The Bioscan
AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES
20(4): 33-43, 2025 www.thebioscan.com

Cyber security and Blockchain for Quality Management Systems in Healthcare

HARIHARAN

Department of Pharmaceutical Quality Assurance, SRM College of Pharmacy, SRMIST Kattankulathur, Chennai, Tamil Nadu, India

+91-6380741016

12haribharath2001@gmail.com

Dr. KELLA ALEKHYA S*

Assistant professor, Department of Pharmaceutical Quality Assurance, SRM College of Pharmacy, SRMIST Kattankulathur, Chennai, Tamil Nadu, India

+91-7397312159

kellaals@srmist.edu.in

Dr. MANIMARAN

Professor and Head, Department of Pharmaceutical Quality Assurance, SRM College of Pharmacy, SRMIST, Kattankulathur, Chennai, Tamil Nadu, India

DOI: 10.63001/tbs.2025.v20.i04.pp33-43

KEYWORDS
Blockchain in Healthcare, Cybersecurity in Digital Health, Electronic Health Records (EHR) Security, Smart Contracts for Compliance, Immutable Audit Trails

Received on:

22-08-2025

Accepted on:

20-09-2025

Published on:

29-10-2025

ABSTRACT

The current pace of digitalization in the healthcare system is becoming dependent upon Electronic Health Records (EHRs), the Internet of Things (IoT), telemedicine and artificial intelligence (AI), but data privacy, security and regulatory compliance have enabled vastly increased exposure of vulnerabilities in the process. The current text looks into ways through which cybersecurity and blockchain technology can enhance Quality Management Systems (QMS) in healthcare therefore offering a certain level of protection to patient information as well as improving the way things are done and enabling the clinicians to be in a better position to deliver a better service. The focus is on cyberattacks multidimensional risks, outdated information systems that do not allow developing the modern performance of the systems, and insider threats, as well as fast-developing legal regulations HIPAA, GDPR, and ISO/IEC 27001. Its use in provision of tamper-proof data infrastructure, immutable audit trail, decentralized trust, and automated compliance within the smart contracts provide an insight of the role that it will play. The examples of such platforms as Hyperledger and MedRec on case study contain three instances of implementing platforms in the real world, managing patient information, supply chain control, and rule enforcement. However, the report also identifies some important technical, regulatory and organization barriers, such as barriers to scalability, conflicts between GDPR and blockchain, and lack of staff in cybersecurity and blockchain skills. The research, therefore, suggests a systemic and forward-looking perspective on introducing cybersecurity and blockchain into the QMS, hoping to encourage the more sustainable, transparent, and patient-oriented digital healthcare ecosystem in the future.

INTRODUCTION

A new era of innovation has been brought about by the incorporation of digital technologies into healthcare systems, which has changed how medical services are provided, administered, and received. Digital tools have improved the effectiveness, accessibility, and general quality of care, from wearable technology and AI to telemedicine and electronic health records. But there are also a lot of obstacles associated with this digital revolution, especially when it comes to protecting the privacy and security of private information about patients. Strong cybersecurity measures are more important than ever in the healthcare sector because cyber threats are getting more complex. It investigates how technology and healthcare are changing together, looking at both the revolutionary advantages and new risks that characterize healthcare in the digital era (1).

The key issue with EHRs is the possibility of threats to patient information accessibility, privacy, or honesty, as well as the systems and devices that generate, receive, store, or send this data. The rising usage of networked devices and the growing complexity of healthcare data, systems, and devices significantly increase the attack surface, which makes it simpler for cybercriminals to identify weaknesses. Large volumes of sensitive data, such as financial data, medical histories, plans for treatment, and personal identification numbers, are

consolidated in electronic health records (EHRs). Hacking attempts and data breaches on healthcare businesses have increased as a result of cybercriminals viewing this information as an attractive target. Unauthorized access can result in financial scams, stolen identities, and the sharing of private health information, all of which can seriously undermine patients' confidence in their medical professionals.

Furthermore, the accuracy of medical records is essential. EHRs have to guarantee that patient data is correct and never changes. Illegal or unintentional data corruption or manipulation can result in incorrect diagnoses, ineffective treatments, and even life-threatening circumstances. To stop manipulating information, healthcare providers need to put strong integrity safeguards in place, such as real-time auditing and electronic signatures. For instance, administering inappropriate drugs could cause extreme allergic reactions or even death if a patient's allergy information is changed or removed.

EHR system accessibility is equally crucial. To access patient data and provide prompt care, healthcare providers depend on these systems' continuous availability. Healthcare businesses are increasingly being targeted by attacks involving ransomware, which encrypt records and demand payment to unlock it. Attacks like these have the potential to impede access to vital patient data, postponing medical interventions and jeopardizing patient safety (2)(3).

The alert continued by saying that healthcare is "poorly protected and ill-equipped for dealing with fresh cyber-attacks exposing patient medical records" and that "the health care industry is not as resistant to cyber intrusions" as other important infrastructure sectors (such as energy, financial services, public transit systems, etc.). Similarly, there has been a sharp increase in healthcare data breaches across the EU. The European Union Agency for Cybersecurity (ENISA) reports that in 2022, cyberattacks in the healthcare industry increased by 60% over the previous year, making it the fifth most affected sector in Europe. One of the most significant hacks happened in Ireland in 2021 when a ransomware attack on the Health Service Executive (HSE) forced the closure of national IT systems and caused disruptions to healthcare services nationwide(4).

To overcome these obstacles and protect patient safety and privacy, healthcare businesses need to create and implement strong Enterprise Cyber Risk Management (ECRM) programs and cybersecurity approaches. In order to guarantee data protection at every point, these methods must cover the full data lifecycle, from production to storage to disposal. All of the devices and systems connected to this data must also be included. The General Data Protection Regulation (GDPR), which imposes strict requirements for the protection of health data, has raised the bar for how enterprises handle personal data in the EU (5). Patients are more inclined to believe their healthcare providers when they are certain that their private information is secure. Establishing enduring patient relationships and promoting candid communication depend on this trust.Patients are more likely to provide full and accurate information when they feel confident about their data, which improves diagnosis and treatment strategies. Healthcare professionals can obtain accurate and unedited patient data thanks to a secure EHR system.

In the end, this improves patient safety by lowering the possibility of medical mistakes, incorrect diagnoses, and ineffective therapies. Secure EHRs, for instance, guard against unauthorized changes to vital information, such as prescription histories or allergy information, which could have fatal results (2).

A distributed ledger that keeps track of transactions in "blocks" is called a blockchain. A chain of progressively ordered Blocks is created when a set of transactions are saved in a Block that has a link to the Block before it. The primary component of Blockchain is a distributed ledger, which allows data to be added and changed via the network's nodes' consensus mechanism. A copy of every record in a sequence of the linked system is kept on each cooperating node in a blockchain. With discussions concerning the technology's potential to upend a number of industries, including medical care, transport, land ownership, public domains, manufacturing, property rights, education, and financial services, its development has been likened to the internet's emergence (6).Blockchain technology, also known as secure ledger technology, has drawn a lot of attention in recent years. Fundamentally, blockchain technology is a distributed database or public ledger of all digitally completed transactions or proceedings that share information with other participating entries. All parties involved in the arrangement have mutually agreed to certify each transaction performed in the public ledger. Furthermore, once information has been entered, it cannot be removed. With blockchain technology, any transaction conducted within the system can be readily logged and validated.Because of its special qualities and features that allow for data security, confidentiality, and integrity without the involvement of a third party managing the transaction, this technology has grown in popularity. As a result, many researchers are motivated to learn more about it by comprehending its applications, limitations, and challenges. Blockchain technology has special advantages, including the capacity for trust, cooperation, organization, recognition, legitimacy, and transparency (7).

