International Journal of Applied Engineering Research

Exploring Benefits, Challenges and Security Considerations of Cloud Computing and Blockchain Technology to Enhance Healthcare Services

Fareedullah[1]*,Ziauddin[1,]MudasirMahmood[1,] Muhammad Ijaz Khan[1,] Muhammad Farhan[1,]
Syed Muhammad Ali Shah[1],
fareedkamran44@yahoo.com,ziasahib@gmail.com,mudasir@gu.edu.pk,ijazkhan@gu.edu.pk
farhan@gu.edu.pk, alishah@gu.edu.pk
[1]Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan, Pakistan 29050
*Corresponding Author:ziasahib@gmail.com
fareedkamran44@yahoo.com

Abstract:This study explores the benefits and challenges of incorporating cloud computing and blockchain technology in the healthcare sector. Cloud computing offers advantages such as scalability, cost-effectiveness, remote accessibility, etc.However, security concerns, data breaches, encryption limitations, and cybersecurity threats need to be addressed.Although, blockchain technology providesdecentralization, immutability, enhanced security, transparency, and trust.But, challenges related to scalability, storage capacity, performance, regulatory frameworks, and maintenance costs hinder its widespread adoption in healthcare. Several healthcare applications, such as MedRec, Patientory, and Medicalchain, have been developed using cloud and blockchain technologies independently. Though, these applications face challenges related to security, privacy, scalability, and storage capacity. To fix these concerns, integration between Cloud computing and Blockchain is essential, which enables organizations to establish a highly secure and reliable cloud infrastructure. By leveraging the strengths of both technologies, create a secure and efficient environment across various industries, including healthcare.

Keywords: Security, Privacy, Healthcare, Cloud, Blockchain

Introduction:

1. Cloud Computing

Cloud computing is a pay-per-use model that offers computing resources over the Internet. Users can access and utilize various resources like storage, software applications, and processing power without relying on local infrastructure or hardware. This approach eliminates the need for extensive administrative tasks and facilitates effective resource management (8). Cloud computing provides applications, data storage, and file management(1).its key benefits include scalability,cost effectiveness, and the ability to adjust resources based on demand(3). Users can speedily access several resources or reduce their usage without investing in new hardware. Cloud computing revolutionizes data storage and access, offering convenience and accessibility from any location (4). It eliminates the need for expensive hardware investments and allows organizations to deploy virtual machines on a large scale, optimizing expenses and avoiding resource waste (3). Cloud computing authorizes users with centralized and accessible computational resources, making it a game changer in the digital era (4). Modern technological advancements enable efficient handling of large data volumes and cloud computing offers shared computing resources for seamless information control (21, 22). It enables constant accessibility to IT services, offering on-demand resource availability, scalability, and on-demand pricing models, revolutionizing traditional computing models (1). Cloud computing allows users to access resources as needed with short-term availability, making it attractive for organizations with limited resources and infrastructure (3). It transfers IT storage responsibility to third-party providers, reducing expenses and improving flexibility. Upgraded ICT utilities and web-based application enhances access and mobility while cloud services meet the computing demands of the eHealth system and promote energy efficiency (23).

Major Characteristics of Cloud Computing

- Resources pooling: Numerous clients' access shared their resources, upholding efficient utilization and cost savings.
- Quick elasticity: Computing resources can be speedily scaled up / down based on demand, offering flexibility and agility. Broad network access: Cloud computing services are accessible from various client platforms, enhancing accessibility.
- Measurable service: Resource utilization can be monitored and reported, ensuring transparency and accountability.
- On-demand self-service:Users can provision and manage resources without human intervention, improving efficiency.

2. Architecture

Cloud computing is an information technology service delivery model where customers can access and use services over the Internet. These services are scalable and rented from third-party providers who own the necessary infrastructure. It comprises two fundamental models: the first one is the Cloud service model, which defines the types of services offered, and the second one is the Cloud deployment model, which determines how the infrastructure is deployed.

