AMERICAN ACADEMIC PUBLISHER

International journal of IoT (ISSN: 2692-5184)

Volume 05, Issue 02, 2025, pages 15-22
Published Date: - 01-08-2025

Decentralized and Secure IoT for Plant Disease Detection: A Web3.0 and Blockchain Enhanced Framework

Dr. Nurul Aisyah Binti Ismail
Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia

ABSTRACT

Plant diseases pose a significant threat to global food security, leading to substantial crop losses and economic instability. The emergence of Internet of Things (IoT) technologies offers promising avenues for early and precise plant disease detection through real-time data collection. However, traditional centralized IoT architectures are susceptible to critical vulnerabilities, including data integrity breaches, security risks, privacy concerns, and single points of failure. This article proposes an enhanced framework for IoT-based plant disease detection systems by integrating blockchain technology and Web3.0 principles. Drawing insights from secure data management in other critical sectors like healthcare [1, 4, 13, 14, 15, 16, 19, 20, 28, 30], this framework leverages blockchain's decentralized, immutable ledger for secure and verifiable data storage, and Web3.0's emphasis on data ownership and decentralized applications (dApps) for enhanced user control and transparency. The proposed integration aims to establish a robust, trustworthy, and efficient ecosystem for agricultural data, facilitating more accurate disease diagnosis, enabling secure data sharing among stakeholders, and fostering a new paradigm of decentralized, intelligent agriculture.

KEYWORDS

Decentralized IoT, plant disease detection, Web3.0, blockchain, smart agriculture, secure data sharing, precision farming, IoT security, distributed ledger, agricultural technology.

INTRODUCTION

Agriculture, as the backbone of global food supply, faces persistent challenges, among which plant diseases stand out as a primary cause of crop loss, impacting yield, quality, and ultimately, farmer livelihoods and food security worldwide. Traditional methods of plant disease detection, often relying on manual inspection or laboratory analysis, are time-consuming, resource-intensive, and frequently lead to delayed interventions, resulting in widespread crop damage [23]. The advent of the Internet of Things (IoT) has revolutionized numerous industries, and its application in agriculture, commonly known as "smart agriculture," holds immense potential for transforming disease detection. IoT devices, such as networked sensors, cameras, and drones, can collect real-time data on environmental conditions (e.g., temperature, humidity), soil parameters, and plant health indicators (e.g., spectral imaging, leaf color changes) directly from fields [31]. This continuous data stream enables early anomaly detection and informed decision-making, promising to mitigate the impact of diseases significantly.

Despite the transformative potential of IoT in agriculture, its widespread deployment is hindered by inherent architectural limitations. Conventional IoT systems typically operate on centralized cloud platforms, which, while offering scalability, introduce critical vulnerabilities. These include single points of failure, susceptibility to cyberattacks, data integrity issues, and privacy concerns regarding sensitive agricultural data [3, 5, 6]. For instance, the tampering or unauthorized alteration of sensor data could lead to misdiagnosis, inappropriate pesticide use, or even deliberate sabotage, with severe economic and environmental repercussions. Furthermore, farmers often lack complete control over their generated data, which resides with third-party cloud providers, raising questions of data ownership and monetization. Similar challenges regarding data security, privacy, and integrity have been extensively studied and addressed in other data-sensitive domains like healthcare, where the secure management of electronic health records (EHRs) is paramount [1, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 20, 23, 28, 30, 32].

To overcome these centralized vulnerabilities, blockchain technology has emerged as a promising solution. Blockchain, a decentralized and immutable distributed ledger technology, offers unparalleled capabilities for ensuring data integrity, transparency, and security without reliance on a central authority [17, 18]. Its cryptographic foundations and consensus mechanisms make it highly resistant to tampering and unauthorized access, making it an ideal candidate for securing IoT data streams. Moreover, the evolution towards Web3.0, often termed the "decentralized web," extends these principles beyond just data storage to encompass decentralized applications (dApps) and user-centric data ownership [26, 33]. Web3.0 aims to create an internet where users have more control over their data and can interact peer-to-peer without intermediaries, fostering a more transparent and equitable digital ecosystem.

