Ushus-Journal of Business Management
2024, Vol. 23, No. 3, *1-17*
ISSN 0975-3311 | https://doi.org/10.12725/ujbm.68.1

A Blockchain Framework for Securing Ambient Health Care Systems

Anita Jasmine R*, M Ramla† and M Ramesh‡

Abstract

In the world of wearable technology, smart homes and cities, innovation continues to thrive. Computing is pervasive, and ambient computing is ubiquitous integration of computer into the background of everyday environments and situations. With contact-free sensors and wearables that require interaction, ambient computing is increasingly finding use in the healthcare industry. This ubiquitous nature of ambient computing raises concerns on privacy, confidentiality, data protection, informed consent and fairness. The continuous collection of massive health care data not only unobtrusively monitors the health condition of the patient and trajectory for high quality care but also has a detrimental effect in terms of privacy, bias and fairness. This paper discusses the main ethical issues in ambient health care systems and explores the blockchain based solutions for ambient health care systems emphasizing on patient dignity and autonomy. Furthermore, a secure EHR access using RBAC and Cryptographic techniques for the responsible development and use of ambient health care systems is proposed in this research work.

Keywords: Ambient Computing, AIoT, Pervasive Computing, Ethics, Responsible AI, AmI

* SRM University, SRM Nagar, Kattankulathur, Chengalpattu District, Tamil Nadu, India; anitajar1@srmist.edu.in

† Department of Computer Applications, Faculty of Sciences and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu District, Tamil Nadu, India; anitajar1@srmist.edu.in

‡ Department of Computer Applications, Faculty of Sciences and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu District, Tamil Nadu, India; anitajar1@srmist.edu.in

1. Introduction

1.1. Background

As defined by World Health Organization, "Health is defined as the state of complete physical, mental and social well-being and not merely the absence of disease or infirmity". Health is the prime asset and without complete health the full potential and involvement is missed in the mundane tasks. Recent advancements in Science and technology have contributed a major role in the health domain. End-to-end solutions for ambient supported living are now a reality due to notable advancements in computer, communications, and sensor downsizing, as well as the increased usage of mobile and linked devices that represent the Internet of Things (IoT). Internet of Things (IoT) is the revolutionary technology in the recent decade. Smart health monitoring mechanism [1]. According to the WHO, health is more than just the living free from disease; it is a state of complete well-being. Health is a fundamental asset, and lacking it can diminish one's ability to fully engage in everyday activities.

1.2. Motivation

Recent advancements in science and technology, particularly in telecommunications, computing, and sensor miniaturization, have significantly impacted the health sector. The proliferation of connected mobile devices, underpinned by the Internet of Things (IoT), has made a significant contribution in the development of comprehensive solutions for ambient assisted living. This technological evolution is seen as a pivotal moment, paving the way for innovative intelligent health monitoring systems [2].

1.3. Objectives

The objectives of this research paper are highlighted:

- Explore Ambient Computing in healthcare
- Address Ethical Concerns
- Propose blockchain solution
- Develop Secure Access Protocol

2. Contemporary Technologies in Healthcare

Specifically integrating IoT, with sensors and machines, patients can be monitored 24X7 and timely actions can be made for life support. Ambient Assisted Living (AAL), points to smart device interconnection, data analytics, and seamless connectivity leading to an advanced era of healthcare services. It represents an environment becoming intuitively responsive to the needs of patients and medical professionals. The crux of these applications is the real-time monitoring through IoT-enabled wearable devices, clever environmental sensors in conjunction with an event-driven intelligent system, offering a monitoring and assessment tool as well as the ability to initiate help when required. By harnessing the power of data analytics and AI, ambient intelligence enhances diagnosis options for healthcare professionals. AI algorithms' capability to rapidly analyse patient data and medical literature can assist clinicians in making timely diagnosis. Ambient intelligence brings voice-activated Natural Language Processing (NLP) capabilities to provide seamless communication between the health care systems and patients. Patients can engage with these assistants to schedule appointments, access health information, and receive personalized health advice, making healthcare more accessible and user-friendly. Ambient intelligence with latest technologies like Virtual Reality (VR) and Augmented Reality (AR) also gives immersive training experiences for healthcare professionals, simulate surgical procedures, and assist in patient education and rehabilitation. VR and AR applications enable enhanced learning, decision-making, and therapeutic interventions, contributing to advanced medical education and patient care. In fact, the research finding[3] revealed that a general practice clinic's exterior, layout, decoration, space, cleanliness, service delivery, and overall ambiance are vital components to gain trust in health care services. In the realm of ambient intelligence in healthcare, the integration of sensors, smart devices, and interconnected systems helps recreate environmental stimuli that contribute to a positive patient experience. Health care sector has the biggest use of IoT providing health tracking facilities. Essentially, IoT involves connecting computers to the internet using sensors and networks, allowing for seamless data flow and communication between devices [4,5].