Bitcoin's development method is called blockchain. It is a centralized record of cryptocurrency transactions that is digital and decentralized. Four categories of terms are crucial for comprehending blockchain technology. Open, distributed or decentralized ledger, efficient, verifiable, and permanent are the five keywords. The first word is "open," meaning that whatever data you enter into the blockchain should be available to everyone, allowing them to view and verify it. The second term is a distributed ledger, which allows the platform to be either dispersed or decentralized depending on the application. A copy of the public ledger is preserved for each individual party present on the platform and their communication with one another.Efficiency is the third keyword. Ensuring the effectiveness of the protocol and the information is crucial. The protocol must also be scalable and quick. Verifiable is the fourth crucial phrase. It is an important term that enables everyone on the network to verify the accuracy of information. All data entered in the blockchain is persistent, as indicated by the fifth keyword, permanent. Another name for it is tamper proof. As a result, the blockchain technique guarantees that every bitcoin transaction is documented, arranged, and kept in cryptographically protected blocks that are persistently and verifiably chained (8).

The significance of cybersecurity in safeguarding confidential information and maintaining the integrity of data management systems has increased due to the growing digitization of industrial and healthcare settings. For instance, the switch from paper to electronic health records (EHRs) has greatly increased patient information accessibility in the healthcare industry, improving the precision of diagnosis and treatment. It looks at cutting-edge cybersecurity procedures made to handle the particular difficulties these industries experience. It examines a range of dangers, including as ransomware, phishing, and insider threats, in addition to system flaws discovered in cloud computing, IoT and medical devices, and legacy systems.Malware, including ransomware, is one of the most common threats. It can encrypt data and demand a fee to unlock it, seriously impairing operations and possibly resulting in large financial losses. A thorough analysis is conducted on the deployment of strong security measures such intrusion detection systems, multi-factor authentication, and encryption.Two essential methods used to guarantee data secrecy are encryption and data masking, which transform private data into unreadable formats without the right authorization. These techniques work especially well to stop data breaches and illegal access. The results demonstrate how important these steps are to protecting data management systems, especially when combined with frequent employee training and awareness campaigns. Organizations can better safeguard their sensitive data from changing cyberthreats by utilizing modern technology and proactive security procedures (9). Today's healthcare data management systems must overcome significant obstacles to preserve data security, immutability, traceability, and transparency.One particularly noteworthy revolutionary answer is blockchain technology, which provides a novel and decentralized method that has the potential to completely

rethink healthcare data management (10). Because it may save medical expenses and deliver high-quality medical services, the Electronic Medical Record (EMR) system is appreciated and has become an essential component of medical services (11). EMR datasets were helpful during the COVID-19 pandemic (12). The structure and format of the enormous amounts of patient privacy data seen in EMR (Electronic Medical Records) systems are not standardized (13).

2. BACKGROUND AND THEORETICAL FOUNDATIONS

2.1. Quality Management Systems in Healthcare

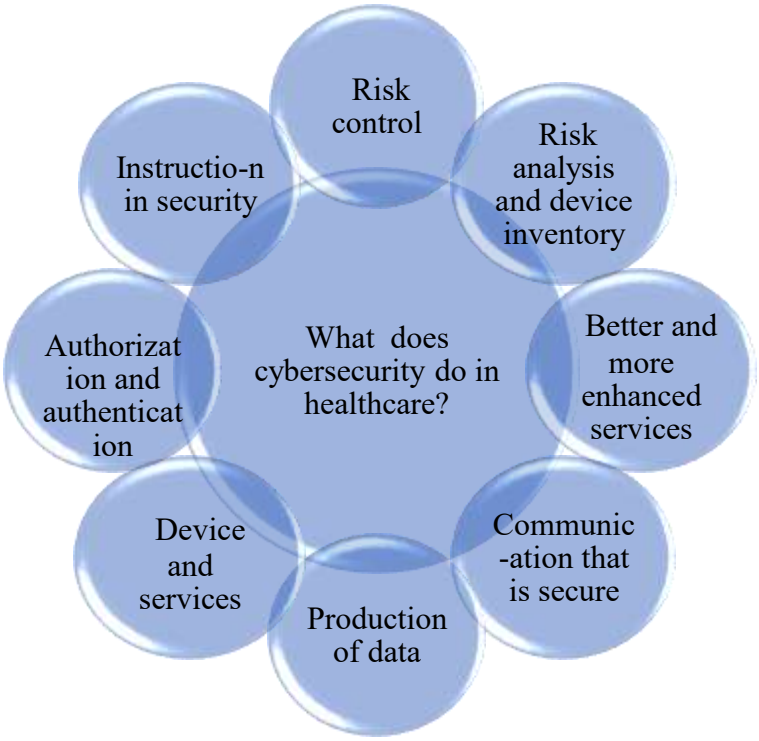
The International Organization for Standardization (also known as ISO) 9001 is the current standard for quality management systems (QMS). It is a general corporate standard based on quality assurance (QA). It is based on the rules that the US and UK governments use to buy military equipment. The first particular QMS norm for general business was BS5750. The ISO originally issued ISO 9001 in 1987. The 2015 version included risk-based thinking instead of preventive measures (14). Quality management is the set of actions that businesses do to manage, regulate, and coordinate quality. Making an efficient regulation and creating quality goals are two of these tasks. They also comprise the planning of quality, control of quality, assurance of quality, and quality enhancement [15,16].

A quality management system (QMS) was a group of parts that work together or affect each other that businesses use to monitor and regulate how quality policies are put into action and how quality goals are met. A process-based QMS takes a process-based approach to make sure that its quality policy is followed and its quality goals are met. A based on processes QMS is made up of a lot of different processes (components) that are all connected to each other. Every method utilizes resources to change inputs into outputs. Processes are connected and interact with one other through input-output connections, which show how the output of a particular procedure gets the input of another. These interactions between processes constitute a single process-oriented QMS [17].

The article stresses that digital transformation in QMS improves patient safety by allowing for continuous surveillance, risk evaluation, and process standardization. It makes sure that mistakes, non-conformities, and negative consequences are found and dealt with quickly, which lowers the number of medical mistakes and improves clinical results. Adding digital tools like automated processes and online medical records is a big step toward creating an innovative security culture in health care systems (18). In another study, it was shown that digital QMS in pharmaceutical production helps to create risk mitigation measures that directly improve patient safety, especially by included observing and systems that support decisions (19). Data integrity is a key part of both legislative and operational perfection in the pharmaceutical sector. Using digital platforms makes sure that documents are organized, data can be traced, and electronic validations are used. All of these things help keep data accurate, comprehensive, and reliable (20). In the context of the digital revolution, it goes on to say that having consistent data across systems reduces mistakes, helps make better healthcare judgments, and makes regulatory reporting easier. Digital QMS technologies cut down on human data entry, which stops data from being changed or lost (18). One of the main goals of QMS is to make sure that companies follow the rules. The paper talks about how digital transformation may help companies keep up with changing global standards like ISO 13485, FDA 21 CFR Part 11, and GMP requirements. Automated systems make it easier to be ready for audits, maintain electronic documents, and report to regulators. The digital QMS lowers the risks of not following the rules by making sure that the rules are always being followed and monitored. This makes organizations more accountable (18). Digital transformation makes it easier to handle regulatory filings safely by keeping audit trails that can't be changed and document management systems that have been checked. The GDPR study (21) also talks about how data protection laws change digital strategy. It stresses that companies must follow not only pharmaceutical requirements but also larger data governance frameworks.

