Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202522741

Artificial Intelligence-Driven Algorithmic Frameworks for Health Security Management and Hospital Administration

Samih Mohammed Hassan Mousa[(1)] , Mansour Mayudh S. Alharthi[(2)] , Ali Mohammed Ali Hamdi[(3)] , Faisal Mohammed Mohammed Hazazi[(3)] , Bandar Mahdi Ahmed Mobarki[(3)] , Khalid Hassan Yousef Mobarki[(3)] , Rahaf Hussain Ali Daghriry[(3)] , Norah Saleh Fathuldeen Sumayli[(3)] , Fahhad Muflih Faleh Aldawsari[(4)]

(1)Al Wasli Primary Health Care Center, Jazan,Ministry of Health, Saudi Arabia
(2)Jeddah Second Health Cluster,Ministry of Health , Saudi Arabia
(3)Al Harth General Hospital, Jazan,Ministry of Health , Saudi Arabia
(4)Al Sulayyil General Hospital, Ministry of Health , Saudi Arabia

Abstract

Background: The rapid digital transformation of healthcare has significantly improved clinical efficiency, interoperability, and patient-centered care through the widespread adoption of electronic health records, Internet of Medical Things (IoMT) devices, telemedicine, cloud computing, and artificial intelligence. However, this increased connectivity has simultaneously expanded the cybersecurity threat landscape, exposing healthcare organizations to sophisticated attacks that threaten patient privacy, data integrity, and service continuity. Blockchain technology and intelligent algorithmic approaches have emerged as promising solutions for strengthening healthcare cybersecurity while ensuring secure and transparent data management.

Aim: This review aimed to examine blockchain-based and algorithm-driven health security systems, evaluate their effectiveness in mitigating major cyber threats, and identify current challenges, limitations, and future research directions for securing modern healthcare information systems.

Methods: A comprehensive narrative review of recent literature was conducted, focusing on blockchain architectures, artificial intelligence, cryptographic techniques, intrusion detection systems, access control mechanisms, and cybersecurity frameworks designed for healthcare environments. The reviewed studies were analyzed according to system architecture, security performance, attack mitigation capabilities, and implementation challenges.

Results: The reviewed evidence demonstrated that blockchain-based systems significantly improve data integrity, authentication, transparency, traceability, and secure information sharing. Integrated artificial intelligence and cryptographic algorithms effectively mitigated unauthorized access, ransomware, denial-of-service, man-in-the-middle, data tampering, and privacy leakage attacks. Despite these advantages, challenges related to scalability, computational overhead, latency, interoperability, and user adoption remain barriers to widespread implementation.

Conclusion: Blockchain integrated with advanced algorithmic security provides a robust foundation for protecting healthcare information systems. Continued advancements in artificial intelligence, scalable blockchain architectures, and adaptive cybersecurity strategies will be essential for developing resilient, secure, and trustworthy digital healthcare ecosystems.

Keywords: Blockchain, Healthcare Cybersecurity, Artificial Intelligence, Health Security Systems, Electronic Health Records, Internet of Medical Things, Cryptography, Cyber Attacks, Data Privacy, Healthcare Informatics.

Introduction

Introduction:

The rapid digital transformation of healthcare has fundamentally reshaped the delivery, management, and accessibility of medical services worldwide. The widespread adoption of electronic health records (EHRs), cloud computing, telemedicine, artificial intelligence (AI), wearable medical devices, and the Internet of Things (IoT) has significantly improved healthcare efficiency, clinical decision-making, and patient-centered care. These technological innovations have enabled healthcare organizations to enhance diagnostic accuracy, facilitate real-time communication among healthcare providers, optimize resource utilization, and improve the continuity of patient care. However, this increasing dependence on interconnected digital systems has simultaneously expanded the cyber threat landscape, exposing healthcare organizations to sophisticated cybersecurity risks. As healthcare institutions continuously generate, transmit, and store enormous volumes of highly sensitive patient information, they have become one of the most attractive targets for cybercriminals seeking financial gain, identity theft, or disruption of essential healthcare services [1]. Healthcare data are among the most valuable forms of

*Corresponding author e-mail: ficmaac@gmail.com (amih Mohammed Hassan Mousa).
Receive Date: 07 December 2025, Revise Date: 29 December 2025, Accept Date: 31 December 2025

digital information because they contain comprehensive personal, clinical, financial, and biometric records that can be exploited for multiple malicious purposes. Unlike financial information, which can often be replaced or modified after a breach, medical records contain permanent patient identifiers and lifelong clinical histories that cannot easily be altered. Consequently, the confidentiality, integrity, and availability of healthcare information have become critical priorities for healthcare organizations and national health systems. The continuous exchange of patient information across hospitals, clinics, laboratories, pharmacies, insurance providers, and public health agencies further increases the complexity of maintaining secure healthcare information systems. Although digitalization has greatly enhanced healthcare delivery and operational efficiency, it has also introduced substantial cybersecurity challenges that require continuous technological innovation and organizational preparedness [2].

\The integration of IoT technologies into healthcare has further accelerated this transformation by enabling continuous patient monitoring, remote healthcare delivery, intelligent medical devices, and automated clinical workflows. Connected medical equipment, wearable sensors, implantable devices, and smart monitoring systems generate real-time clinical information that supports early diagnosis and personalized treatment strategies. Despite these significant clinical benefits, increased connectivity has substantially enlarged the attack surface available to cyber adversaries. Every connected device, communication channel, and cloud-based application represents a potential entry point for unauthorized access, data theft, or malicious system disruption. Consequently, protecting interconnected healthcare ecosystems has become increasingly challenging as healthcare organizations seek to balance accessibility, interoperability, and cybersecurity [1,2]. Healthcare data breaches continue to represent one of the most significant cybersecurity concerns facing modern healthcare systems. In many countries, regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule establish strict standards governing the protection, confidentiality, and secure management of patient information. Nevertheless, healthcare organizations continue to experience substantial numbers of data breaches arising from human error, insider threats, theft, ransomware attacks, system vulnerabilities, and accidental data loss. Among these causes, human error remains one of the most common contributors, reflecting inadequate cybersecurity awareness, insufficient staff training, weak authentication practices, and improper handling of confidential information. Although technological vulnerabilities receive considerable attention, organizational and human factors remain equally important determinants of healthcare cybersecurity performance [3].

