



SafeTravel–Application with Blockchain Technology

Yu-Sheng Goh, Lee-Ying Chong^(✉), and Siew-Chin Chong

Faculty of Information Science and Technology (FIST), Multimedia University, Melaka,
Malaysia

lychong@mmu.edu.my

Abstract. The first COVID-19 case was detected in Malaysia on 25th January 2020. Given the serious situation of COVID-19, Malaysia Government implemented the Movement Control Order (MCO) in the same year by restricting citizen movement. The COVID-19 outbreak in Malaysia under MCO 1.0 is successfully controlled as only a hundred and below daily infected cases were reported. However, Malaysia's nightmare began after the government lightened the movement control, where more than 10,000 infected cases were reported daily. When the people realise that they cannot eliminate the COVID-19 pandemic, they should prevent another outbreak with their responsibilities, such as self-isolation when in close contact with a confirmed infection. Therefore, the SafeTravel mobile application is proposed to allow users to record their travel data in the system when performing the cross-state activity. In this application, the location, purpose, start date and end travelling data are provided by users and stored in the database using blockchain technology. Besides that, the users can update their daily health status in the mobile application to be aware of the COVID-19 symptoms and always monitor their body status.

Keywords: Blockchain · Travel · Hashing · Mobile application

1 Introduction

COVID-19 pandemic, also known as coronavirus pandemic, has affected the people and countries globally. Although Malaysia Government has implemented the Movement Control Order (MCO) against the increment of COVID-19 cases [1], the MCO implementation is not a long-term solution for the country's development. In MCO, Malaysia Government restricts citizen movement by prohibiting business operations to avoid crowd gathering and spreading the virus. This move led Malaysia's economy to fall into recession. Besides that, Malaysia Government has provided financial aid for the M40 and B40 citizen multiples times to overcome the situation caused by this pandemic [2]. As a result, the Malaysian government's national debt is drastically increased. The Malaysia Government removes the travel restriction and allows interstate travel for citizens to recover the economy and life balance.

Data and information retrieved from the human, such as the user's location, the purpose of travelling, and others, serve as the privacy of users that should be protected to prevent an attacker from retrieving and editing these personal data. However, if the attacker hacked users' information, then he may use the information to threaten the users for ransom, which is a situation that is unwilling to happen. Therefore, to ensure the data and information are protected, this application utilises blockchain technology to protect the travel records of the user. As for now, blockchain technology is still reliable as the attacker cannot easily hack it.

In addition to this, the symptoms of COVID-19 can be easily identified, such as cough, fever, the difficulty of breath, loss of smell, loss of taste and so on. However, people are not aware that these symptoms might occur in their bodies. If people can recognise their symptoms earlier, they can quickly take action, such as performing a swab test or quarantine to prevent the outbreak of COVID-19. Therefore, the proposed application allows the user to update their health status or condition while travelling to ensure that they are alert if they have the COVID-19 symptoms. This move serves as a good step to prevent and control another outbreak in Malaysia. Users will get the alert message if they have any symptoms of COVID-19 during their travel.

Blockchain is a distributed, immutable ledger that is used to record transactions, track assets, and build trust among the nodes of a computer network. The person who conceptualised the first blockchain was called Satoshi Nakamoto in 2008. He significantly improved the design, adding blocks to the initial chain. Instead of requiring them to be signed by a trusted party, he uses a hashcash-like method to timestamp blocks. After that, Nakamoto implemented the first blockchain on the cryptocurrency bitcoin, which served as the public ledger for all transactions made in 2009 [3]. In 2014, blockchain technology was no longer specific to cryptocurrency, and it is used for financial, inter-organisational cooperation such as smart contracts, financial services, supply chains, healthcare, etc. In the same year, Ethereum, the second generation blockchain system, was introduced after bitcoin. The most important feature of Ethereum is the "smart contract" [4]. The difference between Ethereum and bitcoin is that Ethereum can record financial instruments such as loans and contracts, rather than just currency performed by Bitcoin.

Blockchain is the combination of two words, block and chain [5]. The blockchain stores the data inside a block such as the amount of money, record of the medical, digital certificate of ownership or any other information. Besides that, each block contains its previous and current hash value. The hash value is generated and calculated from a text string using a mathematical function [6]. The hash value is unique for each block that is used to identify its content. In addition, when a new data is added, the data is placed inside the block, and this new block is referenced to the previous block to form the chain. One of the features of the blockchain is the data inside the block remain immutable. If the block content is altered, it caused the current hash value of the particular block changes. Hence, this feature shows the someone has modified the data.