This article aims to propose and detail an enhanced framework that integrates IoT devices, blockchain technology, and Web3.0 principles for a robust and secure plant disease detection system. By synergizing these advanced technologies, we seek to address the current limitations of centralized IoT architectures in agriculture, providing a foundation for trusted data, secure transactions, and decentralized applications. This conceptual framework draws heavily from lessons learned in securing sensitive data in healthcare and other industries, extrapolating their applicability to the unique demands of smart agriculture. The subsequent sections will elaborate on the existing challenges, the foundational roles of blockchain and Web3.0, the proposed architectural design, its expected benefits, and the implications for the future of intelligent agriculture.

METHODS

This section delineates the methodological approach for developing an enhanced framework for IoT-based plant disease detection systems by integrating blockchain and Web3.0. As this is a conceptual framework study, the "materials" primarily consist of existing technological principles and empirical findings from related domains, particularly healthcare, where blockchain and secure data management have seen significant research and application. The "methods" involve a structured synthesis of these components to propose a novel architecture.

1. Overview of Current IoT-based Plant Disease Detection Systems

Contemporary IoT-based plant disease detection systems typically comprise several core components:

- Sensor Layer: A network of diverse sensors (e.g., temperature, humidity, soil moisture, pH, spectral cameras, image sensors) deployed in agricultural fields to collect real-time data on plant health and environmental conditions.
- Gateway Layer: Local gateways aggregate data from various sensors, perform preliminary data filtering or aggregation, and then transmit this data.
- Cloud Layer: A centralized cloud infrastructure is commonly used for storing, processing, and analyzing the vast amounts of collected IoT data. Machine learning algorithms, often deep learning models, are trained on this data to identify patterns indicative of plant diseases [35].
- Application Layer: User-facing applications (e.g., mobile apps, web dashboards) allow farmers and agricultural experts to visualize data, receive disease alerts, and access diagnostic reports.

These systems aim to provide early warnings and actionable insights, enabling precise and timely interventions to manage plant diseases [23].

2. Challenges in Traditional Centralized IoT for Agriculture

Despite their utility, traditional centralized IoT architectures for plant disease detection face several critical challenges, many of which mirror those encountered in other sensitive data domains:

- Security Vulnerabilities: Centralized servers are attractive targets for cyberattacks (e.g., DDoS, data breaches, ransomware), which could compromise the entire system [3, 27]. In agriculture, this could lead to false disease alerts, manipulation of crop data, or even disruption of automated farming processes.
- Data Integrity and Verifiability: The lack of transparent and immutable records makes it difficult to verify the authenticity and integrity of sensor data. Data could be tampered with by malicious actors or even accidentally corrupted, leading to incorrect disease diagnoses and suboptimal management decisions [5, 6].
- Privacy Concerns: Sensitive farm data, including crop yields, soil conditions, and specific disease outbreaks, is often stored and managed by third-party cloud providers. Farmers may lack control over how their data is used, shared, or monetized, raising significant privacy concerns [25]. This parallels the extensive privacy challenges faced by electronic health record (EHR) systems [6, 7, 8, 10, 11, 12, 23, 28, 30, 32].
- Single Point of Failure: A centralized architecture is inherently prone to a single point of failure. If the central server or cloud platform experiences an outage or attack, the entire system can become inoperable, disrupting critical disease monitoring and detection capabilities.
- Interoperability and Data Silos: Different IoT platforms and agricultural systems often operate in silos, making seamless data sharing and interoperability challenging. This hinders collaborative efforts in disease surveillance and research across diverse farming entities.

3. Blockchain as a Foundation for Trust and Security

Blockchain technology provides a robust solution to address many of the aforementioned challenges by offering a decentralized, immutable, and transparent ledger system [17, 18]. Its core principles include:

- Decentralization: Data is distributed across a network of nodes, eliminating single points of failure and reducing reliance on central authorities.
- Immutability: Once a record (transaction block) is added to the blockchain, it cannot be altered or deleted, ensuring the integrity and verifiability of all stored data [15]. This is crucial for maintaining trustworthy agricultural records.
- Consensus Mechanisms: All participating nodes must agree on the validity of new data before it is added to the ledger, preventing malicious tampering.
- Cryptography: Data is cryptographically secured, ensuring privacy and authentication [21, 22]. Access control can be managed through cryptographic keys and smart contracts [7, 8, 11, 12, 14, 20, 23, 28, 30].

