International Journal of AI, BigData, Computational and Management Studies
Noble Scholar Research Group | Volume 6, Issue 3, PP 26-31, 2025
ISSN: 3050-9416 | https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I3P104

Original Article

The Integration of Blockchain Technology to Enhance the Security of Healthcare Cloud Computing System

Syeda Hajira Kawsar
Independent Researcher, USA.

Received On: 25/05/2025 ***Revised On: 13/06/2025*** ***Accepted On: 26/06/2025*** ***Published On: 12/07/2025***

Abstract: *One area where cloud computing has transformed the field is in the healthcare aspect; it has been able to offer scalable, efficient, and cost-effective storage abilities for patient data. Nevertheless, as the concept of cloud computing is increasingly being utilized; the challenges when it comes to the safety and privacy of sensitive data are of much concern to healthcare institutions. An opportunity to resolve these issues may lie in Blockchain, which has decentralized, transparent, and immutable features. The present paper deals with the integration of blockchain technology into healthcare cloud computing systems; the discussion of the potential of blockchain technology to enhance security, preserve patient privacy, and enhance data integrity is provided. This paper, based on a literature review, addresses the possible advantages, obstacles, and future of using Blockchain in cloud computing in the healthcare field.*

Keywords: *Blockchain Technology, Healthcare Cloud Computing, Data Security, Cloud Security, Medical Data Privacy, Secure Data Sharing, Decentralized Systems, Health Information Management, Patient Data Protection, Interoperability, Cryptography, Access Control, Data Integrity, Healthcare IT, Privacy-Preserving Technologies.*

1. Introduction

Healthcare is becoming a particularly attractive field for cloud computing because of the enormous amount of sensitive data it holds about its patients, which it needs to store, manage, and analyze. Healthcare organizations should find that cloud computing offers scalable, affordable, and flexible services capable of processing everything, including electronic health records (EHRs), advanced medical imaging, and research data. The healthcare organizations that use cloud environments will enable sharing of data between the healthcare providers, provide greater operational efficiency, and offer more patient-focused services (Rayan et al., 2021). Nevertheless, the advantages of cloud computing are accompanied by tremendous problems, especially in the area of data security and patient privacy. Since healthcare institutions are retaining such sensitive data on cloud systems, major healthcare records, treatment history, diagnostic, and insurance are the most likely targets of cyberattacks. Healthcare-related data breaches are not simple and pose a high risk to the privacy of the patient, whose personal information can grievously hurt the concerned patient.

The Ponemon Institute (2020) also supports that healthcare data breaches have been on the rise in the last decade and makes specific reference to the shrinking number of breaches on cloud-based stores, showing the drawbacks of both centralized data storage. Such events illustrate the necessity of new methods of healthcare data protection. The best solution to these security issues is blockchain technology, which has a decentralized nature and an immutable ledger (Zou et al., 2021). Blockchain, through the use of cryptographic algorithms, eliminates the likelihood of data manipulation and alteration after being captured, and thus, it provides trust and transparency in the data management of healthcare information. In this paper, the problem addressed is the implementation of the blockchain technology in healthcare cloud-based computing to be deployed as a method of enhancing the security of patient data in healthcare, in addition to the protection of user privacy and ensuring the compliance with laws like the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe. By exploring this topic, this paper shall analyze the future opportunities, limitations, and future uses of blockchain technology in healthcare cloud systems.

2. Literature Review

2.1. Cloud Computing in Healthcare

Cloud computing has emerged as a disruptive technology within the health sector. The capacity to hold large patient records and retrieve them on demand has transformed the way health organizations maintain their medical files, diagnostic, patient history, and so on. The introduction of cloud computing in the healthcare sector permits scalable, flexible, and cost-effective solutions, which enable cooperation between healthcare providers and permit real-time decision-making. In

the healthcare industry, cloud solutions have helped institutions and organizations to increase efficiency within operations, streamline processes, and lessen the administrative workload. Cloud-based electronic health records (EHRs) are perhaps the most pertinent illustration of the applications of cloud computing in the medical field. EHRs enable healthcare caregivers to read the entire medical history of the patient, monitor the prescriptions, appointments, and even the billing procedures, all in a cloud-based system. Also, to obtain a more comprehensive picture of the health of a patient, it supports integrating healthcare data across multiple sources, including wearable devices, diagnostic imagery, and laboratory work.