2.1. Cloud Service Model: it is a scalable IT delivery model that offers services over the Internet. It encompasses Software as a service, platform as a service, and Infrastructure as a Service (IaaS), providing a range of computing capabilities at different infrastructure levels.

2.2.1. Software as a Service (SaaS): this model**i**s a service delivery model where users can access data and applications on demand through a web browser. Examples include Microsoft365 and google docs. Software as a service eliminates the need for individual software installation and maintenance, reducing costs and simplifying software deployment [27].

2.2.2. Platform as a Service (PaaS): Itoffers a software platform for application development, managing the hardware and software infrastructure on the provider's network. Users can focus on their applications without worrying about the underlying management. Platform as a service eliminates the need for in-house hardware and software, simplifying the development and deployment of new applications [28].

2.1.3. Infrastructure as a Service (IaaS): This is a cloud computing model where providers offer infrastructure resources like servers, storage, and load balancers to organizations. It eliminates the need for purchasing and maintaining physical hardware, allowing quick and easy access to scalable and flexible infrastructure. IaaS enables organizations to reach a large number of users remotely, freeing them from server management and maintenance tasks [27].

2.2. Cloud Deployment Model: there are main four cloud computing deployment models for customers to choose from when deploying a cloud computing solution [27, 28].

2.2.1. Public Cloud: Cloud computing resources accessible to anyone on a chargeable basis, owned and operated by third-party providers. This model offers economical access to hardware and software resources with shared infrastructure.

2.2.2. Private Cloud: This model has restricted access to a specific group or organization, providing exclusive services tailored to their needs. Offers greater control over security and data handling compared to the public cloud.

2.2.3. Hybrid Cloud: The hybrid cloud is comprisedof public and private cloud infrastructures, allowing scalability and resource utilization from multiple providers. It enables on-demand scalability and maintains data control and security.

2.2.4. Community Cloud: Various organizations collaborate and share infrastructure, hosted by a third-party provider or one of the organizations. It enables collaboration and resource sharing while adhering to respective policies.

3. Cloud Computing in Healthcare

The cloud computing model has transformed the healthcare sector by providing convenient access and storage of patient medical records, improving patient care (39). Healthcare providers are increasingly adopting cloud technologies to meet growing data storage and network requirements (40). Technological advancements like cloud computing, telemedicine, and electronic health records are transforming healthcare services, leading to positive changes in patient care (38). Cloud technologies play a vital role in healthcare applications, enabling efficient data collection, storage, and analysis for medical research and patient care (39).Cloud computing streamlines access to medical records, improving the efficiency and quality of healthcare services (21). It offers infrastructure and services on-demand, reducing operational costs and providing high availability and disaster recovery capabilities crucial for the healthcare sector (37).

4. CloudComputing Challenges in Healthcare

When examining the healthcare sector, challenges such as patient mobility, data transfer across jurisdictions, resource scarcity, an aging population, public funding scrutiny, medical errors, and system inefficiencies jeopardize its resilience. Healthcare organizations adopt cloud computing (43, 44) to improve service quality, reduce errors, and enhance data access. Cloud computing offers collaboration, cost reduction, speed, scalability, flexibility, and streamlined data-sharing benefits (40). However, security concerns and service costs hinder full adoption, necessitating careful consideration (41). Balancing data availability and confidentiality is crucial for ethical use (42). Addressing challenges and security issues will facilitate the effective use of cloud computing in healthcare (44). This study aims to identify barriers, challenges, and security solutions for cloud computing in healthcare, promoting its utilization while ensuring security.

