JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(3), 2074-2086
ISSN: 2589-1316

Enhancing Healthcare Data Security and Transparency with Blockchain Technology at a Tshwane Hospital in South Africa

Philisiwe Christina Msibi[1], Tsakani Violet Ndobe[2], Solly Matshonisa Seeletse[3*]

[1]*Department of Computer Science and Information Technology Department, Sefako Makgatho Health Science University, Pretoria, South Africa*
[2]*Department of Statistical Sciences, Sefako Makgatho Health Science University, Pretoria, South Africa,*
[3]*Solly Matshonisa Seeletse, Department of Statistical Sciences, Sefako Makgatho Health Science University, Pretoria, South Africa, solly.seeletse@smu.ac.za*

*__Corresponding Author:__ solly.seeletse@smu.ac.za

Citation: Msibi, P. C., Ndobe, T. V., & Seeletse, S. M. (2025). Enhancing Healthcare Data Security and Transparency with Blockchain Technology at a Tshwane Hospital in South Africa. *Journal of Cultural Analysis and Social Change*, *10*(3), 2074–2086. https://doi.org/10.64753/jcasc.v10i3.2712

Published: December 02, 2025

ABSTRACT

In South Africa, the healthcare sector experiences significant challenges in data management, such as data silos, interoperability issues, and concerns over data security and privacy. These inadequacies impede effective care delivery and erode patient trust. Despite advancements in healthcare technology, the risk of data breaches and compromised patient data remains a pressing concern. Blockchain technology has emerged as a promising solution to address these challenges by providing a decentralized, secure, and transparent platform for managing healthcare data. This study aims to investigate the potential of blockchain technology to enhance healthcare data management at a hospital in Tshwane, South Africa. The focus is on improving security, transparency, and efficiency in data management. A qualitative research methodology was employed, involving surveys of healthcare professionals. The qualitative questions were presented through a tool on Likert scale and statistical methods were used for data analysis. The surveys assessed current data management issues, explored blockchain's potential benefits, and identified key system requirements. The results highlighted data security, system inefficiencies, and interoperability as the most pressing challenges. Blockchain's ability to enhance data security and management efficiency was highly valued. Essential features for blockchain implementation included data integrity, secure data sharing, regulatory compliance, and ease of integration with existing systems. The study concludes that blockchain technology could significantly improve healthcare data management by addressing security and interoperability issues. However, challenges such as system integration and implementation costs should be addressed. Recommendations for healthcare organizations include prioritizing data security, simplifying technology complexity, and nurturing transparency through blockchain adoption. Blockchain can enhance patient trust and improve the efficiency of healthcare services by addressing these challenges.

Keywords: Blockchain Technology, Data Transparency, Decentralized Systems, Healthcare Data Security, Healthcare Management, Interoperability.

INTRODUCTION

The healthcare sector of South Africa faces significant challenges in data management, which include data silos, interoperability gaps, and concerns over data security and privacy. These inefficiencies impede the effective delivery of healthcare services and jeopardize patient trust and data integrity. Ahanger *et al.* (2024) decry the ruined condition of healthcare data storage systems that aggravates these issues. It creates barriers to seamless data sharing and increases the risk of errors in patient care. Furthermore, Ewoh and Vartiainen (2024) accentuate that medical

records, due to their sensitive content, are particularly vulnerable to cyberattacks. This could lead to unauthorised access and misuse of patient data.

The arrival of blockchain technology seems to present optimism towards addressing these challenges by offering a decentralized, secure, and transparent platform for healthcare data management (Abraha, 2025). Blockchain technologies were initially developed to support cryptocurrencies. However, blockchain applications have expanded into various sectors, including healthcare. Its decentralized nature ensures that no single entity has control over all the data, and therefore enhances both security and transparency (Ahmed, 2025). Blockchain's ability to securely share data, maintain data integrity, and protect patient privacy makes it a valuable tool in addressing the current inefficiencies and trust issues within healthcare data management.

A significant problem in healthcare data management is the presence of data silos, where patient information is stored in separate systems. This makes it difficult for healthcare providers to access and share crucial data (Eun-Mee, 2025). According to Torab-Miandoab *et al.* (2023), this division results in a lack of interoperability, complicating care coordination and increasing the likelihood of errors. Additionally, the centralized nature of traditional data storage systems poses a significant risk of single points of failure. This, coincidentally, can be mitigated by blockchain's decentralized architecture (Borycki & Kushniruk, 2022).

Data security and privacy concerns are also paramount in the healthcare sector. Medical records are highly sought after by cyber attackers due to their sensitive nature. Unauthorised breaches can lead to the misuse of patient information, further eroding trust in the healthcare system (Alhasan, 2025). Blockchain technology, with its distributed ledger system, offers a robust solution to these challenges. According to Karthikeyan *et al.* (2025), blockchain cryptographic methods play a crucial role in ensuring data integrity and immutability, thereby preserving the accuracy of medical records.

Moreover, blockchain's transparency enhances trust among stakeholders by providing a clear audit trail of all transactions, accessible to authorized participants. This level of transparency is particularly beneficial in healthcare, where trust in the accuracy and security of information is critical (Oriekhoe *et al.*, 2024). However, despite the growing interest in blockchain technology, its application in healthcare data management, particularly in the South African context, remains underexplored. This research seeks to address this gap by evaluating the potential of blockchain technology to enhance healthcare data security and transparency at a hospital in Tshwane, South Africa.

In the digital age, healthcare data management faces major challenges, including data silos, interoperability issues, and heightened security and privacy concerns (Saberi *et al.*, 2025). These problems lead to inefficiencies in care delivery and threaten patient trust. According to Ahanger *et al.* (2024), the fragmented nature of data storage systems exacerbates these issues, increasing error risks and hindering seamless data sharing. Blockchain technology, initially developed for cryptocurrencies, offers a promising solution by providing a decentralized, secure, and transparent platform for managing healthcare data (Attaran *et al.*, 2022). Its ability to prevent single points of failure, ensure data integrity through cryptographic methods, and maintain a clear audit trail enhances both security and transparency (Gao *et al.*, 2025). Although blockchain's potential in healthcare, especially in regions such as Tshwane, South Africa, is still being explored. It presents a valuable tool for addressing current data management inefficiencies and improving trust in the healthcare system (Duan & Zhu, 2024).

The purpose of this study was to address the inefficiencies, inequalities, and trust challenges in implementing blockchain technology for secure and transparent healthcare data management. The objectives were: to identify and assess existing challenges and inefficiencies in healthcare data management (such as data silos, lack of interoperability, and issues with data security and privacy); to evaluate the potential of blockchain technology to address these challenges and improve the security, transparency, and efficiency of healthcare data management and to identify the key features and requirements of a blockchain-based healthcare data management system that can ensure data integrity, patient privacy, and secure data sharing among stakeholders.

