Multi-Modal IoT Remote Health Monitoring Framework With Blockchain, Encryption and ZKP

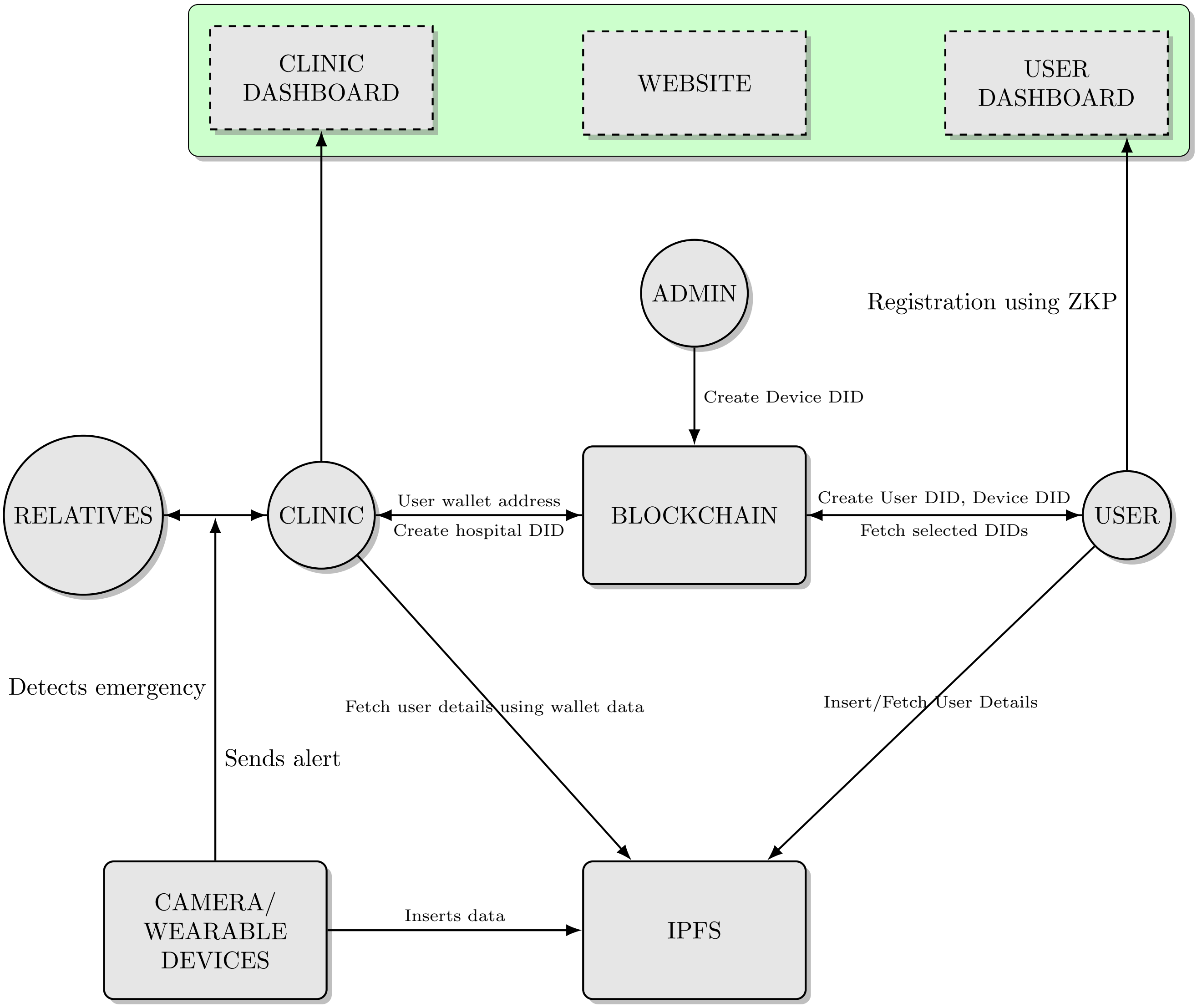
Alosh Denny, Abhinav CV, Fidha Fathima, Harshed Abdulla, Mishal Faisal

Abstract

Taking care of and keeping track of the elderly, Alzheimer's, Parkinson's, etc has been done in clinics, hospitals and therapy centers. Some may prefer it be done from the care of their homes and around their family. But owing to reasons of busy lifestyle or lack of proper care, this is rarely observed and families tend to take the alternative 'clinical' care route as resident patients. Only in the past decade has this paradigm now slowly started to shift to remote/at-home care. This remote care of patients via telecommunications technology, called telemedicine, has been a real game changer in the health industry. Remote patient monitoring (RPM) is a complementary technology to telemedicine that involves collecting, transmitting and analyzing patient health data using wearable devices, sensors and mobile apps. We believe that an IoT-based framework that could help remote patients to keep track of their health and receive necessary at-home support from the clinics without any privacy concerns would hold promise in this scenario. This is the primary motivation for this project.

