Vac-Check: A User-Controlled Digital Vaccine Certification Solution

1st Jacob Hopkins
Department of Computing Sciences
Texas A&M University - Corpus Christi
Corpus Christi, TX, USA
jhopkins2@islander.tamucc.edu

2nd Carlos Rubio-Medrano
Department of Computing Sciences
Texas A&M University - Corpus Christi
Corpus Christi, TX, USA
carlos.rubiomedrano@tamucc.edu

***Abstract*—The COVID-19 pandemic has been a disruptive element for the past two years in the world. People are experiencing fatigue in having to deal with the pandemic and the measures to control it. As a result, governments are exploring ways to resume daily life while ensuring the safety of the public. One measure that has been proposed is the use of vaccine passports, a.k.a., Digital Vaccine Certification (DVC) systems, in which individuals are issued a digital document stating their vaccination status, which can be verified by external parties depending on different contexts, e.g., before entering a restaurant or while admitted into a hospital. Yet, many individuals have expressed concern about or outright refused to use said DVC systems. For instance, existing solutions in the literature are designed using a technology built for deregulation and transparency, e.g., blockchains, but health records require regulation and privacy. This results in sensitive vaccination data being wrongly shared with external parties and users lacking ownership over the data. To overcome these issues, we propose a novel DVC system, Vac-Check, that enables users to control what information can be released depending upon whom that information is released to, e.g., hospitals, schools, restaurants, etc. To determine the effectiveness of our proposed approach, we have envisioned a use case study to measure the change in responses about acceptance and use rates. By placing access control of the users' data in their hands, we expect that users, once are trained to effectively our approach, will be less likely to leak their data to wrong individuals or organizations.**

***Index Terms*—health records, vaccine passports, authorization policies**

I. Introduction

The COVID-19 pandemic has been a disruptive force in many sectors of the global society. As of February 2022, there have been approximately 400 million cumulative cases and 5.7 million deaths due to COVID-19 globally [1]. The exact extent of the disruption won't be known without thorough study but it can be assume that it will be significant due to the disease itself and the responses to the pandemic. Given that it has been two years since the beginning of the pandemic, many politicians of many nations are deciding to allow their citizenry to live a normal life without COVID-19 restrictions [2]. In order to prevent a resurgence of COVID-19 infections or one of its variants, multiple methods have been proposed in particular vaccine passports or digital vaccine certificates.

Digital Vaccine Certifications (DVC) systems are verification systems that operate on a small subset of health data related to some type of vaccination particularly COVID-19 vaccines to support a differential lockdown in order to prevent further infections [3]. These systems have been proposed to support the vaccination efforts in countries and to allow the resumption of daily living through differential lockdown [4]. Since these systems are tied to countries' vaccinations efforts and will promote differential lockdowns, they have been politicized and thus there are supporters and opponents to DVC systems.

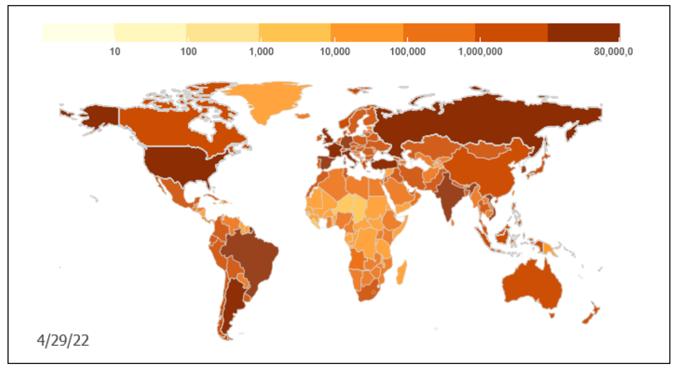

Fig. 1. COVID-19 Cumulative Cases over Time

In broad terms, there are three groups of people in regards to the acceptance and use of these systems. The exact composition and nature of these groups and their reasons for supporting or opposing DVC system is a complex problem that will be further explored in the section II of this paper [5]. In general terms, proponents of these systems are more accepting of mandatory COVID-19 vaccine inoculations and see the use of DVC systems as a positive measure. Opponents of these systems are against the mandatory inoculations of the COVID-19 vaccine with a small subset being against the voluntary inoculations as well. This group also are opposed to the use of DVC systems. The last group is hesitant of DVC systems. These skeptics doubt the efficacy of these systems.

A. Research Questions

The COVID-19 pandemic, though slowing down, is not over and governments are resuming daily life. It is important to explore whether or not these DVC systems will are capable of accomplishing their purpose which is to reduce the infections of COVID-19. This paper aims to answer this question through determining the answer to these two questions:

- Since vaccination passports are based on vaccination records, a type of health record, can the proposed user-defined authorization policies maintain the necessary security level for these types of records?
- Would the use rate of a DVC system increase among individuals who are hesitant of said systems if they were able to define the authorization policies of their own vaccine records?