A Global Perspective of Challenges in Healthcare Data Management

Healthcare data management is critical to the effective functioning of healthcare systems, yet it is often hindered by inefficiencies, data silos, and security concerns, especially in developing countries. These challenges result in fragmented care, compromised patient safety, and a lack of trust in the system (Asamani *et al.*, 2021, Love-Koh *et al.*, 2020). While developed nations, such as the United States and countries in Europe, have made progress in addressing these issues through advanced technologies (Pandey *et al.*, 2022), Gwala and Mashau (2024) complain that many regions, particularly Sub-Saharan Africa and parts of North Africa, continue to struggle with data breaches, privacy issues, and poor interoperability. Gesicho *et al.* (2020) illustrates the ongoing challenges in East African countries such as Kenya and Tanzania, where healthcare data systems continue to suffer from fragmented infrastructure and limited progress in digitalization efforts.

Blockchain technology offers a promising solution to these challenges by providing a secure, transparent, and decentralized method for managing healthcare data. Its ability to enhance data integrity, ensure patient privacy, and

improve system interoperability makes it an attractive option for healthcare systems, particularly in resource-limited settings (Saberi *et al.*, 2025).

Challenges in Healthcare Data Management

The current landscape of healthcare data management is marked by significant challenges that impede the efficient delivery of healthcare services. Data silos, which occur when information is isolated within different departments or systems, present a major barrier to effective care coordination (Raghupathi & Raghupathi, 2014). According to Sowada (2025), the lack of interoperability between different Electronic Health Record (EHR) systems exacerbates this issue, leading to fragmented patient care and increased risk of medical errors. In developing countries, these challenges are particularly pronounced due to limited resources and inadequate healthcare infrastructure (Mabina *et al.*, 2025). Data security and privacy concerns are also prevalent, with many healthcare systems lacking robust mechanisms to protect sensitive patient information from breaches and unauthorized access (Manikandan *et al.*, 2025). These issues compromise the integrity of healthcare data and also erode the trust that patients place in the healthcare system.

Inequities and Trust Issues in Healthcare Data Management

Inequalities in healthcare data management are closely linked to disparities in resource allocation and access to healthcare services. According to Mbunge *et al.* (2022), in regions where healthcare systems are under-resourced, patients often face significant barriers to receiving quality care, partly due to the inefficiencies in data management systems. These inequities are further exacerbated by the lack of transparency in data handling practices, which can lead to mistrust between patients and healthcare providers (Prasai *et al.*, 2025).

In developed countries, efforts to improve healthcare data management through advanced technologies have helped to mitigate some of these concerns (Pandey *et al.*, 2022). For instance, the implementation of secure EHR systems with enhanced interoperability has improved the accuracy and accessibility of patient information, thereby increasing patient trust in the healthcare system. However, even in these contexts, challenges related to data security and privacy persist, highlighting the need for more effective solutions.

Blockchain Technology as a Solution

Blockchain technology offers a promising solution to the challenges experienced in healthcare data management. Islam and Apu (2024) explain that by providing a decentralized and immutable ledger, blockchain can significantly enhance the security and transparency of healthcare data. According to Roopesh (2024), blockchain technology ensures that all transactions are recorded in a transparent and tamper-proof manner, reducing the risk of data breaches and unauthorised access. Moreover, blockchain can address the issue of data silos by enabling seamless data sharing across different healthcare providers. This interoperability can improve the coordination of care and reduce the likelihood of medical errors, thereby enhancing the overall efficiency of healthcare systems (Elsangidy *et al.*, 2025). Additionally, Adeghe *et al.* (2024) point out that blockchain's ability to secure patient data while maintaining privacy is crucial for building trust among stakeholders in the healthcare system.

Key features of Blockchain-based Healthcare Data Management systems

For blockchain technology to be effectively implemented in healthcare, it must incorporate key features that ensure data integrity, patient privacy, and secure data sharing. According to Mohanty *et al.* (2025), robust encryption protocols, smart contracts, and permissioned access are essential components of a blockchain-based healthcare data management system. These features protect sensitive patient information and ensure that only authorized individuals can access specific data, thereby maintaining patient confidentiality (Thakur *et al.*, 2025). In addition to these technical features, the successful implementation of blockchain in healthcare requires a supportive regulatory framework. Clear guidelines on data ownership, consent, and compliance are necessary to ensure that blockchain solutions align with legal and ethical standards (Verma & Yadav, 2025). This is particularly important in developing countries, where healthcare systems may be less equipped to handle the complexities of blockchain technology.

Novelty of this Paper

This study is novel as it applies blockchain technology to address specific challenges in healthcare data management within a localized South African context (Hamunakwadi et al., 2025). Blockchain's decentralized and immutable architecture offers transformative solutions to critical issues such as data security, patient privacy, and operational transparency. According to Thriveni et al. (2025), these are particularly pressing in regions with fragmented healthcare systems. The study leverages blockchain's ability to provide secure, tamper-proof records

to enhance trust between patients and providers while empowering patients with control over their health data. Furthermore, incorporating blockchain in supply chain management can ensure traceability and authenticity of medical products, addressing fraud and inefficiencies. In Chakraborty et al.'s (2025) viewpoint, this localized application could contribute to global discussions on blockchain's potential in healthcare while emphasizing its adaptability to unique challenges experienced by hospitals in developing nations.

MATERIALS AND METHODS

Study Design: This was qualitative research to investigate how blockchain technology can enhance healthcare data management by addressing inefficiencies, inequalities, and trust challenges. Data were collected through a structured survey administered via a Google Form, targeting healthcare professionals at a hospital in Tshwane, South Africa. This approach helps determine how blockchain technology can be leveraged to significantly improve healthcare data management systems (Al-Khasawneh *et al.*, 2024).

Population: The target population consisted of healthcare professionals working at a hospital in Tshwane, South Africa. They included individuals from various departments such as administration, clinical care, IT/Health Informatics, and research.

Sample Size: A small sample is required for qualitative studies, and if saturation is used, the sample size could be anything between three and six (Braun & Clarke, 2021). However, the guideline was reached when face-to-face interviews were used. In this study, Google Forms was the approach and n = 32 sample size was used. This was because the qualitative questions were addressed in a Likert scale form and therefore made closed ended.