2.2. Cybersecurity in Healthcare

Cybersecurity protects computer systems and networks from losing information, having their computer equipment, software, or digital information stolen, having their services interrupted or misdirected, or having their hardware, computer programs, or electronic data damaged. For almost any business that deals with digital data, digital security is one of the biggest problems they face. Unfortunately, hackers often targeted the healthcare industry. Because they don't often document network or system activities or keep an eye on attacks to find cyber breaches, many hospitals don't do a good job of tracking, reporting, and managing risks (22,23). They might be able to limit harm and find faults if they can examine and interpret threat data. Healthcare cybersecurity is one of the biggest threats to the healthcare business. Because IT has to help patients and healthcare security breaches might hurt their lives, IT has to always deal with healthcare data security issues (24,25,26). Hackers that want to do harm are especially curious about the healthcare industry. Cybersecurity is very important in healthcare since fraudsters are continually looking for weak spots in healthcare systems. This includes contact information, social security numbers, personal data and financial information (27,28). Medical staff can easily get to patient's information. There are several ways that criminals might mess up stolen data. They may utilize this information to steal someone's identity, make fake purchases, or blackmail them. These can get into a computer and installation harmful software or steal login information. Because of this, the whole network is hurt. Asking for sign-in credentials from internet sites via email is one of the most common ways that malware spreads. The most important thing to do to acquire patients' trust is to make sure that their electronic health records (EHR) and personal health information (PHI) are safe throughout a medical visit. It makes sure that future healthcare delivery systems like robotics, patient care analytics, and online healthcare are safe and dependable. As data breaches and cyberattacks in healthcare become more common, it is expected that restrictions will get harsher. This will make healthcare firms need to do more to protect themselves from cyber threats (29,30,31). Keeping healthcare information safe is becoming a big job for both individuals and companies in the healthcare field. Hackers routinely go for new medical devices and healthcare software, which are important for taking care of patients. Attackers are also quietly working on healthcare data. Once a hacker gets into an internet connection, they might use ransomware to shut down important services or secure files until a certain amount of money is paid. It's not very frequent, but hackers may take control network-connected gadgets and use them to change how a machine works or send out the wrong drugs. To safeguard any information, healthcare has to use cyber security. Compared to other fields, security jobs in healthcare are quite diverse and novel. Lab and hospital data, insurance records, fitness applications, trackers and devices, health portals, and many more places collect information about a specific patient. Cybersecurity technology makes it easy to keep it safe (32).



The current digital security landscape is getting more complicated all the time. Many major threats are aimed at businesses in all sectors, but notably those in healthcare, banking, and vital infrastructure. Ransomware, phishing, threats from insiders, and IoT vulnerabilities are some of the more important ones. Hackers have been trying to get information from the health industry lately. If they have a chance to utilize the network, they are going to install ransomware easily to lock the files or services they need or encrypt the contents and ask for a payment. Businesspeople pay a ransom to get their data back since the medical field is time-sensitive. Even if very few networked devices are giving out the wrong drugs, the device's functionality can nonetheless be changed (33). Most of the time, this kind of attack works through analyzing the emails that hackers send to check their accuracy. These emails can link to a virus website or add a text file that has a virus in it. As soon as you connect to the internet or download a file, the virus you downloaded might infect your computer. The assault may then go through all of the data that can be encrypted, such hard drives, network documents, and remote drivers [34,35]. A hacker keeps the "key" to access the data safe once they are encrypted. The key is not given out until the victim pays the ransom (36).Phishing is a way for bad people to try to get valuable information, like usernames, passwords, or medical information, by sending targeted messages, like emails or texts, that encourage people to click on links to websites with malicious code or install or download malware. Phishing usually needs the person who gets the message to do anything, therefore it uses social engineering tactics. As a result, many of the contacts look like they come from trustworthy sites like banks or, in the case of medical data, IT professionals or healthcare workers (37). Insider threats are security hazards that come from inside an organization, usually from workers, subcontractors, or other trusted people who have access to critical information and systems. Insider threats are frequently harder to find and stop than outside threats because the people who do them have legal access to and understanding of the organization's structures and processes (38). In healthcare, insider threats can take many forms, such as accessing patient records without permission, changing data, sabotaging important systems, stealing patented algorithms, committing fraud, and being careless with private information. A recent survey found that 59% of healthcare organizations had insider-related events in the last year, and 28% of these incidents resulted to the disclosure of patient data [39]. The Internet of Things (IoT) Vulnerabilities are flaws in a system or its architecture that let an intruder run commands, get data they shouldn't have, or launch denial of service assaults [40, 41, 42]. There are several places in IoT systems where vulnerabilities might be detected. They can be flaws in the hardware or software of the system, flaws in the policies and procedures that govern the system, or flaws in the users of the system [43].

REGULATORY REQUIREMENTS

Cyberattacks like ransomware, phishing scams and data breaches are happening more and more often, which puts this information's privacy, security, and accessibility at danger. The Health Insurance Portability and Accountability Act (HIPAA) imposes severe rules for keeping public health information (PHI) safe in response. The HIPAA compliance framework says that healthcare providers must use administrative, physical, and technological safeguards to keep patient data safe. Three important principles make up the HIPAA compliance framework. These standards are meant to keep patient health information safe. The Privacy Rule (2003) offers people control over their medical data and specifies rules for how healthcare organizations can use and share it. The Security Rule (2005) says that electronic PHI (ePHI) must be protected by administrative, physical, and technological measures. The Breach Notification Rule (2009) says that healthcare institutions must tell people who have had their unprotected PHI breached and the Department of the Health and Human Services (HHS). These principles work together to make sure that healthcare is private, safe, and open (44). The General Data Protection Regulation (GDPR), which went into effect in May 2018, is a game-changer for data protection and cybersecurity throughout the world. The GDPR is one of the most comprehensive data privacy law to date, and it has major effects on businesses all over the world, forcing them to rethink and improve their cybersecurity procedures (45, 46, 47). The GDPR lays forth a strong set of rules to protect people's rights and privacy. It stresses the need of being open, responsible, and taking steps to protect personal data. Its extraterritorial breadth means that it has an effect outside of Europe, forcing enterprises that operate throughout the world to follow its rules (45). The GDPR is a big change in how data is protected across the world. Its goal is to offer people more control over their personal data while putting tight rules on enterprises that handle that data (48, 49). GDPR is based on basic ideas like legality, fairness, and openness. These ideas say that businesses must be upfront about why they acquire data and how they use it. It also requires purpose limitation, which means that data can only be acquired for clear,