In this paper, we propose a mobile application to protect and keep track of the travel record using blockchain technology. This proposed mobile application is named as SafeTravel. This mobile application utilises blockchain technology to secure the user's travel data when they perform interstate travel. All the travel records added by the user are hashed and linked to the previous block containing the hash value of the previous block to ensure the integrity of the data. If the previous hash value on the current block is mismatched with the previous block's current hash, this indicates that someone has modified the data. The travel record data protected by blockchain technology is users' location, data, and time. Once users add a new record, the new record block is linked to the previous block to perform the chaining.

Besides, the proposed application enables the user to perform the daily health check by updating the symptoms during travel time. This proposed application allows the users to perform daily health checks based on the users' date of travel record. Users must select all the options given to complete the daily health check fully. If the users have any symptoms of the COVID-19, the system will send an alert message to the users and ask the user to perform the self-test at home or swab test at a nearby hospital and clinic.

2 Literature Review

2.1 Data Breaches in Malaysia

In March 2021, Malaysia Airlines has suffered a data breaches incident via a third-party IT service provider [7]. The incident compromised the personal information of Enrich frequent flyer members such as Enrich member names, date of birth, contact details, status, and tier level information within a nine-year period from March 2010 to June 2019. However, the incident did not affect the itineraries, reservation, ticketing, ID card or payment card information, according to the Malaysia Airlines statement. As for the safety purposes, Malaysia Airlines advised the Enrich frequent flyer member to change their password to avoid the data get leaked again.

In October, a news released claimed that mobile subscribers' data in Malaysia was stolen and leaked on to the dark web exceeds more than 46 million [8]. The first discovered is from the Malaysian technology news website, Lowyat.net, informed that someone was trying to sell a huge database of personal details from at least 12 Malaysian mobile operators as well as a vast amount of personal data was also stolen from Jobsteet.com, and six different official Malaysian organisations. In the end, the Malaysian Communications and Multimedia Commission (MCMC) confirmed that the data breach of 46 million mobile subscribers were affected and issued a statement on Facebook a day later. This is the biggest data breaches in Malaysia because Malaysia has a population of 32 million, of which 46 million of data has been stolen.

2.2 Cryptography Study

The cryptography is a method that transform the intelligible messages into the unintelligible messages, and then retransform the messages to the original messages that can be understand by people. There are two types of encryption approaches which are symmetric encryption and asymmetric encryption. The symmetric encryption is also called as private key encryption because the encryption and decryption process have shared a common key. Moreover, asymmetric encryption is also called as public-key encryption approaches which two keys are involved in encryption and decryption process which are public key and private key. The public key is known by anybody that used to encrypt messages and verify signatures while private key is known only by the recipient that used to decrypt messages and sign signatures. In a nutshell, the encryption process involved the public key and decryption process involved the private key where private key should not be known by others.

Besides that, hashing is another method that used to transform the plaintext messages to the ciphertext messages. The most popular method for hashing algorithm is SHA-1, SHA-2 and SHA-3. SHA-1 hashing algorithm is not recommended to use because the methods may produce collisions and considered as insecure. Therefore, SHA-2 is developed to replace the SHA-1. In SHA-2, there are 3 additional versions which are SHA-256, SHA-384 and SHA-512 which the number represented as the number of bits used. Fortunately, SHA-2 hashing algorithm has not any vulnerabilities found recently, and it is widely used by many people to protect their data and information.

2.3 Existing Application

There are many tracking applications available for user but each of them has their own purpose and objectives. The comparison between SafeTravel and the existing applications is shown in Table 1. Each of application has different target and features. SafeTravel provide additional features which date is protected by the blockchain technology.

2.3.1 iSharing

iSharing is a GPS Location Tracker mobile application offered by iSharingSoft Inc [9]. iSharing was released on 29 January 2011. iSharing Location Tracker application provides a real-time tracker service on both Apple and Android devices. iSharing allows family to communicate and stay connected with each other at any time. Besides that, iSharing aim to help parent and caregivers reduce anxiety and minimise concern about the movements of their family members.