Reliability, Validity, and Objectivity: This study ensured reliability and validity through a structured data collection process complemented by meticulous documentation. Purposive sampling enabled to capture a diverse range of perspectives. A critical reader checked the accuracy of participant responses. Objectivity was upheld by practicing reflexivity, documented potential biases, and maintained transparent reporting throughout the research process.

Ethical considerations: The ethical protocols of the hospital were observed, which include privacy, confidentiality and honesty.

Analysis: The following results were obtained from the individuals, who participated in the study in which n = 32 participants were involved. The next demographic visual display indicates the different occupations of these participants.

Table/Figure Combo 1. Occupations of participants.

Table 1. Occupations of participants (in number)

Occupation	Frequency	Percentage
Doctor	5	15.6
Nurse	4	12.5
Administrator	3	9.4
IT/Health Informatics Specialist	10	31.3
Researcher	3	9.4
Other	7	21.9

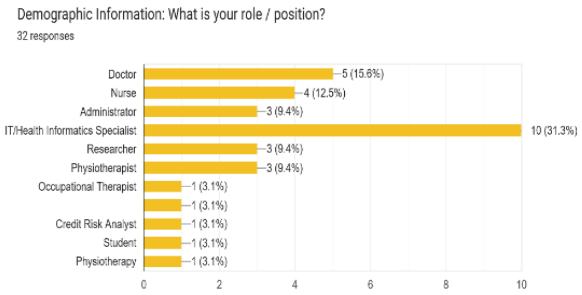

Figure 1. Occupations of participants (in percentages).

The display shows that IT/Health Informatics Specialists are the most common at 31.3%, followed by "Other" at 21.9%. Doctors (15.6%) and nurses (12.5%) were not highly prevalent. Administrators (9.4%) and researchers (9.4%) were fewest. The graph visually represents these percentages, likely as a bar or pie chart, allowing for an immediate understanding of the distribution. This dual presentation enables readers to quickly grasp both the specific numbers and relative proportions of each occupation, offering a clear overview of participant demographics (Bozkurt & Gursoy, 2025). The next display gives divisions in which the participants were deployed.

Table/Figure Combo 2. Departments of participants.

Table 2. Departments of participants.

Department	Frequency	Percentage
Emergency	2	6.3
Outpatient	6	18.8
Inpatient	6	18.8
Administration	4	12.5
IT/Health Informatics Specialist	8	25
Researcher	3	9.4
Other	3	9.4

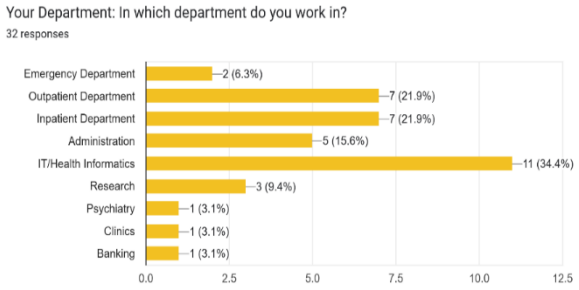

Figure 2. Departments of participants (in percentages).

The data presented above provide insights into the distribution of participants across different departments. The IT/Health Informatics Specialist department has the highest representation, with 8 (25%) participants of the total. The Outpatient and Inpatient departments each have 6 (18.8%) participants. Administration and Other departments each have smaller representations, with 4 (12.5%) and 3 (9.4%) participants respectively. The Emergency department has the least representation with only 2 (6.3%). Researchers also account for 3 (9.4%) participants. The distribution highlights a strong presence of IT and health informatics specialists among the participants. This aligns with Alhur and Aldosari (2024) who consider IT and health informatics as vital components when blockchain is implemented. The next visual display shows the level of participants' familiarity with blockchain.

Table/Figure Combo 3. Participants' familiarity with blockchain.

Table 3. Blockchain familiarity (in number)

Familiarity level	Frequency	Percentage
Very familiar	5	15.7
Somewhat familiar	4	12.5
Not familiar	3	9.4

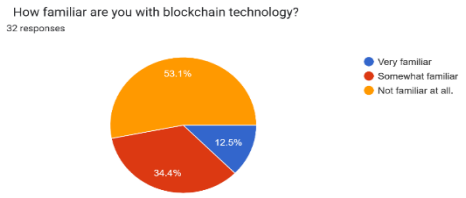

Figure 3. Blockchain familiarity (in percentages)

This display provides insights into the level of familiarity with blockchain technology among the respondents. It expresses that out of the total 32 respondents, 5 (15.7%) are very familiar with blockchain, 4 (12.5%) are somewhat familiar, and 3 (9.4%) are not familiar. This suggests that a significant portion of the respondents have some level of familiarity with blockchain, with the majority being either very or somewhat familiar. However, there is no information on the remaining respondents to offer a more comprehensive understanding of the overall familiarity levels. Nonetheless, the data indicates that blockchain awareness is present, albeit with varying degrees of familiarity among the respondents. The next visual display explains the benefits of blockchain in healthcare management. The question posed was, "Did you think blockchain technology could be beneficial for healthcare data management?"

Table/Figure Combo 4. Awareness of benefits of blockchain in healthcare management

Table 4. Awareness of blockchain benefits in healthcare.

Benefits awareness	Frequency	Percentage
Yes	24	75
No	8	25
Not sure	0	0

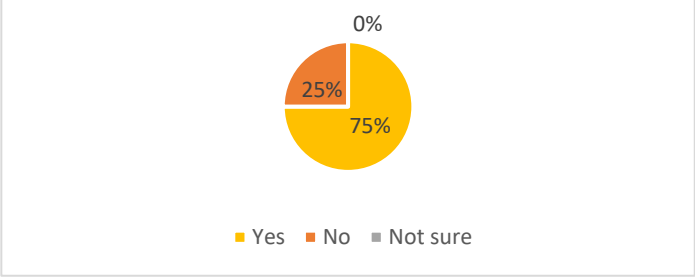

Figure 4. Awareness of blockchain benefits (in percentages)

These displays highlight the awareness of blockchain benefits in healthcare among respondents. According to Table 4, 75% of participants (24 individuals) were aware of the benefits of blockchain technology in healthcare, while 25% (8 individuals) were not aware, and none expressed uncertainty. Figure 4 visually reinforces this distribution, showing that three-quarters of respondents recognize blockchain's advantages, such as improved data

security, enhanced communication, and streamlined processes. These results emphasize a significant level of awareness among respondents, suggesting potential receptivity to blockchain adoption in healthcare systems. The next visual display explains challenges in healthcare management. The question was, "What were the main challenges in the current in healthcare data management system?"

Table/Figure Combo 5. Challenges in healthcare management.