specific, and legal reasons, and it forbids unrelated secondary usage. The concept of data minimization says that just the data that is needed should be gathered. Accuracy, on the other hand, says that personal data should be maintained up to date and fixed when it is wrong (50, 51). GDPR also restricts how long corporations may keep data. They must set clear deadlines and not keep data longer than necessary. GDPR requires businesses to put in place robust technological and organizational protections against data breaches, unauthorized access, and data loss in order to protect their data. Being responsible is a key part of this, which means that companies must keep thorough records of their processing, do Privacy Impact Evaluations, and hire a Data Protection Officer as needed (52, 53, 54). One of the most important things about GDPR is that it applies to any organization that handles the data of EU citizens, no matter where they are (55, 56). This has caused people all across the world to rethink privacy rules and set a higher bar for protecting data. In the end, GDPR sets a global standard for data protection by promoting a culture of confidence, honesty, and following the rules. The Cybersecurity Framework created by NIST is a collection of best practices, guidelines, and suggestions that help businesses make their cybersecurity stronger. It focuses on utilizing business drivers to direct cybersecurity efforts and including cybersecurity risks in the organization's overall cybersecurity risk management. In this way, the framework brings together standards, principles, and practices that are functioning well today to create a common organizational structure for different cybersecurity methods (57). The NIST Cybersecurity Framework (CSF) was first created for U.S. critical infrastructure firms to help them manage and organize their cybersecurity operations better. But because of its flexible structure, many businesses and governments, both in the U.S. and throughout the world, including Italy, Israel, and Uruguay, have chosen to use it. The Framework is currently an important tool for federal agencies to evaluate and disclose cybersecurity threats. This is thanks to important industry surveys and an executive order 13800 in 2017. The new version makes the guidelines clearer without affecting its main ideas. It stresses that cybersecurity activities should be based on risk and cost, making it easy for businesses of all sizes to use (58). ISO security standards, especially the ISO/IEC 27000 series, are very important for improving the cybersecurity of businesses all around the world. These guidelines give you a structured way to handle sensitive information so that it stays private, safe, and accessible. ISO/IEC 27001 is well-known for helping businesses find, manage, and reduce cybersecurity risks. It focuses on creating an Information Security Management System (ISMS). Organizations that use ISO standards have better risk management, better incident response, and better compliance with rules like GDPR and HIPAA(59). ISO/IEC 27001 helps businesses find probable security risks, set up the right controls, and make policies to protect their information assets from attacks, unlawful availability, and other breaches. The Plan-Do-Check-Act (PDCA) model, which is the basis for the ISO/IEC 27001 framework (60), encourages a process of continuous improvement.

CHALLENGES INVOLVED IN CYBERSECURITY

The previously mentioned legislative and executive branch initiatives are primarily intended to address a number of well-established short-term cybersecurity needs, including preventing cyber-based espionage and disasters, lessening the effects of successful attacks, enhancing collaboration between and within sectors, defining the roles and responsibilities of federal agencies, and combating cybercrime. Nevertheless, those requirements are present in the framework of more challenging long-term issues with design, incentives, consensus, and environment(DICE):

• Design: According to experts, good security must be a fundamental component of ICT design. For financial reasons, developers have historically prioritized features over security. Additionally, a lot of future security requirements are unpredictable, which presents a challenge fordesigners.

• Incentives: It has been said that the financial incentives for cybersecurity are skewed or even twisted. For the criminals, cybercrime is considered to be inexpensive, lucrative, and relatively safe. On the other hand, cybersecurity can be costly, is inherently flawed, and the financial returns on investments are frequently uncertain.

• Consensus: There is frequently minimal shared understanding among stakeholders regarding the definition, application, and hazards of cybersecurity. There are also significant cultural barriers to reaching an agreement, not just across industries but also within industries and even inside organizations. In the hyperconnected world of internet, traditional security methods might not be enough, but reaching an agreement on substitutes has proven difficult.

• Environment: In terms of both scope and characteristics, cyberspace has been dubbed the fastest-evolving technological area in human history. Though they can also present opportunities for enhancing cybersecurity, such as through the economies of scale offered by cloud computing and big data analytics, new and emerging properties and applications—particularly social networks, mobile computing, massive data sets, cloud computing, and the Internet of Things—further complicate the dynamic threat environment. These issues may be significantly impacted by executive orders and legislation in the 114th and subsequent Congresses. For instance, federal efforts in cloud computing and other new aspects of cyberspace may help shape the future direction of cybersecurity, cybersecurity research and development may impact the design of ICT, cybercrime penalties may impact the structure of incentives, and the NIST framework may help reach a consensus on cybersecurity (61).

2.3. Blockchain Technology Overview

Since transactions cannot be changed or removed once they have been successfully validated and entered into the blockchain, immutability, also known as irreversibility, is said to be a key property of blockchain technology. Blockchain transactions are unchangeable once they are recorded, avoiding fraud and data manipulation. gives a trustworthy and verifiable transaction history, which is essential for compliance and auditing. increases confidence in online transactions, particularly in sectors like legal paperwork and healthcare. Rarely, the blockchain's records have actually been reversed (62).

The foundation of blockchains is the idea of perfect transparency, which states that all participating nodes may see transactions, even if they are hashed or encrypted, allowing for validation [62,63]. Therefore, it is difficult to provide transactional privacy in blockchains since every node on the network can see the content of every transaction. Through the application of access control measures, privacy and secrecy are typically maintained far more effectively in permissioned blockchainswhere the nodes are knownthan in permissionless ones. However, numerous studies have shown that there are still significant dangers to users' privacy, even while user accounts in blockchains without permission can remain mostly anonymous and are therefore believed to offer a number of privacy advantages to their users (64,65,66).

Decentralization, in which no third-party validation is required and only two nodes at a time complete each network transaction.Decentralization enables the Blockchain to operate without a central authority. This gives nodes in the network virtually equal voting power, which is subsequently used to control the Blockchain using the consensus algorithm (67). Blockchain is a decentralized digital ledger system that distributes the verification process among a network of separate organizations to guarantee efficiency, security, and transparency of data. From secure data transfer to automated verification processes, such decentralized technology presents a potential remedy for a number of health-related problems. Blockchain technology is being used in new application areas such as transparency, confidentiality, and authenticity, which use cryptography to improve data security and verifiability beyond what is possible with conventional databases (68).

By guaranteeing confidentiality, integrity, and limited access to sensitive patient data, blockchain's cryptographic security is essential to protecting healthcare data. To keep electronic health records (EHRs) immutable, blockchain systems mostly rely on cryptographic hash functions (such SHA-256). The integrity and reliability of medical records are maintained when any

illegal modifications to the data cause the hash value to change, immediately indicating tampering. Furthermore, smart contracts reduce the need for middlemen by enabling safe and automatic data-sharing arrangements between insurers, patients, and healthcare providers. When combined, cryptographic security makes it possible for blockchain technology to facilitate safe, open, and patient-centered data management in the medical field, lowering fraud, improving interoperability, and giving patients more control over their private health data. Strong encryption techniques used by blockchain's cryptographic security features prevent transactions from being accessed or altered by unauthorized parties, protecting participant privacy and sensitive data. Additionally, blockchain enables the implementation of smart contracts, which automate contractual procedures and enforce compliance without the need for intermediates. Smart contracts are self-executing contracts with conditions explicitly encoded into code (69). Blockchain makes it possible to record transactions in a transparent and safe manner that is impervious to manipulation by utilizing decentralized consensus procedures and cryptographic techniques. Data integrity and transparency are guaranteed by the blockchain's historical chain of blocks, which is created by cryptographically connecting each transaction to the one before it. This unchangeable ledger lowers the possibility of manipulation, fraud, and illegal access.

TYPES OF BLOCKCHAINS

1) PUBLIC BLOCKCHAIN

The public blockchain allows everyone to participate in the consensus and verification procedures of the blockchain. Since the Public Blockchain is a permissionless blockchain, public nodes can join it without needing any special permissions. The nodes of a public blockchain have complete reading and writing capabilities. Two examples of public blockchains are Ethereum and Bitcoin. These cryptocurrencies are being developed in an open-source manner, which allows anybody to inspect or modify them.

2) CONSORTIUM BLOCKCHAIN

Consortium Blockchain only chooses a portion of nodes from a public or private branch to oversee the blockchain's verification and consensus procedure. A hybrid of a public and private blockchain, this type of blockchain is sometimes referred to as a permissioned blockchain since it employs the same authorization mechanism, allowing only a select few nodes to read and add data to the blockchain. Two examples of consortium blockchains in the financial and healthcare industries are Hashed Health and IBM/Maersk.

