



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

 9940 572 462

 6381 907 438

 ijirset@gmail.com

 www.ijirset.com

Blockchain-Enabled Privacy-Preserving Contact Tracing For COVID-19 Pandemic Management

Surekha Vishwanath Magar, Avhad G.T.

Student, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, India

Assistant Professor, Department of Computer Engineering, Vishwabharati Academy's College of Engineering,
Ahmednagar, India

ABSTRACT: In the context of the COVID-19 pandemic, effective contact tracing has emerged as a crucial tool in curbing the spread of the virus. However, conventional contact tracing methods often raise concerns regarding privacy infringement and scalability. This paper explores the potential of blockchain technology to address these challenges and enable large-scale and privacy-preserving contact tracing solutions. By leveraging blockchain's inherent properties of decentralization, transparency, and immutability, a novel framework for contact tracing can be devised. Such a system would allow for the secure and efficient recording of individuals' interactions while preserving their anonymity. Through the use of cryptographic techniques and smart contracts, sensitive health data can be securely managed and accessed only by authorized entities, thereby safeguarding individuals' privacy rights. Furthermore, blockchain-based contact tracing systems offer scalability by enabling seamless data sharing and interoperability among various healthcare institutions and government agencies. This paper presents a comprehensive analysis of the potential benefits, technical considerations, and implementation challenges associated with integrating blockchain technology into contact tracing efforts during the COVID-19 pandemic.

KEYWORDS: COVID-19 pandemic, Contact tracing, Privacy-preserving, Blockchain technology, Decentralization, Transparency, Immutability, Cryptographic techniques, Smart contracts, Interoperability, Implementation challenges.

I. INTRODUCTION

Contact tracing has emerged as a critical strategy in combating the transmission of COVID-19, necessitating efficient and privacy-preserving methods to track and manage interactions among individuals. However, traditional contact tracing approaches often encounter significant hurdles, particularly concerning privacy infringement and scalability. In response to these challenges, this paper investigates the potential of blockchain technology as a foundational framework for developing large-scale and privacy-preserving contact tracing solutions amidst the COVID-19 pandemic. Blockchain's distinctive attributes, including decentralization, transparency, and immutability, offer promising avenues for addressing the shortcomings of conventional contact tracing methods. Leveraging these properties, a novel approach can be formulated to securely record individuals' interactions while safeguarding their anonymity and privacy.

The proposed blockchain-based contact tracing framework capitalizes on the decentralized nature of blockchain networks to establish a tamper-resistant and transparent ledger of individuals' interactions. By employing cryptographic techniques and smart contracts, sensitive health data can be securely managed and accessed only by authorized entities, thereby mitigating concerns related to data privacy and security. Moreover, blockchain's immutability ensures that once recorded, data entries cannot be altered or tampered with, enhancing the reliability and integrity of the contact tracing system. This approach not only addresses privacy concerns but also instills trust and confidence in the collected data, fostering collaboration among stakeholders involved in pandemic response efforts.

Furthermore, the scalability of blockchain technology facilitates seamless data sharing and interoperability among diverse healthcare institutions, government agencies, and other relevant entities involved in contact tracing initiatives. Through standardized protocols and interoperable systems, blockchain-based contact tracing solutions can streamline data exchange and enhance the efficiency of pandemic response efforts on a global scale. This paper aims to provide a comprehensive examination of the potential benefits, technical intricacies, and implementation challenges associated with integrating blockchain technology into contact tracing endeavors during the COVID-19 pandemic.

II. RELATED WORK

In the realm of contact tracing amid the COVID-19 pandemic, traditional methods have encountered notable limitations, particularly concerning privacy and scalability. Existing contact tracing approaches primarily rely on centralized databases or mobile applications that collect and store individuals' sensitive health data. However, such centralized systems raise significant privacy concerns, as they necessitate the disclosure of personal information to a central authority, potentially exposing individuals to surveillance and data breaches. Moreover, the scalability of these conventional methods is often hindered by the fragmented nature of healthcare systems and the lack of interoperability among different institutions and jurisdictions. Consequently, there is a pressing need for alternative solutions that can address these inherent shortcomings while ensuring effective and privacy-preserving contact tracing on a large scale.