Table 5. Healthcare challenges

Challenges	Frequency	Percentage
Data silos	6	18.8
Lack of interoperability	6	18.8
Data security issues	8	25
Privacy concerns	5	15.6
Inefficiencies in data handling	7	21.9

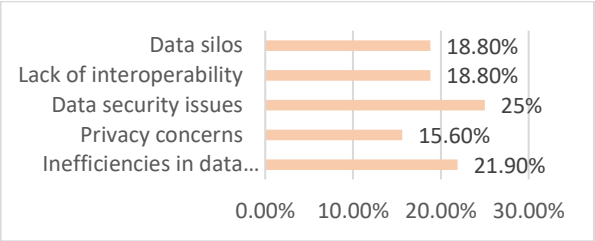

Figure 5. Healthcare challenges (in percentages)

Table 5 highlights key challenges in healthcare data management, emphasizing issues such as data security (25%), inefficiencies in data handling (21.9%), and data silos and lack of interoperability (each at 18.8%). These challenges stem from fragmented systems, inadequate integration, and the exponential growth of healthcare data, which complicates seamless information exchange and decision-making (Almadani et al., 2025; Awrahman et al., 2022; Sagili, 2024). Privacy concerns (15.6%) further exacerbate the situation, as sensitive health information should be protected from breaches while ensuring accessibility for care providers (Goyal & Malviya, 2023). Margam (2023) explains that addressing these challenges requires robust solutions such as improved interoperability standards, advanced analytics, and secure data-sharing platforms to enhance efficiency and patient outcomes. The next visual identifies those considered by the participants as the most critical challenges in healthcare management. The question was, "Which of these do you regards as the most critical of the challenges in the current in healthcare data management system?"

Table/Figure Combo 6. Most critical challenges in healthcare management.

Table 6. Healthcare challenges.

Most critical challenges	Frequency	Percentage
Data security	5	15.7
Data privacy	4	12.5
System inefficiencies	3	9.4
Interoperability issues	10	31.3

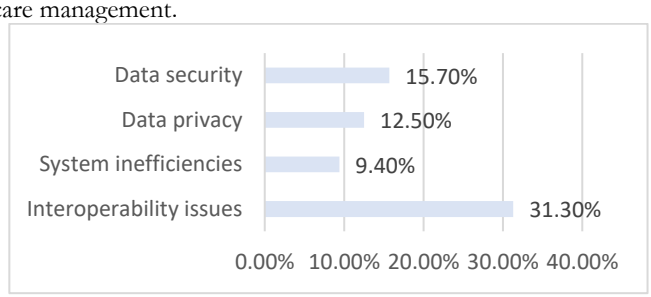

Figure 6. Most critical challenges (in percentages).

The critical challenges in healthcare systems, as highlighted in the above display, emphasize interoperability issues as the most significant concern, accounting for 31.3% of the identified challenges. According to Jain et al. (2025), this reflects the difficulty in achieving seamless data exchange across different healthcare systems. This can also delay patient care and inflate costs (Bayya, 2025). Figure 6 also shows that data security (15.7%) and data privacy (12.5%) follow as major concerns. These emphasize the risks of unauthorized access and breaches in sensitive patient information (Snigdha et al., 2025), especially with the growing reliance on digital health technologies. System inefficiencies are also notable at 9.4%, pointing to operational hurdles that can delay or complicate healthcare delivery. These challenges collectively highlight the pressing need for robust solutions to ensure secure, efficient, and interoperable healthcare systems. The next visual deals with benefits considered to be most appealing in blockchain. The question was, "What potential benefits of blockchain technology in healthcare data management are most appealing to you?"

Table/Figure Combo 7. Most appealing potential benefits of blockchain.

Table 7: Most appealing potential blockchain benefit

Benefits	Frequency	Percentage
Enhanced data security	10	31.3
Improved transparency	5	15.7
Improved data management efficiency	11	34.4
Secure data sharing	6	18.8

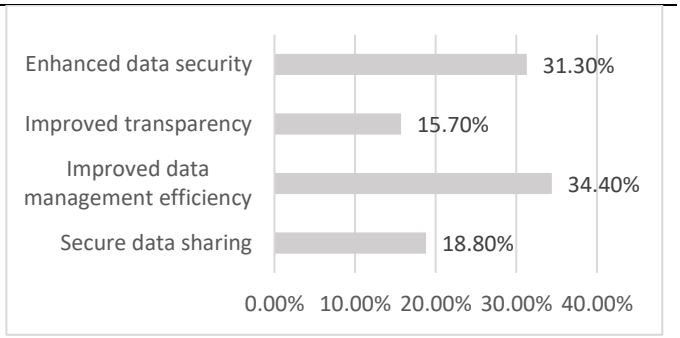

Figure 7. Most appealing potential blockchain benefits (in percentages).

The data presented in Table 7/Figure 7 highlights some appealing potential benefits of blockchain technology. Among the surveyed respondents, improved data management efficiency was the most frequently cited benefit, with 11 mentions, accounting for 34.4% of the responses. Enhanced data security was the second most popular benefit, noted by 10 respondents, which equates to 31.3%. Other notable benefits included secure data sharing (18.8%) and improved transparency (15.7%). These figures confirm that the primary appeal of blockchain lies in its ability to streamline data management processes and enhance security (Kukman & Gričar, 2025). Patil et al. (2025) concur that these are necessary for organizations that seek to leverage blockchain technology effectively. The next visual presented concerns regarding implementation of blockchain technology. The question was, "What concerns do you have regarding implementation of blockchain technology?"

Table/Figure Combo 8. Concerns regarding blockchain technology.

Table 8. Concerns regarding implementing blockchain technology

Concerns	Frequency	Percentage
Cost of Implementation	8	25
Complexity of the Technology	10	31.3
Integration with existing systems	9	28.1
Data Privacy Issues	4	12.5
Other	1	3.1

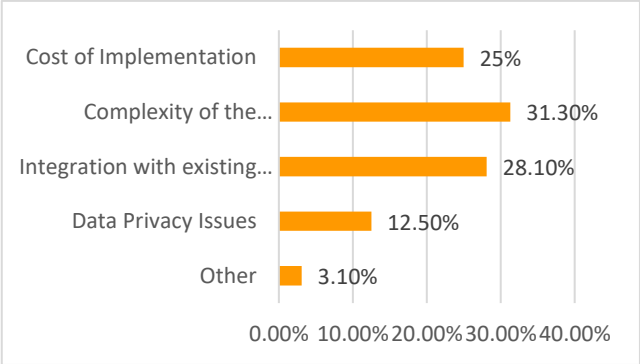

Figure 8. Concerns regarding implementing blockchain technology (in percentages).