The global healthcare sector has witnessed an unprecedented escalation in cyber-attacks over the past decade. Unfortunately, cybersecurity preparedness has not progressed at the same pace as digital transformation in many healthcare organizations. Information systems security continues to be underestimated in numerous countries, where healthcare institutions frequently allocate only a limited proportion of their operational budgets to cybersecurity infrastructure, workforce training, and incident response capabilities. This imbalance creates substantial vulnerabilities that increase the likelihood of successful cyber intrusions, service interruptions, and large-scale data breaches. The shortage of cybersecurity specialists within healthcare organizations further compounds these challenges by limiting the ability to proactively detect, prevent, and respond to sophisticated cyber threats [2,4]. The Coronavirus Disease 2019 (COVID-19) pandemic further intensified cybersecurity challenges across the healthcare sector. The rapid expansion of telemedicine services, remote working environments, digital communication platforms, and cloud-based healthcare applications significantly increased organizational exposure to cyber threats. During the pandemic, healthcare organizations experienced substantial increases in ransomware attacks, phishing campaigns, fake online identities, misinformation campaigns, supply chain attacks, and attempts to compromise critical healthcare infrastructure. These attacks not only threatened patient privacy but also disrupted essential healthcare services, delayed clinical operations, and endangered patient safety. The growing frequency and sophistication of cyber-attacks have highlighted the urgent need for innovative cybersecurity technologies capable of protecting increasingly complex healthcare information systems [5].

In response to these evolving threats, healthcare organizations have begun exploring advanced technological solutions capable of strengthening cybersecurity while maintaining efficient information sharing and clinical interoperability. Among the most promising innovations are blockchain technology and artificial intelligence-driven algorithmic security approaches. These technologies offer complementary capabilities that enhance data protection, automate threat detection, improve authentication mechanisms, and strengthen the resilience of healthcare information systems against emerging cyber risks. Blockchain technology provides a decentralized and tamper-resistant framework for securely managing healthcare information. Unlike conventional centralized databases that rely on a single controlling authority, blockchain distributes data across multiple

interconnected nodes, thereby eliminating single points of failure and reducing the likelihood of unauthorized data manipulation. Every healthcare transaction, including updates to electronic health records, patient consent management, prescription verification, laboratory reporting, and pharmaceutical supply chain monitoring, is cryptographically encrypted, timestamped, and permanently recorded within an immutable distributed ledger. Each newly generated record is mathematically linked to the preceding transaction through unique cryptographic hash functions, ensuring complete traceability while preserving data integrity and transparency throughout the healthcare ecosystem [6]. One of blockchain's most significant advantages is its ability to provide patients with greater control over access to their personal health information. Through decentralized identity management and permission-based access control, patients can securely authorize healthcare providers, insurers, researchers, and other stakeholders to access specific portions of their medical records without compromising privacy. This patient-centered model enhances transparency, strengthens trust, and supports regulatory compliance while facilitating secure information exchange among authorized users. Furthermore, blockchain technology improves pharmaceutical supply chain management by verifying drug authenticity, preventing counterfeit medications, tracking product distribution, and enhancing recall management. The technology also streamlines health insurance processes by automating claims verification, eligibility assessment, and payment authorization through secure distributed ledgers, thereby reducing administrative inefficiencies, operational costs, and fraudulent activities [6].

From a technical perspective, blockchain relies on sophisticated cryptographic principles and distributed consensus mechanisms to maintain network integrity and security. Every participant within the blockchain network possesses a unique cryptographic key pair used for secure authentication and digital signature verification. Healthcare transactions are grouped into sequential blocks, with each block containing a cryptographic reference to the previous block, thereby creating an immutable chronological chain of information. This architecture ensures that any attempt to modify historical records immediately alters the associated cryptographic hash values, making unauthorized data manipulation readily detectable. Rather than relying on centralized oversight, blockchain networks achieve data validation through consensus mechanisms, including proof of work, proof of stake, or proof of authority, depending on the network architecture. These mechanisms enable independent network participants to collectively verify transaction authenticity before new information is permanently incorporated into the distributed ledger. By combining decentralization, cryptographic security, immutable data storage, and consensus-based validation, blockchain establishes a highly secure, transparent, and trustworthy infrastructure capable of supporting the growing cybersecurity requirements of modern healthcare information systems [7][8].

Overview of Health Security Systems

The rapid digital transformation of healthcare has fundamentally changed the way medical information is generated, transmitted, stored, and utilized across healthcare organizations. Electronic health records, medical imaging systems, cloud computing platforms, artificial intelligence applications, telemedicine services, wearable technologies, and Internet of Things (IoT)-enabled medical devices have become indispensable components of modern healthcare delivery. These technologies have significantly improved clinical efficiency, communication, diagnostic accuracy, and patient-centered care. However, the increasing dependence on interconnected digital infrastructures has also introduced unprecedented cybersecurity challenges that threaten the confidentiality, integrity, and availability of healthcare information. Consequently, health security systems have emerged as an essential component of contemporary healthcare organizations, providing comprehensive frameworks designed to safeguard digital assets, ensure uninterrupted clinical services, and protect sensitive patient information from increasingly sophisticated cyber threats. Health security systems encompass a broad spectrum of administrative, technical, organizational, and technological measures developed to protect healthcare information systems from unauthorized access, cyberattacks, data manipulation, and service disruption. These systems extend beyond conventional cybersecurity by integrating risk assessment, access control, encryption, network monitoring, incident response, regulatory compliance, disaster recovery, and continuous security surveillance into a unified framework. Their primary objective is not only to protect confidential patient information but also to preserve clinical accuracy, maintain operational continuity, and ensure patient safety. As healthcare increasingly depends on digital technologies for diagnosis and treatment, the reliability and resilience of health security systems have become directly associated with the quality and safety of healthcare delivery. One of the most significant concerns in contemporary healthcare cybersecurity is the integrity of clinical data. Healthcare professionals rely extensively on digital information to make diagnostic and therapeutic decisions, meaning that even minor alterations to patient records may produce severe clinical consequences. Malicious modification of laboratory reports, medication histories, radiological images, or electronic health records can result in delayed diagnosis, inappropriate treatment, medication errors, unnecessary surgical interventions, or life-threatening clinical outcomes. Unlike many other industries where

data manipulation primarily results in financial losses, compromised healthcare information directly threatens patient health and survival. Consequently, ensuring the integrity of digital medical records has become one of the highest priorities within modern health security systems.