3. Remote Health Monitoring

Internet of Healthcare Things (IoHT) aids with remote health monitoring. The smart healthcare is productive for all stakeholders, but the flip side of these advantages is ethical issues. Under these circumstances, health care is now brought into resident homes. These gadgets and technologies come in many forms, including health information websites, online networks, automated phone counselling, interactive health promotion initiatives, and email correspondence. As a result, personal data is also moved from paper to the digital realm. Exchange of health-related information across different hospitals among the health care providers and patients is the ultimate goal of Interoperability. There is a serious threat and vulnerability when institutional EHR and PHR are exposed to third party [6]. Unauthorized access and exposing of personal health information, can upset the patients physically and emotionally. [7] However, in the context of both institutional EHR and Personal Health Records (PHR), there is a risk of exposing sensitive health data to inappropriate third parties. Such unauthorized access and disclosure can not only compromise individual privacy but also lead to potential embarrassment, along with other physical and mental harms to the individuals involved, highlighting significant ethical challenges in the deployment of IoHT technologies [8].

Ambience Assisted Living (AAL), the confluence of IoT with AI based technologies like ML algorithms for disease diagnosis and prediction, proactive actions for maintaining sound health, NLP based technologies for communication and VR technology assures a promising health environment than the conventional hospital environment. But the security threats happened in AAL in the recent days have posed a challenge and demands swift action as it a danger to human life. This research paper quests to highlight the security breaches in AAL and presents a novel secured framework for AAL using the Block chain technology.

However, recent security breaches in AAL systems have highlighted significant vulnerabilities that pose real dangers to human life. These incidents underscore the urgent need for enhanced security measures. This research paper aims to shed light on these security issues within AAL systems and proposes

a novel, secure framework utilizing blockchain technology. This framework aims to bolster the integrity and security of AAL systems, thereby protecting sensitive personal health information from potential threats.

4. Block Chain in Healthcare

Blockchain Technology is predominantly applied in healthcare domain. This coolest technology resolves all challenges related to data security, privacy, sharing and storage. Blockchain technology is now being investigated for use in a number of healthcare applications, including Internet of Medical Things (IoMT) data management, storage, device connectivity, and security. Blockchain technology is increasingly recognized as a transformative tool in healthcare. Its potential lies in addressing various challenges associated with data security, privacy, sharing, and storage [9]. This technology offers a rich solution for ensuring the integrity and confidentiality of medical data across different platforms and stakeholders.

5. Related Works

Several approaches have been adopted by many researchers in recent years for harvesting the benefits of AAL without harming the security. New avenues for health data management and patient convenience in accessing and sharing their health data are emerging with advancements in electronic health data, cloud healthcare data storage, and patient privacy protection policies. [10]. Interconnection of blocks that are timestamped and encrypted with hashes is a Blockchain. These blocks are sealed in a secure and immutable manner [11]