5. Blockchain

Blockchain is a decentralized and transparent digital ledger technology (11), which ensures the secure and immutable recording of transactions. It has the potential to revolutionize industries by providing enhanced security, traceability, and efficiency, eliminating intermediaries, and enabling peer-to-peer transactions with increased trust. Introduced in 2008 by Nakamoto, the blockchain was initially created to support Bitcoin, with the first Bitcoin block being established in 2009(15). Blockchain technology is decentralized and distributed among network nodes, promoting trust and eliminating the need for a central authority (18). It enables secure and automated information exchange through cryptographic blocks that are verified and added to the chain, creating an immutable record (19). In blockchain technology, each block contains a header with important details like the hash of the previous block and a timestamp. Blocks are connected in chronological order using these hash values. The size of a block supports processing numerous transactions, consisting of a block header and a list of transactions. The block header contains metadata, while transactions can be organized in a Merkle tree structure. A block serves as a fundamental unit with a header and validated transactions, linked to the previous block to ensure chronological order and immutability (9, 14). Cryptographic hashes and timestamps are used to maintain data integrity and confidentiality within a blockchain network (17). Enhanced cryptographic methods provide security for accounts and transactions. Blockchain acts as a public ledger, recording transactions in chronological and linear order by continuously adding new blocks to the chain (2). Blockchain technology operates as a decentralized and architecturally decentralized system, ensuring data integrity and reducing infrastructure failure risks (5). Primarily, proof of work (PoW) consensus was used, but there is a shift towards proof of stake (PoS) for energy efficiency and scalability (16). The base service layer of blockchain provides interconnected services like network communication, identity management, consensus mechanisms, and distributed ledger technology. Smart contracts enable interaction with the blockchain, and events management notifies relevant parties of ledger changes (17). Blockchain ensures secure resource transfer through peer-to-peer communication and cryptographic techniques for data integrity and confidentiality (17). Blockchain technology (2) is characterized by decentralization, immutability, transparency, security, and smart contracts. It provides an effective and secure method for recording and managing assets, operating on a decentralized peer-to-peer network with a distributed ledger system (11). There are four types of blockchains: public, private, and consortium. Public blockchains offer transparent security, while private and consortium blockchains provide increased privacy and control (12).

Main characteristics of Blockchain: These are the few main characteristics of blockchain technology

- **Decentralization:** There is no central authority that controls the blockchain, and transactions are validated through a peer-to-peer network (13).

- **Transparency:** Entirely participants share the same ledger, allowing for visibility of transaction history and enhancing trust (20).
- **Immutability:** When a transaction is added to the blockchain, it cannot be altered, ensuring data integrity (19).
- **Traceability:** The replication of events enables easy tracing and auditing (35).
- **Trustless:** Applicants can exchange information anonymously, relying on the consensus mechanism for trust (33).
- **Time Stamped:** Transactions are recorded with timestamps, providing an audit trail (24).
- **Append Only:** Information can only be added sequentially, maintaining data integrity (26).Security: Blockchain employs secure algorithms and encryption, reducing the risk of fraud or corruption (13).

5.1. Blockchain Architecture:

Blockchain technology employs digitally signed blocks and algorithms to ensure secure, real-time transactions and documentation without relying on centralized control. Proposed by Satoshi Nakamoto for Bitcoin, the blockchain uses interconnected blocks with pointers to maintain data integrity. Consensus algorithms validate new blocks, and the architecture incorporates multiple components for seamless transaction processes.