The emergence of sophisticated cyber threats has demonstrated that attackers increasingly target not only healthcare databases but also advanced diagnostic technologies. One particularly concerning example involves the manipulation of diagnostic imaging data through artificial intelligence-based attacks. Researchers have demonstrated that malicious software can alter computed tomography (CT) and magnetic resonance imaging (MRI) scans by inserting or removing pathological findings such as tumors. These manipulated images may deceive experienced radiologists into diagnosing diseases that do not exist or overlooking clinically significant abnormalities. Such attacks have profound implications because they undermine clinician confidence, compromise diagnostic accuracy, and expose patients to unnecessary invasive procedures or delayed treatment. The development of malware capable of introducing fictitious pathological conditions, including tumors or serious infectious diseases such as acquired immunodeficiency syndrome (AIDS), severe acute respiratory syndrome (SARS), and Ebola, illustrates the rapidly evolving sophistication of cyber threats targeting healthcare systems [5].

Medical imaging infrastructures are particularly vulnerable because of their extensive integration with hospital information systems and clinical communication networks. The Picture Archiving and Communication System (PACS), which serves as the primary platform for storing, retrieving, transmitting, and managing digital medical images, represents one of the most critical components of contemporary healthcare information systems. PACS enables seamless communication among radiologists, physicians, surgeons, and other healthcare professionals while facilitating rapid access to diagnostic imaging across multiple healthcare facilities. Despite its clinical importance, PACS remains exposed to numerous cybersecurity vulnerabilities because it interfaces with electronic health records, imaging modalities, cloud storage platforms, laboratory information systems, and external communication networks. This extensive connectivity significantly expands the potential attack surface available to cybercriminals seeking unauthorized access to healthcare infrastructure. Compromising PACS may allow attackers not only to manipulate diagnostic images but also to infiltrate interconnected hospital information systems, thereby gaining access to broader repositories of confidential patient information. Unauthorized access may result in theft of personal health information, alteration of clinical documentation, disruption of imaging services, ransomware attacks, or unauthorized disclosure of sensitive medical records. Because radiological images frequently serve as the foundation for critical clinical decisions involving oncology, neurology, cardiology, trauma care, and surgical planning, maintaining the integrity and authenticity of imaging data is essential for ensuring accurate diagnosis and safe patient management. Consequently, protecting PACS has become a strategic priority within healthcare cybersecurity programs [8].

Modern health security systems employ multiple layers of defense to mitigate these evolving threats. Network segmentation limits unauthorized lateral movement within healthcare infrastructures, while strong authentication mechanisms, including multi-factor authentication, restrict system access to authorized personnel. Advanced encryption techniques protect sensitive patient information during storage and transmission, thereby reducing the risk of unauthorized disclosure. Continuous network monitoring, intrusion detection systems, behavioral analytics, and artificial intelligence-driven threat detection enable healthcare organizations to identify suspicious activities before significant damage occurs. Regular software updates, vulnerability assessments, penetration testing, and comprehensive incident response planning further strengthen organizational resilience against cyberattacks. Artificial intelligence and machine learning technologies have become increasingly important components of health security systems because they enable proactive identification of emerging threats through continuous analysis of network behavior, user activities, and system performance. Unlike conventional rule-based security mechanisms, intelligent algorithms can identify abnormal patterns indicative of cyber intrusions, insider threats, malware infections, or unauthorized data manipulation. Predictive analytics further supports healthcare cybersecurity by identifying vulnerabilities before exploitation occurs, enabling preventive interventions that reduce organizational risk. These intelligent security solutions significantly improve the speed and accuracy of threat detection while reducing the burden on cybersecurity personnel [6][7][8].

In addition to technological safeguards, effective health security systems require comprehensive organizational governance and continuous workforce education. Human error remains one of the leading causes of healthcare cybersecurity incidents, making cybersecurity awareness training essential for all healthcare professionals. Regular education regarding phishing attacks, password management, secure handling of patient information, and incident reporting strengthens organizational security culture and reduces preventable vulnerabilities. Healthcare leaders must

also establish clear cybersecurity policies, regulatory compliance programs, and multidisciplinary collaboration among information technology specialists, clinicians, administrators, and security professionals to ensure effective implementation of security measures. Extensive research has documented the development of numerous health security frameworks designed to address the growing complexity of cybersecurity threats within healthcare environments. These systems incorporate diverse technologies, including blockchain, cryptographic authentication, secure cloud computing, artificial intelligence, zero-trust architectures, and advanced access control mechanisms, each addressing specific categories of cyber threats while collectively strengthening overall healthcare resilience. Comprehensive evaluation of these security systems demonstrates that maintaining the confidentiality, integrity, and availability of healthcare information remains fundamental to ensuring accurate diagnoses, preserving patient safety, maintaining public trust, and supporting the delivery of high-quality healthcare services in an increasingly digital world [8].

Security Systems Based on Blockchain Approaches

The rapid digitalization of healthcare has substantially increased the need for advanced cybersecurity frameworks capable of protecting sensitive medical information throughout its lifecycle. Modern healthcare information systems continuously collect, process, transmit, and store large volumes of confidential patient data originating from electronic health records, Internet of Medical Things (IoMT) devices, diagnostic imaging systems, wearable sensors, laboratory information systems, and cloud-based healthcare platforms. As healthcare organizations become increasingly interconnected, the attack surface available to cybercriminals continues to expand, exposing critical infrastructures to sophisticated cyber threats. Consequently, considerable research efforts have focused on the development of blockchain-based health security systems that strengthen data confidentiality, integrity, availability, authentication, and traceability while supporting secure healthcare operations. Across the literature, the primary objective of these systems is to establish secure mechanisms for collecting, transmitting, sharing, and managing healthcare information without compromising system performance or clinical efficiency. A common characteristic observed across the reviewed blockchain-based healthcare security systems is their emphasis on comprehensive security architecture combined with rigorous performance evaluation. Most investigations assess both the design characteristics of the proposed systems and their effectiveness in mitigating cybersecurity threats under simulated or real-world conditions. Security evaluation typically focuses on resilience against unauthorized access, data tampering, identity spoofing, communication interception, malware attacks, denial-of-service incidents, and privacy breaches. Simultaneously, system performance is evaluated through metrics including computational efficiency, communication overhead, transaction latency, scalability, throughput, energy consumption, storage requirements, and response time [8-15]. This balanced approach reflects the recognition that healthcare security solutions must simultaneously provide robust protection while maintaining the operational efficiency required for time-sensitive clinical environments. The majority of recently developed healthcare security frameworks combine blockchain technology with algorithmic approaches, artificial intelligence, cryptographic techniques, and distributed computing architectures. Algorithm-driven security mechanisms have become particularly valuable because they provide automated threat detection, adaptive access control, intelligent authentication, anomaly detection, and predictive cybersecurity capabilities that exceed the performance of conventional rule-based security systems. These intelligent approaches enable continuous monitoring of healthcare networks while minimizing computational complexity and preserving the functionality of connected medical devices. Consequently, algorithmic security has become an integral component of next-generation blockchain-enabled healthcare infrastructures [16-25].