The implementation of blockchain technology raises several concerns, as highlighted in Table 8/Figure 8. The most significant concern is the complexity of the technology, with 10 (31.3%) of respondents citing this as a major issue. Integration with existing systems is another significant challenge, affecting 9 (28.1%) of respondents. The cost of implementation is also a considerable concern, affecting 8 (25%) of respondents. Data privacy issues are a concern for 12.5% of respondents, while other miscellaneous concerns account for one (3.1%). These findings suggest that while blockchain offers promising solutions (Khawaldeh et al., 2025). However, Al Senani and Masengu (2025) as well as Alabdali et al. (2025) point out that blockchain adoption is impeded by technological, financial, and systemic barriers that need to be addressed for successful integration. The next visual explain features perceived to be essential for blockchain-based data management system. The question was, "Which features do you think are essential for blockchain-based data management system?"

Table/Figure Combo 9. Features perceived to be essential for blockchain system.

Table 9: Features perceived essential for blockchain system

Concerns	Frequency	Percentage
Data Integrity	9	28.1
Secure data sharing	5	15.7
Easy integration with current systems	6	18.8
User-Friendly interface	6	18.8
Compliance with data protection regulations	6	18.8

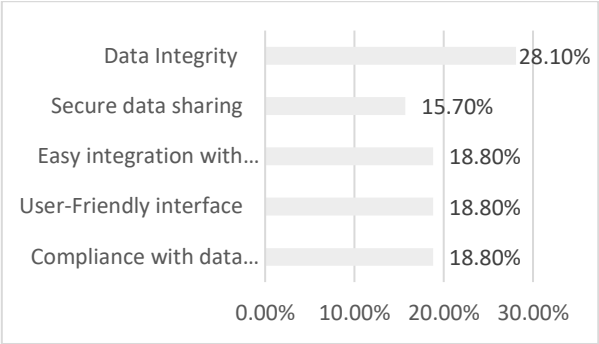

Figure 9. Features perceived essential for blockchain system (in percentages).

Table 9/Figure 9 highlights the essential features perceived necessary for a blockchain system. The most critical feature is *Data Integrity*, with 9 (28.1%) of respondents identifying it as crucial. This is an emphasis on the importance of maintaining accurate and reliable data within blockchain networks (Ahmed, 2025). Other significant features include *Compliance with data protection regulations*, *Easy integration with current systems*, and *User-Friendly interface*, each noted by 6 (18.8%) of respondents. *Secure data sharing* is also important, though less emphasized, with 5 (15.7%) of the responses. These findings suggest that security and compliance are vital (Song et al., 2025). On the other hand, Almutairi (2025) argue that usability and integration are equally important for the successful implementation of blockchain systems. The next visual explains perceived importance of data security. The question was, "How important is it to ensure data integrity in your data management system?"

Table/Figure Combo 10. Perceived importance of data security

Table 10. Perceived importance of data security

Perceived importance level	Frequency	Percentage
Very important	22	68.8%
Important	8	25%
Somewhat important	2	6.3%
Not important	0	0%

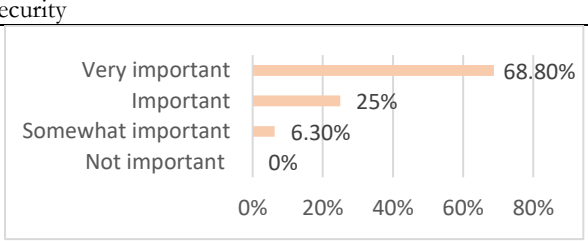

Figure 10. Perceived importance of data security (in percentages).

Table 10/Figure 10 features the perceived importance of data security among respondents. A significant majority of respondents, 22 (68.8%), consider data security to be "very important," while 8 (25%) view it as "important." A small minority, 2 (6.3%), perceive it as "somewhat important," and none of the respondents consider data security "not important." This indicates a strong consensus on the critical role of data security, with nearly all respondents acknowledging its significance. The visual representation in Figure 10 likely reinforces this trend, showing a clear dominance of the "very important" category. These underscore the widespread recognition of data security as a crucial concern (Akinade et al., 2025). The next visual presents perceived importance of secure data sharing. The question was, "How important is it to ensure secure data sharing in your data management system?"

Table/Figure Combo 11: Features perceived to be essential for blockchain system.

Table 11. Features perceived essential for blockchain system

Perceived importance level	Frequency	Percentage
Very important	22	68.8%
Important	10	31.3%
Somewhat important	0	0%
Not important	0	0%

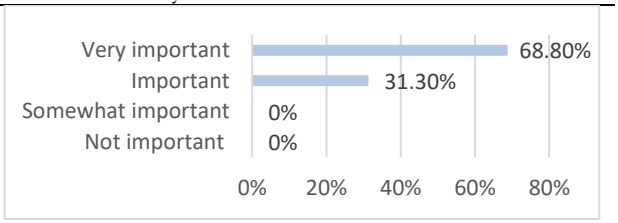

Figure 11. Features perceived essential for blockchain system (in percentages).

Table 11/Figure 11 highlights the perceived importance of features in a blockchain system. Most of respondents, 22 (68.8%), consider certain features to be "very important," while 25% view them as "important." No one perceives these features as "somewhat important." Notably, no respondents found these features to be "not important." This is a robust consensus on the essentiality of these features for a blockchain system. This

suggests that they are crucial for its functionality and adoption (Sulaeman, 2025). The visual representation in Figure 11 reinforces this by showing the distribution of perceived importance levels. Dubey et al. (2025) agree that these provide a clear overview of the level at which these features are valued.

RESULTS

The first objective was to assess the challenges and inefficiencies in healthcare data management (e.g. data silos, lack of interoperability, and issues with data security and privacy). The main challenges in the healthcare data management system were Data Security (n=8, 25%) and Inefficiencies in Data Handling (n=7, 21.9%). This was the most pressing challenge. These were followed by Data Silos (n=7, 21.9%), Lack of Interoperability (n=6, 18.8%)) and Privacy (n=5, 15.6%) was the least.

The challenges found to be most critical were Data Security (n=10, 31.2%); Data Privacy (n=9, 28.1%); System Inefficiencies (n=7, 21.9%), and Interoperability (n=6, 18.8%).

The highest priority concerns (top 70%) were *Complexity of the Technology* (n=10, 31.2%), *Integration with Existing* (n=9, 28.1%), and *Cost of Implication* (n=8, 25%).