B. Advantages and Disadvantages of Existing Methods

Many of the existing DVC solutions have been proposed to implement a blockchain system. A blockchain system lends multiple advantageous properties to DVC systems. A DVC system built using a blockchain would be difficult to tamper its records because of its cryptographic validation properties and distribution of the ledger [6]. Each record can be verified on the chain thus making it difficult to falsify records onto the blockchain [7]. This helps to combat fraud within a DVC system. Since blockchain systems are decentralized, there is no single point of failure [8].

Despite the many advantageous properties that blockchains can confer to DVC systems, the disadvantages of blockchains in a DVC systems is that they are not completely compatible with the vaccine health data. In order to be compliant with various legal frameworks, the blockchain systems will have to be designed to be private and permissioned [9]. By designing the blockchain system in this manner, the blockchain loses its advantages of decentralization and anonymity [9]. Instead of using a blockchain system, an encrypted database can achieve the same outcomes as a private permissioned blockchain system.

C. Contributions of Proposed Study

The proposed study will contribute to the body of research through these contributions.

- The proposed study will implement a use case study to evaluate the proposed system. The use case study will get information about how people will respond to the proposed system.
- The proposed system will implement an access control system that will allow the users direct control over how much of their data to give out.

II. Related Works

Vaccine certificates or vaccine certification policies are not a new idea with the advent of COVID-19. These ideas can be traced back to Italian city states during the renaissance [10]. It was common for crews of ships to to be issued a health license that insured the health of the crew. In fact, immunity passports have been used when an outbreak of a disease has occurred [11]. During the yellow fever outbreak of 1828 in Gibraltar, officials would issue ”fever passes” to individuals who contracted yellow fever and survived it [11]. These passes allowed the now immune individuals the freedom to move about in the fortress [11].

A recent implementation of these ideas before COVID-19 was the WHO’s International Certificate of Vaccination or Prophylaxis (ICVP) [10]. This vaccination certificate weas designed to reduce the spread of various diseases, but now it is only used in regards to yellow fever and only in a select number of countries [10]. Some reasons for this role reduction in IVCP were the weak enforcement and forged documentation [10]. The history of the use of ICVP illustrates some of the challenges that all vaccination certification systems, both digital and analog, face. Consequently, a framework needs to be used in order to measure whether a DVC system meets the necessary criteria [9].

As mention the section I, multiple governments and private businesses are in the process or have implemented a DVC system. Some notable DVC systems or vaccine certificates have come from Israel with its Green Pass Policy (GPP) [12] and the European Union’s Digital COVID Certificate (EUDCC) [13].

Israel, during the COVID-19 pandemic, aggressively acted to prevent the spread of the disease especially in regards to the vaccinations and vaccine certificates [12] [14]. When the vaccines became readily available at the beginning of 2021, Israel began a campaign to vaccinate as many of its population as fast as possible [12]. This resulted in a massive uptake of the vaccine in population with as many as 90% of its at-risk population being fully vaccinated by October 2021 [14]. Since much of the population was getting vaccinated as quickly as possible, the Israeli government implemented the GPP in late February 2021 [12] with citizens being issued these certificates

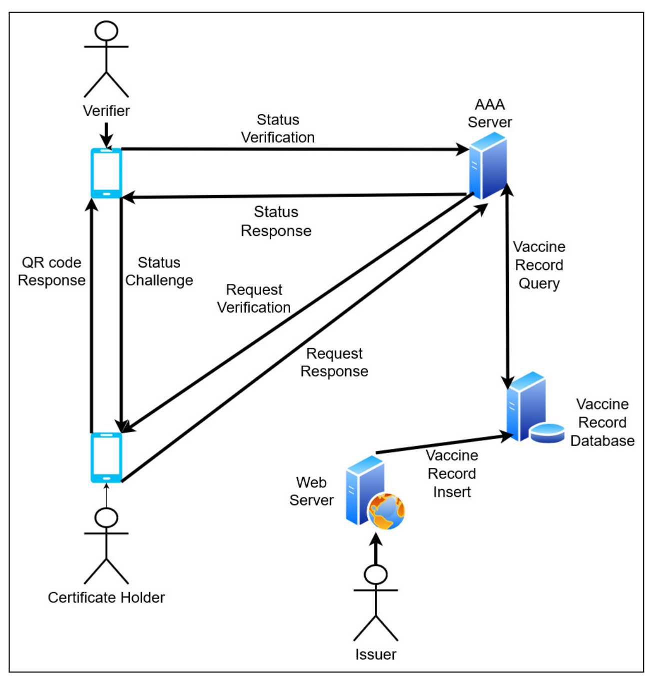

Fig. 2. System Architecture of Proposed Method

in early March 2021 [14]. The impetus for the GPP was allow for the resumption of life and business by allowing citizens access to more non-essential services and to reduce the spread of COVID-19.

The EUDCC was first proposed in March 2021 as a framework for developing DVC systems for Member States of the European Union(EU) [13]. The main impetus for the EUDCC was to have a standardize way of verifying COVID-19 status among the EU Member States to enable international travel [13].

III. Proposed Work

A. Proposed Method

The proposed method will consist of these components: an encrypted database to store vaccination health records, a verification server that verifies the users and their requests for the encrypted vaccination health records, a mobile application that the users will use, and a secure website and web server to update the encrypted database.

