JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Contact Tracing For Communicable Diseases Using BlockChain

[1]Aadarsh Neeraj Singh, [1] Aditi Garg, [1]Aditi Arya, [1]Aditya Sharma

[2] Girish Kumar B C

[1]CSE Department, JSS Academy of Technical Education, Noida , India

[2] CSE Department, Assistant Professor , JSS Academy of Technical Education, Noida , India

Abstract : At its foundation, contact tracing is a simple and intuitive exercise. If a person tests positive for any Communicable Disease (eg-Covid-19), the testing center or healthcare facility that provided the test notifies the local public health department. The infected person is then contacted by the health department, who requests that they name people they have come into contact with for a specified period of time previous to the test. Following that, the health department contacts such individuals to seek a test. If any of those patients test positive, the procedure is repeated until all of the patients tested negative. Patients who have tested positive for a disease are frequently advised of the length of time they must remain in quarantine and are formally notified after they have "recovered."To maintain the confidentiality of student health records, blockchain technology can anonymize patient records and provide additional levels of security. The name or identity of students cannot be identified by merely browsing or querying the blockchain since test results are linked to a student's public/private key instead of their university ID. Furthermore, because all blockchain entries are cryptographically signed, bad actors cannot change a record without invalidating all subsequent records. Using identity access management software, further controls can be introduced to limit what information an individual can read on the blockchain.

IndexTerms - World Health Organization(WHO),General Data Protection Regulation (GDPR)

I.INTRODUCTION

To combat the spread of communicable diseases, contact tracking has been widely used. It allows for the identification, assessment, and management of those who might have been exposed to the infection or also the confirmed cases which is helpful in stopping the virus from spreading further. A number of Contact tracing methodologies, tools, and solutions on the market today falls short of delivering decentralized, transparent, auditable, traceable, irreversible and also it is quite secure and has many trustworthy features. We are going to describe a blockchain-based decentralized contact tracing solution in this paper. During a pandemic it becomes necessary to engage in a quick response action which becomes easier with the help of contact tracing. The use of blockchain properties like immutability and tamper-proofing to impose trust, accountability, and transparency. On-chain and off-chain data are linked using trusted and registered oracles. The user's medical information is not at risk of being invaded, hacked, or abused because no third parties or centralized systems are involved. The digital medical passport (a Bluetooth ID) of each user is used to register them. The users' whereabouts are updated after a 20-minute delay to safeguard their anonymity. Any Ethereum smart contract conducts transactions on-chain, with emitted events and immutable records. The implemented algorithms, as well as the results of their testing, are thoroughly detailed. To demonstrate the success of the suggested approach, we analyze it using security, cost, and privacy characteristics.

Several elements are needed such as timely accurate tests, a system that enables patient information to be passed from provider, to public health department, to patient contacts and a workforce to call patients and possible contacts. Secured and Traceable Transaction Mechanism: All cryptocurrency transactions are verifiable and traceable in the chain, resulting in safe checkpoints and ownership of faults. As a result, the safety of the patient is ensured.

Motivation : As a result of the COVID-19 epidemic, many meetings and activities have shifted from in-person to virtual implementation. SPS welcomes these developments not just to help its members and Chapters increase their reach, but also to engage and empower current and potential members to interact locally and worldwide.

While the epidemic brought with it a slew of negative consequences, it also changed the computer sector, as people began to seek out ways to communicate online in the same way they did in face-to-face meetings.

The study presents a framework for smart contracts that incorporates both disruptive technologies to improve data management, trust, and automation.

Contributions to Research : We propose a smart contract system based on blockchain that allows for interoperability and trust among participants. Following that, a smart contract layer is presented, which executes multiple smart contracts to facilitate communication between authorities and patients. Finally, a design framework is presented that evaluates itineraries of the patients/users , trace it and alert the users of the infection.

Organization of the Paper: This paper is organized within the following sections. Section II discusses the previous work on smart contact tracing. Section III discusses the proposed framework related to usage of blockchain. Finally, Section IV concludes the paper.

II. PREVIOUS WORK

COVID-19 smartphone applications are being developed by countries all over the world to assist their local health agencies with contact tracing and quick response and communication to their citizens whenever their COVID-19 infection has been verified. The goal is that widespread use of these applications would help to prevent the spread of the coronavirus and allow governments to ease their lockdown restrictions sooner. The majority of these applications employ Bluetooth LE[15] radio waves to monitor and track the proximity of smartphone users to one another, and then analyze the data using either "centralized" or "decentralized" methods. Similarly, a method[16] for limiting COVID-19 outbreaks has been developed, which involves identifying a safe moving distance from a Bluetooth PAN producer.