Blockchain technology has emerged as a promising candidate to overcome the privacy and scalability challenges associated with conventional contact tracing methods. By leveraging blockchain's decentralized architecture, transactions recorded on the blockchain can be distributed across a network of nodes, eliminating the need for a central authority to manage and control the data. This decentralized approach not only enhances data privacy by minimizing the risk of unauthorized access but also ensures data integrity through cryptographic techniques and consensus mechanisms. Additionally, blockchain-based smart contracts can enable the implementation of privacy-preserving protocols, allowing for the secure sharing and verification of contact tracing data while preserving individuals' anonymity. Despite these potential advantages, the integration of blockchain technology into contact tracing efforts requires careful consideration of various technical and implementation challenges.

One of the primary technical considerations in deploying blockchain-based contact tracing systems is the design of scalable and efficient protocols for data collection, validation, and dissemination. Achieving high throughput and low latency is crucial for real-time contact tracing applications, necessitating the optimization of blockchain consensus algorithms and network performance. Moreover, ensuring the interoperability of blockchain solutions with existing healthcare infrastructure and regulatory frameworks poses significant implementation challenges. Addressing these issues requires interdisciplinary collaboration among healthcare professionals, blockchain experts, policymakers, and privacy advocates to develop robust and standards-compliant solutions that prioritize both privacy and public health objectives.

III. EXISTING METHODOLOGY

In the current landscape of contact tracing amidst the COVID-19 pandemic, several challenges persist within existing methodologies, necessitating a critical examination of their shortcomings. One significant issue lies in the scalability of conventional contact tracing approaches, which often struggle to handle the vast volumes of data generated during widespread outbreaks. Traditional methods reliant on centralized databases encounter bottlenecks when attempting to process and analyze data from numerous sources concurrently. This limitation not only impedes the timely identification of potential virus transmission chains but also hampers the ability to swiftly implement targeted containment measures. Additionally, existing contact tracing mechanisms frequently encounter privacy concerns, particularly regarding the centralized storage and management of sensitive personal information. The aggregation of individual health data within centralized repositories increases the risk of unauthorized access or data breaches, raising legitimate apprehensions among the populace regarding privacy infringement and data misuse.

Moreover, conventional contact tracing methods often lack robust mechanisms for preserving individual privacy rights while simultaneously enabling effective virus containment efforts. The reliance on centralized data repositories exposes individuals to heightened risks of privacy violations, as their personal health information is susceptible to unauthorized access or exploitation. Furthermore, the centralized nature of existing contact tracing systems presents a single point of failure, rendering them vulnerable to cyberattacks or data breaches that could compromise the integrity and confidentiality of stored data. Consequently, the inherent deficiencies in scalability and privacy protection within current contact tracing frameworks underscore the urgent need for innovative solutions capable of addressing these critical shortcomings, particularly in the context of the ongoing COVID-19 pandemic.

IV. PROPOSED SYSTEM WORKING

The proposed system methodology for achieving large-scale and privacy-preserving contact tracing during the COVID-19 pandemic through a blockchain perspective involves several key steps. Firstly, the design and development of the blockchain-based contact tracing system entail the creation of a decentralized network where data pertaining to

individuals' interactions and potential exposure to the virus are recorded securely and anonymously. Smart contracts are employed to enforce predefined rules and automate certain aspects of the contact tracing process, such as notification of potential exposure based on proximity and duration thresholds. Cryptographic techniques, such as zero-knowledge proofs or homomorphic encryption, are utilized to ensure the privacy of individuals' sensitive health information, allowing for the verification of contact events without revealing specific details to unauthorized parties.

Secondly, the implementation of the system involves the integration of blockchain technology with existing contact tracing infrastructure and data sources, such as healthcare databases and mobile applications. Interoperability standards and protocols are established to facilitate seamless data sharing and communication among different stakeholders, including healthcare providers, public health authorities, and individuals. Furthermore, user-friendly interfaces are developed to enable individuals to securely access and manage their own contact tracing data, while maintaining control over who can view or use this information. Continuous monitoring, evaluation, and refinement of the system are conducted to address emerging challenges and ensure compliance with privacy regulations and ethical guidelines. Overall, the proposed methodology leverages blockchain technology to create a robust and scalable framework for contact tracing that prioritizes privacy and confidentiality while effectively mitigating the spread of COVID-19.

V. SYSTEM WORKING

The proposed system operates through a combination of hardware and software components, aiming to facilitate large-scale and privacy-preserving contact tracing during the COVID-19 pandemic. The system utilizes Bluetooth 5.0 technology integrated into smartphones such as Google Pixel 2 and OnePlus 6, along with Bluetooth beacons, to enable proximity-based interactions between individuals. These interactions are recorded and stored securely using blockchain nodes deployed on Alibaba Cloud. The software components, programmed in Java, Kotlin, and C++, ensure efficient communication, data processing, and cryptography operations necessary for contact tracing while preserving user privacy. Additionally, the system incorporates OpenSSL for cryptographic functions and Bitcoinj-core for blockchain implementation, ensuring robust security and decentralized operation.