2.3.2 Jibble 2

Jibble 2 is an employee attendance tracker mobile application available on both iOS and Android devices [10]. Jibble company released the Jibble 2 application in 2021, which eventually to replace Jibble 1. Jibble 2 is the newest and advanced version of Jibble. Jibble 2 improved existing features of Jibble 1 and added some new features. Besides that, it also improved the overall experience and design. Jibble 2 allows the employee to

Table 1. Comparison of SafeTravel and Existing Application

Comparison	Application				
	iSharing	Jibble 2	AfterShip	MySejahtera	SafeTravel (The proposed app)
Platform Support	iOS & Android	iOS & Android	iOS & Android	iOS & Android	Android
Application	Mobile application	Mobile and Web application	Mobile application	Mobile application	Mobile application
Services	Mainly used to tracking the family's movement	Mainly used to taking the attendance of employee	Mainly used to tracking the parcel movement	Mainly used for government to control the citizen	Mainly used to track the location of user been travel
Target	Family	Organizations	Online Buyer	Malaysia Citizen	Traveller
Data Protection	No	No	No	Weak Protection	Blockchain
Features	-Alert message when family reached at destination	-Easily to manage the clock in and clock out of employees	-Instant update of order delivery status	-Check in and check out function	-Data is protected using the blockchain technology involved the hashing
Cost	Free to download but have to subscribe for more advance feature	Free to download but have to become "Premium" for advanced services	Totally free to download and use	Totally free to download and use currently	Totally free to download and use for all services

easily report themselves in every working day by using the feature of clock in and clock out. In additions, Jibble 2 helps the organization to track the employee's working time for payroll.

2.3.3 AfterShip Package Tracker

AfterShip Package Tracker is a parcel shipment tracker mobile application developed by AfterShip Limited and can be downloaded on iOS and Android devices [11]. AfterShip allows users to track their online orders and shipments in a real-time delivery update with

AfterShip mobile application. Besides that, AfterShip have partnered with 870 carriers over the countries such as FedEx, SkyNet, GD Express, City-link and etc. AfterShip give the user convenient as it sends the notification for the user once the delivery status has been updated.

2.3.4 MySejahtera

MySejahtera is used to manage the COVID-19 outbreak developed by the Malaysia Government [12]. MySejahtera was developed to assist the Malaysia Government in managing and mitigating the COVID-19 outbreak and allows the user to monitor their health status and get treatment if they are infected. Besides that, this application also allows Malaysian citizens to apply for or register for the vaccination. Malaysian citizens or foreigners are required to scan the MySejahtera with the QR code scanner function wherever they go.

Unfortunately, violation of data privacy has raised concern among Malaysians [13]. Malaysia Government intentionally sold MySejahtera to a private company consisting of sensitive and personal data such as IC, email, phone numbers, addresses and more. Thus, these actions may take the privacy of Malaysians at risk. Besides that, Malaysia Government will not be liable for any loss or damage obtained from the MySejahtera application, which is claimed by MySejahtera's disclaimer [14]. Furthermore, the privacy policy of MySejahtera does not give information on how personal information is processed and where the data has been stored, increasing the concern of Malaysian citizens. Therefore, the data protection for the MySejahtera application is weak as it cannot guarantee the privacy of Malaysians.

3 Proposed Solution

3.1 Context Diagram

Figure 1 illustrates the context diagram for the SafeTravel application that shows the relationship between the systems with other external entities. Figure 1 shows that users can register, add travel data, add health, and view travel records. Besides, based on the health data submitted by the user, the system sends a notification to the user if suspicious symptoms of COVID-19 are detected.

3.2 Data Flow Diagram

From Fig. 2, the data flow diagram has 6 processes: Register, Add Travel Record, View Travel Record, Receive Health Data and Notify the User's Health. Besides that, there are 3 data sources included: User file, Travel file, and Health file used to store the data submitted from the user.