Unauthorized access remains one of the most frequently reported cybersecurity threats affecting healthcare information systems. According to Selvarajan and Mouratidis (2023), attackers continuously attempt to obtain unauthorized access to confidential medical information through credential theft, privilege escalation, identity impersonation, or exploitation of software vulnerabilities [26]. Successful unauthorized access may expose electronic health records, diagnostic reports, prescription histories, financial information, and personally identifiable patient data. Because healthcare information possesses exceptionally high commercial value, protecting against unauthorized disclosure remains a primary objective of blockchain-based healthcare security systems.

Distributed denial-of-service (DoS) attacks constitute another major cybersecurity challenge facing modern healthcare organizations. These attacks intentionally overwhelm healthcare servers, communication networks, or cloud infrastructures with excessive malicious traffic, rendering critical healthcare services unavailable to legitimate users. During emergency situations, disruption of clinical information systems may delay diagnosis, interrupt treatment, impair communication among healthcare providers, and jeopardize patient safety. Blockchain-based architectures improve resilience against DoS attacks by distributing information across decentralized nodes rather than relying on centralized servers, thereby reducing single points of failure and improving service availability [26]. Man-in-the-middle attacks also represent a significant threat

within healthcare communication networks. In these attacks, malicious actors intercept communications between healthcare providers, patients, medical devices, or information systems without authorization. Attackers may modify transmitted information, steal confidential patient records, or manipulate clinical instructions before forwarding altered communications to the intended recipient. Blockchain technology, combined with strong cryptographic authentication and consensus mechanisms, significantly reduces susceptibility to these attacks by ensuring message authenticity, integrity verification, and secure communication channels [26]. Among the rapidly evolving cyber threats targeting healthcare organizations, ransomware has emerged as one of the most destructive attack vectors. Ransomware attacks encrypt healthcare databases and critical information systems, preventing authorized users from accessing essential clinical data until financial demands are satisfied. These attacks frequently disrupt hospital operations, delay medical procedures, and compromise patient care. Although ransomware has been widely recognized throughout the healthcare cybersecurity literature, Javaid et al. (2023) [2] observed that only a limited number of studies comprehensively evaluate ransomware within integrated healthcare security frameworks. Abuasal et al. (2024) [38] specifically identified ransomware as a primary cybersecurity threat and incorporated detailed analysis of ransomware prevention, detection, and mitigation strategies within their proposed healthcare security model. This broader consideration highlights the growing importance of designing healthcare security systems capable of addressing evolving malware threats alongside conventional cyberattacks.

Medical image security represents another emerging research area within healthcare cybersecurity. Anand et al. (2024) [30] evaluated the robustness of their proposed healthcare security framework against several categories of image manipulation attacks. Their analysis included noise removal attacks involving Gaussian noise injection, geometric attacks including image rotation, zooming, resizing, cropping, and JPEG compression, as well as protocol-based attacks targeting image transmission processes. These evaluations demonstrate the increasing recognition that medical images require protection not only against unauthorized access but also against subtle manipulations capable of altering clinical diagnoses. Ensuring the authenticity and integrity of radiological images has therefore become an important objective of blockchain-supported healthcare security architectures. Intrusion detection systems have likewise become essential components of modern healthcare cybersecurity. Ravi (2023) [14] evaluated the performance of the N-IDS intrusion detection framework using multiple healthcare datasets to assess its capability for identifying malicious network activities. Intelligent intrusion detection systems continuously monitor healthcare communication networks, identify abnormal traffic patterns, and generate early alerts that enable rapid incident response. Integration of blockchain with intelligent intrusion detection enhances system transparency while improving the reliability and traceability of detected cybersecurity events. Blockchain technology has become one of the most extensively investigated approaches for strengthening healthcare cybersecurity. Numerous researchers have proposed innovative blockchain-enabled healthcare security frameworks that combine decentralized data management, cryptographic authentication, artificial intelligence, smart contracts, and distributed consensus mechanisms to address diverse healthcare cybersecurity challenges.

One of the earliest comprehensive frameworks was introduced by Tariq et al. (2020) [15], who developed a blockchain-based security solution for Internet of Things-enabled smart healthcare systems. Their framework utilized blockchain to create a distributed and scalable infrastructure for secure medical transaction management while maintaining immutable patient records. The proposed architecture enhanced secure communication among healthcare providers, strengthened patient ownership of medical information, and improved transparency throughout healthcare information exchange. Puri et al. (2021) [16] further advanced this concept by integrating blockchain with artificial intelligence to establish a decentralized patient data management system. Their framework employed blockchain-based smart contracts combined with rule-based artificial intelligence algorithms to detect malicious IoT devices while simultaneously improving energy efficiency, minimizing communication delays, and optimizing transaction performance. The system focused primarily on protecting personal health records while automatically identifying suspicious network activities through embedded intelligent decision-making mechanisms. Abid et al. (2022) [17] proposed a decentralized healthcare access control framework utilizing smart contracts together with the Generalized Temporal Role-Based Access Control model. Unlike conventional access control systems, this approach incorporated time-dependent authorization policies that dynamically regulated access privileges according to predefined temporal constraints. Experimental evaluation demonstrated low computational latency and reduced transaction costs, indicating that sophisticated access control mechanisms can substantially improve healthcare security without imposing excessive computational burdens.