There are three parties that the proposed system is designed for: the issuer, the verifier, and the certificate holder. The issuer is a validated entity that administers a vaccine and issues the vaccine certification. The verifier is a entity that authenticates the vaccine certification to determine if its a verified certification. The certificate holder is the entity that presents the certificate and determines which data is given to determine their vaccination status. The system architecture is detailed in Figure 2.

1) Vaccine Certificate Issue Process: The issuance of digital vaccine certificates begins with the administering a vaccine to the certificate holder. The issuer will administer the vaccine and record the information of the certificate holder. Using the web server, the issuer will create the digital vaccination record and sign it with the issuer's private key to validate the certificate. The signed certificate will then hashed to create a unique identifier of the certificate. The certificate and its identifier will be upload to encrypted database. The web server will create a QR code that the certificate holder scan and the identifier will be saved in the mobile app which is on the certificate holder's device. This process is detailed in figure 7.

2) Vaccine Status Verification Process: The vaccine status verification process is the key process of the proposed system. This process encapsulates the main use case of the system that a certificate holder will verify their vaccination status with a verifier, typically not involved in the medical field. The vaccine status verification process begins when the verifier asks the certificate holder for their vaccine certificate. The certificate holder will then use the mobile app to generate a QR code; the QR code generation will be detailed in the next subsection. The QR code will contain the certificate's unique identifier. The identifier will be signed with the certificate holder's private key.

Once the verifier has the signed identifier from the scanned QR code, the verifier will contact the verification server through a secure channel. The verifier will send the signed identifier to the verification server which will confirm that the signed identifier has originated from a legitimate certification holder. The verification server will only contact the encrypted database if it can verify the signed identifier. The verification server will construct a query to request the designated fields that the certificate holder has decided to release. The verification server will retrieve the requested information and also contact the certificate holder to re-authenticate the request.

Once the verification server has received the information and the request has been re-authenticated, the verifier will receive the information. This process is furthered details in figure 8.

3) Vaccine Certification Access Control Process: The verification certification access control process is what enable the certificate holder to decide which data is released to whom. When the certification holder is asked to present their status, the certification holder can decide which information to release. Depending on the situation, the certification holder can decide what information to release from the certificate. The most likely scenario that the certification holder is likely to present their status is by going into regular businesses and interacting with non-medical individuals. In this situation, the least amount of information is needed to be given out.

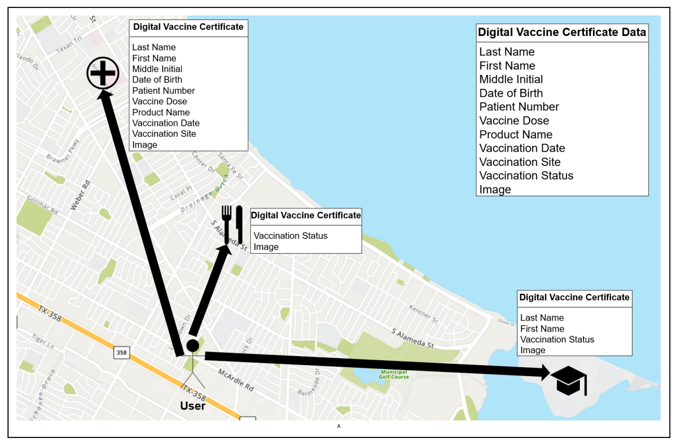

Fig. 3. User-Defined Authorization Policies

B. Proposed Dataset

As will be outlined in the section V, a use case study will be implement to determine the acceptance and use rate of the proposed DVC system. Thus, no existing data set will be used. Instead, a data set will be generated from the responses of the participants.

C. Difference between Proposed and Existing Methods

One of the difference between the proposed method and other existing methods is that the proposed method uses a centralized architecture. The other existing methods implement a distributed system through the use of a blockchain [7] [6] [8]. Another difference between the proposed system and existing systems is that the proposed system implements an access control mechanism that allows the users to share whatever amount of data they want. Some existing solutions [7] [6] express that their systems can make use of a Self Sovereign Identity (SSI) system to enable the user to have access rights, but their systems don't implement this because SSI is outside of the scope of their work. Another difference between the existing methods and the proposed method is the method of evaluation. The proposed method will be evaluated through a use case study and the existing methods are evaluated using a performance study of their proposed systems.

D. Benefits of Proposed Method

The primary benefit of the proposed solution is that certificate holders will be in control over what information from their vaccination records is released and to whom. The proposed DVC system will enable users to determine what set of access permissions about their own vaccination records that they want give out in any interaction. This is important because this empowers the users to be in control of their privacy. This would be an improvement over the existing methods because the proposed solution would be the first to implement a user-defined authorization policy system.

Another benefit of the proposed solution is that it will be the first to use a use case study as an evaluation approach such that it will be able to collect real data about how an individual would use a DVC system and how their opinion changed after using a DVC system. For these systems to be useful, they have to widely used and used in such a manner that privacy is maintained. If a significant portion of the population refuses to use a DVC system then a government will be unable to use lockdowns in a differential manner. As far as the authors are aware, this is the only study of its kind in the field right now doing this research.

