delegated to the owner of the information. Immunity certificates are envisaged to verify that a person has developed relevant antibodies to militate against COVID-19 and is consequently not a threat to (cannot infect) other people. We envisage this to have been achieved either through a past infection of COVID-19 or through vaccination (when available). Although we acknowledge the significance of this challenge, however, as our focus is on technological perspective of the challenge, we render the medical aspect of this challenge out of scope of this paper. Therefore, they can be exempted from physical and social restrictions as they are immune to the disease. This information can also be part of the patient smart contract and it can also be announced using an immutable transaction by the COVID-19 Testing Center. The center can announce it after an antibody test and the time-frame the patient is immune would also be announced (depending upon the vaccine strength and relevant medical advice).

Algorithm

Furthermore, by using on-chain digital medical passports and immunity certifications, our approach aids in the prevention of the COVID-19 virus. Because the data on-chain is immutable, it may be trusted as if it came from a trustworthy source. We've also included self-sovereign identification, proxy encryption techniques, and distributed and decentralized computing in our system.

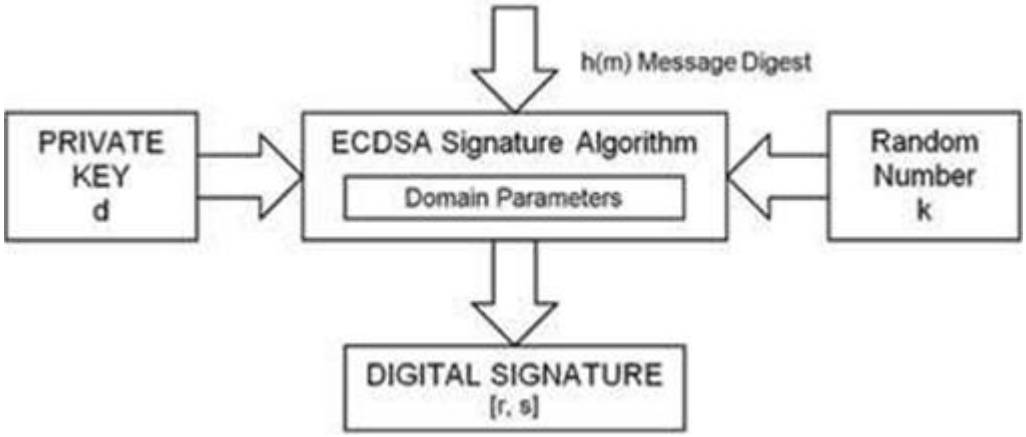

Figure 4.2.0: Block Diagram of Elliptic Curve Digital Signature Algorithm (ECDSA)

Consider an Elliptic curve E over prime finite field Fq of characteristic q where q is a prime number greater than 3 and choose parameter a, b and generating point G of order n such that n× G = O. G is treated as the private key of signer. Now randomly select an integer d, $1 \leq d \leq n-1$. Calculate public key Q by point multiplication of G and random number d using group law. Make d and Q as public parameters. Now Generate a one-time random number k such that 0< k<n-1. Using the same k for two different signatures is a major security breach in the use of this algorithm.

Construct a digital signature of a document. Let z be an integer that represents a hash of the document M which is to be signed. The digital signature s is calculated by first calculating the elliptic curve point k ×G and retaining only its x-coordinate modulo n, if the modulo operation produces a zero value then opt a different value of k. And then by means of formula s = (z× d) × k−1 (mod n), s is computed, where k−1 is the multiplicative inverse of k modulo n that can be obtained with the Extended Euclid's Algorithm.

A. Key-Pair generation

Using generating point G and random integer d, public key Q is computed through following steps:

1) Select a random integer d in the interval [0, n-1].
2) Compute Q = d× G, obtained by point Multiplication. Q, G are points on the elliptic curve.
3) Now key-pair is (G, Q) where G is the Private Key and Q is the Public key.

B. Signature Generation

Signer utilizes parameters q, a, b, p, n, d and private key G, to sign a message M where a, b, p and q are constants in elliptic curve equation. To sign a message signer does the following:

1) Chooses a random integer k with $1 \leq k \leq n-1$.
2) Compute k×G = (x1, y1).
3) Compute hash value z of message M, z=h-1 (M) 2.
4) Compute s = (z×d) × k-1 mod n. If s = 0 then return to step 1.
5) Signature for the message M is (s, x1).