3) PRIVATE BLOCKCHAIN

A private blockchain manages the consensus and verification process using private nodes from an organization or group that is not accessible to the general public. Moreover, not every node can participate in both processes, even if they belong to the exact same group or organization. The private blockchain is a permissioned blockchain that uses the same concept of selected authoritative nodes since it functions similarly to the private blockchain. The difference is that instead of being combined from a single group, the Consortium's authoritative nodes are composed of multiple separate groups. Examples of private blockchains include Hyperledger and Corda, where only a limited number of nodes are allowed to be changed.

4) PREMISSIONED BLOCKCHAIN

Blockchains can be categorized into two classes based on user access. The permissionless blockchain (P2P) enables free participation with equal right to vote for all users. Through distributed processes with a reliable third party, the permissioned blockchain maintains a common mediating state between stake exchanges. This permissioned blockchain manages consensus by restricting the consensus protocol's access to a select group of governing nodes, which could result in a centralized scenario. The issue with permissioned blockchains, however, is that they have become reliant on the consensus-generating controlling nodes. This raises a trustworthiness issue because nodes would need to trust these controlling nodes in order to come to an agreement for the Blockchain. But in our opinion, a permissionless blockchain would result in a lawless system where consensus might be dominated by majority voting. Reliability and confidence issues in permissioned blockchains can be addressed by permitting the selection of the governing nodes to be decentralized and autonomous (67)(70).

HEALTHCARE SPECIFIC PLATFORMS

Using well-known and tested technology, Hyperledger Fabric is a distributed ledger platform for smart contract execution. Its modular design enables pluggable implementations of different features. It is one of several initiatives within the Hyperledger Project that are presently incubating. In June 2016, the Hyperledger Fabric's "v0.5-developer-preview" developer preview was made public. The fabric's distributed ledger protocol is operated by peers. Two types of peers are distinguished by the fabric: A node on the network that manages consensus, validates transactions, and keeps track of the ledger is known as a validating peer. A node that serves as a proxy to link customers (issuing transactions) to validating peers is known as a non-validating peer. Transactions may be validated by a non-validating peer, but they are not executed(71). Users can erase data using Hyperledger Fabric. A delete is a transaction that just labels specific data as deleted; no data has been removed. When deleted transactions stay intact, the number of blocks continues to rise. The only action made by the blockchain designers to adhere to the GDPR is marking transactions as destroyed. It takes more action than its colleagues, even if this might not be sufficient to adhere to different laws (72). In order to prevent equipment failure, the Hyperledger blockchain was proposed as a solution for intensive medicine, particularly ICU data management. The so-called blockchain tree, which joins three blockchains to store various kinds of data independently, is another method to improve security [73].

When working with sensitive data, MedRec is in charge of data interchange, accountability, secrecy, and authentication—all crucial considerations. By integrating with the local data storage choices that providers currently offer, our system's modular design makes it convenient, versatile, and interoperable.MedRec is a decentralized, secure blockchain-based system for managing electronic medical records that guarantees data ownership, access management, and integrity. To automate and monitor important state changes, such permission updates or the production of new records, it makes use of smart contracts on the Ethereum blockchain. These contracts record cryptographic hashes to preserve record authenticity and guard against tampering, as well as patient-provider relationships, viewing rights, and data retrieval instructions. Providers can add new records and patients can consent to data sharing; all modifications will result in alerts for validation. MedRec has a centralized contract that compiles all patient-provider interactions and provides a single interface for managing medical history in order to improve usability. It uses a DNS-like method to translate real-world IDs to blockchain addresses and public key cryptography for identity verification. Following blockchain-based permission checks, a syncing mechanism controls the off-chain data transmission between patient and provider databases (74,75).

Ethereum is a decentralized blockchain platform that enables the creation of smart contracts, which are self-executing programs that execute agreements automatically and without the need for middlemen. Ethereum features sophisticated programmable logic, which makes it possible to create decentralized applications, in contrast to more conventional blockchains like Bitcoin. It is ideal for delicate industries like healthcare because of its transparent, safe, and unchangeable infrastructure. Ethereum can be used to guarantee data integrity, traceability, and regulatory compliance in the context of healthcare Quality Management Systems (QMS). Smart contracts, for instance, can automate processes like managing supplier certifications, verifying compliance paperwork, recording quality audits, and monitoring the lifespan of medical information. These characteristics, which are crucial elements of a strong QMS, lower human error, increase accountability, and promote transparency in clinical operations. Furthermore, through programmable access controls, Ethereum-based solutions can guarantee patient consent and privacy rights while facilitating safe data sharing among parties.

3. APPLICATIONS AND INTERSECTIONS

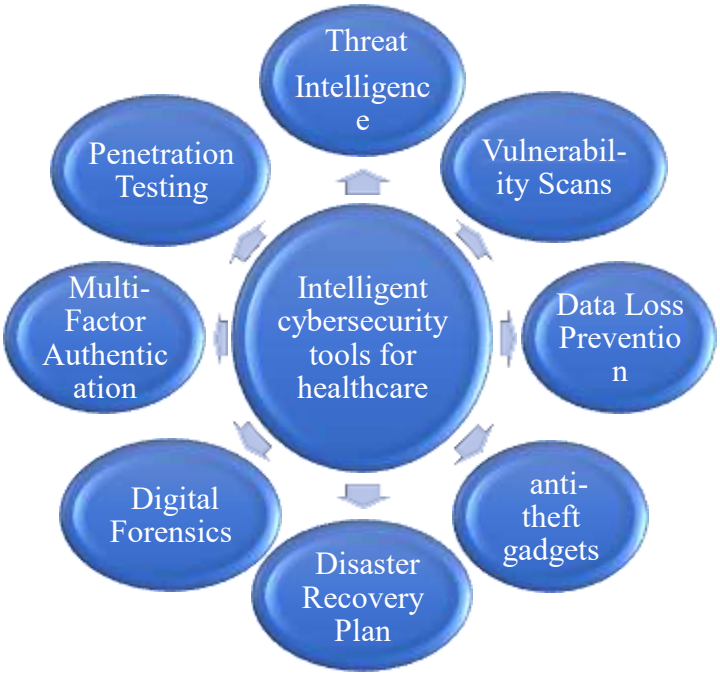
3.1. Blockchain for QMS Enhancement

The health sector is a complex system, and the health quality management system depends on a number of aspects. The system as a whole is made up of corporate management, precise disease diagnosis and treatment, patient satisfaction, and supply management. By making all employees more dependable and trustworthy, the implementation of a quality management system in the healthcare industry enhances the effective use of resources (76).

Blockchain technology provides creative answers to a number of issues facing the healthcare sector. Unauthorized individuals should not be able to access patient data, which should be kept in a safe location. The proper environmental conditions should be used when supplying medications and other equipment. By storing medical information in a secure environment with immutability features that prevent unauthorized individuals from accessing it and also prevent it from being altered, supply chain management using blockchain technology is a framework that can be used to address issues in the health sector. Original medications and other healthcare products are required; counterfeit goods are not permitted. However, because of drug fraud, counterfeit products are sold instead of authentic ones, which leads to a number of treatment-related issues. Any counterfeiting of the products is avoided because the entire process of producing and purchasing things using Blockchain technology is simultaneously and impenetrably recorded (77, 78).

