Blockchain-Based Solution for Secure and Efficient Management of Pet Health Records

Md Facklasur Rahaman, Gifar Arif Haryadi, Paul Angelo Oroceo, Dong-Seong Kim, and Jae-Min Lee
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(facklasur, gieworld, oroceopaul, dskim, and ljmpaul)@kumoh.ac.kr

***Abstract*—The widespread adoption of pets has highlighted the need to replace inefficient paper-based systems with electronic pet health records (PHR), which streamline and secure pet healthcare data. This paper introduces a blockchain-based system for managing pet health records using smart contracts to ensure secure access and information integrity for pet hospitals and owners. We employ a cryptographic scheme to encrypt Pet Health Records (PHR) before uploading them to the InterPlanetary File System (IPFS). The smart contracts have been tested in the Remix Integrated Development Environment (IDE), demonstrating their effectiveness in access control and data security. This integration of blockchain, smart contracts, and cryptographic encryption significantly enhances the security and efficiency of pet health record management.**

***Index Terms*—Blockchain, pet health record (PHR), smart contract, InterPlanetary File System (IPFS).**

I. Introduction

Pets play a vital role in human well-being, offering companionship and reducing stress, but the rising number of pet households worldwide highlights an urgent need for more efficient health record management. Traditional pet healthcare systems often rely on dispersed, paper-based records that can hinder quick access to crucial health information and are susceptible to security breaches and unauthorized access [1]. This fragmentation complicates effective care, especially when immediate medical decisions are necessary. Although some centralized systems exist, they often lead to security breaches and are vulnerable to a single point of failure [2].

To overcome these challenges, the integration of blockchain technology, smart contracts, and encryption offers a transformative solution for pet healthcare records management. Blockchain ensures that records are immutable [3] and accessible exclusively to authorized users [4], significantly enhancing security and transparency. Smart contracts facilitate automated access control, granting specific permissions to pet hospitals as needed, while encryption protects sensitive data from breaches. This approach not only streamlines the management and retrieval of pet health records but also supports seamless care transitions between owners and pet doctors, ensuring that pets receive optimal care promptly and securely.

In this paper, a blockchain-based system for managing pet health records has been presented, utilizing smart contracts and encryption to enhance data security. The system encrypts Pet Health Records (PHR) and stores them on the InterPlanetary File System (IPFS), with access controlled through smart contracts for pet hospitals. A reliable third party manages key generation, ensuring that only authorized pet hospitals can access and decrypt the data, thereby maintaining the integrity and confidentiality of sensitive information.

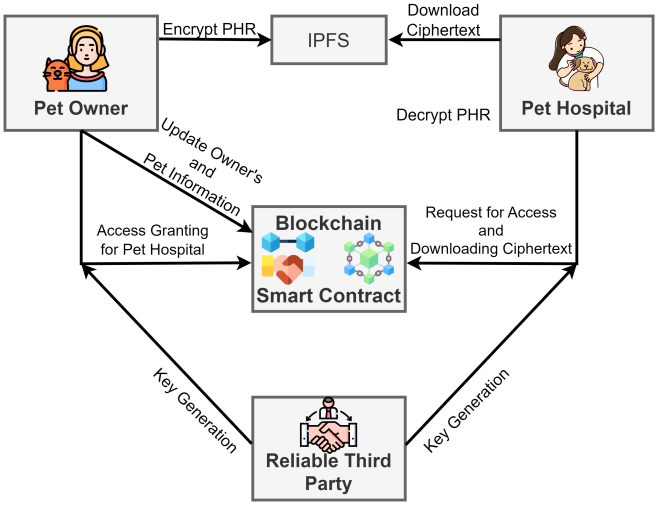

Fig. 1: Proposed System

II. Proposed System

The proposed system for managing pet health records efficiently integrates blockchain technology, the InterPlanetary File System (IPFS), and a reliable third party to ensure confidentiality, data security, and accessibility which is depicted in Fig. 1. In this system, the pet owner begins by updating vital information about the pet—including its name, category, breed, age, sex, blood group, vaccination history, and previous medical history—along with the owner's details into a blockchain network through a smart contract. This comprehensive data collection is critical not only for maintaining detailed health records but also for facilitating any potential future changes in ownership.

Once a pet requires medical attention, the owner grants the pet hospital access to these blockchain-stored records. Access is managed through smart contracts, ensuring that only authorized personnel can view or modify the pet's health information. When access is granted, the hospital can then download the encrypted health records from IPFS, which serves as a decentralized storage solution to enhance data availability and prevent loss.