C. Signature Verification

Authenticity of the received message can be verified by receiver exploiting the following steps:

1) First verify that s is integer in the interval [1, n −1].
2) Calculate hash z of the message/document M
3) Calculate the number w = s−1 z (mod n)
4) Using this number compute the point (x, y) = w× Q on the curve, and, finally, authenticate the signature by checking whether the equivalence x=x1 holds.

D. Correctness of Algorithm

If the signature (s, x) on the message M was indeed generated by authenticated party then s = (z× d) ×k−1 (mod n). Using this information correctness of algorithm can be proved through following methods:

For signature verification receiver compute
(x, y) = s-1zQ
= s-1zdG as Q=d× G, step 2 of key pair generation
= (z ×d)-1 (z× d) k× G
= k× G
As (x1, y1) = k× G Thus (x1, y1) = (x, y)

4. Technical Specifications

4.1 Technical Specifications

1) We are going to implement this project using Elliptic Curve Digital Signature Algorithm (ECDSA) is a Digital Signature Algorithm (DSA) that utilizes elliptic curve cryptography keys to generate signatures (ECC).
2) The programming language will be python and we will be working it out in Python 3.7.0 IDE.
3) OPENCV, MATPLOTLIB, TENSORFLOW, SKLEARN are the libraries we are going to use with python.
4) MySQL will be used to store the database of patient's medical reports, vaccination status, test reports.

a) OPEN CV

OpenCV is the huge open-source library for the computer vision, machine learning, and image processing and now it plays a major role in real-time operation which is very important in today's systems. By using it, one can process images and videos to identify objects, faces, or even handwriting of a human. When it integrated with various libraries, such as NumPy, python is capable of processing the OpenCV array structure for analysis. To Identify image pattern and its various features we use vector space and perform mathematical operations on these features. It has C++, C, Python and Java interfaces and supports Windows,

Linux, Mac OS, iOS and Android. When OpenCV was designed the main focus was real-time applications for computational efficiency. All things are written in optimized C/C++ to take advantage of multi-core processing.

b) MATPLOTLIB

Matplotlib is a Python library that helps in visualizing and analyzing the data and helps in better understanding of the data with the help of graphical, pictorial visualizations that can be simulated using the matplotlib library. Matplotlib is a comprehensive

c) Tenser Flow:

TensorFlow is an open-source software library. TensorFlow was originally developed by researchers and engineers working on the Google Brain Team within Google's Machine Intelligence research organization for the purposes of conducting machine learning and deep neural networks research, but the system is general enough to be applicable in a wide variety of other domains as well. TensorFlow is basically a software library for numerical computation using data flow graphs where:

- Nodes in the graph represent mathematical operations.
- Edges in the graph represent the multidimensional data arrays (called tensors) communicated between them. (Please note that tensor is the central unit of data in TensorFlow).

d) SKLEARN:

Scikit-learn is largely written in Python, and uses NumPy extensively for high-performance linear algebra and array operations. Furthermore, some core algorithms are written in Cython to improve performance. Support vector are implemented by a Cython wrapper around LIBSVM; logistic regression and linear support vector machines by a similar wrapper around LIBLINEAR. In such cases, extending these methods with Python may not be possible. Scikit-learn integrates well with many other Python libraries, such as Matplotlib and plotly for plotting, NumPy for array vectorization, Pandas data frames, SciPy, and many more.

e) MySQL:

MySQL is currently the most popular database management system software used for managing the relational database. It is open-source database software, which is supported by Oracle Company. It is fast, scalable and easy to use database management system in comparison with Microsoft SQL Server and Oracle Database. It is commonly used in conjunction with PHP scripts for creating powerful and dynamic server-side or web-based enterprise applications.

It is developed, marketed, and supported by MySQL AB**,** a Swedish company, and written in C programming language and C++ programming language. The official pronunciation of MySQL is not the My Sequel; it is My Ess Que Ell. *However, you can pronounce it in your way.* Many small and big companies use MySQL. MySQL supports many Operating Systems like Windows, Linux, MacOS, etc. with C, C++, and Java languages.

MySQL is a Relational Database Management System (RDBMS) software that provides many things, which are as follows:

1) It allows us to implement database operations on tables, rows, columns, and indexes.
2) It defines the database relationship in the form of tables (collection of rows and columns), also known as relations.
3) It provides the Referential Integrity between rows or columns of various tables.
4) It allows us to updates the table indexes automatically.
5) It uses many SQL queries and combines useful information from multiple tables for the end-users.

Summary

This chapter represents the technical specifications of the project which will be used while implementation.