IV. Implementation

Given the individual components as outlined in section III-A, these components are grouped into three subsystems: the mobile subsystem, the web subsystem, and the back-end subsystem.

A. Mobile Subsystem

The primary implementation decision for the mobile subsystem, which is the mobile app, was which OS to use to develop the app. Currently, the primary mobile OS are Google's Android and Apple's iOS. These two OS account for 95% of the global market share of smartphone OS. The two criteria used to decide between which OS to use for the implementation was global market share of the OS and development accessibility. Currently, Android, approximately 70 %, has a greater market share than iOS, which roughly is 25% [15]. Considering the accessibility of development of the two operating systems, iOS development is a closed ecosystem meaning that third party apps must be developed using tools like Xcode specifically developed by Apple if the app is to be published in Apple's app store. Android development does not have much of these hurdles because it is an open ecosystem. Thus given these considerations, the mobile app was developed using the Android OS.

Once the Android OS was selected, two other implementation decisions needed to be resolved: which API level of Android to use and what device targets to use? In the same way older computers are unable to support new operating systems, older smartphones either haven't been updated or are unable to support newer versions of Android. Thus choosing an appropriate API level to develop in needs to account for older phones that don't support newer API levels and what newer features provided by newer APIs are necessary for the application to operate. The API level that was selected was Android API level 25 or Android 7.1.1 because this API level is supported by approximately 89% of devices.

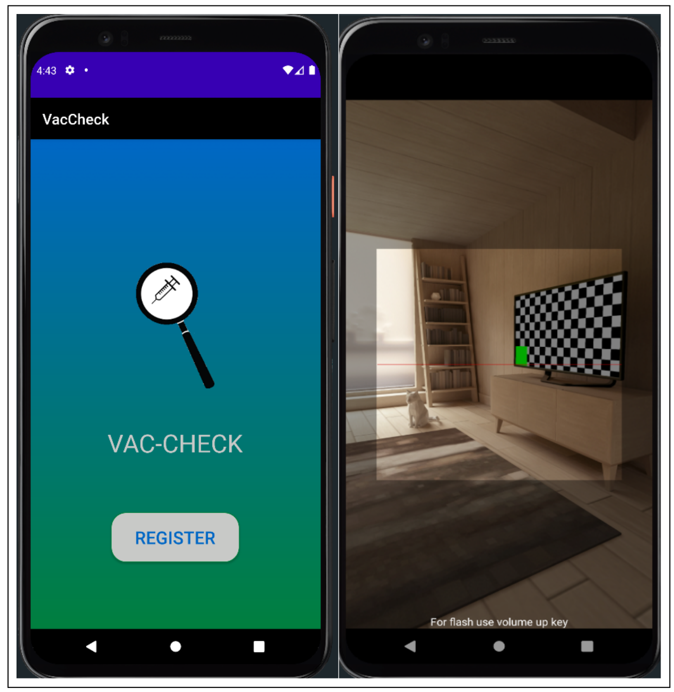

Fig. 4. The Main Activity and Registration Scanner Activity of Vac-Check

Another implementation decision was determining which device targets to initially design the mobile application for. The Android OS is used by a variety of devices that have different specifications. It is important for the mobile application use that all devices can view and use the application as intended. However, due to limited time and resources, the development of the Vac-Check mobile application could only be developed for a few device targets. For implementation and testing of the mobile application, the device targets, the Samsung Galaxy Note 10+ and the Google Pixel 4, were used because these device targets were available.

The Vac-Check mobile application was to implemented to enable users to accomplish these 4 tasks: register their device with the Vac-Check system, quickly make an authorization policy and generate a QR code, create and save authorization policies, and load previously save authorization policies and generate a QR code. The registration task is completed with two activities in the application: main and register scanner. The main activity prompts the user to register their device by using a button. Once the user presses the register button, they are redirected to the register scanner activity.

The register scanner activity will allow the user to scan a QR code that is generated when the user has been vaccinated. With the QR code scanned, the user will initiate the registration process which will connect the user's device with their vaccination record which will be held on the encrypted database. The users' devices will store the unique identifier of their vaccination record in Android's internal shared preferences system.

The Vac-Check mobile application accomplishes the task of quickly generating an authorization policy and a corresponding QR code by implementing two dialog activities: qr_generate_dialog and qr_code_dialog. The qr_generate_dialog will create an AlertDialog that contains check boxes that corresponds to permissions that are associated with the fields of the vaccine record. The user can select the permissions of the information that they want to release to the third party verifier. With the permissions selected, the user can then press the generate button of the dialog. This button will return an authorization policy object to menu activity, qr_generator. The qr_generator can be viewed in figure 9 which is in section VIII.