Numerous researchers have recently adopted various strategies to leverage the advantages of Ambient Assisted Living (AAL) without compromising security. Blockchain records transactions across multiple computers, ensuring that records cannot be altered without changing all subsequent blocks and obtaining the network's consensus. Each block in a blockchain is time-stamped and cryptographically connected to the previous one, ensuring the data is securely sealed and immutable. While public blockchains allow any organization to join, potentially raising concerns about data confidentiality, private blockchains

restrict participation to vetted entities. This selective participation makes private blockchains more suitable for the healthcare domain where confidentiality and security of information are paramount. Mettler et al [12] reviewed the use of blockchain technology in healthcare applications. The three corner stones was public health, personalized medical and drug counterfeiting. Kuo et al. [13] published a review paper on healthcare and biomed apps usig block chain technology in the year 2017. Similar kind of a study was also done by Stagnaro et al. [14] with various usecases like supply chain management (SCM). Hölbl et al. [15] discussed numerous aricles from 2008 to 2019 and presented a systematic literature review. However, critical analysis of the experiments were not available. In another related work, Radanovi´c and Liki´c [16] reviewed blockchain technology in medicine, including health insurance, EHRs, drug supply, biomedical research, procurement processes, and medical education. Siyal et al. [17] covered a number of blockchain-based healthcare applications, such as EHR, clinical research, fraud detection, and neuroscience research. McGhin et al. [18] reviewed the requirements of the healthcare industry for medical data protection. This survey in [19] discussed limited applications for healthcare such as OmniPHR [20], Medrec [21], Pervasive social network (PSN) [22], MeDshare [23] and Healthcare Data Gateway [24]. Although it provides a basic introduction of blockchain's possibilities in the healthcare industry, it focuses more on the technology's practical advantages than its technical aspects or difficulties.

Table: 1 Comparison of Existing Literature

Literature	**Proposed Methodology**	**Potential Gaps**
Mettler et al.	Provides a broad perspective on key areas such as public health management and drug counterfeiting, emphasizing the functional benefits of blockchain technology.	Focuses on functionality and neglects the deeper technical aspects, such as implementation challenges and

Literature	Proposed Methodology	Potential Gaps
		potential barriers to adoption.
Kuo et al.	This study addresses traditional blockchain features and their relevance to medical records and insurance claims	The absence of detailed discussions on central knowledge distribution is a notable shortcoming, as understanding how information is managed and shared is crucial for real-world applications.
Stagnaro et al.	Outlined use cases related to interoperability and patient records	Leaves a gap in understanding the full capability of blockchain in healthcare settings.
Radanović and Likić:	Reviewed various applications in blockchain technology	Overlooks significant concepts like smart contracts and data sharing, which are integral to the technology
McGhin et al.	Focus on patient information protection is essential but highlights limited applications	Broader discussions on the diversified applications of blockchain in healthcare for holistic understanding are missing.

While the reviewed literature offers useful insights into blockchain applications in healthcare, several studies fall short in addressing technical challenges and exploring comprehensive applications. Our proposed framework extends beyond functional benefits to include potential barriers, risk and enhance the block chain implementation in healthcare domain.

6. Proposed Methodology

6.1. The Proposed Block Chain Framework

Blockchain technology presents a tamper-proof series of encrypted records joined in a chain for auditing. [25]. This technology resembles a traditional accounting ledger where once entries are made, they cannot be altered, and new entries must be authenticated by a trusted authority. However, the distinguishing feature of blockchain is its verification process, which is carried out by a decentralized network of nodes, each holding a ledger copy, removing the need for a central verifying authority. In a blockchain, every new block is linked to the previous one through a cryptographic hash contained within the current block, as illustrated in Figure 1. This structure ensures the blockchain's integrity and its resistance to unauthorized modifications. Should any attempt be made to alter an older block, the change in its hash value would necessitate updating the hash in all following blocks to restore the blockchain's validity. Every participant who are involved will hold a copy of the blockchain, allowing any alterations to be immediately verified by others. With each new block added, these copies are updated, ensuring the entire network remains in sync and secure. Visibility of the block varies based on the access levels set by the administrator. Blockchain technology employs cryptographically secure hash algorithms like Secured Hash Algorithm - SHA-256 and SHA-512 to safeguard the integrity of the data contained within each block. Each block is distinguished by a distinct hash value. For example, Ethereum utilizes Keccak-256 and Keccak-512, whereas Bitcoin relies on a double application of SHA-256. These SHA algorithms are designed to be collision-resistant, ensuring that no two distinct pieces of input data will yield identical output (hash value). Therefore, SHA algorithms serve as reliable tools for verifying whether data has remained unchanged.