The capacity to store and process data in the cloud also helps meet the increased demand in the sphere of telemedicine, which is gaining popularity since the COVID-19 pandemic. Cloud platforms may enable virtual consultation between healthcare practitioners and the patient, and thereby, healthcare services are being made more accessible, particularly to remote locations. Moreover, healthcare organizations can use cloud computing to gain access to a variety of advanced analytics tools and AI algorithms, which can support diagnosis and treatment planning and research. Nevertheless, as more healthcare organizations rely on the cloud when it comes to storing sensitive patient information and managing it using cloud-based systems, it is evident that several major security and privacy challenges will emerge. The aspect of a centralized system in cloud computing makes it questionable on the grounds of who owns the data and controls it, and whether this is accessible to other individuals through unauthorized means. The shared responsibility of cloud providers dictates that even though the cloud vendors might be handling the security of healthcare organizations' infrastructure, healthcare organizations must maintain the confidentiality, integrity, and availability of data stored in the cloud.

2.2. Security Challenges in Healthcare Cloud Computing

The technology poses risks to the security and privacy of data in healthcare, although the cloud computing system provides the sector with many advantages. The data about healthcare, such as medical records, personal information, and treatment histories, is very sensitive. In case of compromise, this information can result in devastating effects to both the patient and the healthcare organization, or even to society (Khan et al., 2022). Stolen health data may be used by cybercriminals to commit identity theft, insurance fraud, or other malicious acts. There is a threat to the breach of this type of sensitive information, which is also augmented by the increase in cloud-based services and an increase in complexity of the healthcare IT infrastructure. Among the major issues in cloud security is data breaches. According to a report released by the Ponemon Institute in 2020 about healthcare breaches of information, it was evident that the trend of breaches of information concerning cloud computing escalated. According to the report, cloud-based breaches achieved close to 30 percent of all healthcare data breaches that year, which was a reasonable percentage considering the variety of prospective attack vectors.

In addition, the costs of breaches to healthcare data are high, with the average cost of a healthcare data breach being more than 7 million dollars, as the 2021 Cost of a Data Breach report conducted by IBM illustrates. These are violations in most cases as a result of not having effective encryption and access controls in the healthcare organizations or misconfigured cloud settings that have revealed data to be accessed inappropriately. The other issue is data integrity. Clinicians depend on correct and real-time information in order to make critical decisions with regard to patient care. Misdiagnoses, ineffective treatment, and even death are possible when the data is corrupt or tampered with unintentionally or deliberately. It is essential that patient records are not tampered with or falsified because this will ensure that there is trust in healthcare systems. A conventional cloud storage system might not be sufficient to counteract these risks since the information can be accessed and amended by individuals with the necessary credentials, which could leave a path of unauthorized changes. The healthcare data also hinders cloud security through the regulatory environment in which it operates.

In the United States, there is HIPAA, and in the United Kingdom, GDPR has been in the European Union since 2018. Other national data protection laws must be observed. These rules oblige healthcare organizations to exercise close control over the gathering, storing, and sharing of patient information. Difficulty in meeting these specifications could become an issue in the decentralized cloud environment where data of particular patients can be located on different servers or even in different jurisdictions, imposing different legal jurisdictions. Another interest regarding healthcare cloud computing would be interoperability. Various healthcare facilities, organizations, and even nations might have adopted various cloud systems, and thus, the sharing of patients' records in a safe, harmonized, and comparable form may be a challenging topic. Interoperability is crucial to facilitate healthcare professionals' access to the latest information on the health of a patient; unless done, it is possible that care providers would err in diagnosis and care (Khanna et al., 2022). Moreover, the patient records can lack the security that they ought to have in the absence of adequate data exchange standards.