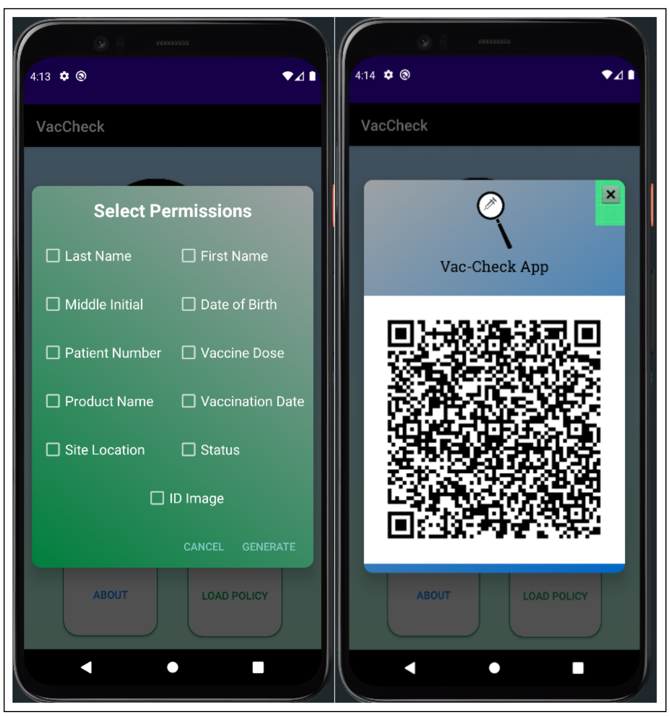

Fig. 5. User Authorization Policy and QR Code Generation

When the qr_generator activity receives a new policy object, it create an instance of the qr_code_dialog dialog. This dialog will convert the policy object to a string object. This string object will be encode into a QR code as a Bitmap which is done by the Android package zxing. This Bitmap object is displayed using the created dialog. Figure 5 shows the created QR code from a quickly user-defined authorization policy.

The task, creating and saving authorization policies, is implemented using a single activity, policy_creator. The policy_creator activity has a similar layout to the qr_generate_dialog. The user can select permissions of fields within the vaccine passport using check boxes. The user also has to provide a name for the policy that they creating using an EditText view. With a filename and a set of selected permissions, the activity will create a new policy object and save it as text in a text file. This text file will be stored in the internal storage of the user's mobile device. Since the internal storage is regarded as private in the Android OS, the text files will only be made available to the Vac-Check application. This activity can be viewed as figure 10 in section VIII.

The last task, loading saved authorization policies and generating QR codes, is enacted using an activity, load_policies, and the qr_code_dialog dialog. In the load_policies activity, a list of the saved authorization policy is generated by scanning the internal storage. With the list of saved authorization policies, a radio button group adds a new radio button, that correspond to one of the authorization policies, for all of the authorization policies in the list. The radio button group and its radio buttons are rendered to the screen during run-time.

The user then can select the radio button that corresponds to the desired authorization policy. The selected authorization policy is loaded into a policy object and is returned back to the menu activity. Similar to how a quickly user defined authorization policy's qr code is generated, the loaded policy object is converted to a string and that string is encoded into a Bitmap object. This Bitmap is displayed to the third party verifier using the qr_code_dialog dialog. The load_policy activity and the generated QR code can be viewed in figure 6 in section VIII.

B. Web Subsystem

The web subsystem is encompasses the web application of the Vac-Check system. The web application will make use of the web hosting functionality of the back-end subsystem from Firebase. The tasks that the web application handles are certificate holders' sign-up and updating the database with certificate holders' vaccination records. The web subsystem is still within the design phase.

C. Back-end Subsystem

The back-end subsystem of the Vac-Check system is comprised of the encrypted database, the authorization, authentication, and accounting server, and the web server. The back-end subsystem needs to have these characteristics, real-time processing of requests and scalability, in order to handle both the mobile subsystem and web subsystem. Cloud computing technology is able to ensure these characteristics in the back-ed subsystem. Another benefit of cloud computing is that hardware like servers has been abstracted and thus the maintenance of the hardware is no longer a factor. Thus, the back-end subsystem design makes use of cloud computing technology.

With the design of the back-end subsystem using cloud computing, the next major design decision is to determine which service to use to implement the back-end subsystem. There are a number of cloud computing services on the market, but Google's Firebase was selected for implementing the back-end subsystem. Firebase is a Platform-as-a-Service cloud computing model that is designed for web and mobile integration. Firebase is capable of supporting Android, iOS, and web applications. Firebase offers these services that the back-end will use: a JSON real-time database, cloud functions that supports server-side logic without server setup, cloud messaging to users' devices, and web hosting.

The tasks that back-end subsystem implements handling and authenticating vaccine status verification request, maintaining the database and handling database queries, and enacting and supporting public key infrastructure for signing and encrypting vaccine certificates. The back-end subsystem is being implemented now.