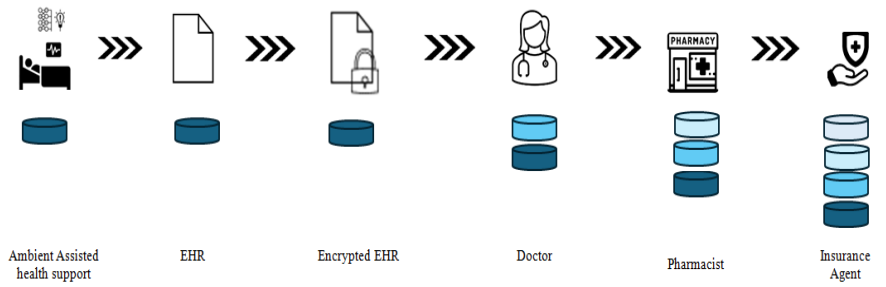

Fig: 1.1 Secured Ambient Assisted Living (AAL) Pipeline

Similar to a traditional accounting ledger, entries in a blockchain once recorded, cannot be modified, and each new entry requires authentication by a trusted entity. The unique aspect of blockchain, however, is its decentralized verification process. This process is handled by a network of nodes, each possessing a ledger copy, thus removing the need for a centralized authority to confirm transactions. This linkage shown in Fig. 2 ensures the integrity of the blockchain and its resilience against unauthorized changes. If a modification is attempted on an older block, the hash of that block would change, necessitating an update of all subsequent block hashes to maintain the chain's validity. The visibility of each block can be adjusted based on the permissions set by the administrator.

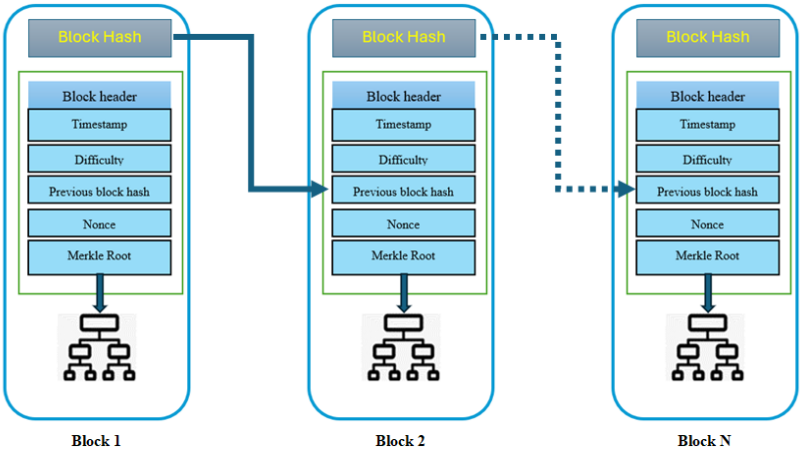

Fig.2: Blockchain Structure

Blockchain-based framework is used for EHR data transmission and storage. This ensures tamper-proof and transparent transactions by recording data in blocks linked together cryptographically.

Consensus mechanism is implemented with Proof of Authority (PoA), which requires nodes to be authorized before participating in the consensus process. This ensures that only trusted entities can validate transactions. The proposed framework deals with the healthcare domain users viz., Patients, Doctors, Pharmacies, Insurance Companies.