The application of blockchain in securing sensitive data, particularly in healthcare, provides a strong precedent for its use in agriculture. Blockchain has been successfully proposed and implemented for privacy-preserving healthcare architectures [1, 4], secure EHR sharing [7, 8, 10, 11, 12, 14, 15, 16, 19, 20, 23, 28, 30], medical image retrieval [23, 24], and even lightweight blockchain solutions for healthcare IoT [13, 36]. These principles are directly transferable to agricultural data, where data security and integrity are equally vital.

4. Web3.0 Integration for Decentralized Governance and Data Ownership

Web3.0 represents the next generation of the internet, envisioned as a decentralized, semantic, and user-centric web. It leverages blockchain technology to empower users with greater control over their data and enables true peer-to-peer interactions without intermediaries. Key aspects of Web3.0 relevant to this framework include:

- Decentralized Applications (dApps): Applications built on blockchain networks, offering transparency, censorship resistance, and eliminating central control [26]. For plant disease detection, dApps can serve as interfaces for farmers, researchers, and consumers.

- Self-Sovereign Identity: Users (e.g., farmers) retain control over their digital identities and data, deciding precisely who can access what information and under what conditions [25].
- Tokenization and Incentives: Web3.0 often incorporates cryptocurrencies or utility tokens to incentivize participation, reward data sharing, or facilitate payments for services [26, 33]. This could enable farmers to monetize their valuable agricultural data.
- Smart Contracts: Self-executing contracts stored on the blockchain, automatically enforcing agreements when predefined conditions are met. This allows for automated alerts, data sharing agreements, and payments without intermediaries [24, 33].

Integrating Web3.0 ensures that the entire ecosystem for plant disease detection is not just secure at the data layer (blockchain) but also decentralized at the application and governance layers, empowering stakeholders directly.

5. Proposed Framework Architecture

The proposed enhanced framework integrates IoT, blockchain, and Web3.0 into a multi-layered architecture for secure and efficient plant disease detection:

1. IoT Device Layer:
   - o Sensors: Collect real-time data on plant health (e.g., leaf color changes, spectral signatures, growth patterns), environmental factors (temperature, humidity, light), and soil conditions (moisture, pH, nutrients).
   - o Edge Computing Units: Locally process raw sensor data, filter noise, aggregate relevant information, and perform initial anomaly detection. This reduces the data load on the blockchain and minimizes latency [31].
   - o IoT Gateways: Securely connect edge devices to the blockchain network, ensuring authenticated and encrypted data transmission.
2. Blockchain Layer (Consortium/Private Blockchain):
   - o Data Storage: Instead of storing raw, large image/video data directly on-chain, only metadata, hashes of the raw data, and critical sensor readings (e.g., temperature, humidity, timestamps, disease flags) are stored on the immutable ledger. Raw data can be stored off-chain on decentralized storage solutions like IPFS, with its hash stored on the blockchain for integrity verification.
   - o Smart Contracts:
     - ▪ Data Ingestion Contracts: Define rules for how IoT data is formatted, validated, and recorded on the blockchain.
     - ▪ Access Control Contracts: Manage permissions for data access by different stakeholders (e.g., farmers, researchers, agricultural extension services, AI models), ensuring privacy and controlled sharing.
     - ▪ Alert & Notification Contracts: Trigger automated alerts to farmers or specific authorities when disease indicators are detected by AI models.
     - ▪ Data Sharing/Monetization Contracts: Facilitate agreements for sharing agricultural data with researchers or businesses, potentially with associated micro-payments for farmers.
   - o Consensus Mechanism: A suitable consensus mechanism (e.g., Proof of Authority, Delegated Proof of Stake) would be chosen for efficiency and scalability in an agricultural consortium setting.
   - o Ledger: Maintains an immutable history of all recorded sensor data, disease events, and related transactions.
3. Web3.0 Application Layer (dApps):
   - o Farmer Dashboard dApp: Provides farmers with a secure, transparent interface to view their plant health data, receive real-time disease alerts, manage data access permissions, and potentially participate in data marketplaces.
   - o Expert/Researcher dApp: Allows authorized agricultural experts and researchers to access aggregated,

anonymized, or specific farm data for analysis, research, and developing improved disease models.

o Marketplace dApp: A decentralized marketplace for agricultural data or specialized disease diagnostic services, where farmers can monetize their data or subscribe to advanced analytical tools.

o AI/ML Integration: dApps interact with off-chain AI/ML models. The integrity of the AI model updates or inference results can be cryptographically linked to the blockchain.