3.3 Activity Diagram

The users using the proposed application for the first time should register themselves on the Signup Page. Then, the users are required to provide a username that should be

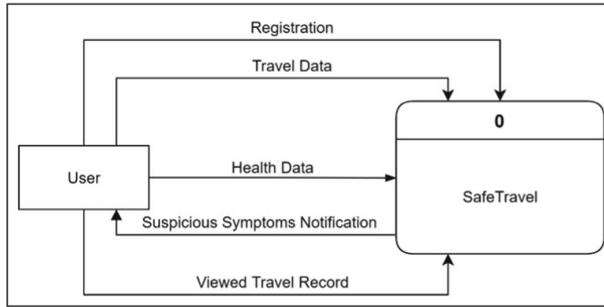


Fig. 1. Context diagram

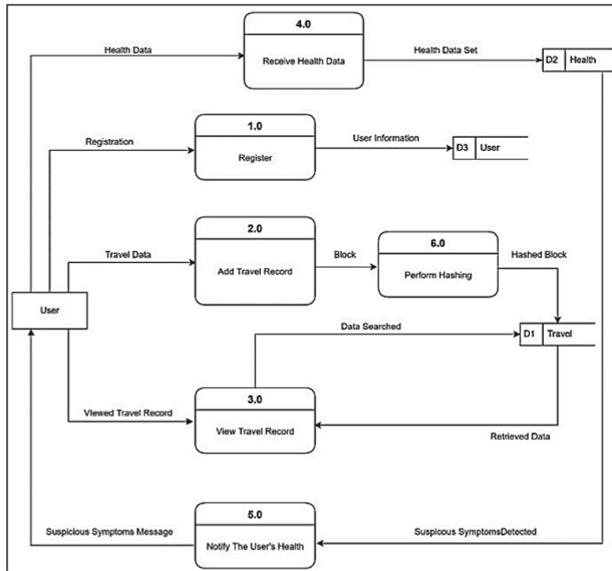


Fig. 2. Data flow diagram

unique and a password that should be satisfied the requirement. After that, users can perform the add travel record, update and view travel record, and update their health status during travel, as showed in Fig. 3.

3.4 Flow Chart

3.4.1 Hashing Function

The SHA-256 hashing algorithm is applied in the proposed application as displayed in Fig. 4. The travel record added by the user is stored into the block, and that particular block is hashed. After that, the hashed block is chain to the previous hash block added.

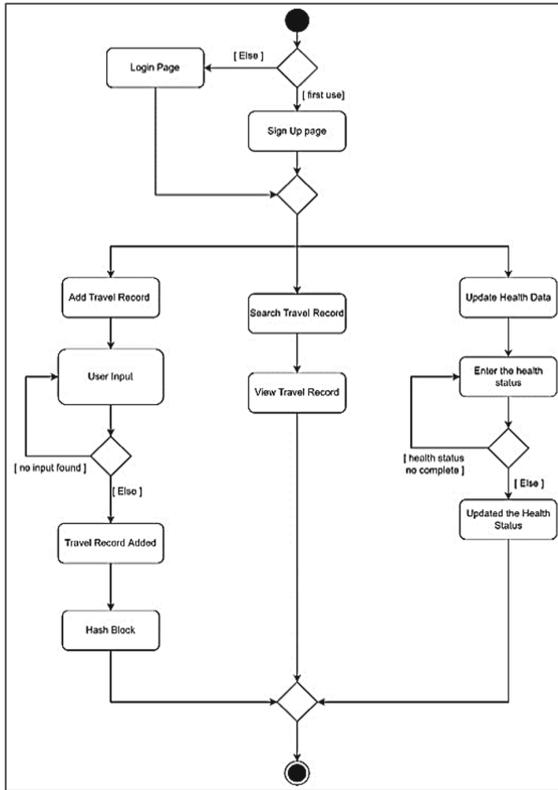


Fig. 3. Activity diagram (User)

3.4.2 Register Feature

Figure 5 shows the flow chart of user’s registration process. The users must provide the valid email address, and satisfied password for creation of account. If the user failed to do it, the system ask the users to re-enter again.

3.4.3 Add Travel Record

Three main data require the users to provide: the start and end of the travel date, travel location and purpose of travelling, as exhibited in Fig. 6. Once all the information required is filled, the users successfully add a new travel record to the system.

3.4.4 View Travel Record

This proposed application allows the users to view their travel records by following the process showed in Fig. 7. Users can use the search function to search for the travel record and the record is displayed to the users.