2.3. Blockchain Technology: A Promising Solution

Blockchain Technology has seen a lot of attention in various industries as a possible solution to most of the security and privacy issues that have been facing centralized information storage systems, including cloud computing in the health care industry. In essence, Blockchain is a decentralized and distributed ledger platform through which transactions on a series of computers are documented. Every transaction, or block, is connected to the next, forming a chain of immutable (but transparent) blocks (Zhang et al., 2022). This means that it

is almost impossible to change or modify any given data after it is added to the blockchain chain, hence high security and data integrity. The cryptography computations inherent in Blockchain make sure that data is encoded and retained in a manner in which the information is only accessible and adjustable by those with proper permission. The blockchain network is made up of participants, each of whom is identified using a unique cryptographic key, which is used in verification and authorizing transactions.

This has given it a safe, clear-cut way of ascertaining the authenticity of data, which makes Blockchain a suitable remedial method in overcoming the privacy and security issues in cloud computing in health care. The most important property of Blockchain is that it can be used to construct smart contracts. They are self-executable and deal with the agreement stipulations being directly coded into lines of code. Access to data can be automated through smart contracts in the healthcare sector. To illustrate, in a scenario where a healthcare provider requires access to the medical details of a patient, the smart contract would allow the latter to grant or deny access to the same, depending on who needs to see it, so that highly confidential information is not accessed by malicious parties. This decreases the possibility of the wrong people gaining access to the information and gives patients more control (of their data).

2.4. Applications of Blockchain in Healthcare Cloud Systems

Some of the possible advantages of integrating Blockchain in healthcare cloud systems are as follows. Among the main benefits is the increase in data protection. Through Blockchain, it is possible to save patients' data in a decentralized way with a decreased possibility of a single point of failure threat (Habib et al., 2022). A typical cloud system features the storage of the data on a central server, thus being subject to hacking and other types of unauthorized access. This risk is minimized by the decentralized structure of Blockchain, where the data is shared on several different nodes on the network. Blockchain also has the potential to enhance interoperability among various healthcare systems. Blockchain can help healthcare organizations to exchange patient information across various systems without breaking any security systems by offering a secure and standardized technology platform. To illustrate, the electronic health records (EHRs) can be exchanged in a secure manner, whereby they will be transferred between hospitals, clinics, and research institutions using blockchain technology, securing their safety and preventing them from being damaged or altered during the process (Amanat et al., 2022).

The management of patient consent is another area in which Blockchain may create an impact. Governing the consent of patients in the sharing of health data is a factor when it comes to healthcare privacy. Blockchain would make it possible to manage patient consent in a secure, decentralized, and transparent manner by allowing a transparent recording of consent-related transactions on a decentralized trustless ledger that cannot be altered (Awadallah et al., 2021). This would help guarantee that patients will have easy access to monitoring and managing their consent choices in real-time and have even more control over data utilization. A number of blockchain pilot projects in healthcare have already been successfully run. The MedRec project, created by the Massachusetts Institute of Technology (MIT), targets the ability to implement blockchain technology to establish a decentralized environment via which the EHRs would be managed. The system enables the patients to be in control of who has access to their medical records, and simultaneously, the healthcare providers have access to the information they require to provide care easily. The FHIRChain project uses Blockchain to enhance the HL7 Fast Healthcare Interoperability Resources (FHIR) standard to support data exchange in a secure way.

2.5. Challenges and Limitations of Blockchain in Healthcare

There are a number of issues that threaten the seamless incorporation of Blockchain in health cloud computing systems, despite the possible advantages (Samala & Rawas, 2024). Among the major drawbacks there is scalability. As blockchain networks grow, they may develop into sluggish and ineffective networks with an increase in transactions. This is especially worrying in the healthcare sector, where huge amounts of data are created day by day. With the increased scale of blockchain networks, they can encounter difficulties with handling huge real-time data created by healthcare providers and delays in accessing and processing data. Regulatory compliance is the other hurdle. Although Blockchain is more secure, it is not easy to be regulation-compliant, like the HIPAA and GDPR, because of its decentralized nature. According to these regulations, healthcare organizations also need to keep patient information under strict control; in other words, data should be kept in particular places and could be guarded by specific security measures.