4. AI/ML Processing Layer (Off-Chain with On-Chain Verification):

o Disease Detection Models: Machine learning models (e.g., Convolutional Neural Networks for image analysis, recurrent neural networks for time-series data) analyze the data to detect disease patterns. These models are often trained on secure, blockchain-verified datasets [35].

o Model Integrity: Hashes of trained models and their performance metrics can be stored on the blockchain to ensure transparency and verifiability of the AI components.

o Edge AI: Integration of AI directly on edge devices to enable faster, localized disease detection without constant cloud communication, linking to the blockchain for secure record-keeping [31].

6. Key Technologies and Tools

The framework would leverage:

- Blockchain Platforms: Ethereum, Hyperledger Fabric, or custom consortium blockchains for smart contract functionality and distributed ledger.
- Decentralized Storage: IPFS (InterPlanetary File System) for storing large raw image/video data files, with their content hashes secured on-chain.
- Smart Contract Languages: Solidity (for Ethereum-compatible chains) or specialized languages for other platforms.
- IoT Protocols: MQTT, CoAP for efficient device communication.
- AI/ML Frameworks: TensorFlow, PyTorch for developing and deploying disease detection models.

RESULTS

Given that this article proposes a conceptual framework, the "results" section outlines the expected benefits and capabilities of implementing a blockchain and Web3.0 enhanced IoT-based plant disease detection system, derived from the theoretical integration of these technologies and existing applications in related fields, particularly healthcare. These represent the anticipated improvements over traditional centralized IoT models.

The primary outcome of this enhanced framework is the establishment of a highly secure, transparent, and decentralized ecosystem for agricultural data, addressing critical vulnerabilities present in current systems.

1. Enhanced Data Integrity and Security

- Immutable and Verifiable Records: By utilizing blockchain, all sensor data related to plant health and environmental conditions, along with disease detection events, are recorded on an immutable ledger. This ensures that once data is committed, it cannot be tampered with, providing a verifiable audit trail [15, 17, 18]. This significantly reduces the risk of malicious data alteration or accidental corruption, a common concern in centralized systems.
- Reduced Cyberattack Surface: Decentralization inherent to blockchain eliminates single points of failure, making the system more resilient to targeted cyberattacks such as DDoS or ransomware that could cripple a centralized cloud infrastructure [27]. Security principles applied to EHRs [7, 8, 11, 12, 14, 20] directly translate to securing agricultural data.
- Cryptographic Security: The use of cryptographic techniques for data authentication and access control [21, 22] ensures that only authorized entities can access or write data, bolstering the overall security posture of the agricultural IoT network [28, 30, 36].

2. Decentralized Data Ownership and Control

- Farmer Empowerment: Web3.0 principles enable farmers to regain control and ownership of their generated data. Through self-sovereign identity and smart contracts, farmers can define granular permissions for who can access their data and for what purpose [25]. This shift from third-party custody to user ownership enhances privacy and trust.
- Transparency and Auditability: The decentralized and transparent nature of blockchain ensures that all data interactions and processing activities are auditable by authorized participants. This fosters greater trust among stakeholders (farmers, researchers, insurers, consumers) regarding the provenance and reliability of agricultural data.

3. Improved Efficiency and Automation via Smart Contracts

- Automated Disease Alerts and Management: Smart contracts can automate crucial processes. For instance, once an AI model detects a high probability of a specific plant disease from blockchain-verified data, a smart contract can automatically trigger alerts to the farmer, initiate recommended pesticide orders, or even inform agricultural extension services, streamlining disease management workflows [24, 33].
- Secure Data Sharing and Monetization: Smart contracts can facilitate secure, conditional data sharing agreements. Farmers could choose to share anonymized or aggregated data with researchers or seed companies in exchange for tokenized incentives, creating new economic models for agricultural data without compromising individual farm privacy. This incentivizes data contribution for collective benefit [26].