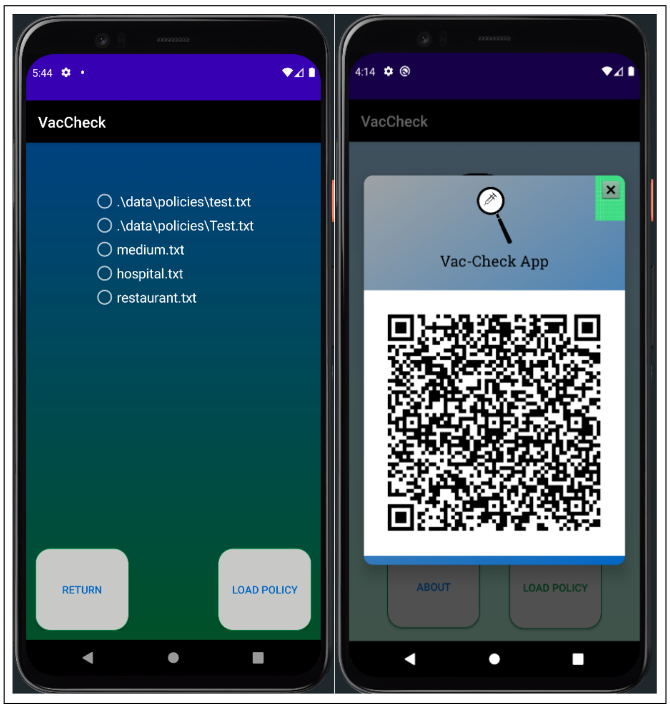

Fig. 6. Vac-Check Load Policy Activity: load_policy

V. Evaluation

The evaluation of the proposed solution will be done by performing a use case study of the system. The research questions proposed in the section I requires a use case study to answer these questions. The use case study will allow randomly recruited individuals a chance to interact with the Vac-Check system and to collect data about how they used the system.

The design of the use case study will consist of 6 phases. The first phase is the recruitment phase where the study will recruit 40 to 60 random individuals to ensure an assortment of backgrounds. The next phase is the pre-survey phase. The recruits will take an initial survey to measure what are their attitudes and perceptions towards DVC systems. After the pre-survey phase, the recruit will enter in the training phase where they will learn how to use the system. Once trained, the individuals will be split into two groups based on the certificate holder and verifier roles. With their assigned roles, the participants will enter into the experiment phase where they will use the system. Before getting The recruits will be split into either a certificate holder or verifier roll in order to simulate the full use of the Vac-Check system. With the completed experiment phase, the recruited individuals will surveyed again in the post-survey phase. The last phase will be the comparison phase where the participants' answers to the pre-survey and the post-survey will be measured and compared to one another.

To determine how well user-defined authorization policies ensure the confidentiality of the vaccine records are preserved, individuals need to be recruited and allowed to use a prototype of the Vac-Check system. In an experimental setting, the behavior of the recruited certificate holders can be monitored to determine how well their policies conserve the confidentiality of their vaccine records. Answering the second research question will require a pre-survey to first establish the recruited individuals' attitudes and perceptions of DVC systems are and then a post-survey to compare how their attitudes and perceptions changed after using the Vac-Check system.

VI. Future Work

There is more work on the Vac-Check system that needs to occur before a prototype is ready for use. Of the three subsystems that comprises Vac-Check, the web subsystem for enrolling newly vaccinated certificate holders and the cloud based back-end subsystem need to be implemented. The design of the back-end has been determine with it being implemented using Google's Firebase and its tools.

The website is still in the design phase, but in keeping with the current web development processes, the website will be implemented based on HTML/CSS, JavaScript , and a framework like Angular or React. Given these unfinished components, we are estimating that a working prototype will be finished within 4 to 6 weeks.

After the working prototype is completed, the next step of this project is to evaluate it. As previously discussed, the prototype system will be evaluated using a use case study. With the current timeline, the earliest time frame that the use case study can be completed is during Summer 2022.

Another factor that needs to be considered is Institutional Review Board (IRB) approval. Since the use case study will be using human participants, the IRB will need to approve of the study before the study can begin. This may lead to a longer timeline of completing the prototype and evaluating it.

After the initial prototype is finished and the use case study is completed, the next step would be to make the mobile subsystem more accessible to more devices, operating systems, and people. To make the mobile application more accessible for more devices would be to optimize the layouts of the mobile application to fit to more target devices. By porting the mobile application into iOS and thus creating an iOS application for Apple smartphones, this would allow more devices of other operating systems to use the mobile application. Another way of making the mobile application more accessible would be to support multiple languages such that people who don't speak English can still use the application.

VII. Conclusion

The exact extent of the disruption caused by the pandemic and the responses to it won't be determine for some time, but it will be significant. An aspect about these type of infectious events is that they are recurring. Bouts of pandemics and epidemics occur regularly such as the 2014 Ebola Epidemic, the 2009 Swine Flu Pandemic, and the 2002 SARS outbreak. Pandemics and epidemics are a norm of our existence as a species on this planet. Given this fact, it is important to have multiple sets of tools to prevent or mitigate the effects of new pandemics and epidemics. Digital vaccine certification systems are one such tool that can be used to mitigate the spread of a disease while allowing daily life to occur.