3.2. Cybersecurity for QMS Protection

The healthy cybersecurity infrastructure, which includes role-based access control, the secure authentication system, and communication channel encryption, is a requisite to protecting Quality Management systems (QMS) in the healthcare sector, therefore guaranteeing that sensitive systems and data are only available to authoritative personnel. The use of frameworks that facilitate immediate detection, containment, and resolution of cyber threats, and synchronize their incident-response initiatives (irrespective of the various QMS risk-management frameworks) eliminate quality processes. In addition, cybersecurity protects the integrity of compliance records and audit trails that cannot be done away with in continuous quality control as well as a regulatory inspection. By making a gradual process of incorporating such protection, healthcare organizations will be able to ensure compliance with regulations, traceability, and system integrity.



3.3. Integrated Cybersecurity and Blockchain Approach

The emerging concept of using blockchain technology with Quality Management Systems (QMS) links the recent innovation in cybersecurity and regulatory compliance domains and suggests that the corporate governance structure will be transformed, especially with highly regulated sectors, including healthcare, pharmaceuticals, and financial businesses. Integrating blockchain into a QMS system, organizations will be able to build an end-to-end traceability of cybersecurity activities and produce time-stamped reports, which cannot be modified. As a result, they will have enough data to conduct an audit compatible with the HIPAA or GDPR standards. As an example, QMS at a hospital can document security activities such as firewall changes, vulnerability scan, access of patient data on the block chain where they can be openly documented and verifiable. Automatic triggers are also possible in forms of creating smart contracts which are functions written in the blockchain to initiate automatic notifications or CAPA (Corrective and Preventive Action) practices when pre-defined criteria are met i.e. repeated log in failures or exporting authorization violations. Besides, QMS also monitors the training programs of the employees and the blockchain ensures both accountability and verifiability with the completion certificates. Besides making the organization more transparent and accountable to the partners, auditors, and the customers, this loosely-coupled architecture also enables an organization to respond to a crisis in a short time. Gradually, it develops the culture of constant improvement of cybersecurity that transforms it not only into a compliance metric but into a quality dimension.

4. CHALLENGES AND LIMITATIONS

TECHNICAL

Two of the biggest issues facing blockchain technology are still scalability and energy consumption, particularly in resource-sensitive contexts like the Internet of Things (IoT). One significant drawback of well-known blockchain networks like Bitcoin is their limited block size and poor transaction throughput, which limits the quantity of transactions that can be completed in a second. This limitation causes network congestion, excessive latency, and increased transaction fees as the number of users and devices rises. Consensus mechanisms like Proof of Work (PoW), which demand a lot of computing power to validate transactions, exacerbate the problem. For example, it is estimated that mining Bitcoin uses more than 4,000 kilograms of CO_2 each currency, which makes it environmentally unsustainable on a wide scale. Furthermore, IoT devices are not well-suited to carry out or even support energy-intensive blockchain operations since they usually have limited memory, processing power, and battery life. These difficulties underscore the necessity of lightweight blockchain designs designed for scalability and sustainability in practical applications, as well as more effective consensus processes (79).

Modern cybersecurity tools and standards are incompatible with legacy systems, which are frequently constructed on antiquated technologies. Since these systems are usually customized for certain hardware or operating systems, it is challenging to add sophisticated features like encryption, authentication, or real-time monitoring without undergoing extensive re-engineering. Additionally, they usually have out-of-date documentation and little vendor support, which makes implementing new security solutions more difficult. The study highlights that these systems can have inadequate or out-of-date security standards, leaving them vulnerable to threats including illegal access and data breaches. This issue is made worse in an Industry 4.0 setting because of the increased interconnection and data dependence, which raises the possible attack surface. If the cybersecurity posture is not updated concurrently, there are hazards when integrating contemporary technologies like artificial intelligence (AI), the Internet of Things (IoT), and cloud computing with these previous infrastructures. Secure integration efforts are also frequently hampered by a shortage of qualified staff who are conversant with both legacy environments and contemporary cybersecurity techniques. To bridge the gap between secure, modern systems and legacy processes, these difficulties highlight the necessity of strategic planning, specialized training, and possibly the usage of middleware or microservices (80).

REGULATORY AND ETHICAL

The possibility of a collision of the right to erasure provided by the General Data Protection Regulation (GDPR) and the principle of immutability integrated into the blockchain technology is one of the major barriers to legal integration of distributed ledger systems. However, under GDPR, people have a statutory right to have personal data erased, which puts them in a stark contrast to the technical nature of blockchain that makes records permanent and immutable, an issue legally and technically challenging. The paradox created has significant ethical and regulative implications, especially in the case of applying it to the realm of public or permissionless networks where the indelible information is stored in a distributed constellation of nodes in the world. In addition, by definition, the use of blockchain technologies improves transparency in terms of the possibility of participants to review transactions, but pseudonymous identities of their own can easily display sensitive or personal data. As a result, the storage of the health records, finance data, or identity management data on the blockchain makes it complicated to maintain privacy, at the same time ensuring transparency. Investigative activities are currently directed at reduction measures of data storage off the chain, data encryption, and so-called zero-knowledge proofs, but all of these approaches, invariably, incur significantly more complexity on the body of blockchain designs, and would in most cases, only partially address GDPRs strict requirements. On such terms, businesses face a difficult task of building distributed ledger systems, which would both meet elementary regulatory needs, safeguard the privacy of users, and maintain their inherent advantages of decentralization and transparency.

ORGANIZATIONAL

The lack of the necessary knowledge and qualified professionals within the company can be resolved as a significant challenge on the way to the effective implementation of cybersecurity practices and Quality Management Systems (QMS). The lapses in organizational compliance, risk management and operational security are often golden by lack of proper understanding why cybersecurity should be incorporated into QMS framework and this may be the case among the small and medium-sized businesses. Another aggravating element is that although there is a severe lack of practitioners, very few of those have mastered the quality standards which are well established; as well as new methods of cybersecurity practice. What is behind organizational reluctance when it comes to the embodiment of new tools and systems, is either the fear of change, worries about the viable expenses, or the possible interference with the running operations. As such, a legacy mentality, lack of proper training opportunities, executive support hinders the transition to more standardized and secure digital infrastructures. The points mentioned above explain why tightening instructional programs, maintaining training processes, and the use of change management strategies are essential ideas that can aid in streamlining the adoption process of an integrated cybersecurity and QMS application.

FUTURE DIRECTIONS AND INNOVATIVE OPPORTUNITIES

In the framework of healthcare systems digitalization, the integration of innovative technologies into Quality Management Systems (QMS) introduces possibilities of improved safety and innovation. The notable example is AI-enhanced threat discovery, which has the potential to identify cyber threats in a near-real-time and enable immediate response mechanisms when combined with blockchain-based audit logs that can create an unchanging history of all activities in a system. With the help of blockchain-based cybersecurity and cloud-based QMS, companies will have easier and safer control over the data because it can provide a secure and flexible scale of managing data which is especially effective in the case of healthcare enterprises with multiple locations. An even higher level of protection of the healthcare network and patient data is the Zero Trust architecture, which presupposes no trust towards anyone and requires constant checking. Decentralized Identity (DID) is another newly developed solution and allows patients to have control over who might use their health data, improving patient privacy and legal awareness. At the same time, the continuous investigation of quantum resistant blockchain algorithms is essential in safeguarding the data in the healthcare system against the quantum computing attacks. In an attempt to meet the demands brought about by laws, including the General Data Protection Regulation (GDPR), it becomes all the more necessary to have flexible legal and ethical frameworks; these frameworks need to balance the immutability of the blockchain with the requirements of a law to delete the data and seek informed consent by the user. All these are bound to make healthcare QMS safer, visible and answerable.