Role Based Access Control (RBAC) is implemented for users to assure authenticated data sharing and implementing data integrity

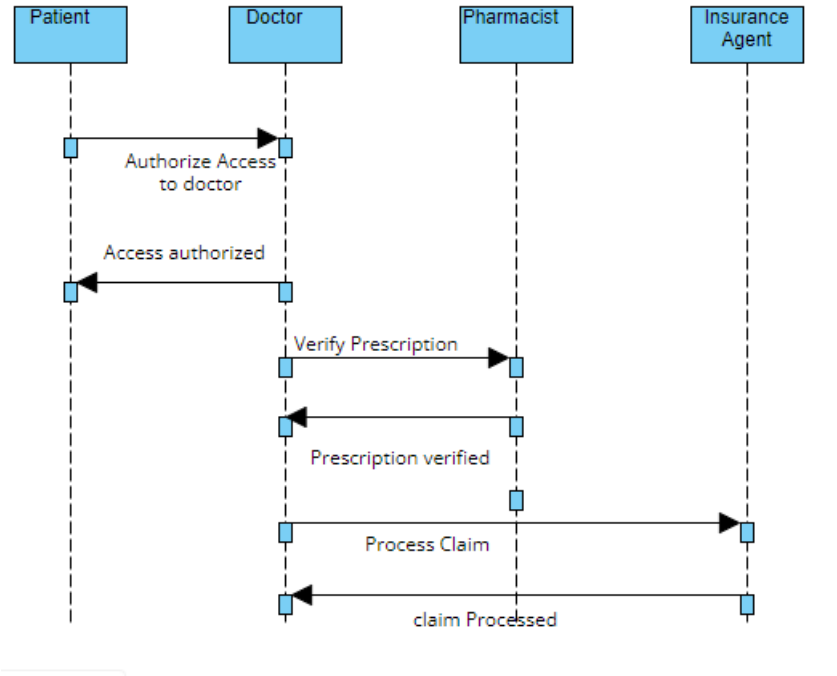

Fig 3: Sequence Diagram

6.2. Interactions using Sequence Diagram

This sequence diagram in Fig. 3 illustrates the interactions where the patient authorizes access for the doctor, the doctor verifies the prescription with the pharmacy, and the doctor processes a claim with the insurance company. Each message indicates a specific interaction between the participants in the system.

Node Roles:

Patients: Patients have access to their medical records and can authorize the sharing of specific data with healthcare providers, pharmacies, and insurance companies.

- View own medical records.
- Authorize sharing of medical data with specific doctors, pharmacies, or insurance companies.
- Grant temporary access to emergency medical personnel if required.

Doctors: Doctors can update patient records, add medical diagnoses, treatment plans, and prescriptions.

- View patient medical records (authorized by patients).
- Update patient medical records with diagnoses, treatments, and prescriptions.
- Access relevant medical data necessary for providing healthcare services.

Pharmacies: Pharmacies can verify prescriptions and dispense medication.

- Verify prescriptions issued by authorized doctors.
- Access patient information related to prescribed medications.
- Maintain records of dispensed medications for regulatory compliance.

Insurance Agent: Insurance Agent can access relevant medical data for processing claims and providing coverage. Access control mechanisms guarantees that only entities that are authorized can access certain data or perform specific actions within the blockchain network.

- Access patient medical records for processing insurance claims.
- Verify treatment procedures and medications prescribed.
- Maintain confidentiality of patient data in compliance with regulations.

6.3. Assuring Confidentiality, Integrity and Authentication (CIA)

A patients' health information is updated in the EHR and is ssent to the doctor. The doctor sends prescriptions to the pharmacist. Insurance agents get information from patients and doctors for claiming money. The steps of cryptographic techniques with digital signature and private key cryptography to achieve, 1. authentication of patient, doctor and pharmacist. 2. integrity of EHR data.

Step 1: Preparation for Sending the Message

Digital Signature for Authentication and Integrity:

The sender creates a hash (a fixed-size, unique representation) of the original message.

The created hash is encrypted with the private key of the sender, creating a digital signature. This step ensures that any recipient can verify the sender's identity (authentication) and that the message has not been altered in transit (integrity).

Encryption for Confidentiality:

The sender generates a symmetric session key for the efficient encryption of the message.

The message is then encrypted using this symmetric session key.

The symmetric session key is then encrypted with the receiver's public key to ensure that only the receiver can decrypt it.

Step 2: Sending the Message

The encrypted message, the encrypted session key, and the digital signatures are sent to the receiver.

Step 3: Receiving and Verifying the Message

Decrypting the Session Key:

The receiver decrypts the encrypted session key with their private key.