The second objective was to evaluate the potential of blockchain technology to address these challenges and improve the security, transparency, and efficiency of healthcare data management. The leading need was *Better Data Management Efficiency* (n=11, 34.4%) and *Enhanced Data Security* (n=10, 31.2%). These priorities indicate that the primary focus is on streamlining operations and ensuring data protection. Moderate priority areas are *Secure Data Sharing* (n= 6, 18.8%) and *Improved Transparency* (n=5, 15.6%).

The third objective was **t**o identify the key features and requirements of a blockchain-based healthcare data management system that can ensure data integrity, patient privacy, and secure data sharing among stakeholders. These were *Data Integrity* (n=9, 28.1%), *Easy Integration with Current Systems* (n=6), *User Friendly Interface* (n=6, 18.8%) and *Secure Data Sharing* (n=5, 15.6%).

DISCUSSION

Objective 1: To assess the current challenges and inefficiencies in healthcare data management.

The most frequently cited challenges: data security issues (8 mentions), inefficiencies in data handling (7 mentions), and a lack of interoperability (6 mentions). Several researchers (Farayola *et al.*, 2024; Samira *et al.*, 2024) concur as there can be reputation tempered with, improper use of sensitive information, stolen ownership, lack of privacy, and so on.

Critical challenges focus primarily on data security (10 mentions) and data privacy (9). System inefficiencies (7 mentions) and interoperability issues (6) also remain prominent obstacles. Farayola *et al.* (2024) emphasize security and privacy as core to the use of technology.

Concerns are the complexity of technology (10 mentions), integration with existing systems (9), and high cost of implementation (8). Zhao *et al.* (2024) explains that when easing items are introduced, new challenges emerge.

Objective 2: To evaluate the potential of blockchain technology to address these challenges and improve the security, transparency, and efficiency of healthcare data management.

- Organisations seem to prioritise *Better Data Management Efficiency* (frequency 11) and *Enhanced Data Security* (10) as their primary benefits
- *Secure Data Sharing* (frequency 6) and *Improved Transparency* (frequency 5) are also important, appearing to be secondary concerns, with a slightly lower emphasis compared to efficiency and security.

Objective 3: To identify the key features and requirements of a blockchain-based healthcare data management system that can ensure data integrity, patient privacy, and secure data sharing among stakeholders.

- A blockchain-based healthcare data management system must prioritize data integrity, secure data sharing, and regulatory compliance, while also offering ease of integration with existing systems and user-friendly interfaces. By focusing on these areas, healthcare organisations can ensure a resilient, secure, and efficient solution for managing sensitive patient data.

CONCLUSION

The objectives of this study were threefold. First, it aimed to assess the current challenges and inefficiencies in healthcare data management, including data silos, lack of interoperability, and issues with data security and privacy. Key obstacles in implementing blockchain-based healthcare systems are primarily related to data security, privacy concerns, system inefficiencies, and integration with existing systems, as well as the high cost of

implementation. Overcoming these challenges, especially around data privacy and system integration, will be crucial for successful blockchain adoption. Second, the study evaluates the potential of blockchain technology to address these challenges, focusing on improving security, transparency, and efficiency in healthcare data management. Healthcare organizations prioritize enhanced data security and operational efficiency, with secure data sharing and transparency viewed as secondary benefits. Finally, the study identifies the key features and requirements for a blockchain-based system, emphasizing the importance of data integrity, secure data sharing, regulatory compliance, ease of integration with existing systems, and user-friendly interfaces to ensure effective healthcare data management.

RECOMMENDATIONS

On objective 1, the study recommends that healthcare organisations should

- prioritise strengthening data security measures
- address data privacy and compliance risks
- improve efficiencies in data handling
- focus on solving interoperability issues
- simplify technology complexity
- manage high implementation costs effectively
- promote cross-departmental collaboration to address data challenges

Regarding objective 2, the study recommends that healthcare organisations should

- optimise data management systems
- strengthen data security protocols
- balance security and collaboration in data sharing
- promote transparency with a focus on accountability
- review and integrate benefits based on organizational goals

Regarding objective 3, the study recommends that healthcare organisations should

- ensure robust data integrity
- facilitate secure data sharing
- ensure compliance with data protection regulations
- ensure easy integration with existing healthcare systems
- develop a user-friendly interface
- enhance security and privacy
- scalability and performance optimization
- establish a governance model

ACKNOWLEDGEMENT:

We would like to express our heartfelt gratitude to team members for playing the roles beyond their mandate, and the mentors for their invaluable guidance and support throughout this research. Lastly, we thank all the participants and institutions involved for their cooperation, which made this study possible.

REFERENCES

Abraha, D. T. (2025). Blockchain-based solution for addressing refugee management in the Global South: Transparent and accessible resource sharing in humanitarian organizations. *Frontiers in Human Dynamics*, *6*, 1391163. https://doi.org/10.3389/fhumd.2024.1391163

Adeghe, E. P., Okolo, C. A., & Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. *Open Access Research Journal of Science and Technology*, *10*(2), 013-020.

Ahanger, A. S., Masoodi, F. S., Khanam, A., & Ashraf, W. (2024). Managing and securing information storage in the Internet of Things. In *Internet of Things Vulnerabilities and Recovery Strategies* (pp. 102-151). Auerbach Publications.

Ahmed, S. (2025). Enhancing Data Security and Transparency: The Role of Blockchain in Decentralized Systems. *International Journal of Advanced Engineering, Management and Science*, *11*(1), 593258. https://ijaems.com/DOI:https://dx.doi.org/10.22161/ijaems.111.12

Ahmed, S. (2025). Enhancing data security and transparency: The role of blockchain in decentralized systems. *International Journal of Advanced Engineering, Management and Science*, *11*(1), 593258. https://dx.doi.org/10.22161/ijaems.111.12

Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud security challenges and solutions: A review of current best practices. *International Journal of Multidisciplinary Research and Growth Evaluation*, *6*(1), 26-35. https://doi.org/10.54660/.IJMRGE.2025.6.1.26-35

Al Senani, Y. K. M., & Masengu, R. (2025). Evaluating factors influencing the integration of intelligent technologies in. *GSJ*, *13*(1).