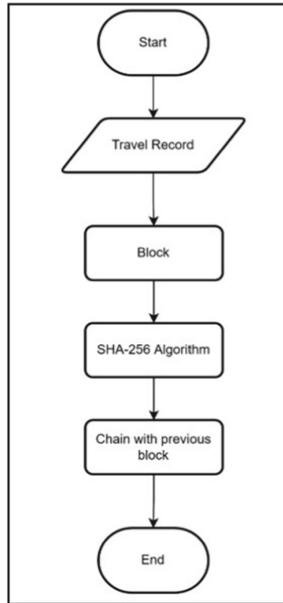


Fig. 4. Flowchart of hashing

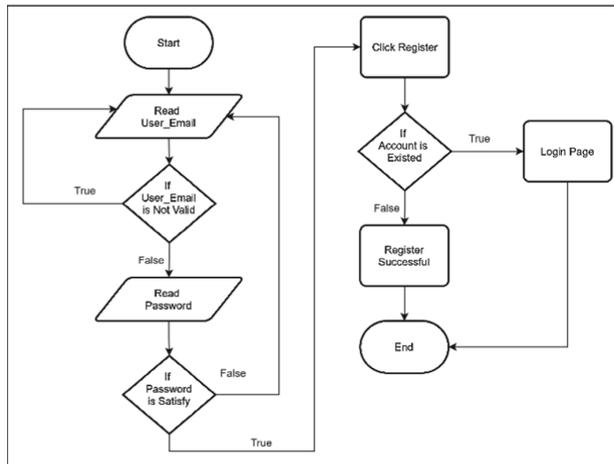


Fig. 5. Flowchart of register

3.4.5 Receive Health Data

Figure 8 shows the process flow of receiving health data. In this process, users are required to choose all the questions options. If all options are selected, users successfully update their health status.

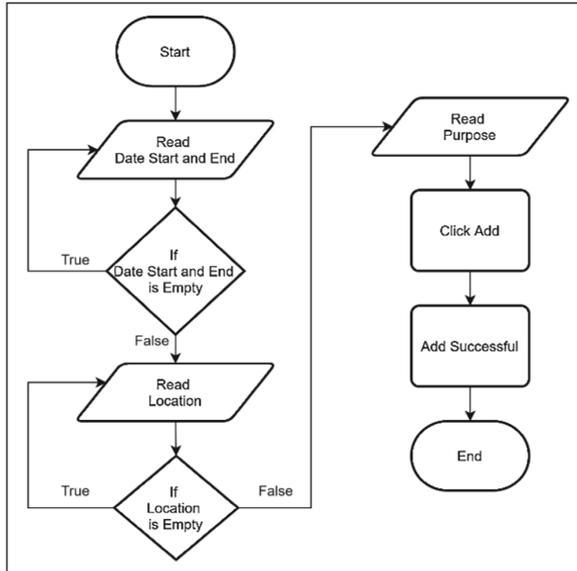


Fig. 6. Flowchart of add travel record

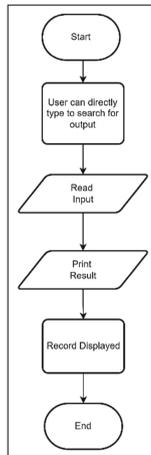


Fig. 7. Flowchart of view travel record

3.4.6 Notify User’s Health

Based on the health data submitted by the users, the system will notify the users if the suspicious symptoms of COVID-19 are detected as illustrated in Fig. 9. The notification is sent to the users.

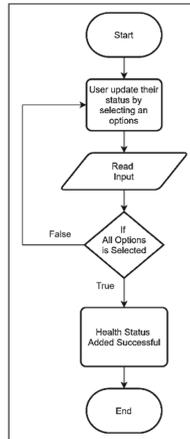


Fig. 8. Flowchart of receive health data

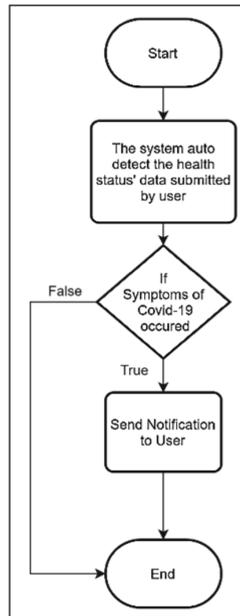


Fig. 9. Flowchart of notify user's health

3.5 System Implementation

3.5.1 Add Travel Page

Figure 10 shows the primary page for the add travel which requires user to fill the location, date start, date end and the purpose.