Digital vaccine certification systems use a specialized type of health record that, unlike regular health records, individuals or third parties outside of the medical field will also need some kind of access to those records. However, vaccination records are still a health record and consequently has a security need that must be addressed. The proposed solution, Vac-Check, implements a novel authorization policy scheme which gives the users of the system control over what information of theirs is released. The users defined their own authorization polices by determining what set of access permissions other third parties have. This is done either during the verification process or with a saved policy previously defined by the certificate holder.

This research aims to answer two questions: are the user-defined authorization policies enough to protect the confidentiality of their vaccination records and will the attitudes and perceptions of those who are hesitant to use DVC systems improve if they are in control of how their vaccination records are released? These questions will be answered through a use case study. The use case study will recruit randomly selected individuals to simulate test scenarios for the system. During this experiment, the behavior of the participants will be monitored to determine how they are creating authorization policies. Changes in attitudes and perceptions about DVC systems of the participants will also be measured using a pre-survey and a post-survey.

References

[1] World Health Organization, "WHO COVID-19 Dashboard," Accessed Feb, 10,2022 [Online], 2020. [Online]. Available: https://covid19.who.int/

[2] F. O'Brien, L. Tim, and P. James, "The era of pandemic restrictions is fast coming to an end," Feb 2022. [Online]. Available: https://www.bloombergquint.com/business/the-era-of-pandemic-restrictions-is-fast-coming-to-an-end

[3] Ada Lovelace Institute, "International monitor: Vaccine passports and covid status apps," Jun 2020. [Online]. Available: https://www.adalovelaceinstitute.org/project/international-monitor-vaccine-passports-covid-status-apps/

[4] S. S. Mithani, A. B. Bota, D. T. Zhu, and K. Wilson, "A scoping review of global vaccine certificate solutions for covid-19," *Human vaccines immunotherapeutics*, vol. ahead-of-print, no. ahead-of-print, pp. 1–12, 2021.

[5] J. Drury, G. Mao, A. John, A. Kamal, G. J. Rubin, C. Stott, T. Vandrevala, and T. M. Marteau, "Behavioural responses to covid-19 health certification: a rapid review," *BMC public health*, vol. 21, no. 1, pp. 1–1205, 2021.

[6] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based solution for covid-19 digital medical passports and immunity certificates," *IEEE access*, vol. 8, pp. 222 093–222 108, 2020.

[7] J. L. Hernández-Ramos, G. Karopoulos, D. Geneiatakis, T. Martin, G. Kambourakis, and I. N. Fovino, "Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation," *Wireless communications and mobile computing*, vol. 2021, pp. 1–12, 2021.

[8] F. Ishengoma, "Nfc-blockchain based covid-19 immunity certificate: Proposed system and emerging issues," *Information Technology and Management Science*, vol. 24, pp. 26–32, 2021.

[9] M. Foy, D. Martyn, D. Daly, A. Byrne, C. Aguneche, and R. Brennan, "Blockchain-based governance models for covid-19 digital health certificates: A legal, technical, ethical and security requirements analysis," *Procedia computer science*, vol. 198, pp. 662–669, 2022.

[10] M. A. Riva, M. E. Paladino, S. Brambilla, and M. Belingheri, "Covid-19 health passes. lessons from the past," *Journal of Travel Medicine*, 2021.

[11] L. A. Sawchuk and L. Tripp, "Managing an epidemic in imperfect times: encampment and immunity passes in 19th century gibraltar," *BMJ global health*, vol. 6, no. 8, p. e006713, 2021.

[12] R. Waitzberg, N. Triki, S. Alroy-Preis, T. Lotan, L. Shiran, and N. Ash, "The israeli experience with the "green pass" policy highlights issues to be considered by policymakers in other countries," *International journal of environmental research and public health*, vol. 18, no. 21, p. 11212, 2021.

[13] O. J. GSTREIN, "The eu digital covid certificate: A preliminary data protection impact assessment," *European journal of risk regulation*, vol. 12, no. 2, pp. 370–381, 2021.

[14] S. Kamin-Friedman and M. Peled Raz, "Lessons from israel's covid-19 green pass program," *Israel journal of health policy research*, vol. 10, no. 1, pp. 1–61, 2021.

[15] F. Laricchia, "Market share of mobile operating systems worldwide 2012-2022," Feb 2022. [Online]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/statisticContainer