Key management is handled by a reliable third party, which is entrusted to generate and manage encryption keys and

parameters securely. The encryption and key management process involves several steps.

First, the reliable third party initializes the system by generating a master secret key MK and public parameters PP based on a security parameter Λ and a system attribute set U through

$$\text{Initialize}(\Lambda) \rightarrow (MK, PP).$$

Following this, the third party produces a secret key SK_h and an attribute vector A for the hospital based on its attributes H, using the process

$$\text{GenerateKey}(MK, PP, H) \rightarrow (SK_h, A).$$

The pet owner then encrypts the health record, producing two types of ciphertext: CT_{msg} for the message and CT_{idx} for the keyword index, through the operation

$$\text{Encrypt}(PP, W, m, P) \rightarrow (CT_{msg}, CT_{idx}).$$

These ciphertexts are subsequently stored on IPFS, with the URI of CT_{idx} uploaded to blockchain to ensure integrity and traceability. When the hospital needs to access the records, it generates a search trapdoor TD using its secret key SK_h and the required keyword set W, and sends it to the blockchain. The blockchain system verifies the hospital's attributes and matches the keyword set. If validated, it provides the URI to download CT_{msg}. The hospital uses the URI to access the ciphertext from IPFS and decrypts it using the intermediate parameter $Param$ along with their secret key SK_h to access the health record, represented by the decryption operation

$$\text{Decrypt}(CT_{msg}, Param, SK_h) \rightarrow m.$$

Post-treatment, the pet owner updates the pet's health records, re-encrypts them, and uploads the new ciphertext to IPFS. This method ensures that each piece of data entered into the system remains secure, up-to-date, and readily accessible to authorized entities while being protected against unauthorized access. This system enhances pet healthcare by efficiently securing and streamlining the exchange of health records between owners and providers

III. Implementation and Performance Analysis

This section details the implementation of the system using the Remix Integrated Development Environment (IDE) to deploy smart contracts written in Solidity. These smart contracts are crucial for managing pet health records, enabling pet owners to securely update essential information and grant specific hospitals access as needed. Fig. 2 and Fig. 3 demonstrate the successful upload of pet information and the granting of access to hospitals, respectively.

After a pet receives treatment, the owner encrypts and uploads the updated health records to the IPFS, which generates a unique URI for these records. This URI is recorded on the blockchain via the smart contract, ensuring the data remains secure and traceable. Authorized hospitals can then access and download the ciphertext, and decrypt this data using the URI, facilitating accurate and effective treatment.

Fig. 2: Updating Pet Information by Pet Owner

Fig. 3: Pet Hospital's Access Granting by Pet Owner

IV. Conclusion and Future Work

In conclusion, the proposed system detailed in this paper significantly enhances the management and security of pet health records. By employing smart contracts and advanced encryption within a decentralized architecture, the system ensures that only authorized parties can access sensitive pet health information, thereby maintaining data integrity and preventing unauthorized access. Future work will focus on further integrating machine learning algorithms to predict health issues based on historical data, which will further refine the care process and improve outcomes for pets.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government(MSIT) (IITP-2024-2020-0-01612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 33%) and by project for Industry-University-Research Institute platform cooperation R&D funded Korea Ministry of SMEs and Startups in 2022(S3310783, 34%)

References

[1] A. B. Siddik, P. Das, A. Islam, S. Fahim, M. F. Rahman, E. Hasan, M. F. T. Nasim, and M. M. Islam, "Real-time patient monitoring system to reduce medical error with the help of database system," in *2022 4th International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE)*. IEEE, 2022, pp. 1–4.

[2] M. F. Rahaman, M. Golam, M. A. P. Putra, G. A. Haryadi, D.-S. Kim, and J.-M. Lee, "Blockchain empowered secure medical appointment for the patients using smart contract," , pp. 868–869, 2023.

[3] I. S. Igboanusi, K. P. Dirgantoro, J.-M. Lee, and D.-S. Kim, "Blockchain side implementation of pure wallet (pw): An offline transaction architecture," *ICT Express*, vol. 7, no. 3, pp. 327–334, 2021.

[4] M. F. Rahaman, M. Golam, E. A. Tuli, D.-S. Kim, and J.-M. Lee, "Decentralized metaverse governance using blockchain with attribute-based identity," , pp. 320–321, 2024.