Fig. 10. Add travel main page

After the search button is clicked, another page appears, which allows the user to search the location exhibited in Fig. 11. First, the user must insert the location's name and click on the "Search" button. As a result, the map is moved to the location stated by the user. Finally, the user can click "Confirm" to confirm their address.

3.5.2 Travel Record Page

All the added travel record is listed at the travel record page according to the start date of the travel record in descending order as shown in Fig. 12. The first ten characters of the current hash and previous hash value also display at the travel record page.

3.5.3 Health Check Page

Health check page is used for the user to update their current health status during their travel time. There are several questions required to answer as exhibited in Fig. 13.

Besides that, there are two kinds of the pop-up message. If the user forgets to do their health check during their travel date, a pop-up message is shown to remind them to do the daily health check, as shown in Fig. 14. Furthermore, if the daily health check results "Unwell" symptoms, another alert message appears to the user to notify them to stop their travel, as illustrated in Fig. 15.

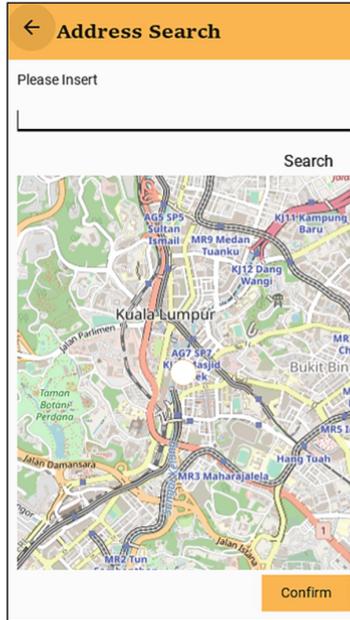


Fig. 11. Address search page

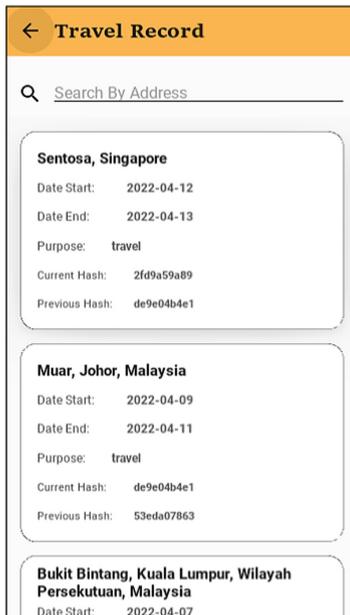


Fig. 12. Travel record page

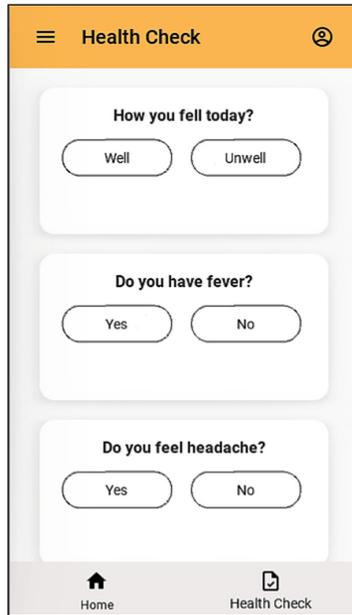


Fig. 13. Health check page

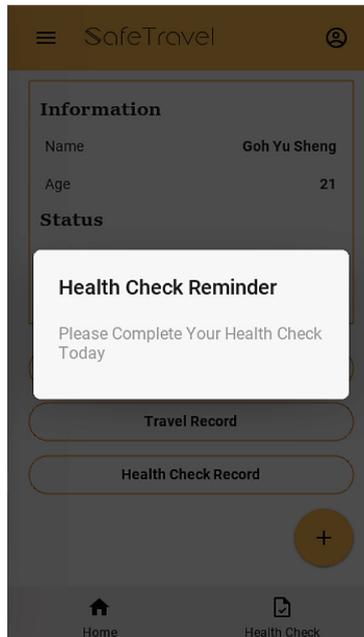


Fig. 14. Health check reminder

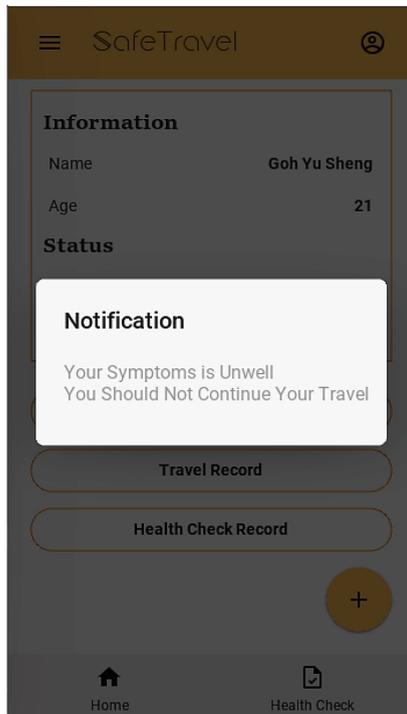


Fig. 15. Notification from the application

3.5.4 Health Check Record

The health check done by the user can be viewed from the health check record page as shown in Fig. 16. User can click on the small “eye” button to view all the content that inserted before.

3.5.5 Blockchain Function