The distributed ledger system operated by Blockchain across an array of nodes and across jurisdictions may hamper adherence to these regulations. Another obstacle is the incorporation of Blockchain into current healthcare systems (Samala & Rawas, 2024). Lots of healthcare organizations are supported by the legacy IT infrastructure, which is incompatible with Blockchain. It may be quite expensive and time-consuming to integrate Blockchain into such existing systems, which implies substantial investments in hardware and software. Also, it is possible to oppose the decision made by healthcare professionals and healthcare administrators who have no experience with blockchain technology and its possible advantages.

2.6. Conclusion

Through literature, it was found that cloud computing has changed healthcare by offering scalable, flexible, and affordable ways to manage patient data. It, however, also points out major security concerns, such as the occurrence of data breaches, data integrity, and regulatory provisions. The

development of blockchain technology presents an auspicious method of dealing with these issues, as blockchains create secure, decentralized, and unchangeable systems of storing and sharing information on healthcare. Blockchain could transform how healthcare organizations handle and secure patient data through better data security, enhanced interoperability, and the streamlining of patient consent management. Even though its use in the sphere implies some difficulties concerning scalability, regulatory compliance, and integration with existing systems, studies and pilot testing prove that Blockchain can be an essential tool in the safety maintenance of healthcare cloud-based systems in the future.

3. Blockchain Technology: Overview and Principles

The basic structure of blockchain technology is a distributed ledger used to provide high levels of security and transparency. Its technology started as a base technology for Bitcoin, but it has been used to cover a large scope of applications in many fields, including healthcare. In essence, Blockchain is a decentralized database that captures transaction history in an immutable and transparent way. As opposed to central systems in which one central party maintains the data, Blockchain works in a distributed system composed of nodes, each of which possesses the full ledger (Amanat et al., 2022). The advantage of this decentralized strategy is that it negates the existence of single points of failure and increases its resilience against cyberattacks. Blocks, chains, cryptographic hash functions, and consensus mechanisms are some of the main elements in the design of blockchain architecture. New blocks include a timestamp and transactional data, which are connected to the prior block to form a chain.

A block in a chain, once added to the chain, cannot be modified without modifying all blocks after that block, and as such, it is a tamper-proof blockchain. The transactions are validated using a consent mechanism such as Proof of Work (PoW) and Proof of Stake (PoS). All such mechanisms provide consensus on the network where each node agrees on the ledger status, and the integrity of data remains sustained. The main benefits of blockchain decentralization to healthcare are data security and privacy in an area where stored data, such as health records, needs to be impenetrable by external forces. Blockchain makes it harder to hack and access patient data since the information is not stored in an individual repository but is divided into several nodes. More so, Blockchain prevents the accessibility of sensitive health data to malicious users by guaranteeing the ability of authorized users to log onto the system using the right cryptographic keys and an extra security level.

3.1. Security Challenges in Healthcare Cloud Computing

The numerous security accidents that result in various threats to a healthcare organization when operating in cloud computing systems occur during the storage and management of patient data. Healthcare data is an issue of concern and safety since it is sensitive information. The concerns around healthcare cloud security are data breaches, compromises on data integrity, unauthorized access, and failure to comply with regulatory requirements. Data breaches are one of the most burning security problems. In 2020, the healthcare sector experienced a record increase in the number of cyberattacks, and cloud computing systems are a primary target in that case. Medical records, social security numbers, and insurance information are sensitive information that is of value to cybercriminals, which explains why healthcare organizations are lucrative targets (Samala & Rawas, 2024). According to the Ponemon Institute (2020), close to 30% of the 2020 healthcare data breaches were those that relied on cloud-based systems, which is a considerable amount, pointing to the weakness of centralized systems on the cloud.

The other important factor is data integrity. Healthcare information should be transparent and valid in order to provide efficient care to the patients. When providers are unable to trust the information upon which they are relying, the results can be dire, resulting in misdiagnoses, wrong methods of treating, and could even causing injuries to patients. By its nature, Blockchain ensures the immutability of data and the presence of a secure, verifiable audit trail, which ensures that the information regarding healthcare, once saved, cannot be tampered with (Samala & Rawas, 2024). Another struggle is adherence to compliance standards, such as the HIPAA and GDPR. Medical institutions must observe very high standards of privacy and data security, but it is not easy to ensure these due to the distributed and decentralized nature of blockchain actions. Nevertheless, the lack of integrity of patient data can be addressed by such blockchain properties as transparency and traceability, thus providing safer access control and audibility.