CONSLUSION

Speed-driven digitalization of healthcare has produced a wide range of benefits, and it has brought unprecedented risks, especially the risks connected with data security and privacy, compliance with regulations, along with regulations connected with regulatory compliance. The empirical case above reveals that the combination of cyber security systems with blockchain technology in Quality Management Systems (QMS) is a reliable method of combating such emerging menace. Cybersecurity protects information assets use mechanisms, which limit the access of information to legitimate users, respond to incidents accordingly and protect integrity of the data. Blockchain on the other hand adds transparency, immutability and decentralized trust hence easing the trace of activities and improving accountability in all operations in the healthcare sector. Although they bring lots of obvious benefits, the practical implementation of these technologies is accompanied by a great number of technical, legal, and organizational barriers. The limitations are scaling, legacy systems being unable to run with newer architectures, as well as a conflict between blockchains and GDPR immutability and the right to erasure. Also, implementation capacity and readiness within the workforce and institutions are lopsided thus limiting the implementation process. In the future, the development of innovation might be characterized by intrusion detection on the basis of AI, cloud-native QMS architectures, and based on secure blockchain foundations, and Zero Trust and Decentralized Identity (DID) paradigm. At the same time, the efforts to research the quantum-resistant cryptography and coordinate the compliance frameworks are essential. In a nutshell, a combination of cybersecurity and blockchain design within QMS has a potential to transform the area of digital healthcare in such a way that it can establish cultures of security, trust, compliance, and constant enhancement. This would be much more than a technological improvement, but rather a strategic necessity, with patient safety, honesty, and high-quality care being on the top of the agenda in the modern digital world.

REFERENCES

- Chavan DS, Kanade TM. Blockchain and Cybersecurity Revolutionizing Healthcare in the Digital era. InEnsuring Security and End-to-End Visibility Through

Blockchain and Digital Twins 2024 (pp. 72-101). IGI Global.
- Porwal S, Chaput B. Assuring Patient Privacy and Safety through Robust Enterprise Cyber Risk Management (ECRM).
- Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain. Private Industry Notification (PIN) #: 140408-009., Vols. Available from: https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf, p. FBI Cyber Division. 2014
- Porwal S, Chaput B. Assuring Patient Privacy and Safety through Robust Enterprise Cyber Risk Management (ECRM). InElectronic Health Records-Issues and Challenges in Healthcare Systems 2025 Feb 4. IntechOpen.
- Porwal S, Chaput B. Assuring Patient Privacy and Safety through Robust Enterprise Cyber Risk Management (ECRM). InElectronic Health Records-Issues and Challenges in Healthcare Systems 2025 Feb 4. IntechOpen.
- Sidiqqui A, Tansen KJ. Blockchain: A disruptive technology. InBlockchain Technology and Computational Excellence for Society 5.0 2022 (pp. 48-58). IGI Global Scientific Publishing.
- Singh G, Garg V, Tiwari P. Introduction to Blockchain Technology. InTransforming Cybersecurity Solutions using Blockchain 2021 Apr 14 (pp. 1-18). Singapore: Springer Singapore.
- Senthilkumar D. Blockchain and Its Integration as a Disruptive Technology. InAI and Big Data's Potential for Disruptive Innovation 2020 (pp. 261-290). IGI Global.
- Joy ZH, Islam S, Rahaman MA, Haque MN. Advanced Cybersecurity Protocols For Securing Data Management Systems in Industrial and Healthcare Environments. Global Mainstream Journal of Business, Economics, Development & Project Management. 2024;3(4):25-38.
- Huang W. Enhancing Medical Information Security Through Blockchain Technology. Advances in Economics, Management and Political Sciences. 2024 Oct 25;120:23-34.
- Sun, S., Xie, Z., Yu, K., Jiang, B., Zheng, S., & Pan, X. (2021). COVID-19 and healthcare system in China: challenges and progression for a sustainable future. Globalization and Health, 17, 1-8.
- Wang, Z., Zheutlin, A. B., Kao, Y. H., Ayers, K. L., Gross, S. J., Kovatch, P., ... & Li, L. (2020). Analysis of hospitalized COVID-19 patients in the Mount Sinai Health System using electronic medical records (EMR) reveals important prognostic factors for improved clinical outcomes. MedRxiv, 2020-04.
- Zhang, L., Zheng, Z., & Yuan, Y. (2021). A Blockchain-Based Controllable Sharing Model for Electronic Medical Records. Acta Automatica Sinica, 47(9), 2143-2153.
- Pope AK. Quality Management Systems (QMS) and their role in assisted reproductive technology. Fertility & Reproduction. 2025 Mar 14;7(01):4-12.
- Allen LC. Role of a quality management system in improving patient safety—laboratory aspects. Clinical Biochemistry. 2013 Sep 1;46(13-14):1187-93.
- Quality management. Available at http://www.praxiom.com/iso-definition.htm. [Accessed on 4 March 2013].
- Quality management system. Available at http://www.praxiom.com/iso-definition. htm. [Accessed on 4 March 2013].
- Ullagaddi, P. (2024d). *Digital Transformation in the Pharmaceutical Industry: Enhancing Quality Management Systems and Regulatory Compliance*. International Journal of Health Sciences, 12(1), 31–43
- Ullagaddi P. Leveraging digital transformation for enhanced risk mitigation and compliance in pharma manufacturing. Journal of Advances in Medical and Pharmaceutical Sciences. 2024 Jun 24;26(6):75-86.
- Ullagaddi P. Digital transformation in the pharmaceutical industry: ensuring data integrity and regulatory compliance. The International Journal of Business & Management. 2024 May 17;12(3).
- Ullagaddi P. GDPR: Reshaping the landscape of digital transformation and business strategy. International journal of business marketing and management. 2024;9(2):29-35.
- Tomaiko E, Zawaneh MS. Cybersecurity threats to cardiac implantable devices: room for improvement. Current Opinion in Cardiology. 2021 Jan 1;36(1):1-4.
- Pears M, Konstantinidis ST. Cybersecurity training in the healthcare workforce–utilization of the ADDIE model. In2021 IEEE Global Engineering Education Conference (EDUCON) 2021 Apr 21 (pp. 1674-1681). IEEE.
- Alami H, Gagnon MP, Ahmed MA, Fortin JP. Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. Health Policy and Technology. 2019 Dec 1;8(4):319-21.
- Chua JA, Pmp C. Cybersecurity in the healthcare industry. Physician Leadership Journal. 2021;8(1).
- Luh F, Yen Y. Cybersecurity in science and medicine: Threats and challenges. Trends in biotechnology. 2020 Aug 1;38(8):825-8.
- Wyant DK, Bingi P, Knight JR, Rangarajan A. DeTER framework: A novel paradigm for addressing cybersecurity concerns in mobile healthcare. InResearch Anthology on Securing Medical Systems and Records 2022 (pp. 381-407). IGI Global.
- Burke W, Oseni T, Jolfaei A, Gondal I. Cybersecurity indexes for eHealth. InProceedings of the australasian computer science week multiconference 2019 Jan 29 (pp. 1-8).
- Rios B. Cybersecurity expert: medical devices have 'a long way to go'. Biomedical instrumentation & technology. 2015 May;49(3):197-200.
- Shackelford SJ, Mattioli M, Myers S, Brady A, Wang Y, Wong S. Securing the Internet of healthcare. Minn. JL Sci. & Tech.. 2018;19:405.
- Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, Petrozzino C, Zuk M. The evolving state of medical device cybersecurity. Biomedical instrumentation & technology. 2018 Mar 1;52(2):103-11.
- Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023 Dec 1;1:100016.
- Abirami T, Parameshwari V. Cybersecurity Threat Landscape of Smart and Interconnected Healthcare Systems. InCybersecurity and Data Science Innovations for Sustainable Development of HEICC (pp. 76-92). CRC Press.
- Thamer N, Alubady R. A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In2021 1st Babylon international conference on information technology and science (BICITS) 2021 Apr 28 (pp. 210-216). IEEE.
- D. Zakus, O. Bhattacharyya, and X. Wei, "Health Systems, Management, and Organization in Global Health," Med. Access, pp. 445–462, 2013.
- E. Berrueta, D. Morato, E. Magana, and M. Izal, "A Survey on Detection Techniques for Cryptographic Ransomware," IEEE Access, vol. 7, pp. 144925–144944, 2019.
- Priestman W, Anstis T, Sebire IG, Sridharan S, Sebire NJ. Phishing in healthcare organisations: Threats, mitigation and approaches. BMJ health & care informatics. 2019 Sep 4;26(1):e100031.
- Viradia V, Muthukrishnan H, Yadav D. Insider Threats in Healthcare Application: Harnessing AI To Mitigate The