5. Results

Registration Page

At initial stage we used OPENCV libraries to start our project and getting familiar with the tools and also with the aim of merging all our projects into one. Some of them are mentioned below:

Step 1

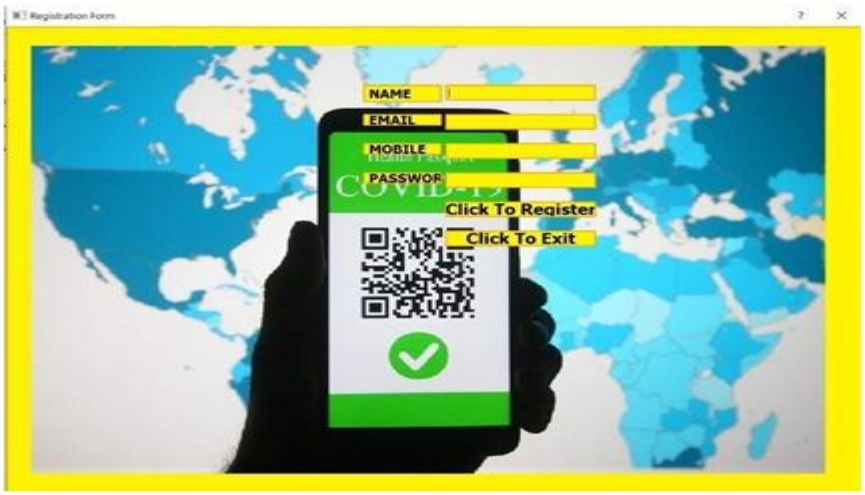

Figure 6.1.1: Screenshot showing the Registration page

As we run the code we can see the Registration page on our desktop screen. Then we can fill the information like Name, Email, Mobile NO, Password at the time of registration.

User Registration (Step-2)

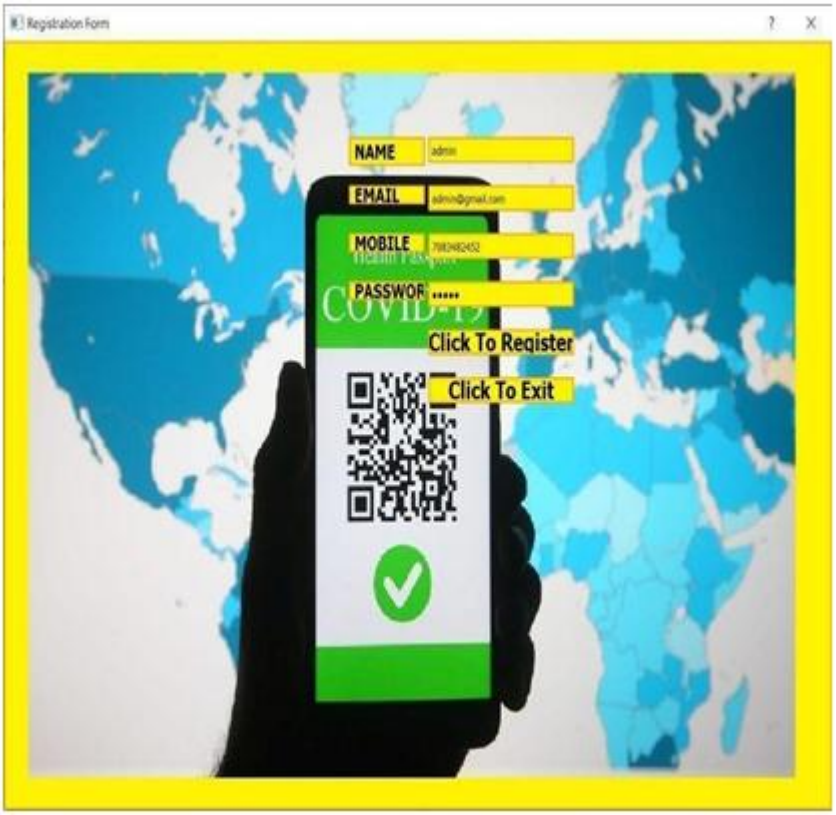

Figure 6.2.1: Screenshot showing user information

As we see the registration page, we can fill all the correct information and then click to Register button. There are two buttons on this screen Click to Register and Click to Exit.