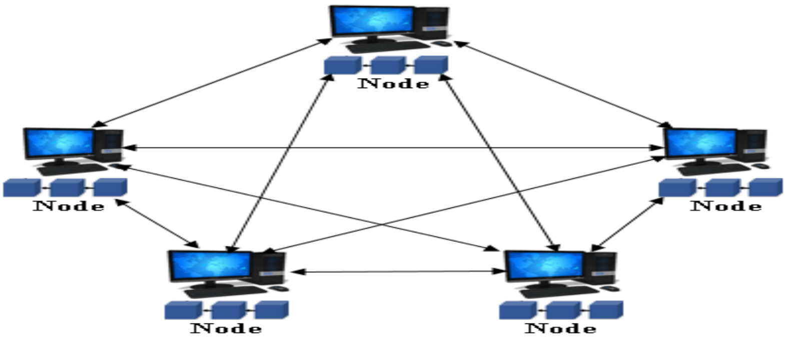

Figure 3 Blockchain Architecture Model

- **Nodes:** The devices that actively participate in the blockchain network, contributing to transaction validation and network security.
- **Peer-to-Peer Network:** Peer to peer network is a decentralized network where participants maintain a copy of the entire blockchain ledger.
- **Blocks:** This is the fundamental units of information in a blockchain that store transaction data and are secured using cryptographic techniques.
- **Consensus Mechanism:**The consensus mechanism is an algorithm that ensures only valid transactions are included in the ledger, such as proof-of-work (PoW) and proof-of-stake (PoS).
- **Distributed Ledger:** Distributed ledger is a digital system that stores information across a peer to peer network, providing enhanced security and transparency.
- **Cryptographic Hashes:** This is a mathematical function used to create unique identifiers for blocks, ensuring data integrity.

- **Smart Contracts:** Smart contract programs are stored on a blockchain that automatically executes when specific conditions are met, enhancing efficiency and transparency (7, 13, 14, 32, and 67).

2. Types of Blockchain:

The types of blockchains can be classified into four main categories (13, 19):

5.1.1. Public Blockchainispermissionless and allows anyone with internet access to join and interact with them. Examples include Bitcoin and Ethereum. Participants can contribute as miners or key validators, and transactions are transparent and visible to all nodes in the network. Public blockchains operate on incentive-based economic mechanisms and unique consensus algorithms to ensure security and efficiency.

5.1.2. Private Blockchains. These are permissioned and require authorization from the network administrator to participate. These blockchains are favored by organizations handling sensitive data, as they offer controlled access and maintain data integrity. Examples include Ripple and Hyperledger, which provide private blockchain networks managed by a single organization or a trusted third party.

5.1.3. Consortium Blockchain: It involves multiple institutions working together in a partially decentralized manner. They use a permissioned approach to prevent manipulation and control access. Consortium blockchains can be used within a single industry or across multiple organizations, allowing limited public access while maintaining partial centralization and trust. The classification of consortium blockchains is still debated in the literature.

5.1.4. Hybrid Blockchain: It combines features of both private and public blockchains. They are used when a combination of private and public information access is required. Users on a hybrid blockchain platform can freely access certain data based on relevance or be granted permissioned access as needed.

5.2 Blockchain in Healthcare:

Blockchain technology in healthcare deals with several benefits and applications. The electronic health record (EHR) contains personal health information and requires protection. Blockchain, initially introduced by Bitcoin and expanded through Ethereum, enables secure information exchange without compromising patient confidentiality. Ethereum introduced smart contracts, eliminating the need for new blockchains.Ethereum's use cases include decentralized file storage. However, blockchain technology is still being developed to address performance, scalability, and security concerns. It relies on cryptography to establish trust and consensus (36).The eHealth system provides real-time access to patient records, enhancing healthcare services and response to epidemics. Sharing medical data raises privacy and security concerns, necessitating effective privacy measures (10). Blockchain can facilitate clinical information sharing, consent for research, data monetization, and reduce fraudulent activities (5).Blockchain technology is applied in various sectors, including healthcare, finance, government, and transportation (24). It offers distribution, decentralization, and data integrity, enhancing information exchange, access control, and provenance. It promotes trust-building and facilitates data maintenance and sharing in healthcare (25) it ensures the secure exchange of data among stakeholders (26).