TraceTogether[9] is a Bluetrace protocol-powered app that uses a technology called Bluetooth low energy (LE) to identify and record any clients in close proximity to the user. The user is obliged to keep the device in an active broadcasting mode under this system, which consumes the user device's battery. All Bluetooth-based contact tracing systems are subject to threats such as snooping, sniffing, and jamming due to the Bluetooth technology's sensitive wireless interface. There is a significant possibility of replay assaults on the contact tracking network, which might result in widespread fear among the population.

Bluetooth LE, Google Apple Contact Tracing[10] takes a similar method. It differs from TraceTogether in terms of user privacy because the service provider does not have access to the user's true identity, ensuring privacy. However, the user is compelled to use their central server for any contact matching and for receiving notifications, raising concerns about potential attacks on user privacy and allowing the reconstruction of the user's profile using server access information. Similarly, the NHS COVID-19 App[12] in the United Kingdom has the danger of exposing user privacy. The health code, on the other hand, is only scanned when passing checkpoints, saving the user energy and consuming no data. Furthermore, because of its extremely central architecture, the coverage may be simply expanded.

III. PROPOSED FRAMEWORK

The proposed framework for the contact tracing includes an interface provided through an app for the user. Downloading the app on devices of all the users and giving it permission to access Bluetooth where Bluetooth will stay ON during the time the user is traveling outside. It will keep track of every device that will come in contact with the user.
Every user will be provided a Bluetooth ID which will be assigned within the app whenever a new user registers on the app. This Bluetooth ID will be stored in the blockchain rather than the actual name of the user to provide more security. The user will be prompted to stay on alert only when there arises a case of positive infection and the user comes in contact with such a person. The smart contract is designed so that it searches for all those contacts which were in contact with the patient within 14 days.

We want to minimize the spread of contagious and communicable illnesses by employing a contact tracing tool which will be hosted over a blockchain. We use the inherent capabilities of blockchain technology to address the contact tracking difficulties. As a consequence, the solution in place safeguards the personal information of its users. It's immutable, transparent, and built with accountability in mind. A decentralized shared ledger with tamper-proof and unchangeable logs that is spread across numerous computers is known as blockchain. It's a linked list where each node has a local copy of the others. In the context of the COVID-19 pandemic, blockchain proves to be a very effective technology that may be used in a variety of applications to prevent the spread of contagious diseases. Contact tracking is only one of the many ways blockchain has shown to be useful in mitigating the pandemic's effects. All participants or users may be transparent, accountable, and trustworthy thanks to the Ethereum blockchain and the programmable logic of smart contracts. Problems relating to user identity theft as well as the problems of Third-party servers were all eliminated with our method. Our method will also solve the problem of centralized storage of data. Users will find the program to be basic and easy to use.

Transparency and trust are enforced through the distributed ledger's immutable logs. Every transaction on the blockchain is signed by the person who initiated it. As a result, each on-chain member is responsible for their actions.

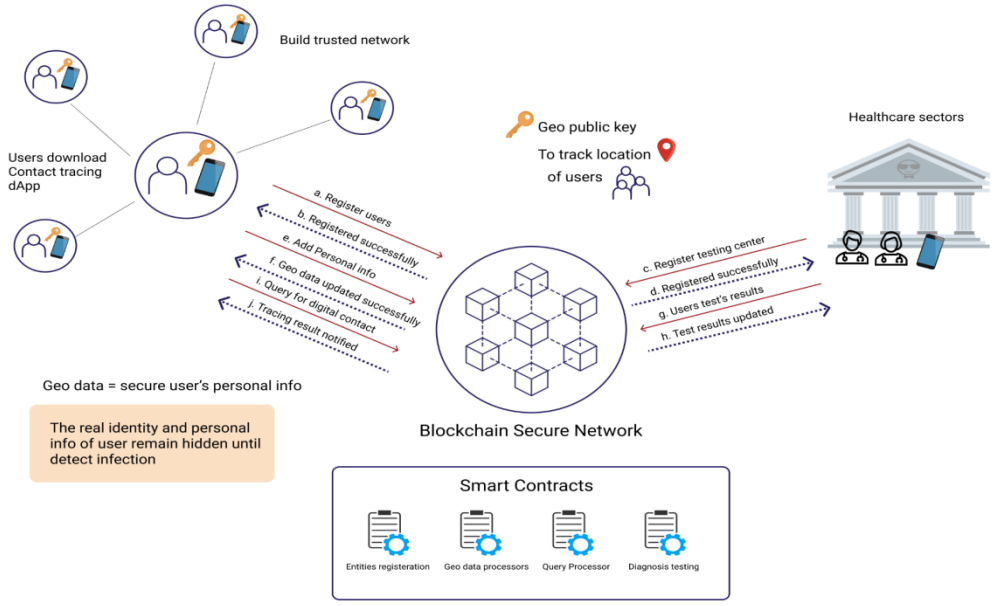

Fig 1.Basic architecture of a contact tracing system

To desensitize the user ID and location information, we suggest using blockchain to connect the user (which can also be the patient) with the authorized solvers. Our technique outperforms recently proposed contact tracking systems in terms of security and privacy, as well as being battery friendly and internationally accessible. Both the server and the mobile phone exhibit feasibility in terms of the necessary resource. Recognizing the obstacles and issues raised above, post-pandemic contact tracing will require improved privacy protection, improved tracing performance, and improved capabilities to combat disinformation. We believe that there should be no trade-off between privacy and tracing efficiency, thus we've created a blockchain-enabled contact tracing system that meets both needs.