User Registration Successful (Step-3)

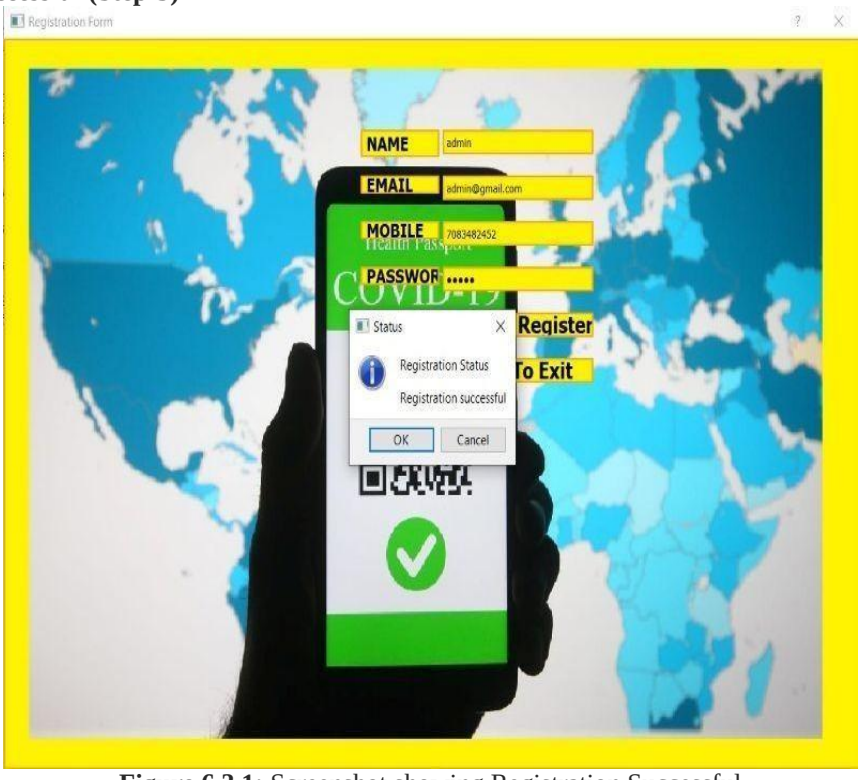

Figure 6.3.1: Screenshot showing Registration Successful

As we can fill all the correct information for Registration then we can click to Register button. Then we see Registration Status on our desktop screen that Registration Successful.

6. Summary

The above experimentation results all are the stepping stones towards our final model which has now reached an accuracy of 85%.

References

[1] Haya R. Hasan, Khaled Salah, Raja Jayaraman, Junaid Arshad, Ibrar Yaqoob, Mohammed Omar, Samer Ellahham "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates" [IEEE, 8 December 2020]
[2] Min Cheol Chang, Donghwi Park, "How Can Blockchain Help People in the Event of Pandemics Such as the COVID-19?" [Journal of Medical System, 16 April 2020]
[3] Vinay Chamola, Vikas Hassija, Vatsal Gupta and Mohsen Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing Its Impact" [IEEE, 4 May 2020]
[4] Samen Anjum Arani, Md. Rashed Ibn Nawab, Md. Tanvir Rahman, Moniruz Zaman "A Blockchain-based Approach to Prevent Hidden Contagion of Covid-19" [Research gate, 1 November 2020]
[5] José L. Hernández-Ramos, Georgios Karopoulos, Dimitris Geneiatakis, Tania Martin, Georgios Kambourakis, and Igor Nai Fovino "Sharing Pandemic Vaccination Certificates through Blockchain: Case Study and Performance Evaluation" [Wiley/ Hindawi 26 August 2021]
[6] Sofia Maria Dima, Alexandros Hasikos, Stylianos Kampakis, Theodosis Mourouzis, and Andreas Papageorgiou "A Secure, Smart, Privacy-Preserving and Interoperable Blockchain Solution for The Covid-19 Pandemic" [Upf Barcelona, Electi Consulting Ltd 22 July 2021]
[7] Ammar Ayman Battah, Mohammad Moussa Madine, (Member, Ieee), Hamad Alzaabi, Ibrar Yaqoob, (Senior Member, IEEE), Khaled Salah, (Senior Member, IEEE), and Raja Jayaraman "Blockchain-Based Multi-Party Authorization for Accessing IPFS Encrypted Data" [IEEE, 27 October 2020]
[8] Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne "Blockchain and AI-based Solutions to Combat Coronavirus" (COVID-19)-like Epidemics: A Survey [Paperprints, 19 April 2020]
[9] Laura Ricci Damiano Di Francesco Maesa, Alfredo Favenza, And Enrico Ferro "Blockchains for COVID-19 Contact Tracing and Vaccine Support: A Systematic Review" [IEEE, 2 March 2021]
[10] Mohamed Torky and Aboul Ella Hassanien, "COVID-19 Blockchain Framework: Innovative Approach [Scientific Research Group in Egypt"