5.3. Blockchain challenges in Healthcare.

The usage of wearables and healthcare monitoring technology has generated a vast amount of individual health data. However, data management and secure retrieval are crucial for data-driven decision-making in healthcare. Patients generate data through their interactions with healthcare professionals, but data ownership is often retained by providers, leading to fragmented data trails and limited patient access. Healthcare data is abundant, diverse, and requires real-time analysis, but it is often inaccessible, lacks standardization, and is challenging to comprehend and exchange effectively (24).The current state of medical history and record-keeping in healthcare is characterized by fragmentation, lack of interoperability, limited patient access, inconsistent data quality, and inefficient data retrieval processes (24, 29). Communication between patients and doctors fails to utilize the data effectively, making healthcare processes time-consuming and lengthy. Important patient data is dispersed among systems, leading to inadequate care and management inefficiencies. Healthcare data lacks security and dependability, with most medical records still on paper, hindering care coordination, quality assessment, and error mitigation (23).The challenge lies in capturing, storing, and securely transmitting digital healthcare data across applications and systems without adding complexity (18). Blockchain technology offers benefits for record-sharing, security, and privacy in healthcare, but challenges include scalability, storage limitations, standardization needs, and implementation expertise (35, 34). Maintaining a balance in store and exchange operations is crucial, particularly in high-volume scenarios (32). Storing unprocessed data, like raw genetic information, on a blockchain is not recommended due to its large size (33).Blockchain-based systems may face performance degradation and increased deployment expenses due to the multiple parties involved in transactions (6, 31). Consensus and verification challenges can lead to longer processing times, and scaling issues can affect transaction verification (30). In emergency situations, blockchain solutions may have limitations in addressing patient difficulties and granting access to surgeons or other parties (10).

Cloud computing offers scalability, cost-effectiveness, and remote accessibility, providing benefits to healthcare organizations. It allows for efficient resource allocation, eliminates infrastructure investments, and supports remote work and collaboration. Cloud-based solutions like electronic health records improve data management and enhance healthcare services. However, security concerns such as data breaches, encryption, and trust need to be addressed, along with maintaining confidentiality and control over data. On the other hand emerging Blockchain technology offers benefits like decentralization, immutability, security, transparency, and efficiency. It eliminates the need for a central authority, ensures data integrity, and provides robust security through cryptographic methods. Transparency and trust are fostered through a public ledger. However, challenges in scalability, storage capacity, computational cost, lack of clear regulations, and high maintenance costs hinder the widespread adoption of blockchain in healthcare.

6. Discussion

Cloud computing technology has changed the way data is stored and accessed, it providing numerous benefits such as scalability, cost-effectiveness, flexibility, etc. Though, it also introduces security and privacy concerns, as sensitive data is entrusted to third-party servers. Unauthorized access, data breaches, and lack of control over data, etc. are some of the challenges that arise in this context. Luckily, by integrating blockchain technology into cloud computing, many of these concerns can be effectively addressed.

One of the main advantages of integrating blockchain into cloud computing is the enhancement of data security. Cloud storage relies on centralized servers, making them vulnerable to attacks and unauthorized access. On the other hand,Blockchain technology offers a decentralized approach, where data is distributed across a network of nodes. This decentralization makes it difficult for attackers to compromise the system as they would need to manipulate multiple nodes simultaneously. Moreover, the blockchain's immutable nature ensures that once data is recorded on the blockchain, it cannot be modified or tampered with, providing an additional layer of security.

Data Security: Cloud computing technology involves storing sensitive data on third-party servers, which raises concerns about unauthorized access and data breaches. By integrating blockchain into cloud computing, the data can be encrypted and stored in a decentralized manner. Blockchain's distributed ledger ensures that data remains tamper-resistant and transparent, reducing the risk of unauthorized access and enhancing data security

Trust and authenticity: These elements are in cloud computing, particularly when dealing with sensitive data. Blockchain's decentralized nature and consensus mechanisms enable trust and authenticity in the cloud. Through consensus algorithms, participants in the blockchain network agree on the validity of transactions and data. This agreement ensures that data stored in the cloud remains tamper-resistant and authentic. Any changes or modifications made to the data are recorded on the blockchain, creating an auditable trail that can be used to verify the integrity of the data and mitigate the risk of unauthorized alterations.