We propose an IoT based framework that integrates Multimodal Machine Learning, Blockchain and encryption techniques to remotely monitor patients from the care of their homes and securely relay this information between healthcare providers and families. The multi-modal style of this data allows the doctors to diagnose the patient from multiple angles. Modalities such as at-home CCTV feed and smartwatch vitals are analyzed continuously. Encryption allows secure computation on this data without decrypting it. Smartwatch vitals are encrypted and continuously streamed to the servers where algorithms may assess any real-time abnormalities in the state of the patient. Onsite, the video data is processed, analyzed and if any activities such as fall is detected, the incident is alerted to both healthcare providers and near relatives, and finally stored in a distributed manner. Zero knowledge proofs play a vital role in the authentication of users. Blockchain allows the immutability of data and permissionless sharing of data. Overall, the real-time interface reduces the operational overhead of emergency response teams in conventional cases.

Data Flow Diagram



Literature Survey

A work similar in concept by Wang et al proposed a homomorphic encryption with blockchain framework, pAuditChain, to leverage batch auditing of energy bills from IoT smart meters, improving security and privacy[1].

Yuntao Wang et al. proposed a scheme for blockchain based smart grids to share people's energy data securely and perform secure computation on it [2].

Yangsheng Hu Et al., in 2022 proposed the use of Health-zkIDM, a decentralized system using zero-knowledge proof and blockchain technology to enhance transparent and secure identity verification across different health fields[3].A similar work was carried out by Luong and Park, 2022 for an IoT-based blockchain and zk-SNARK framework to preserve privacy, a step forward in data security in the health industry[4].

Firouzi et al and Waheed et al conducted a survey on challenges and opportunities in the potential scope of fusion of IoT, AI and Blockchain of which AI, blockchain, edge-fog-cloud computing have found its way into our work[5], [6].Meanwhile a study conducted by Ismail et al. gives us a comprehensive review of existing blockchain-IoT solutions utilizing Multichain[7].

Samaniego et al. specifically addresses the challenge of choosing hosting platforms for blockchain deployment within IoT, evaluating the suitability of both cloud and fog computing environments which might help us choose a suitable host to deploy our blockchain[8].

References

[1] Qin Wang et al. "Blockchain Enables Your Bill Safer". In: *IEEE Internet of Things Journal* 9.16 (2022), pp. 14162–14171. DOI: 10.1109/JIOT.2020.3016721.

[2] Yuntao Wang et al. "SPDS: A Secure and Auditable Private Data Sharing Scheme for Smart Grid Based on Blockchain". In: *IEEE Transactions on Industrial Informatics* 17.11 (2021), pp. 7688–7699. DOI: 10.1109/TII.2020.3040171.

[3] Tianyu Bai et al. "Health-zkIDM: A Healthcare Identity System Based on Fabric Blockchain and Zero-Knowledge Proof". In: *Sensors* 22.20 (2022). ISSN: 1424-8220. URL: https://www.mdpi.com/1424-8220/22/20/7716.

[4] Duc Anh Luong and Jong Hwan Park. "Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK". In: *IEEE Access* 10 (2022), pp. 55739–55752. DOI: 10.1109/ACCESS.2022.3177211.

[5] Farshad Firouzi et al. "Fusion of IoT, AI, Edge–Fog–Cloud, and Blockchain: Challenges, Solutions, and a Case Study in Healthcare and Medicine". In: *IEEE Internet of Things Journal* 10.5 (2023), pp. 3686–3705. DOI: 10.1109/JIOT.2022.3191881.

[6] Nazar Waheed et al. "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures". In: *ACM Comput. Surv.* 53.6 (Dec. 2020). ISSN: 0360-0300. DOI: 10.1145/3417987. URL: https://doi.org/10.1145/3417987.

[7] Shereen Ismail et al. "A Blockchain-based IoT Security Solution Using Multichain". In: *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. 2023, pp. 1105–1111. DOI: 10.1109/CCWC57344.2023.10099128.

[8] Mayra Samaniego and Ralph Deters. "Blockchain as a Service for IoT". In: Dec. 2016, pp. 433–436. DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.