Decrypting the Message:

The receiver then uses the decrypted symmetric session key to get back the message.

Verifying the Digital Signature:

By utilizing the sender's public key to decrypt the digital signature, the recipient can retrieve the message's hash. The receiver generates a new hash from the decrypted message and compares it with the hash obtained from the digital signature. If there is match of the hashes, it confirms that the message was indeed from the sender (authentication) and has not been tampered with (integrity).

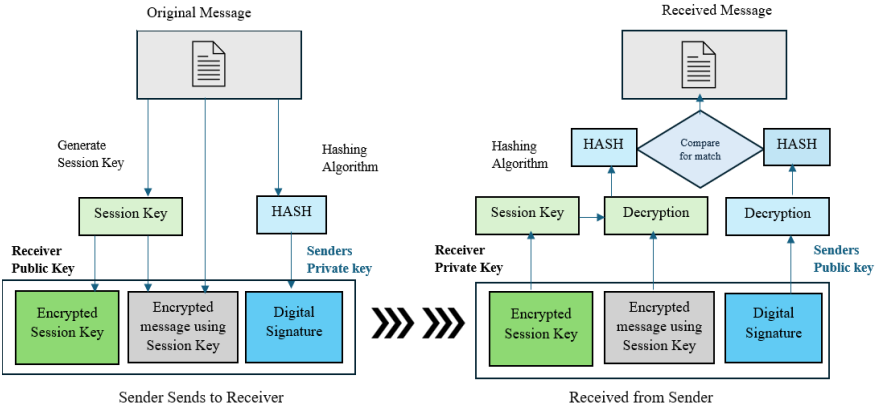

Fig 4: Assuring CIA

Thus, an end-to-end interaction framework is proposed for seamless communication among all healthcare domain stakeholders, including Patients, Doctors, Pharmacies, and Insurance Agents, using a tamper-proof blockchain-based system. The novelty of this work lies in enhancing the security of ambient assisted healthcare systems by integrating blockchain technology with Role-Based Access Control (RBAC) and encryption to ensure Confidentiality, Integrity, and Availability (CIA).

The Novelty of the Framework includes:

1. Consensus through Proof of Authority (PoA)
2. Data sharing and integrity managed via Role-Based Access Control (RBAC)

3. Ensuring Confidentiality, Integrity, and Availability (CIA) through encryption

7. Discussions

In the proposed framework, Blockchain technology promises tamper-proof and transparent transactions by recording in cryptographically linked data blocks. The consensus mechanism is implemented using Proof of Authority (PoA), where nodes must be authorized before participating in the consensus process.

Confidentiality is achieved through the encrypted message with a symmetric session key, which is then securely shared by scrambling it with the public key of the receiver. This ensures that only the intended receiver can decrypt the message. Authentication is provided by the digital signature, as only the sender has the private key necessary to create the signature. The use of the public key of the sender) by the receiver to decrypt the signature assures that the message could only have come from the sender. Integrity is ensured by the hash comparison process. Since altering the message would change its hash, the digital signature verifies that the message received is exactly as the sender intended.

This comprehensive approach leverages the strengths of both symmetric and asymmetric encryption, along with digital signatures, to ensure secure, authentic, and integral communication. Cryptography ensures secure communication and data exchange within ambient healthcare systems. The use of public and private keys enables secure, encrypted data transmission, giving assurance that only authorized individuals can access sensitive patient information. This is crucial for maintaining patient privacy and security. The Cryptographic Hash function takes input data and returns a fixed-size string of bytes. The output, or hash, is unique for different inputs and acting as a digital fingerprint of the data.

Hashing is used for creating the block's hash and for linking blocks securely. Role Based Access control (RBAC) is implemented for Patients, Doctors, Pharmacies, Insurance Companies to assure authenticated data sharing and implementing data integrity

8. Conclusion

While blockchain offers significant security benefits, it is not a panacea. Successful incorporation of blockchain into ambient healthcare systems requires meticulous planning, implementation, and ongoing management to address challenges such as scalability, energy consumption, and the need for interoperability with existing healthcare technologies. Blockchain technology is made up of several key components that work together to create a secure, transparent, and decentralized system for recording transactions and managing data. Understanding these components is crucial to grasping how blockchain function and why they are considered secure and tamper-proof. Data recorded on a block chain are immutable. This immutability ensures the integrity of medical and health-related data, making blockchain an ideal solution for creating tamper-proof records of patient history, treatments, and outcomes.