4. Integration of Blockchain in Healthcare Cloud Systems

4.1. Secure Data Sharing

The secure and transparent sharing of data is one of the main ways in which Blockchain can be used in healthcare. Some ineffective data sharing may be cumbersome and insecure in the traditional cloud systems with healthcare providers. The information about the patients is commonly kept in siloed databases, which causes inefficiencies and the jeopardy of uncontrolled access. Blockchain enables blockchain-based information sharing between various healthcare entities in a way that data sharing is safe and uses smart contracts to automate consent and data access restrictions (Albshaier et al., 2024). Smart contracts are contracts that run automatically, and the code that runs them has the terms of agreement coded. To illustrate, a patient may authorize a medical provider to view his/her medical records, and the Blockchain will administer and revise the privileges of access

transparently and automatically without the need for any human touch. This increases security and efficiency.

4.2. Consent Management

Consent issued by the patient is the most important component of data management in the field of healthcare. Patients should be able to limit access to their medical information, and the process of regulating this permission of patients is inconvenient and allows people to make mistakes. Blockchain enables the establishment of a verifiable, transparent, and unchanging record of patient consent (Samala & Rawas, 2024). Patients can make informed decisions about whether to share their data or to remove it with the use of Blockchain, and the sharing and withdrawal of such information is automatically updated across all the relevant systems. The connection to Blockchain-based systems of managing consent would place the power regarding their health data into the hands of a patient and, at the same time, mean that the healthcare professionals will have to comply with the privacy laws.

4.3. Audit Trails and Data Provenance

The transparency and immutability aspect of Blockchain provides the best option for providing secure audit trails of healthcare systems. An immutable ledger enables each of its transactions, such as data access requests or changes to patient records, to be recorded in a way that is not subject to change. The information in these audit trails ensures data integrity is maintained because it is possible to verify who accessed the data, when, and for which purpose (Samala & Rawas, 2024). Another benefit of Blockchain is that it can also keep track of data provenance--i.e., the history of a piece of data so that healthcare workers can track the ancestry of any medical record or the results of a test. The said degree of transparency not only increases security but also aids healthcare organizations in achieving compliance with their data accessibility.

4.4. Interoperability

Interoperability has also been a big issue in healthcare, especially in the sharing of patient details amongst medical practitioners, laboratories, insurance companies, and other stakeholders. The decentralized characteristic of Blockchain provides a common standard for exchanging healthcare data across different systems to make the data reliable and not subject to tampering (Samala & Rawas, 2024). Through Blockchain, hospitals or healthcare organizations can develop a standardized, interoperable, safe sharing of patient data where information is current, precise, and available across any system.

4.5. Case Studies and Applications

There are case studies that point to the prospects of Blockchain to enhance the data security of healthcare. Meanwhile, the MedRec project has been created at MIT to handle the health records of a patient using blockchain technology so that the patient can determine who can access patient data, and a healthcare provider can also obtain necessary information efficiently and safely. Likewise, the FHIRChain project is an implementation of the Blockchain and HL7 Fast Healthcare interoperability resources (FHIR) standard so that secure and interoperable data sharing could occur between healthcare systems. These projects reflect the fact that Blockchain can be utilized to decrease the amount of time it takes to share data, as well as deploy more layers of security and assist patients. At the same time, they also highlight the technical and regulatory issues that need to be resolved prior to Blockchain's universal application in a healthcare system.

4.6. Challenges and Limitations

As much as Blockchain has numerous advantages, it also has a number of issues when it comes to the incorporation of technology in healthcare cloud systems. Issues of scalability are also pertinent because a blockchain system might not support huge volumes of data that arise within healthcare systems. To process an increasing number of patient data without compromising the performance of the actions entailed, healthcare organizations must ensure that blockchain solutions can scale accordingly. The other hurdle is to adhere to the rules. The decentralized nature of Blockchain may be a challenge when it comes to compliance with privacy regulations, particularly HIPAA and GDPR, as its data must be stored and processed in particular manners. The international character of Blockchain presents another problem: making sure that healthcare organizations adhere to local regulations concerning data security. In addition, it is expensive and time-consuming to incorporate Blockchain within the current healthcare systems. Most healthcare organizations have not moved to a newer IT infrastructure and, as such, may not accommodate blockchain technology. These obstacles will need to be addressed through extensive investment in development as well as an investment in training.