Risks. International Journal of Global Innovations and Solutions (IJGIS). 2024 Dec 28.
- Viradia V, Muthukrishnan H, Yadav D. Insider Threats in Healthcare Application: Harnessing AI To Mitigate The Risks. International Journal of Global Innovations and Solutions (IJGIS). 2024 Dec 28.
- Abomhara M, Køien GM. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015 May 22:65-88.
- D. L. Pipkin, Information security. Prentice Hall PTR, 2000.
- E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures. Springer, 2010, pp. 25–44.
- J. M. Kizza, Guide to Computer Network Security. Springer, 2013.
- Abbasi N, Smith DA. Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2024 Sep 25;3(3):278-87.
- Amoo OO, Atadoga A, Osasona F, Abrahams TO, Ayinla BS, Farayola OA. GDPR's impact on cybersecurity: A review focusing on USA and European practices. International Journal of Science and Research Archive. 2024;11(1):1338-47.
- Alic, D. (2021). The Role of Data Protection and Cybersecurity Regulations in Artificial Intelligence Global Governance: A Comparative Analysis of the European Union, the United States, and China Regulatory Framework.
- Dowd, R., & Dowd, R. (2022). Digitized Data Protection as a Fundamental Human Right. The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU, 27-69.
- Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. Journal of Business Ethics, 168, 565-578.
- Reinhardt, J. (2022). Realizing the fundamental right to data protection in a digitized society. In Personality and Data Protection Rights on the Internet: Brazilian and German Approaches (pp. 55-68). Cham: Springer International Publishing.
- Ke, T. T., & Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. Management Science, 69(8), 4389-4412
- Štarchoň, P., &Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices-mobile phones. Procedia Computer Science, 151, 303-312.
- Lamoureux, S. (2020). Implementing the General Data Protection Regulation: The experiences of three Finnish organizations.
- Polanco, K. (2020). Trimming the Fat: The GDPR as a Model for Cleaning up Our Data Usage. Touro L. Rev., 36, 603.
- Schade, F. (2023). Dark Sides of Data Transparency: Organized Immaturity After GDPR?. Business Ethics Quarterly, 1-29.
- Burri, M. (2021). Data flows versus data protection: Mapping existing reconciliation models in global trade law. In Law and Economics of Regulation (pp. 129-158). Cham: Springer International Publishing.
- Daniel, N. F. (2022). EU Data Governance: Preserving Global Privacy in the Age of Surveillance (Doctoral dissertation, Johns Hopkins University).
- Möller DP. NIST cybersecurity framework and MITRE cybersecurity criteria. InGuide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices 2023 Apr 19 (pp. 231-271). Cham: Springer Nature Switzerland.
- Calder A. NIST Cybersecurity Framework: A pocket guide. IT Governance Publishing Ltd; 2018 Sep 28.
- Folorunso A, Mohammed V, Wada I, Samuel B. The impact of ISO security standards on enhancing cybersecurity posture in organizations. World Journal of Advanced Research and Reviews. 2024;24(1):2582-95.
- Fauzi, R. and Lubis, M., 2021. Assessment Framework for Defining the Maturity of Information Technology within Enterprise Risk Management (ERM). International Journal of Advanced Computer Science and Applications, 12(10).
- Fischer EA. Cybersecurity issues and challenges: In brief [Internet]. 2014 Dec 16
- Politou E, Casino F, Alepis E, Patsakis C. Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing. 2019 Oct 25;9(4):1972-86.
- K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," Ieee Access, vol. 4, pp. 2292–2303, 2016.
- S. Meiklejohn, "Top ten obstacles along distributed ledgers path to adoption," IEEE Security & Privacy, vol. 16, no. 4, pp. 13–19, 2018.
- S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," Proceedings on Privacy Enhancing Technologies, vol. 2018, no. 4, pp. 179–199, 2018.
- D. F. Primavera, "The interplay between decentralization and privacy: the case of blockchain technologies," Journal of Peer Production, vol. 9, 2016.
- Zarrin J, Wen Phang H, Babu Saheer L, Zarrin B. Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Computing. 2021 Dec;24(4):2841-66.
- Odeh A, Keshta I, Al-Haija QA. Analysis of blockchain in the healthcare sector: application and issues. Symmetry. 2022 Aug 23;14(9):1760.
- Jimmy F. Enhancing Data Security in Financial Institutions With Blockchain Technology. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. 2024 Aug 19;5(1):424-37.
- Lopez, P.G., Montresor, A., Datta, A.: Please, do not decentralize the internet with (permissionless) blockchains! In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 1901–1911. ISBN 1063-6927 (2019).
- Cachin C. Architecture of the hyperledger blockchain fabric. InWorkshop on distributed cryptocurrencies and consensus ledgers 2016 Jul 25 (Vol. 310, No. 4, pp. 1-4).
- Wang Q, Qin S. A hyperledger fabric-based system framework for healthcare data management. Applied Sciences. 2021 Dec 9;11(24):11693.
- Kushch, S.; Baryshev, Y.; Ranise, S. Blockchain tree as solution for distributed storage of personal id data and document access control. Sensors 2020, 20, 3621.
- Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In2016 2nd international conference on open and big data (OBD) 2016 Aug 22 (pp. 25-30). IEEE.
- Wood G. Ethereum: A secure decentralisedgeneralised transaction ledger. Ethereum project yellow paper. 2014 Apr;151(2014):1-32.
- Yılmaz H, Şenvar Ö. Quality Management System Based Blockchain Applications. Journal of Information Systems and Management Research. 2025 Jun 6;7(1):14-28.

- Abdallah S, Nizamuddin N. Blockchain-based solution for pharma supply chain industry. Computers & Industrial Engineering. 2023 Mar 1;177:108997.
- Ghadi YY, Mazhar T, Shahzad T, Amir khan M, Abd-Alrazaq A, Ahmed A, Hamam H. The role of blockchain to secure internet of medical things. Scientific Reports. 2024 Aug 8;14(1):18422.
- Kaur G, Gandhi C. Scalability in blockchain: Challenges and solutions. InHandbook of Research on Blockchain Technology 2020 Jan 1 (pp. 373-406). Academic Press.
- Usmani UA, Happonen A, Watada J. Advancements in industry 4.0 asset management: Interoperability and cyber security challenges and opportunities. InProceedings of the future technologies conference 2023 Oct 19 (pp. 468-488). Cham: Springer Nature Switzerland.