The blockchain function is applied to the travel record data. Every time user successfully adds a new travel record. The new travel record is stored in a block, which is a chain or link to the previous travel record block added by the user. Besides that, the new travel record block is hashed by using the SHA-256, which contains a 32-bytes signature for the block.

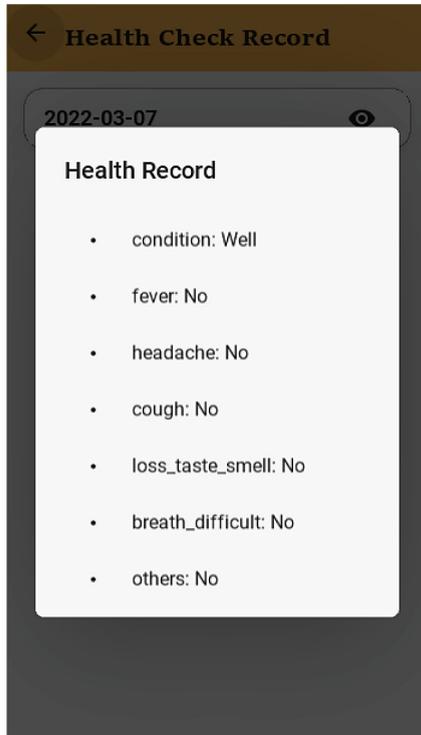


Fig. 16. Health check record page

For example, the previous hash on block 1 is identical to the current hash value on block 2, as shown in Fig. 17. However, the travel record page only showed the first ten characters for both the current and previous hash. The complete hash value for each block can be observed at the system’s backend. For experimental purposes, when the travel destination is purposely modified to the “Muar, Johor, Malaysia”, the hash value for the particular block is changed, which is supposed to be “de9e04b4e1” instead of “5ecc8e6bbc”. Therefore, the previous hash value on block 1 is mismatched with the current hash value on block 2 highlighted, as shown in Fig. 18.

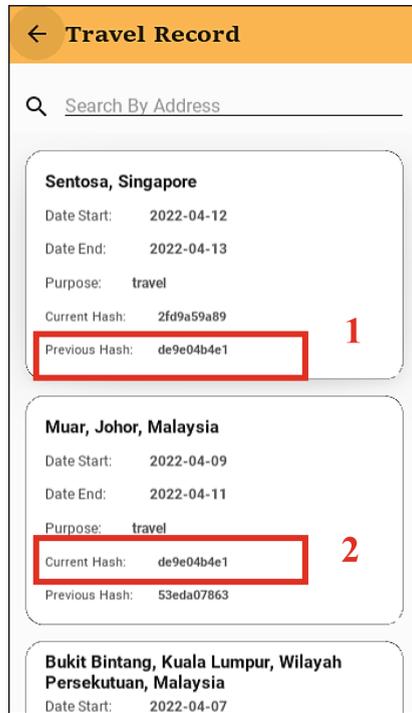


Fig. 17. Blockchain Functions

4 Conclusion

This paper proposes a mobile application named SafeTravel applications, which aims to protect the user's travel record through blockchain technology. The travel record is protected by blockchain technology to prevent data leakage. All the travel record is hashed and chained with the previous travel record block. If the attacker alters the data, the user can immediately discover the data by looking at the hash value inside the travel record page. While users travel, they can update their health status through the health-check feature provided by the application. The proposed application provides a feature that lets users record their daily health status while travelling. If symptoms of COVID-19 are detected, the users receive an alert message to advise them to do the swab test at the clinic or perform the self-test themselves.