Encryption and key management: Encryption and key management play a vital role in securing data in the cloud. Blockchain technology can enhance these aspects by providing a secure platform for storing and managing encryption keys. Encryption keys are essential for protecting data, and with blockchain, they can be securely stored and managed using distributed ledger technology. This reduces the risk of key exposure and strengthens the overall security of data stored in the cloud.

Virtual Machines: In cloud environments Virtual machines are often targeted by attackers seeking to compromise the underlying infrastructure or gain unauthorized access to sensitive data. Blockchain can help address these vulnerabilities by providing a decentralized and secure platform for managing VMs. By incorporating blockchain technology, VMs can be monitored, audited, and their integrity can be ensured. Any unauthorized changes made to the VMs can be detected through the blockchain's transparent and tamper-resistant nature, enhancing overall security in cloud computing environments.

Confidentiality and control:Confidentiality and control over data are critical concerns in cloud computing, where users entrust their data to third-party service providers. Blockchain technology can provide users with greater control and confidentiality over their data. Smart contracts, which are self-executing contracts with predefined rules encoded on the blockchain, can be used to enforce access control policies. Users can define and manage who has access to their data through these smart contracts, enhancing data confidentiality and giving users greater control over their information.

Regulatory compliance: Regulatory compliance is one of utmost importance in certain industries, such as healthcare, where strict regulations govern the storage and handling of sensitive data. Blockchain's transparent and auditable nature can facilitate regulatory compliance by providing a verifiable record of data transactions. Healthcare organizations, for example, can leverage blockchain to ensure the privacy and security of patient data while meeting regulatory requirements. The immutable nature of the blockchain ensures that all data transactions are recorded and can be audited, providing a trustworthy and transparent record for compliance purposes.

7. Conclusion:

Cloud computing technology offers various benefits for healthcare organizations, but there are concerns regarding security, privacy, and trust. Through integrating blockchain technology into cloud computing can address many of the security and privacy concerns associated with cloud computing. Employing leveraging blockchain's features such as data security, trust and authenticity, encryption and key management, virtual machine security, confidentiality and control, and regulatory compliance, the overall security and integrity of data stored in the cloud can be enhanced. Blockchain's decentralized and transparent nature provides a promising solution to mitigate the risks and vulnerabilities associated with cloud computing, particularly in sensitive industries like healthcare. By combining the strengths of both cloud computing and blockchain technology, organizations can achieve a more secure and trustworthy cloud infrastructure.

References:

1. Vasanthanayaki, C. (2020). Secure medical health care content protection system (SMCPS) with watermark detection for multi cloud computing environment. Multimedia Tools and Applications, 79, 4075-4097.
2. Ozercan, H. I., Ileri, A. M., Ayday, E., & Alkan, C. (2018). Realizing the potential of blockchain technologies in genomics. Genome research, 28(9), 1255-1263.
3. Nicolae, B. (2011). On the benefits of transparent compression for cost-effective cloud data storage. Transactions on Large-Scale Data-and Knowledge-Centered Systems III: Special Issue on Data and Knowledge Management in Grid and P2P Systems, 167-184.
4. Qin, Z., Weng, J., Cui, Y., & Ren, K. (2018). Privacy-preserving image processing in the cloud. IEEE cloud computing, 5(2), 48-57.
5. Boulos, M. N. K., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. International journal of health geographics, 17.
6. Hölbl, M., Kompara, M., Kamišalić, A., &NemecZlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470.
7. Langmead, B., & Nellore, A. (2018). Cloud computing for genomic data analysis and collaboration. Nature Reviews Genetics, 19(4), 208-219.