We feel that maintaining user anonymity is important for contact tracing and to gain the trust of its user as well. The efficiency of the tracing network in terms of infection prevention, as well as the degree of technology and network coverage, should be appraised. Current decentralized solutions are restricted to a local network and hence do not affect a larger number of users.

It is commonly understood that privacy should be valued from beginning to finish, necessitating a complete privacy solution for contact tracking. The life cycle of shared data should be handled at the user's fingertips. Users of contact tracing will have complete control over sharing and revocation of sharing via key management at any moment. Users' sensitive information must also be shared only inside a trusted and audited cooperation by government entities. With cryptography, the proposed blockchain platform may provide users and agencies with comprehensive credential management capability. The privacy of the user is protected on every stage of the tracing scheme, and the length of data storage is also supposed to be regulated under the General Data Protection Regulation (GDPR) and health agency recommendations, as provided within the World Health Organization's (WHO) recommendation that a tracing cycle last 14 days long at the very least. In brief, the user's privacy will be maintained throughout the generation, sharing, and deposition processes. However, owing to blockchain's technological limitations, the data cannot be erased from the blockchain, instead, it is kept as cipher text, which no one has the key to read beyond the prescribed storage period.
For safe and reliable contact monitoring and inference, the architecture necessitates adherence to specific design criteria. Here we identify the access control needs and also security needs which gives birth to several design principles which are inter related based on the analysis given in Section II:

Security and privacy : This architecture's major goal is to protect people's privacy in compliance with CIA trinity. Here CIA stands for confidentiality, integrity and availability.

Access control and authentication : Only authorized entities will be allowed to use the contact tracing application for communicable diseases, according to the proposed architecture's authentication and access control. This would also assure non-repudiation and accountability because it will be based on secure credentials linked to individuals.

Scalability and flexibility : Bottlenecks and single points of failure should be avoided. This necessitates a distributed design that is scalable across the many entities that make up the contact tracing program. At the same time, the architecture should be made to adapt enough to fulfill the needs of the many organizations involved in contact tracing.