VIII. Appendix A

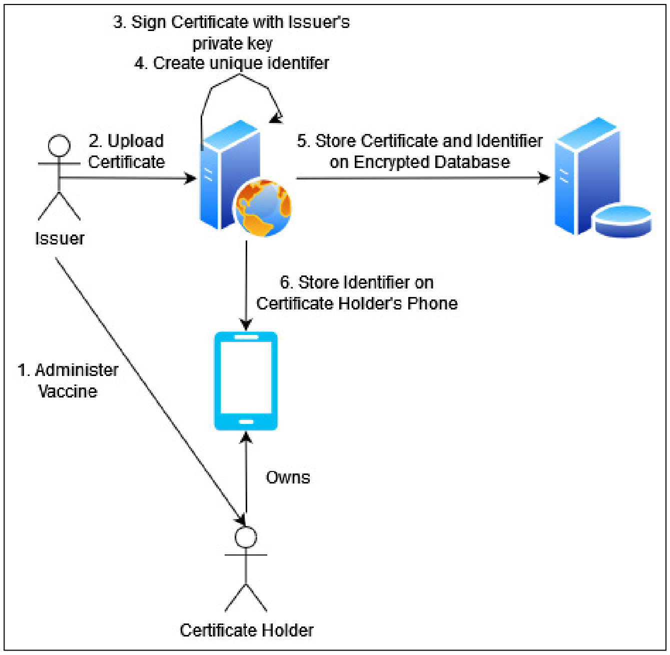

Fig. 7. Vaccine Certification Issuance Process

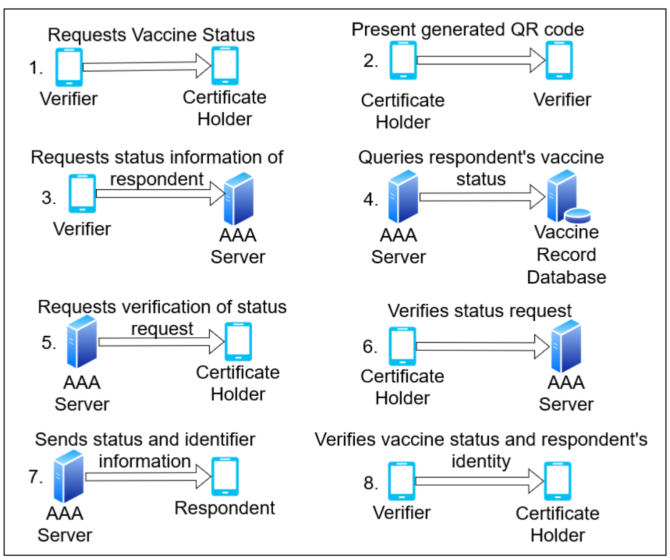

Fig. 8. Vaccine Status Verification Process

Fig. 9. Vac-Check Menu Activity: qr_generator

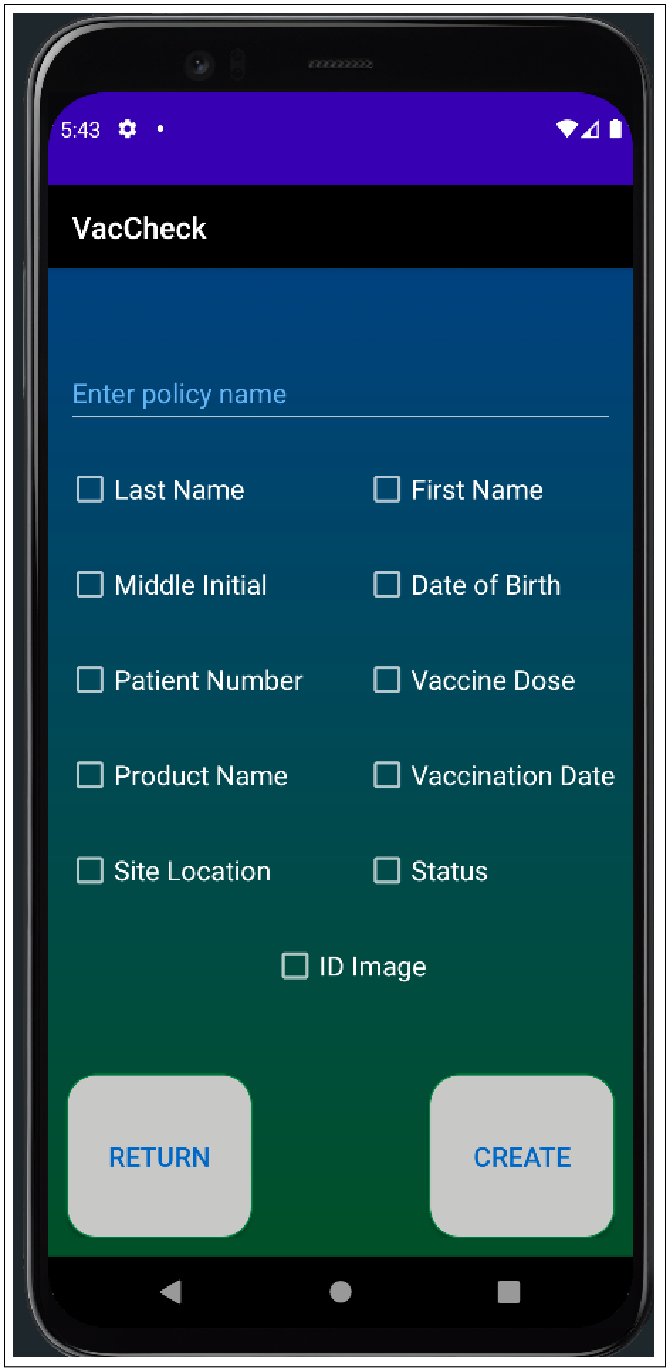

Fig. 10. Vac-Check Policy Creator Activity: policy_creator