Blockchain applications have also expanded into healthcare administrative processes. Sharma et al. (2023) [18] developed an Ethereum-based blockchain application for managing medical certificates through

smart contracts. Their system enhanced transparency, improved document authenticity, reduced fraudulent certificate generation, and strengthened trust among healthcare organizations, patients, and regulatory authorities while maintaining efficient transaction processing. Selvarajan and Mouratidis (2023) [19] introduced the Consultative Transaction Key Generation and Management framework, which combines blockchain with advanced cryptographic techniques for secure healthcare communication. Their architecture utilizes the Quantum Trust Reconciliation Agreement Model to evaluate trust relationships among communicating entities while employing Tuna Swarm Optimization algorithms to validate nonce messages and ensure efficient cryptographic key generation. This combination of optimization algorithms and blockchain technology significantly strengthens authentication and secure data transmission. Similarly, Rani et al. (2023) [20] proposed an Internet of Things-based distributed healthcare framework integrating blockchain, artificial intelligence, smart contracts, and distributed database management systems. Their architecture eliminates single points of failure while improving healthcare transparency, data integrity, operational reliability, and secure remote healthcare delivery. The decentralized nature of the framework significantly enhances resilience against network failures and malicious cyberattacks. Recent studies have continued expanding blockchain capabilities within healthcare environments. Akinola et al. (2024) [21] designed a blockchain architecture integrating cryptographic hashing, digital signatures, Proof-of-Work, and Proof-of-Stake consensus mechanisms while ensuring compliance with both HIPAA and General Data Protection Regulation (GDPR) requirements. Their framework demonstrates how regulatory compliance can be incorporated directly into blockchain architectures while maintaining the integrity of healthcare device data.

Mohammed et al. (2024) [22] proposed the Pattern-Proof Malware Validation framework for distributed cloud-fog healthcare environments. Although specific attack scenarios were not explicitly evaluated, the proposed architecture demonstrated strong performance in malware validation and healthcare workflow protection within distributed computing infrastructures. Wu et al. (2024) [24] applied Hyperledger Composer technology to secure implant supply chain management using blockchain combined with hybrid encryption techniques. Their framework improved traceability, transparency, and security throughout healthcare logistics operations. Mallick et al. (2024) [25] further extended blockchain integration by combining the Internet of Medical Things, fog computing, blockchain, and the InterPlanetary File System into a unified decentralized medical information platform. Their framework employed the Elliptic Curve Digital Signature Algorithm to strengthen authentication while supporting scalable healthcare data storage and secure decentralized retrieval. Idrissi and Palmieri (2024) [26] proposed a blockchain-enabled Attribute-Based Access Control architecture integrating mobile agents and Elliptic Curve Cryptography to achieve efficient mutual authentication and rapid cryptographic key agreement while minimizing communication overhead. Despite these significant advances, blockchain implementation within healthcare continues to face several important challenges. Scalability remains one of the most frequently cited limitations. Akinola et al. (2024) [21] emphasized that although blockchain architectures theoretically support scalability, practical implementation within large healthcare networks requires more sophisticated artificial intelligence algorithms capable of managing extremely high transaction volumes without sacrificing performance. As healthcare organizations continue generating massive quantities of clinical information, maintaining rapid transaction processing becomes increasingly difficult. Performance degradation represents another major concern. The exponential growth of connected medical devices, wearable sensors, diagnostic equipment, and Internet of Medical Things technologies continuously increases blockchain transaction loads, resulting in reduced throughput, increased latency, and greater computational complexity. Such delays may significantly affect time-critical healthcare services where rapid access to patient information is essential for clinical decision-making. Consequently, performance optimization remains a major priority for future blockchain research [21].

Computational efficiency also presents important challenges for distributed healthcare environments. Mohammed et al. (2024) [22] demonstrated that increasing numbers of failed workflow tasks significantly increase computational time within distributed cloud-fog healthcare systems. Federated artificial intelligence has emerged as a promising solution because it distributes computational workloads across edge devices rather than relying exclusively on centralized processing. This decentralized analytical approach reduces communication overhead, minimizes storage requirements, improves scalability, lowers energy consumption, and strengthens patient privacy by avoiding unnecessary transmission of sensitive healthcare information. Finally, successful implementation of blockchain technology depends not only on cybersecurity performance but also on usability and user acceptance. Healthcare organizations operate across highly diverse clinical environments requiring flexible interfaces that accommodate physicians, nurses, pharmacists, administrators, and technical personnel. Wu et al. (2024) [24] emphasized that optimizing user interfaces, maintaining operational efficiency, and minimizing computational complexity remain

essential for achieving widespread adoption of blockchain-enabled healthcare security systems.

Attack Types and Mitigation Strategies

The continuous evolution of healthcare information systems has been accompanied by an equally rapid increase in the sophistication of cyber threats targeting digital healthcare infrastructures. Hospitals, clinics, diagnostic laboratories, telemedicine platforms, cloud-based electronic health records, and Internet of Medical Things (IoMT) devices are increasingly exposed to attacks that threaten the confidentiality, integrity, and availability of sensitive medical information. Consequently, understanding the characteristics of these attacks and the corresponding mitigation strategies has become essential for designing secure healthcare environments. The blockchain- and algorithm-based systems reviewed in this study primarily focus on preventing unauthorized access, preserving data integrity, ensuring secure communication, and maintaining uninterrupted healthcare services. Their effectiveness depends not only on strong cryptographic mechanisms but also on intelligent detection algorithms, decentralized architectures, and adaptive security protocols capable of responding to evolving cyber threats. Before discussing the principal attack categories, it is important to consider systems that were not explicitly evaluated against specific attack scenarios but nevertheless demonstrated significant improvements in healthcare cybersecurity performance. The Elliptic Curve Cryptography-based Energy Efficient Routing Protocol (ECC-EERP) represents one such example. Although its evaluation emphasized system efficiency rather than resistance to individual cyberattacks, experimental results demonstrated remarkable improvements in encryption efficiency, achieving approximately 99% encryption accuracy while simultaneously reducing computational complexity, communication overhead, and energy consumption. The protocol also extended network lifetime and improved processing speed compared with existing healthcare communication frameworks. These findings suggest that efficient cryptographic architectures contribute substantially to healthcare cybersecurity by reducing system vulnerabilities while preserving operational performance, even when explicit attack simulations are not conducted [13].