Alabdali, S. A., Pileggi, S. F., & Cetindamar, D. (2023). Influential factors, enablers, and barriers to adopting smart technology in rural regions: A Literature Review. Sustainability, 15(10), 7908. https://doi.org/10.3390/su15107908

Alhasan, T. K. (2025). Managing legal risks in health information exchanges: A comprehensive approach to privacy, consent, and liability. *Journal of Healthcare Risk Management, 2025,* 1-13. https://doi.org/10.1002/jhrm.70002

Alhur, A., & Aldosari, B. (2024). Strengths and obstacles of health informatics and health information management education and professions in hail city, kingdom of Saudi Arabia: **A** qualitative study. *Cureus*, *16*(1). e52619. https://doi.org/10.7759/cureus.52619

Al-Khasawneh, M. A., Faheem, M., Alarood, A. A., Habibullah, S., & Alzahrani, A. (2024). A secure blockchain framework for healthcare records management systems. *Healthcare Technology Letters*, *11*(6), 461-470. https://doi.org/10.1049/htl2.12092

Almadani, B., Kaisar, H., Thoker, I. R., & Aliyu, F. (2025). A systematic survey of distributed decision support systems in healthcare. *Systems*, *13*(3), 157. https://doi.org/10.3390/systems13030157

Almutairi, B. (2025). Integrating AI, blockchain, and cloud computing for enhanced e-government solutions. In *Harnessing AI, Blockchain, and Cloud Computing for Enhanced e-Government Services* (pp. 331-370). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7678-2.ch011

Asamani, J. A., Alugsi, S. A., Ismaila, H., & Nabyonga-Orem, J. (2021, September). Balancing equity and efficiency in the allocation of health resources—where is the middle ground? In *Healthcare*, *9*(10), 1257. https://doi.org/10.3390/healthcare9101257

Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, *15*(1), 70-83. https://doi.org/10.1080/20479700.2020.1843887

Awrahman, B. J., Aziz Fatah, C., & Hamaamin, M. Y. (2022). A review of the role and challenges of big data in healthcare informatics and analytics. *Computational intelligence and neuroscience*, *2022*(1), 5317760. https://doi.org/10.1155/2022/5317760

Bayya, A. K. (2025). Leveraging advanced cloud computing paradigms to revolutionize enterprise application infrastructure. *Asian Journal of Mathematics and Computer Research*, *32*(1), 133-154. https://doi.org/10.56557/ajomcor/2025/v32i19067

Borycki, E. M., & Kushniruk, A. W. (2022, May). Reinventing virtual care: Bridging the healthcare system and citizen silos to create an integrated future. *Healthcare Management Forum*, *35*(3), 135-139. https://doi.org/10.1177/08404704211062575

Bozkurt, V., & Gursoy, D. (2025). The artificial intelligence paradox: Opportunity or threat for humanity?. *International Journal of Human–Computer Interaction*, *41*(1), 174-187. https://doi.org/10.1080/10447318.2023.2297114

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation asa useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, *13*(2), 201-216. https://doi.org/10.1080/2159676X.2019.1704846

Chakraborty, P., Ganguly, S., & Das, A. (2025). Transformative Impact of Blockchain Technology on Healthcare Systems and Socioeconomic Development. In *Driving Socio-Economic Growth With AI and Blockchain* (pp. 433-460). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-8664-4.ch018

Duan, Y., & Zhu, Q. (2024). Blockchain empowerment: enhancing consumer trust and outreach through supply chain transparency. *International Journal of Production Research*, 1-25. https://doi.org/10.1080/00207543.2024.2434951

Dubey, S., Bailey, A., & Lee, J. B. (2025). Women's perceived safety in public places and public transport: A narrative review of contributing factors and measurement methods. *Cities*, *156*, 105534. https://doi.org/10.1016/j.cities.2024.105534

Elsangidy, M. M., Farag, N. S., & Ibrahim, N. F. (2025). Electronic medical records: Evolution, usability, challenges, and trends in health care settings. *Medicine Updates*, 45-60. https://doi.org/10.21608/muj.2025.355128.1202

Eun-Mee, C. (2025). Global trends in healthcare IT: EMR's central role and google trends insights. *Journal of Wellbeing Management and Applied Psychology*, *8*(1), 43-53. https://doi.org/10.13106/JWMAP.2025.VOL8.NO1.43

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. *Journal of Medical Internet Research*, *26*, e46904. https://doi.org/10.2196/46904

Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. (2024). Data privacy and security in it: a review of techniques and challenges. *Computer Science & IT Research Journal*, *5*(3), 606-615. https://doi.org/10.51594/csitrj.v5i3.909

Gao, L. (2025). Enterprise internal audit data encryption based on blockchain technology. *PloS one*, *20*(1), e0315759. https://doi.org/10.1371/journal.pone.0315759

Gesicho, M. B., Were, M. C., & Babic, A. (2020). Data cleaning process for HIV-indicator data extracted from DHIS2 national reporting system: a case study of Kenya. *BMC Medical Informatics and Decision Making*, *20*(1), 293. https://hdl.handle.net/11250/2757059

Goyal, P., & Malviya, R. (2023). Challenges and opportunities of big data analytics in healthcare. *Health Care Science*, *2*(5), 328-338. https://doi.org/10.1002/hcs2.66

Gwala, R. S., & Mashau, P. (2024). Digitalisation of Healthcare and the Fourth and Fifth Industrial Revolutions in Africa. In *Multi-Sector Analysis of the Digital Healthcare Industry* (pp. 231-258). IGI Global. https://doi.org/10.4018/979-8-3693-0928-5.ch008

Hamunakwadi, P., Mbanga, S., Lujabe, L. K., Mashapure, R., Tapera, J., Mthombeni, A., & Mutanda, B. (2025). Blockchain Technology Adoption in Smart Cities: A Critical Analysis of the Opportunities and Challenges in the African Context. *Disruptive Frugal Digital Innovation in Africa*, 81-97. https://doi.org/10.1108/978-1-83549-568-120251005

Islam, S., & Apu, K. U. (2024). Decentralized vs. centralized database solutions in blockchain: Advantages, challenges, and use cases. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *3*(4), 58-68. https://doi.org/10.62304/jieet.v3i04.195

Jain, A., Singh, R. K., & Bhushan, P. (2025). Policy and regulatory frameworks for financing smart healthcare. In *Driving Global Health and Sustainable Development Goals with Smart Technology* (pp. 367-388). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0240-9.ch015

Karthikeyan, V., Kirubakaran, G., Gopalakrishnan, K., & Raj, S. S. (2025). Creative Strategies to Protect Patients' Health Records and Confidentiality Using Blockchain Technology. *Blockchain-Enabled Solutions for the Pharmaceutical Industry*, 275-318. https://doi.org/10.1002/9781394287970.ch14

Khawaldeh, K., Awamleh, F. T., Al-Shibly, M. S., & Al-Kharabsheh, A. (2025). Data-driven strategic planning: The mediating role of the Blockchain-based supply chain in enhancing digital logistics performance. *International Journal of Innovative Research and Scientific Studies*, *8*(1), 2680-2687. https://doi.org/10.53894/ijirss.v8i1.5041