4.7. Future Prospects and Recommendations

Nevertheless, Blockchain and healthcare look bright in the future. The innovation of blockchain technology is taking new forms as the scalability, interoperability, and compliance of the technology will present its mainstream adoption in the healthcare cloud systems. Healthcare organizations ought to prioritize establishing blockchain solutions that are capable of large-scale processing of the growing patients' data without jeopardizing or undermining the security and functionality. Partnerships with regulatory organizations will also be important to ensure that the blockchain solutions do not contravene current privacy and regulations. Clinics and healthcare providers should also invest in training and educating the staff so that they know the advantages and disadvantages of blockchain technology. More studies and pilot programs would provide a better understanding of what Blockchain can offer to the healthcare industry. Such projects will contribute to the identification of best practices, the

improvement of blockchain solutions, and finding solutions to the existing technical and regulatory dilemma.

5. Conclusion

Use of blockchain technology in healthcare cloud computing systems promises to solve the most critical security and privacy issues in the health industry. The decentralized and immutable ledger provided by Blockchain presents a safe, transparent, and efficient method to provide trustworthiness on patient data, prevent unauthorized access, and improve how data is shared by healthcare providers. The introduction of Blockchain enables healthcare organizations to ensure increased safety of their data, better patient consent tracking, and compliance with privacy regulations like HIPAA and GDPR. However, the use of Blockchain in healthcare is still not easy because of challenges such as scalability, regulatory issues, and even the integration of Blockchain with legacy systems. Nevertheless, there are still continuous studies and pilot programs that prove Blockchain can transform the way healthcare information is handled. With the advances of blockchain technology, healthcare organizations are required to work on scalable systems, collaborate with regulators, and educate stakeholders to fully access the benefits of Blockchain on the security and interoperability of healthcare cloud systems.

References

1. Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A review of security issues when integrating IoT with cloud computing and Blockchain. *IEEE Access*.
2. Amanat, A., Rizwan, M., Maple, C., Zikria, Y. B., Almadhor, A. S., & Kim, S. W. (2022). Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. *Frontiers in Public Health*, *10*, 938707.
3. Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on Blockchain. *IEEE Access*, *9*, 69513-69526.
4. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*, *14*(11), 341.
5. Khan, A. I., ALGhamdi, A. S. A. M., Alsolami, F. J., Abushark, Y. B., Almalawi, A., Ali, A. M., ... & Khan, R. A. (2022). Integrating blockchain technology into healthcare through an intelligent computing technique. *Computers, Materials & Continua*, *70*(2), 2835-2860.
6. Khanna, A., Sah, A., Bolshev, V., Burgio, A., Panchenko, V., & Jasiński, M. (2022). Blockchain–cloud integration: A survey. *Sensors*, *22*(14), 5238.
7. Rayan, R. A., Zafar, I., & Tsagkari, C. (2021). Blockchain technology for healthcare, cloud-based data privacy and security. In *Integration of WSNs into Internet of Things* (pp. 335-349). CRC Press.
8. Samala, A. D., & Rawas, S. (2024). Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability. *International Journal of Online & Biomedical Engineering*, *20*(2).
9. Zhang, G., Yang, Z., & Liu, W. (2022). Blockchain-based privacy-preserving e-health system for healthcare data in the cloud. *Computer Networks*, *203*, 108586.
10. Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2021). Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. *ACM Computing Surveys (CSUR)*, *54*(8), 1-36.
11. Bibi, N., Khan, M., Khan, S., Noor, S., Alqahtani, S. A., Ali, A., & Iqbal, N. (2024). Sequence-Based intelligent model for identification of tumor t cell antigens using fusion features. *IEEE Access*.
12. Nair, S. S., & Lakshmikanthan, G. (2024). Digital Identity Architecture for Autonomous Mobility: A Blockchain and Federation Approach. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(2), 25-36. https://doi.org/10.63282/49s0p265