In terms of performance, the system undergoes rigorous evaluation concerning storage, CPU utilization, power consumption, and latency. The client-side software consumes approximately 120 MB of data memory, while the blockchain system requires around 3.5 GB. The CPU utilization varies across different components, with blockchain mining nodes exhibiting higher usage during block generation. Power consumption is monitored to assess the system's energy efficiency, with Bluetooth signal interactions and computation contributing to varying degrees. Furthermore, the system's latency is evaluated under different conditions, including static and dynamic environments, to understand the impact of factors such as signal propagation, device activity, and network congestion. Overall, these performance assessments provide insights into the system's reliability, scalability, and suitability for real-world deployment in combating the spread of COVID-19.

VI. CONCLUSION

In conclusion, the decentralized blockchain system proposed and implemented in this paper offers a robust solution to address the security, privacy, and operational challenges associated with digital contact tracing during the COVID-19 pandemic. Through the integration of cryptographic techniques and a decentralized blockchain framework, the protocol ensures data security and identity privacy without relying on trusted third parties. The combination of zero-knowledge proof and key escrow effectively safeguards individuals' identity privacy, while the decoupling of cryptographic identity and on-chain proof-of-location commitment enhances transparency while mitigating the risk of tracking. Furthermore, the introduction of a virtual potential field-based incentive allocation method optimizes monitoring coverage, enhancing the system's efficiency. The empirical results demonstrate the effectiveness of the proposed contact tracing and location-proofing technology in real-world scenarios, supported by analyses of power consumption, procedural time delays, and Bluetooth Low Energy (BLE) performance, thereby affirming its suitability for practical implementation in digital contact tracing efforts.

REFERENCES

1. Aruba, Location Service with Aruba Bluetooth Beacons, Jun. 10, 2019. Accessed: Feb. 13, 2020. [Online]. Available: <https://www.arubanetworks.com/products/location-services/aruba-beacons/>
2. J. D. Angrist, S. Caldwell, and J. V. Hall, Uber vs. Taxi: A Driver's Eye View, Tech. report, National Bureau of Economic Research, 2017.

3. S. Bertoni, "Oscar health using misfit wearables to reward fit customers," *Forbes*, December, 2014. [Online] Available: <https://www.forbes.com/sites/stevenbertoni/2014/12/08/oscar-health-using-misfit-wearables-to-reward-fit-customers/#56d693ba93c5>.
4. F. Luca et al., "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, no. 6491, May, 2020.
5. C. Hyunghoon, I. Daphne, and Y. Yun William, "Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs," 2020, arXiv:2003.11511.
6. M. Talasila, R. Curtmola, and C. Borcea, "Link: Location verification through immediate neighbors knowledge," in *Proc. Int. Conf. Mobile Ubiquitous Syst.: Comput., Netw. Services*. Berlin, Germany: Springer, 2010, pp. 210–223.
7. J. Li and X. Guo, "COVID-19 Contact-tracing Apps: A survey on the global deployment and challenges," Mar. 2020, arXiv:2005.03599.
8. Apple Inc., Privacy-Preserving Contact Tracing, Dec. 31, 2019. Accessed: Feb. 20, 2020. [Online]. Available: <https://www.apple.com/covid19/contacttracing>
9. G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using blockchain in a reputation-based model for grouping agents in the Internet of Things," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1231–1243, Nov. 2020.
10. G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using trust and local reputation for group formation in the cloud of things," *Future Gener. Comput. Syst.* vol. 89, pp. 804–815, Dec. 2018.
11. J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.
12. G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "BlockSDN: Blockchain-as-a-Service for software defined networking in smart city applications," *IEEE Netw.* vol. 34, no. 2, pp. 83–91, Mar./ Apr. 2020.
13. G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar, and K. R. Choo, "BloCkEd: Blockchain-based secure data processing framework in edge envisioned V2X environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5850–5863, Jun. 2020.
14. V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K. R. Choo, "Neural-blockchain-based ultrareliable caching for edgeenabled UAV networks," *IEEE Trans. Inf. Theory*, vol. 15, no. 10, pp. 5723–5736, Oct. 2019.
15. J. Wang, C. Jiang, H. Zhang, Y. Ren, K. Chen, and L. Hanzo, "Thirty years of machine learning: The road to pareto-optimal wireless networks," *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 1472–1514, Aug./Sep. 2020



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details