4. Enhanced Accuracy and Reliability of Disease Detection

- Trusted Data for AI/ML Models: AI/ML models used for disease detection will be trained and operate on data whose integrity and authenticity are guaranteed by the blockchain. This significantly improves the reliability and accuracy of disease diagnoses, as the models are fed with uncompromised, verifiable information [35].
- Traceability of Diagnostics: Every step from sensor data collection to AI model inference and final disease alert can be immutably recorded on the blockchain, providing full traceability for diagnostic decisions. This is vital for accountability and for resolving disputes or re-evaluating past diagnoses.

5. Scalability and Interoperability Potential

- Lightweight Blockchain Implementation: Utilizing lightweight blockchain solutions or specific consensus mechanisms can help manage the scalability challenges associated with large volumes of IoT data, particularly at the edge [13, 36]. Edge AI further processes data locally, reducing on-chain load [31].
- Interoperable Ecosystem: The open and standardized nature of blockchain and Web3.0 technologies inherently supports interoperability, allowing different agricultural IoT devices, platforms, and stakeholders to seamlessly share and interact with data, breaking down existing data silos [32, 34].

In essence, the proposed framework offers a transformative leap for plant disease detection systems, moving beyond basic automation to establish a secure, transparent, and user-controlled digital foundation for smart agriculture, drawing valuable lessons from parallel developments in healthcare data security.

DISCUSSION

The proposed framework, integrating IoT, blockchain, and Web3.0 for plant disease detection, represents a significant advancement over traditional centralized approaches. The discussion here delves into the implications of these anticipated "results," highlighting how the enhanced framework addresses existing pain points, its broader significance for smart agriculture, and the challenges that must be overcome for its successful implementation.

The core strength of this integrated framework lies in its fundamental shift from a centralized, trust-requiring model to a decentralized, trustless-by-design paradigm. The immutability and transparency provided by blockchain technology are game-changers for agricultural data integrity. In traditional systems, a single point of compromise could lead to widespread data manipulation, with severe consequences for crop health and economic viability. By contrast, an attacker would need to control a majority of the network nodes to alter data on a blockchain, a task that becomes computationally prohibitive for a well-designed network [27]. This inherent security and verifiability of data are critical for building reliable AI/ML models for disease detection [35], as the output quality is directly dependent on the input data's trustworthiness. The parallels with securing electronic health records [1, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 20, 23, 24, 28, 30, 32], where data integrity and privacy are non-negotiable, are particularly instructive for agricultural applications.

Web3.0's contribution moves beyond mere data security to empower the primary data generators: the farmers. In current models, farmers often relinquish control of their data to cloud service providers, leading to concerns about privacy, data misuse, and lack of monetization opportunities. The Web3.0 layer, with its dApps and self-sovereign identity principles [25], grants farmers unprecedented control over their agricultural data. They can decide precisely who accesses their data, for what purpose, and even potentially monetize it through tokenized incentives for sharing. This fosters a more equitable data economy in agriculture, encouraging greater participation and data contribution, which in turn feeds richer datasets for AI development and disease research. The implementation of smart contracts further automates processes, reducing administrative overhead and enabling real-time, trustless interactions between various stakeholders in the agricultural value chain [24, 33]. For example, automated payments for successful disease detection services or validated healthy crop data could revolutionize agricultural finance and insurance.

However, the path to widespread adoption of such a framework is not without its challenges.

- Scalability: While blockchain offers security, achieving high transaction throughput for real-time, large-scale IoT data from thousands of farms remains a significant hurdle. Lightweight blockchain solutions and off-chain data storage (e.g., IPFS) coupled with edge computing [13, 31, 36] are essential, but managing synchronization and data consistency between on-chain metadata and off-chain raw data needs robust design.
- Energy Consumption: Certain blockchain consensus mechanisms (e.g., Proof of Work) are energy-intensive. Selecting more energy-efficient alternatives (e.g., Proof of Stake, consortium-based Proof of Authority) is crucial for a sustainable agricultural application.
- Cost of Implementation: Developing and maintaining blockchain and Web3.0 infrastructure can be resource-intensive, requiring specialized technical expertise. The cost-benefit analysis for individual farmers or smaller agricultural cooperatives needs careful consideration.
- Interoperability Standards: While Web3.0 promises interoperability, achieving seamless integration across diverse IoT devices, blockchain platforms, and existing agricultural management systems requires the development and adoption of robust industry-wide standards [32, 34].
- Regulatory and Legal Frameworks: The decentralized nature of Web3.0 and blockchain may present challenges for existing regulatory frameworks, particularly concerning data governance, liability, and dispute resolution in a trustless environment. Clear legal guidelines will be necessary to facilitate broad adoption.
- User Adoption and Education: Farmers, many of whom may not be tech-savvy, will require significant education and user-friendly interfaces to interact with complex dApps and manage their decentralized data.