8. Yang, G., & Li, C. (2018, December). A design of blockchain-based architecture for the security of electronic health record (EHR) systems. In 2018 IEEE International conference on cloud computing technology and science (CloudCom) (261-265). IEEE.
9. Abdellatif, A. A., Al-Marridi, A. Z., Mohamed, A., Erbad, A., Chiasserini, C. F., & Refaey, A. (2020). ssHealth: toward secure, blockchain-enabled healthcare systems. IEEE Network, 34(4), 312-319.
10. Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49, 114-129.
11. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In AMIA annual symposium proceedings (Vol. 2017, p. 650). American Medical Informatics Association.
12. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., &Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, 104040.
13. Hemalatha, K., Hema, K., &Deepika, V. (2020). Utilization of blockchain technology to overthrow the challenges in healthcare industry. In Emerging Research in Data Engineering Systems and Computer Communications: Proceedings of CCODE 2019 (pp. 199-208). Singapore: Springer Singapore.
14. Reddy, B., &Aithal, P. S. (2020). Blockchain as a disruptive technology in healthcare and financial services-A review based analysis on current implementations.
15. Justinia, T. (2019). Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. ActaInformaticaMedica, 27(4), 284.
16. Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.
17. Fusco, A., Dicuonzo, G., Dell'Atti, V., &Tatullo, M. (2020). Blockchain in healthcare: Insights on COVID-19. International Journal of Environmental Research and Public Health, 17(19), 7167.
18. Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2020). Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Systems Journal, 15(1), 85-94.
19. Ismail, L., &Materwala, H. (2020). Blockchain paradigm for healthcare: Performance evaluation. Symmetry, 12(8), 1200.
20. Gao, F., &Sunyaev, A. (2019). Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. International Journal of Information Management, 48, 120-138.
21. Rajabion, L., Shaltooki, A. A., Taghikhah, M., Ghasemi, A., &Badfar, A. (2019). Healthcare big data processing mechanisms: The role of cloud computing. International Journal of Information Management, 49, 271-289.
22. Abdullah, T., & Jones, A. (2019, January). eHealth: challenges far integrating blockchain within healthcare. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 1-9). IEEE.

23. De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. ACM Computing Surveys (CSUR), 53(2), 1-27.
24. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., &Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, 104040.
25. Reddy, B., &Aithal, P. S. (2020). Blockchain as a disruptive technology in healthcare and financial services-A review based analysis on current implementations.
26. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.
27. Singh, A., Gupta, P., Lonare, R., Sharma, R. K., & Ghodichor, N. A. (2017). Data security in cloud computing. Int J Emerg Trends Eng Manag Res, 3(2), 1-5.
28. Altowaijri, S. M. (2020). An architecture to improve the security of cloud computing in the healthcare sector. Smart Infrastructure and Applications: Foundations for Smarter Cities and Societies, 249-266.
29. Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.
30. Leible, S., Schlager, S., Schubotz, M., &Gipp, B. (2019). A review on blockchain technology and blockchain projects fostering open science. Frontiers in Blockchain, 16.
31. Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. Applied Sciences, 11(20), 9372.
32. Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and transportation review, 142, 102067.
33. Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. Ieee Access, 9, 12730-12749.
34. Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. Applied Sciences, 11(20), 9372.
35. Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. Future generation computer systems, 95, 420-429.
36. Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, 146-158.
37. Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A systematic review on cloud storage mechanisms concerning e-healthcare systems. Sensors, 20(18), 5392.
38. Madanian, S., & Parry, D. (2019, August). IoT, cloud computing and big data: integrated framework for healthcare in disasters. In Medinfo (pp. 998-1002). International Medical Informatics Association (IMIA) and IOS Press.
39. Mrozek, D. (2020). A review of Cloud computing technologies for comprehensive microRNA analyses. Computational biology and chemistry, 88, 107365.
40. Al-Issa, Y., Ottom, M. A., &Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.

41. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.
42. Javaid, M., Haleem, A., Vaishya, R., Bahl, S., Suman, R., &Vaish, A. (2020). Industry 4.0 technologies and their applications in fighting COVID-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 14(4), 419-422.
43. Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, 146-158.