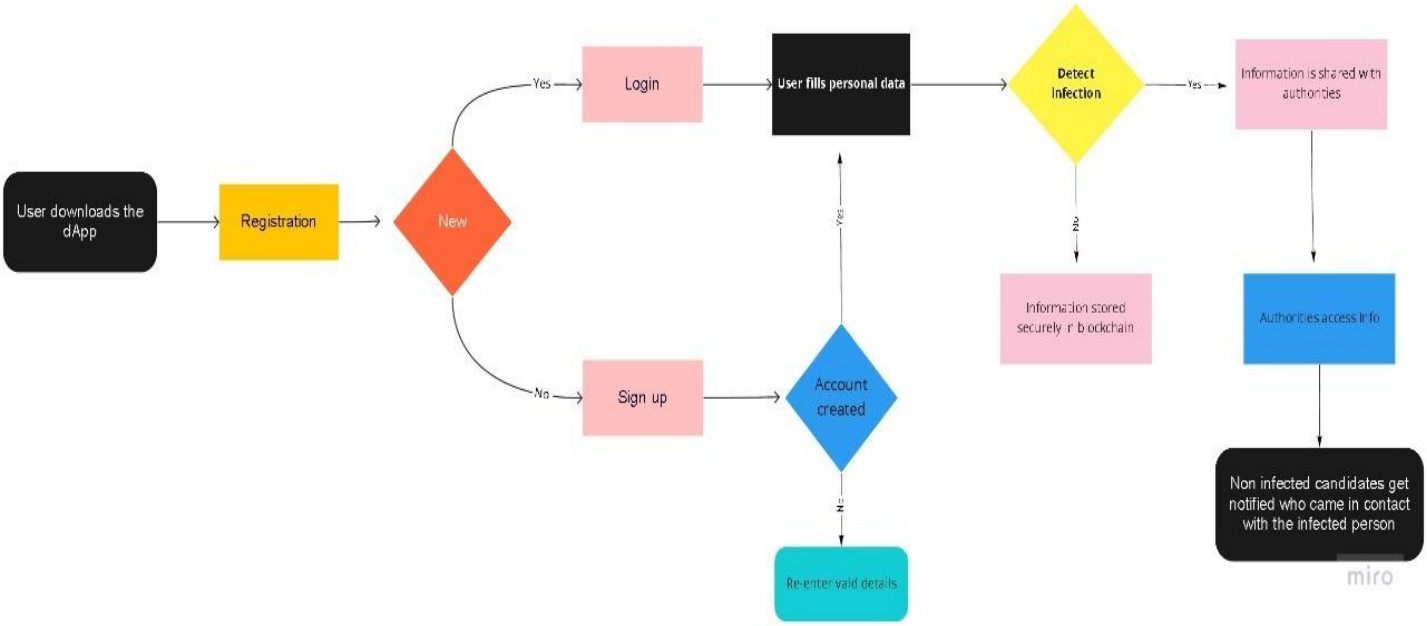

Fig 2.Flowchart of the proposed framework

The application will also provide the user with information of the current cases of the current pandemic's live cases which will be obtained from the internet and updated live. The interface is kept simple so that any person using it finds it easier to access and control which will encourage more people to download and use the app.

Workflow : The user first downloads the app on his mobile phone from the App/Google store. The registration page pops up and the user can register through it. If the user is totally new to the app, he will be required to sign up first and create an account with valid details. If the user has already registered, he can log in directly using his details. If the user has already registered, he can directly log in using his details. After login in/signing up, the user has to fill up the personal details to help the authorities store that information securely for proper detection of the disease. The user has to give their location access to identify their location history and the people that they met during the last 7-14 days.

If the infection is detected, the information is shared with the authorities and the authorities then contact the infected person and ask them to identify people who they have encountered for a defined length of time prior to the test. From there the authorities contact those people to request that they receive a test. If any of those patients tested positive for the disease, then the process is repeated until a set of all negative testing patients are reached.

Often, authorities will advise patients who have tested positive for the disease of the amount of time that they need to remain in quarantine and will give them a formal notification once they are "recovered".

IV. CONCLUSION

This research was done keeping in mind the problems faced by people in the recent outbreak of the CoronaVirus Pandemic. The risk is being faced by the population just waiting to be contacted by a virus and weakening the immune system until the organs themselves reach the point of total failure. Due to the ongoing pandemic many people suffering from ordinary cold fever also feared that they got infected by the covid-19 virus also because of the total lockdown they couldn't get good consultation which could absolve their fears.

The global impact of the coronavirus pandemic, i.e the COVID-19 pandemic on human health has startled the world. Because the pandemic spread so quickly, several countries were unprepared to battle it, resulting in unnecessary deaths. When the hospital system began to show signs of overburdening, nations implemented WHO-recommended lockdown protocols of varying degrees of rigor to prevent the pandemic from spreading throughout the community. A total of 32 countries have launched several smartphone applications that capture data of various types in order to track the people and their movement in lockdown and also monitor their interactions at the community level. This study presents a revolutionary contact tracking architecture that preserves privacy.Contact tracing can help to prevent the spread of infectious and deadly diseases. This facilitates easy identification of infected people from the billions of people on this planet. It will save many lives and support the healthcare sector.

Our decentralized application (dApp) uses Blockchain technology ensuring the safety of people's personal details. It also ensures less battery drainage in an individual mobile phone provided by no Bluetooth consumption. We help healthcare sectors to get patient details accurately and at the right time. This is one of the best mechanisms to share the infected person's data privately with the healthcare department, hence preventing third party risk. The people who come in contact with the infected person immediately get notified about an isolation alert by the health sector.

V. REFERENCES

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

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

3) World health organization et al., "Contact tracing in the context of covid19: interim guidance, 10 may 2020," Tech. Rep., 2020.

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

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

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

7) P. Edemekong, P. Annamaraju, and M. Haydel, "Health insurance portability and accountability act," StatPearls, vol. 72, no. 2, pp. 9–18, 2020.

8) S. Ikeda, "Coronavirus adds an extra layer of challenge to collection and handling of health data under the GDPR," Apr. 2020.

9) J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy, "BlueTrace : A privacy-preserving protocol for community-driven contact tracing across borders," p. 9, 2020

10) Apple Inc. and Google LLC., "Exposure Notification," May 2020

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

12) J. Snow and M. Mallon, "The security behind the NHS contact tracing app," pp. 1–14, 2020

13) A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in AMIA annual symposium proceedings, vol. 2017. American Medical Informatics Association, 2017, p. 650.

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

15) R. Faragher and R. Harle, "Location fingerprinting with bluetooth low energy beacons," IEEE J. Sel. Areas Commun., vol. 33, no. 11, pp. 2418–2428, 2015.

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