Future work should focus on empirical validation of this conceptual framework through pilot projects in diverse agricultural settings. This includes developing prototypes of the proposed layered architecture, conducting performance evaluations regarding scalability and latency, and rigorously testing the security mechanisms. Research into user-centric dApp design tailored for farmers, exploring novel tokenomics models for agricultural data, and addressing the regulatory implications of decentralized agricultural data ecosystems are also critical next steps. Ultimately, this enhanced framework promises not just better plant disease detection but a more resilient, transparent, and equitable future for smart agriculture.

CONCLUSION

The global agricultural sector stands to gain immensely from the ongoing digital transformation, particularly in mitigating the devastating impact of plant diseases through IoT-based detection systems. This article has proposed a novel and enhanced framework that integrates the Internet of Things with blockchain technology and Web3.0 principles to address the inherent security, privacy, and data integrity challenges of traditional centralized IoT architectures. By building upon the robust foundations of decentralized, immutable ledgers and user-centric data ownership, this framework offers a paradigm shift for agricultural data management.

The anticipated benefits are substantial: unparalleled data integrity and security through cryptographic immutability, empowerment of farmers through decentralized data ownership and control, enhanced operational efficiency and automation via smart contracts, and significantly improved accuracy and reliability of plant disease detection through trusted data feeds to AI/ML models. While challenges such as scalability, energy consumption, and regulatory complexities need careful navigation, the framework provides a clear path towards a more resilient, transparent, and equitable smart agriculture ecosystem. This integration of cutting-edge technologies not only promises to safeguard crops more effectively but also to redefine the economic landscape of agricultural data, paving the way for a truly intelligent and sustainable future for food production worldwide.

REFERENCES

1. Koosha Mohammad Hossein, et al., BCHealth: a novel blockchain-based privacy-preserving architecture for IoT healthcare applications, Comput. Commun, vol. 180, pp. 31-47 (2021).
2. Aparna Kumari, et al., Fog computing for Healthcare 4.0 environment: opportunities and challenges, Comput. Electr. Eng. 72 (2018) 1–13.
3. Alexander McLeod, Diane Dolezel, Cyber-analytics: modeling factors associated with healthcare data breaches, Decis. Support Syst. 108 (2018) 57–68.
4. Hussien, Mansur Hassan, et al., Blockchain technology in the healthcare industry: trends and opportunities, J. Ind. Inf. Integrat. 22 (2021), 100217.
5. B. Shickel, P.J. Tighe, A. Bihorac, P. Rashidi, Deep EHR: a survey of recent advances in deep learning techniques for electronic health record (EHR) analysis, in: IEEE Journal of Biomedical and Health Informatics, vol. 22, Sept. 2018, pp. 1589–1604, https://doi.org/10.1109/JBHI.2017.2767063, 5.
6. Z. Ying, L. Wei, Q. Li, X. Liu, J. Cui, A lightweight policy preserving EHR sharing scheme in the cloud, in: IEEE Access, vol. 6, 2018, pp. 53698–53708, https://doi.org/10.1109/ACCESS.2018.2871170.
7. X. Yang, T. Li, W. Xi, A. Chen, C. Wang, A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud, IEEE Access 8 (2020) 170713–170731, https://doi.org/10.1109/ACCESS.2020.3025060.
8. Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain, in: IEEE Access, vol. 7, 2019, pp. 136704–136719, https://doi.org/10.1109/ACCESS.2019.2943153.
9. Y. Zhuang, L.R. Sheets, Y.-W. Chen, Z.-Y. Shae, J.J.P. Tsai, C.-R. Shyu, A patientcentric health information exchange framework using blockchain technology, IEEE J. Biomed. Health Inf.cs 24 (8) (Aug. 2020) 2169– 2176, https://doi.org/10.1109/JBHI.2020.2993072.
10. Y. Yang, et al., Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers, IEEE Access 6 (2018) 46949–46961, https://doi.org/10.1109/ACCESS.2018.2865535.