Similarly, the Encryption Framework for Secure Telehealth and Electronic Health Records emphasized functional validation and system performance rather than comprehensive cybersecurity stress testing. Although the framework was not specifically evaluated against advanced threats such as distributed denial-of-service attacks or man-in-the-middle attacks, its successful functional and performance testing demonstrated reliable encryption capabilities, secure data transmission, and efficient healthcare information management. These characteristics justify its inclusion among modern healthcare security solutions because practical system reliability remains an essential component of cybersecurity preparedness [33]. Among the most significant cybersecurity threats affecting healthcare information systems is the man-in-the-middle attack. In this attack, a malicious actor secretly intercepts communication between two legitimate parties while maintaining the illusion that communication remains secure. During interception, attackers may monitor confidential information, alter transmitted data, inject malicious content, or manipulate clinical communications without detection. Within healthcare environments, such attacks may compromise electronic health records, laboratory results, diagnostic images, prescription information, or physician communications, potentially leading to incorrect clinical decisions and compromised patient safety. Modern blockchain-based healthcare systems mitigate these attacks through advanced cryptographic authentication protocols, secure key agreement mechanisms, digital signatures, and decentralized verification processes. Formal verification tools such as the Automated Validation of Internet Security Protocols and Applications (AVISPA) have demonstrated the effectiveness of these authentication mechanisms in preventing unauthorized communication interception and ensuring secure healthcare data exchange [26]. Denial-of-service (DoS) attacks represent another critical cybersecurity challenge. In these attacks, malicious users deliberately overwhelm healthcare servers or communication infrastructures by transmitting excessive numbers of fraudulent service requests. As computational resources become exhausted, legitimate users experience severe delays or complete inability to access essential healthcare services. The consequences of DoS attacks within hospitals may include interruption of emergency care, delayed diagnostic procedures, disruption of telemedicine consultations, and temporary unavailability of electronic health records. Decentralized blockchain architectures reduce vulnerability to DoS attacks by distributing computational resources across multiple nodes rather than relying on centralized servers, thereby eliminating single points of failure and improving system resilience [31].

Distributed denial-of-service (DDoS) attacks represent an even greater threat because they originate simultaneously from numerous compromised devices forming coordinated botnets. Unlike conventional DoS attacks, DDoS attacks generate substantially greater traffic volumes that may incapacitate entire healthcare networks for prolonged periods. Such attacks may interrupt critical hospital operations, prevent access to patient information, delay life-saving treatments, and compromise organizational continuity.

Contemporary healthcare security systems increasingly employ artificial intelligence, anomaly detection algorithms, traffic filtering mechanisms, blockchain-based decentralized architectures, and intelligent intrusion prevention systems to detect abnormal network behavior and mitigate DDoS attacks before significant operational disruption occurs [39]. Wireless healthcare networks and Internet of Medical Things environments are additionally susceptible to routing attacks that compromise secure communication. One such attack is the Blackhole attack, in which a malicious network node falsely advertises itself as the optimal routing destination before discarding intercepted data packets instead of forwarding them to their intended recipients. This attack effectively disrupts communication while preventing critical medical information from reaching healthcare providers. Blockchain-supported routing protocols, distributed trust management systems, and intelligent node authentication algorithms significantly reduce susceptibility to Blackhole attacks by continuously validating routing behavior and identifying malicious network participants [29]. Selective forwarding attacks similarly target communication reliability by intentionally discarding selected data packets while allowing other transmissions to proceed normally. This selective disruption makes detection considerably more difficult than complete communication failure. In healthcare applications, attackers may specifically target highly sensitive clinical information, thereby delaying or preventing delivery of critical patient data. Blockchain consensus mechanisms and distributed communication verification improve resistance to selective forwarding by maintaining immutable transaction records and validating successful data transmission across multiple network nodes [29].

Another significant routing attack is the Sybil attack, during which a malicious device assumes multiple false identities within a communication network. By creating numerous fabricated identities, attackers manipulate network operations, compromise consensus mechanisms, and gain unauthorized influence over distributed decision-making processes. Healthcare blockchain systems mitigate Sybil attacks through robust identity verification, public-key cryptography, digital certificates, consensus algorithms, and decentralized authentication protocols that ensure each network participant possesses a unique and verifiable digital identity [29]. Hello Flood attacks represent another threat commonly encountered within wireless sensor networks supporting healthcare applications. During these attacks, malicious devices repeatedly transmit fraudulent Hello messages to neighboring nodes, misleading them into establishing inefficient or invalid communication pathways. The resulting communication disruption increases network congestion, wastes computational resources, and reduces overall system reliability. Advanced blockchain routing protocols and intelligent neighbor authentication mechanisms reduce the effectiveness of Hello Flood attacks by validating node legitimacy before establishing communication channels [29]. Privacy leakage remains one of the most critical concerns within healthcare cybersecurity because unauthorized disclosure of patient information may produce severe ethical, legal, financial, and clinical consequences. Privacy violations may occur through inadequate encryption, insecure communication channels, improper access control, insider misuse, or external cyberattacks. Blockchain technology significantly strengthens privacy protection through decentralized storage, cryptographic encryption, permission-based access control, pseudonymization, and immutable transaction records that prevent unauthorized disclosure of sensitive healthcare information [15].

Data tampering constitutes another major cybersecurity threat involving unauthorized modification of healthcare records. Attackers may alter laboratory results, diagnostic reports, medication histories, imaging studies, or treatment plans, potentially leading to incorrect diagnoses and harmful clinical decisions. Blockchain technology effectively mitigates data tampering because each transaction is permanently linked through cryptographic hash functions. Any unauthorized modification immediately alters the cryptographic signature of subsequent blocks, making manipulation readily detectable while preserving complete auditability throughout the healthcare information lifecycle [15,26]. Forgery attacks involve the creation of counterfeit healthcare information, including fabricated medical records, fraudulent prescriptions, falsified laboratory reports, or unauthorized financial transactions. Such attacks undermine healthcare integrity, facilitate insurance fraud, and compromise patient safety. Elliptic Curve Cryptography, blockchain verification, mobile agents, and digital signature algorithms provide strong protection against forgery by ensuring that every healthcare transaction originates from authenticated users and remains cryptographically verifiable throughout its lifecycle [15,26]. Traditional centralized healthcare information systems are additionally vulnerable to single points of failure, whereby failure or compromise of one central server disrupts the entire healthcare infrastructure. Hardware failures, cyberattacks, software corruption, or natural disasters affecting centralized systems may render critical healthcare services unavailable. Blockchain addresses this limitation through decentralized data storage across multiple interconnected nodes, ensuring continuous availability even when individual nodes become compromised or unavailable [15]. Privacy violation attacks specifically target confidential healthcare information through unauthorized access, disclosure, or surveillance. Anonymous authentication protocols, decentralized identity management, cryptographic authentication,

and blockchain-based access control substantially reduce these risks by allowing healthcare professionals to verify identities without exposing unnecessary personal information. These mechanisms simultaneously strengthen patient privacy while maintaining secure clinical communication [26].