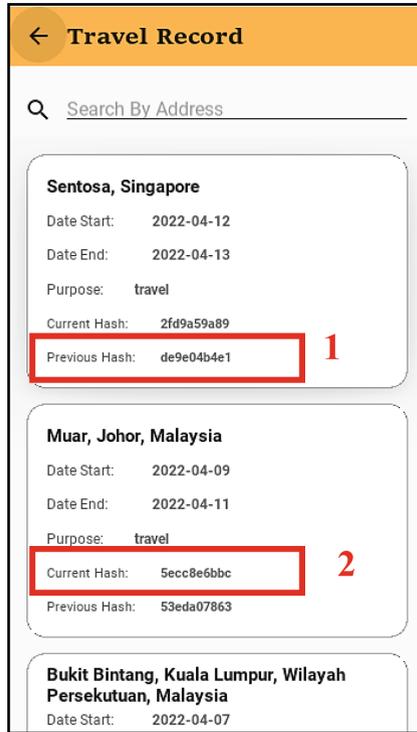


Fig. 18. Hash Value after Modified Data

Acknowledgements. The work presented in this paper was supported by Multimedia University through the IR Fund 2021 (MMUI/210029).

References

1. Amir Yusof. (2021). *Timeline: How the COVID-19 pandemic has unfolded in Malaysia since January 2020*. Available at <https://www.channelnewsasia.com/asia/timeline-how-covid-19-pandemic-has-unfolded-malaysia-january-2020-2082081>
2. Martin Carvalho. (2021). *Covid-19: Ten million Malaysians to receive financial aid from Monday (Sept 6), says PM*. Available at <https://www.thestar.com.my/news/nation/2021/09/01/special-covid-19-assistance-payments-to-start-monday-sept-6>
3. Bernard Marr & Co. (2021). *A Very Brief History of Blockchain Technology Everyone Should Read*. Available at: <https://bernardmarr.com/a-very-brief-history-of-blockchain-technology-everyone-should-read/>
4. Vinay Gupta. (2017). *A Brief History of Blockchain*. Available at: <https://hbr.org/2017/02/a-brief-history-of-blockchain>
5. Swati Sharma. (2020). *21 Amazing Examples of How Blockchain Technology Is Revolutionizing Everyday Life*. Available at <https://www.classicinformatics.com/blog/blockchain-technology-applications>

6. Tania H. (2018). *How the Blockchain Works*. Available at: <https://rubygarage.org/blog/how-blockchain-works>
7. Eileen Yu. (2021). *Malaysia Airlines Suffers Data Security Incident Affecting Frequent Flyer Members*. Available at: <https://www.zdnet.com/article/malaysia-airlines-suffers-data-security-incident-spanning-nine-years/>
8. BBC News. (2017). *Malaysian Data Breach Sees 46 million Phone Numbers Leaked*. Available at: <https://www.bbc.com/news/technology-41816953>
9. Pallavi. (2020). *iSharing: Find Friends, Family*. Available at <https://www.mobileappdaily.com/app-review/isharing>
10. Charlette Beasley, Zenia Lazaro. (2021). *Jibble Review: Is It the Right Time Tracking System for Your Business?* Available at <https://fitsmallbusiness.com/jibble-review/>
11. Jon Russell. (2012). *E-tailer package tracker AfterShip snags seed funding from Australia’s Business Switch*. Available at <https://thenextweb.com/news/e-tailer-package-tracker-aftership-snags-seed-funding-from-australias-business-switch>
12. Joseph Kaos JR. (2020). *Covid-19: Over 9k cases in M’sia tracked via MySejahtera app*. Available at <https://www.thestar.com.my/news/nation/2020/11/19/covid-19-over-9k-cases-in-m039sia-tracked-via-mysejahtera-app>
13. Blake Chen. (2022). *MySejahtera sale sparks widespread concern as Malaysians fear violation of data privacy*. Available at <https://www.thestar.com.my/news/nation/2022/03/27/mysejahtera-sale-sparks-widespread-concern-as-malaysians-fear-violation-of-data-privacy>
14. Boo Su Lyn. (2022). *Government says not liable for damages over MySejahtera Data use*. Available at <https://codeblue.galencentre.org/2022/04/14/government-says-not-liable-for-damages-over-mysejahtera-data-use/>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