Kukman, T., & Gričar, S. (2025). Blockchain for quality: Advancing security, efficiency, and transparency in financial systems. *FinTech*, *4*(1), 7. https://doi.org/10.3390/fintech4010007

Love-Koh, J., Griffin, S., Kataika, E., Revill, P., Sibandze, S., & Walker, S. (2020). Methods to promote equity in health resource allocation in low-and middle-income countries: an overview. Globalization and health, 16, 1-12. https://doi.org/10.1186/s12992-019-0537-z

Mabina, A., Rafifing, N., Seropola, B., Monageng, T., & Majoo, P. (2024). Challenges in IoMT Adoption in Healthcare: Focus on Ethics, Security, and Privacy. *Journal of Information Systems and Informatics*, *6*(4), 3162-3184. https://doi.org/10.51519/journalisi.v6i4.960

Manikandan, A., Sanjay, T., Menon, G., Aswin, R., Bhaskar, P. B., Govind, R. M., & Ramprasad, O. G. (2025). Issues and challenges in security and privacy with e-Healthcare: A thorough literature analysis. *Internet of Things enabled Machine Learning for Biomedical Applications*, 222-247.

Margam, R. (2023). Connecting healthcare ecosystems: the journey of interoperability. *International Journal of Bioinformatics and Blockchain Technology (IJBBCT)*, *1*(1), 1-9. https://doi.org/10.17605/OSF.IO/PG6C9

Mbunge, E., Muchemwa, B., & Batani, J. (2022). Are we there yet? Unbundling the potential adoption and integration of telemedicine to improve virtual healthcare services in African health systems. *Sensors International*, *3*, 100152. https://doi.org/10.1016/j.sintl.2021.100152

Mohanty, M., Mohapatra, A. G., Rath, P. S., & Mohanty, A. (2025). Ensuring data privacy and security with blockchain in health care. In *Using Blockchain Technology in Healthcare Settings* (pp. 175-189). CRC Press.

Oriekhoe, O. I., Oyeyemi, O. P., Bello, B. G., Omotoye, G. B., Daraojimba, A. I., & Adefemi, A. (2024). Blockchain in supply chain management: A review of efficiency, transparency, and innovation. *International Journal of Science and Research Archive*, *11*(1), 173-181. https://doi.org/10.30574/ijsra.2024.11.1.0028

Pandey, N., de Coninck, H., & Sagar, A. D. (2022). Beyond technology transfer: Innovation cooperation to advance sustainable development in developing countries. *Wiley Interdisciplinary Reviews: Energy and Environment*, *11*(2), e422. https://doi.org/10.1002/wene.422

Patil, C. S., Patil, A. P., & Patil, V. B. (2025). Evolution of technologies: A comprehensive analysis of AI, blockchain, and big data analytics. In *AI and Emerging Technologies* (pp. 1-26). CRC Press.

Prasai, R. (2025). The status quo of nursing in Nepal: Challenges, opportunities and future prospects. *International Journal of Multidisciplinary Research in Arts, Science and Technology*, *3*(3), 01-14. https://doi.org/10.61778/ijmrast.v3i3.108

Roopesh, M. (2024). Blockchain technology's role in securing data and preventing cyberattacks: A detailed review. *Academic Journal on Science, Technology, Engineering and Mathematics Education, 4*(3), 16-31. https://doi.org/10.69593/ajsteme.v4i03.86

Saberi, M. A., Mcheick, H., & Adda, M. (2025). From data silos to health records without borders: A systematic survey on patient-centered data interoperability. *Information (2078-2489)*, *16*(2). https://doi.org/10.3390/info16020106

Sagili, C. (2024). Data integration in healthcare: bridging gaps for improved patient outcomes. *International Journal of Computer Engineering and Technology (IJCET)*, *15*(6), 616-630. https://doi.org/10.5281/zenodo.14207989

Samira, Z., Weldegeorgise, Y. W., Osundare, O. S., Ekpobimi, H. O., & Kandekere, R. C. (2024). Comprehensive data security and compliance framework for SMEs. *Magna Scientia Advanced Research and Reviews*, *12*(1), 043-055. https://doi.org/10.30574/msarr.2024.12.1.0146

Snigdha, E. Z., Jalil, M. S., Dahwal, F. M., Saeed, M., Mehedy, M. T. J., & Hasan, S. K. (2025). Cybersecurity in healthcare IT systems: Business risk management and data privacy strategies. *The American Journal of Engineering and Technology*, *7*(03), 163-184. https://doi.org/10.37547/tajet/Volume07Issue03-15

Song, X., Liu, X., Yang, X., Si, C., Zuo, X., He, J., & Cui, Y. (2025). Strategizing data compliance in intelligent healthcare: A four-step solution. *Chinese Medical Journal*, 10-1097. http://doi.org/10.1097/CM9.0000000000003434

Sowada, B. (2025). Healing the fragmented US Healthcare System: Bold solutions for systemic problems. Taylor & Francis. https://doi.org/10.4324/9781003538226-1

Sulaeman, A. A. (2025). Blockchain-powered security framework for IOT data integrity and privacy. *The Journal of Academic Science*, *2*(3), 874-882. https://doi.org/10.59613/jct0gv68

Thakur, A., Ranga, V., & Agarwal, R. (2025). Exploring the transformative impact of blockchain technology on healthcare: Security, challenges, benefits, and future outlook. *Transactions on Emerging Telecommunications Technologies*, *36*(3), e70087. https://doi.org/10.1002/ett.70087

Thriveni, A., Balajee, J., & Vijaykumar, T. (2025). Decentralizing Health: The Future of Blockchain in Health Care. In *Using Blockchain Technology in Healthcare Settings* (pp. 285-323). CRC Press.

Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: a systematic literature review. *BMC Medical Informatics and Decision Making*, *23*(1), 18. https://doi.org/10.1186/s12911-023-02115-5

Verma, G., & Yadav, S. (2025). Blockchain for management of healthcare data. In *Blockchain and Digital Twin for Smart Healthcare* (pp. 419-437). Elsevier. https://doi.org/10.1016/B978-0-443-30300-5.00023-3

Zhao, M., Wu, F., & Xu, X. (2024). How does technological complexity affect manufacturers' innovation? Based on the perspective of vertical separation structure. *Journal of Manufacturing Technology Management*, *35*(2), 226-246. https://doi.org/10.1108/JMTM-09-2023-0380