Healthcare data breaches remain among the most damaging cybersecurity incidents because they expose highly sensitive medical and financial information to unauthorized individuals. Attackers frequently exploit phishing campaigns, credential theft, software vulnerabilities, insider threats, and malware infections to gain unauthorized access to healthcare databases. Data breaches may result in identity theft, financial fraud, legal penalties, reputational damage, and diminished public trust. Comprehensive healthcare security frameworks therefore integrate encryption, multi-factor authentication, continuous monitoring, behavioral analytics, access logging, blockchain verification, and artificial intelligence to minimize breach risk while facilitating rapid detection and incident response [34]. Ransomware has emerged as one of the most disruptive cyber threats confronting healthcare organizations. This malicious software encrypts critical healthcare databases, rendering patient records inaccessible until financial demands are satisfied. Because hospitals depend heavily on uninterrupted access to electronic health records and diagnostic systems, ransomware attacks may delay emergency care, postpone surgeries, interrupt laboratory services, and jeopardize patient safety. Modern mitigation strategies include continuous data backup, blockchain-secured storage, endpoint detection systems, artificial intelligence-based malware detection, network segmentation, zero-trust security architectures, employee cybersecurity education, and rapid incident response planning. Collectively, these measures significantly reduce the likelihood and impact of ransomware attacks while strengthening organizational resilience [40]. Although additional cybersecurity threats exist, including malware variants, stolen devices, offline password attacks, communication protocol vulnerabilities, anonymity attacks, and untraceability exploits, many share common characteristics with the principal attack categories discussed above. Consequently, future healthcare cybersecurity research should prioritize comprehensive evaluation of security systems against these major attack classes while simultaneously developing adaptive protection mechanisms capable of responding to continuously evolving cyber threats. Equally important is the continuous testing, validation, and refinement of hospital information systems under changing operational conditions. Regular security assessments, penetration testing, vulnerability analysis, algorithm updates, and performance optimization are essential to maintaining resilient healthcare infrastructures capable of protecting sensitive patient information while ensuring uninterrupted, safe, and reliable healthcare delivery.

Conclusion:

The increasing digitalization of healthcare has transformed clinical practice while simultaneously introducing complex cybersecurity challenges that threaten healthcare organizations worldwide. Protecting sensitive patient information now requires security solutions that extend beyond traditional centralized approaches. The reviewed evidence demonstrates that blockchain technology, combined with artificial intelligence, advanced cryptographic algorithms, smart contracts, and intelligent intrusion detection systems, provides a secure and transparent framework for safeguarding healthcare information throughout its lifecycle. These technologies strengthen data integrity, authentication, privacy protection, access control, and secure communication while improving resilience against cyber threats such as ransomware, denial-of-service attacks, unauthorized access, data tampering, and communication interception. Nevertheless, important challenges remain, including blockchain scalability, computational complexity, interoperability, latency, and implementation costs. Addressing these limitations through algorithm optimization, federated artificial intelligence, user-centered system design, and standardized healthcare security frameworks will be critical for future development. Continued collaboration among healthcare professionals, cybersecurity experts, policymakers, and informatics specialists is essential to establish resilient health security systems capable of ensuring patient safety, maintaining public trust, supporting regulatory compliance, and enabling secure digital healthcare services in increasingly interconnected healthcare environments.

References:

1. Almalawi, A.; Khan, A.I.; Alsolami, F.; Abushark, Y.B.; Alfakeeh, A.S. Managing Security of Healthcare Data for a Modern Healthcare System. *Sensors* **2023**, *23*, 3612.
2. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends. *Cyber Secur. Appl.* **2023**, *1*, 100016.
3. Lee, I. Analyzing Web Descriptions of Cybersecurity Breaches in the Healthcare Provider Sector: A Content Analytics Research Method. *Comput. Secur.* **2023**, *129*, 103185.
4. Mariettou, S.; Koutsojannis, C.; Triantafillou, V. Security Systems in Greek Health Care Institutions: A Scoping Review Towards an Effective Benchmarking Approach. In Proceedings of the International Conferences e-