References

[1] Rahaman A, Islam M, Islam M, Sadi M, Nooruddin S. Developing IoT based smart health monitoring systems: a review. Rev IntellArtif. 2019; 33:435–40. https://doi.org/10.18280/ria.330605.

[2] Riazul Islam SM, KwakDaehan, HumaunKabir M, Hossain M, Kwak Kyung-Sup. The Internet of Things for health care: a comprehensive survey. IEEE Access. 2015; 3:678–708. https://doi.org/10.1109/ACCESS.2015.2437951.

[3] Ai, Yun, et al. "Determinants of patients' satisfaction and trust toward healthcare service environment in general practice clinics." Frontiers in Psychology 13 (2022): 856750.

[4] Hasan M, Islam MM, Zarif MII, Hashem MMA. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet Things. 2019; 7:100059. https://doi.org/10.1016/j.iot.2019.100059.

[5] Nooruddin S, Milon Islam M, Sharna FA. An IoT based device-type invariant fall detection system. Internet Things. 2020; 9:100130.

[6] Sholla, Sahil, RoohieNaaz Mir, and Mohammad Ahsan Chishti. "Towards the design of ethics aware systems for the Internet of Things." China Communications 17.2 (2020): 239-252.

[7] Denecke, Kerstin, et al. "Ethical issues of social media usage in healthcare." Yearbook of medical informatics 24.01 (2015): 137-147.

[8] Sholla, Sahil, RoohieNaaz, and Mohammad Ahsan Chishti. "Ethics aware object-oriented smart city architecture." China Communications 14.5 (2017): 160-173.

[9] Rawal, V.; Mascarenhas, P.; Shah, M.; Kondaka, S.S. White Paper: Blockchain for Healthcare an Opportunity to Address Many Complex Challenges in Healthcare; CitiusTech: Princeton, NJ, USA, 2017.

[10] Dimitrov, D.V. Blockchain Applications for Healthcare Data Management. Healthc. Inform. Res. 2019,

[11] Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry. Computer 2017, 50, 18–28. [Google Scholar] [CrossRef] [Green Version]

[12] Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; pp. 1–3.

[13] Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. 2017, 24, 1211–1220. [CrossRef] [PubMed]

[14] Stagnaro, C. White Paper: Innovative Blockchain Uses in Health Care. Available online: https://www.freedassociate s.com/ (accessed on 24 April 2019).

[15] Hölbl, M.; Kompara, M.; Kamišali´c, A.; NemecZlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. Symmetry 2018, 10, 470. [CrossRef]

[16] Radanovi´c, I.; Liki´c, R. Opportunities for Use of Blockchain Technology in Medicine. Appl. Health Econ. Health Policy 2018, 16, 583–590. [CrossRef]

[17] Siyal, A.; Junejo, A.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. Cryptography 2019, 3, 3. [CrossRef]

[18] McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. J. Netw. Comput. Appl. 2019, 135, 62–75. [CrossRef]

[19] Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.

[20] Zhang, J.; Xue, N.; Huang, X. A secure system for pervasive social network-based healthcare. IEEE Access 2016, 4, 9239–9250. [CrossRef]

[21]]. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017, 5, 14757–14767. [CrossRef]

[22] Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. 2016, 40, 218. [CrossRef] [PubMed]

[23] Xia, Q. I., et al. "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain." IEEE access 5 (2017): 14757-14767.

[24] Yue, Xiao, et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of medical systems 40 (2016): 1-8.

[25] Z. Zheng, S. Xie, H. Dai, and H. Wang, ''An overview of blockchain technology: Architecture, consensus, and future trends,'' in Proc. IEEE Int. Congr. Big Data, Big Data Congr., Jun. 2017, pp. 557–564.