Society 2024 and Mobile Learning, Porto, Portugal, 9–11 March 2024; pp. 53–60.
5. Coutinho, B.; Ferreira, J.; Yevseyeva, I.; Basto-Fernandes, V. Integrated Cybersecurity Methodology and Supporting Tools for Healthcare Operational Information Systems. *Comput. Secur.* **2023**, *129*, 103189.
6. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology. *Circ. Cardiovasc. Qual. Outcomes* **2017**, *10*, e003800.
7. Azzaoui, A.E.; Chen, H.; Kim, S.H.; Pan, Y.; Park, J.H. Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems. *Sensors* **2022**, *22*, 1371.
8. Riplinger, L.; Piera-Jiménez, J.; Dooling, J.P. Patient Identification Techniques—Approaches, Implications, and Findings. *Yearb. Med. Inform.* **2020**, *29*, 81–86.
9. Ali, R.; Pal, A.K.; Kumari, S.; Sangaiah, A.K.; Li, X.; Wu, F. An Enhanced Three Factor Based Authentication Protocol Using Wireless Medical Sensor Networks for Healthcare Monitoring. *J. Ambient Intell. Humaniz. Comput.* **2018**, *15*, 1165–1186.
10. Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. Available online: **https://ieeexplore.ieee.org/document/9109651**
11. Kanagala, P. Effective Cyber Security System to Secure Optical Data Based on Deep Learning Approach for Healthcare Application. *Optik* **2022**, *272*, 170315.
12. Sardar, A.; Umer, S.; Rout, R.K.; Wang, S.-H.; Tanveer, M. A Secure Face Recognition for IoT-Enabled Healthcare System. *ACM Trans. Sens. Netw.* **2022**, *19*, 1–23.
13. Natarajan, R.; Lokesh, G.H.; Flammini, F.; Premkumar, A.; Venkatesan, V.K.; Gupta, S.K. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. *Infrastructures* **2023**, *8*, 22.
14. Ravi, V. Deep Learning-Based Network Intrusion Detection in Smart Healthcare Enterprise Systems. *Multimed. Tools Appl.* **2023**, *83*, 39097–39115.
15. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and Smart Healthcare Security: A Survey. *Procedia Comput. Sci.* **2020**, *175*, 615–620.
16. Puri, V.; Kataria, A.; Sharma, V. Artificial Intelligence-powered Decentralized Framework for Internet of Things in Healthcare 4.0. *Trans. Emerg. Telecommun. Technol.* **2021**, *35*, e4245.
17. Abid, A.; Cheikhrouhou, S.; Kallel, S.; Tari, Z.; Jmaiel, M. A Smart Contract-Based Access Control Framework for Smart Healthcare Systems. *Comput. J.* **2022**, *67*, 407–422.
18. Sharma, P.; Namasudra, S.; Crespo, R.G.; Parra-Fuente, J.; Trivedi, M.C. EHDHE: Enhancing Security of Healthcare Documents in IoT-Enabled Digital Healthcare Ecosystems Using Blockchain. *Inf. Sci.* **2023**, *629*, 703–718.
19. Selvarajan, S.; Mouratidis, H. A Quantum Trust and Consultative Transaction-Based Blockchain Cybersecurity Model for Healthcare Systems. *Sci. Rep.* **2023**, *13*, 7107.
20. Rani, S.; Chauhan, M.; Kataria, A.; Khang, A. IoT Equipped Intelligent Distributed Framework for Smart Healthcare Systems. In *Studies in Big Data*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 97–114.
21. Akinola, O.; Akinola, A.; Oyekan, B.; Oyerinde, O.; Adebiyi, H.F.; Sulaimon, B. Blockchain-Enabled Security Solutions for Medical Device Integrity and Provenance in Cloud Environments. *Int. J. Sci. Res. Mod. Technol.* **2024**, *3*, 123–135.
22. Mohammed, M.A.; Lakhan, A.; Zebari, D.A.; Ghani, M.K.A.; Marhoon, H.A.; Abdulkareem, K.H.; Nedoma, J.; Martinek, R. Securing Healthcare Data in Industrial Cyber-Physical Systems Using Combining Deep Learning and Blockchain Technology. *Eng. Appl. Artif. Intell.* **2024**, *129*, 107612.
23. An AOI-Aware Data Transmission Algorithm in Blockchain-Based Intelligent Healthcare Systems. Available online: **https://ieeexplore.ieee.org/document/10433851**
24. Wu, C.; Tang, Y.M.; Kuo, W.T.; Yip, H.T.; Chau, K.Y. Healthcare 5.0: A Secure and Distributed Network for System Informatics in Medical Surgery. *Int. J. Med. Inform.* **2024**, *186*, 105415.
25. Mallick, S.R.; Lenka, R.K.; Tripathy, P.K.; Rao, D.C.; Sharma, S.; Ray, N.K. A Lightweight, Secure, and Scalable Blockchain-Fog-IoMT Healthcare Framework with IPFS Data Storage for Healthcare 4.0. *SN Comput. Sci.* **2024**, *5*, 198.
26. Idrissi, H.; Palmieri, P. Agent-Based Blockchain Model for Robust Authentication and Authorization in IoT-Based Healthcare Systems. *J. Supercomput.* **2023**, *80*, 6622–6660.
27. Chakraborty, C.; Nagarajan, S.M.; Devarajan, G.G.; Ramana, T.V.; Mohanty, R. Intelligent AI-Based Healthcare Cyber Security System Using Multi-Source Transfer Learning Method. *ACM Trans. Sens. Netw.* **2023**.
28. Banu, S.A.; Al-Alawi, A.I.; Padmaa, M.; Priya, P.S.; Thanikaiselvan, V.; Amirtharajan, R. Healthcare with Datacare—A Triangular DNA Security. *Multimed. Tools Appl.* **2023**, *83*, 21153–21170.
29. Jabeen, T.; Jabeen, I.; Ashraf, H.; Jhanjhi, N.Z.; Yassine, A.; Hossain, M.S. An Intelligent Healthcare System Using IoT in Wireless Sensor Network. *Sensors* **2023**, *23*, 5055.

30. Anand, A.; Bedi, J.; Aggarwal, A.; Khan, M.A.; Rida, I. Authenticating and Securing Healthcare Records: A Deep Learning-Based Zero Watermarking Approach. *Image Vis. Comput.* **2024**, *145*, 104975.
31. Aldosary, A.; Tanveer, M. PAAF-SHS: PUF and Authenticated Encryption Based Authentication Framework for the IoT-Enabled Smart Healthcare System. *Internet Things* **2024**, *26*, 101159.
32. Gopalakrishnan, N.R.; Kumar, N.R.M.S. Cloud Security System for ECG Transmission and Monitoring Based on Chaotic Logistic Maps. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2024**, *39*, 1–18.
33. Wenhua, Z.; Hasan, M.K.; Jailani, N.B.; Islam, S.; Safie, N.; Albarakati, H.M.; Aljohani, A.; Khan, M.A. A Lightweight Security Model for Ensuring Patient Privacy and Confidentiality in Telehealth Applications. *Comput. Hum. Behav.* **2024**, *153*, 108134.
34. Pichandi, K.V.; Janarthanan, V.; Annamalai, T.; Arumugam, M. Enhancing Healthcare in the Digital Era: A Secure e-Health System for Heart Disease Prediction and Cloud Security. *Expert Syst. Appl.* **2024**, *255*, 124479.
35. Saini, K.K.; Kaur, D.; Kumar, D.; Kumar, B. An Efficient Three-Factor Authentication Protocol for Wireless Healthcare Sensor Networks. *Multimed. Tools Appl.* **2024**, *83*, 63699–63721.
36. Nadhan, A.S.; Jacob, I.J. Enhancing Healthcare Security in the Digital Era: Safeguarding Medical Images with Lightweight Cryptographic Techniques in IoT Healthcare Applications. *Biomed. Signal Process. Control* **2024**, *88*, 105511.
37. Clemente-Lopez, D.; De Jesus Rangel-Magdaleno, J.; Muñoz-Pacheco, J.M. A Lightweight Chaos-Based Encryption Scheme for IoT Healthcare Systems. *Internet Things* **2023**, *25*, 101032.
38. Abuasal, S.; Alsarayra, K.; Alyabroodie, Z. Designing a Standard-Based Approach for Security of Healthcare Systems. *J. Stat. Appl. Probab.* **2024**, *13*, 419–434.
39. Snehi, M.; Bhandari, A. Vulnerability Retrospection of Security Solutions for Software-Defined Cyber–Physical System against DDoS and IoT-DDoS Attacks. *Comput. Sci. Rev.* **2021**, *40*, 100371.

Ali, A. Ransomware: A Research and a Personal Case Study of Dealing with This Nasty Malware. Available online: **https://www.informingscience.org/Publications/3707**.