algorithms

MDPI

Review

Artificial Intelligence and Algorithmic Approaches of Health Security Systems: A Review

Savina Mariettou [1], Constantinos Koutsojannis [2,*] and Vassilios Triantafillou [3]

[1] Health Physics & Computational Intelligence Laboratory, School of Health Rehabilitation Sciences, University of Patras, 26504 Patras, Greece; s.mariettou@go.uop.gr
[2] Medical Physics & Electrophysiology, Health Physics & Computational Intelligence Laboratory, School of Health Rehabilitation Sciences, University of Patras, 26504 Patras, Greece
[3] Network Technologies, Health Physics & Computational Intelligence Laboratory, School of Health Rehabilitation Sciences, University of Patras, 26504 Patras, Greece; vtriantaf@uop.gr
* Correspondence: ckoutsog@upatras.gr

Abstract: This paper explores the overall picture regarding healthcare security systems through an extensive literature review. As the healthcare sector has now become digitalized, the security of healthcare systems and, by extension, the protection of patient data is a key concern in the modern era of technological advances. Therefore, a secure and integrated system is now essential. Thus, to evaluate the relationship between security systems and healthcare quality, we conducted literature research to identify studies reporting their association. The timeline of our review is based on published studies covering the period from 2018 to 2024, with entries identified through a search of the relevant literature, focusing on the most recent developments due to advances in artificial intelligence and algorithmic approaches. Thirty-two studies were included in our final survey. Our findings underscore the critical role of security systems in healthcare that significantly improve patient outcomes and maintain the integrity of healthcare services. According to our approach, the studies analyzed highlight the growing importance of advanced security frameworks, especially those incorporating artificial intelligence and algorithmic methodologies, in safeguarding healthcare systems while enhancing patient care quality. According to this study, most of the research analyzed uses algorithmic technology approaches, many researchers prove that ransomware is the most common threat to hospital information systems, and more studies are needed to evaluate the performance of the systems created against this kind of attack.

Keywords: health security; data protection; cybersecurity in healthcare; algorithmic; artificial intelligence; approaches

check for updates

Academic Editors: Jaafar Alghazo, Ghazanfar Latif and Elena Tanfani

Received: 4 November 2024
Revised: 3 January 2025
Accepted: 17 January 2025
Published: 22 January 2025

Citation: Mariettou, S.; Koutsojannis, C.; Triantafillou, V. Artificial Intelligence and Algorithmic Approaches of Health Security Systems: A Review. *Algorithms* **2025**, *18*, 59. https://doi.org/10.3390/a18020059

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The healthcare sector is a target for cyber-attacks mainly because of the constant movement of sensitive information and data [1]. The digitization of medical information, the transmission of patient data, and the application of the Internet of Things (IoT) to healthcare services offer new levels of efficiency and accessibility, improving the quality of patient care. However, increased connectivity and widespread data storage raise significant security challenges [2]. In modern medical technology systems, patient data are now one of the most critical issues in modern medical technology [1]. The healthcare sector is a target for cyber-attacks mainly because of the constant movement of sensitive information and data [2]. The digitization of medical information, the transmission of patient data,

and the application of the Internet of Things to healthcare services offer new levels of efficiency and accessibility, improving the quality of patient care. However, increased connectivity and widespread data storage raise significant security challenges [1]. Data breaches in healthcare are a serious issue regulated by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Some data breaches can be due to human error, theft, and data loss. Human error breaches have increased rapidly; however, theft and data corruption remain high [3]. It is also important to note that in many countries this issue of information systems security has been underestimated [4]. Despite the increase in attacks, many healthcare organizations are still investing a small portion of their budget in cybersecurity, which increases the likelihood of vulnerability [2]. The COVID-19 pandemic has contributed significantly to the increase in cyber-attacks targeting healthcare organizations, with the most common threats including ransomware, fake accounts, phishing, disinformation campaigns, and supply chain disruptions [5]. The increase in cyber-attacks in the healthcare sector in 2019 has motivated many companies to test more innovative mechanisms and technologies to secure their information systems such as blockchain and algorithmic approaches.

Blockchain provides a secure, decentralized healthcare system for managing sensitive medical data. Each transaction, such as updates to electronic health records (EHRs), patient consent management, or tracking pharmaceuticals, is encrypted, timestamped, and stored in an immutable ledger. Updates generate unique hashes that ensure data integrity and create an auditable trail.

A significant advantage is patient control over data access through decentralized platforms, enabling seamless and secure data sharing among providers while ensuring transparency and compliance. Additionally, blockchain enhances pharmaceutical supply chains by verifying drug authenticity and tracking distribution. It also streamlines insurance claims by automating validation and eligibility processes, reducing inefficiencies and fraud. Through cryptography and consensus mechanisms, blockchain ensures data accuracy, security, and trust among healthcare stakeholders, fostering a more interoperable and reliable healthcare system [6].

Delving deeper into the technology itself, blockchain is a system that uses public key encryption for authentication and records every transaction on a network. Once a transaction is completed, it cannot be modified. The network consists of nodes, where each node records transaction information in blocks in chronological order, with each new block connected to the previous one, forming a chain. This structure ensures data security. This security serves the system well, as if an attacker who would like to compromise one block, they would have to compromise the entire chain. The blockchain uses hashing algorithms, which make any attempt to tamper with the data detectable. Each node communicates with the other nodes in the network and can publish/transmit information. To prevent tampering, a consensus mechanism is in place to ensure the reliability of the information. The block is completed by validating the information created on a network. Therefore, when the information is validated, it is packed into a new block and added to the chain. Note that nodes working in the consensus process are motivated to do so. They are usually rewarded financially for their contribution to the security and stability of the network.

Due to its decentralization, a public blockchain utilizes cryptography and consensus mechanisms such as proof of work or proof of ownership to ensure the integrity and security of the data [7]. All these features come together to create a robust system for secure and trustworthy data management, as seen in the visual representation of a blockchain transaction in Figure 1, where nodes or users agree to a transaction.

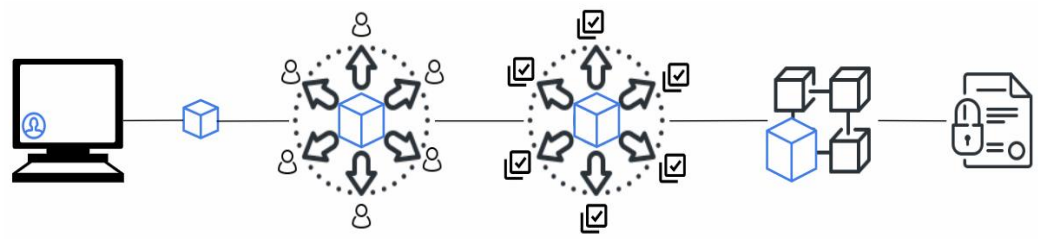


Figure 1. Visual representation of a blockchain transaction.

Similarly, algorithmic approaches are key tools in Health Security Systems, as they enable the accurate matching of patients with their health information. By using demographic information such as first name, last name, gender, date of birth, social security number, and address, algorithms ensure the integrity and reliability of patient data. Techniques range from simple, deterministic approaches, where a unique identifier is compared with a few non-unique attributes, to more complex probabilistic matching techniques that use thresholds. The contribution of algorithmic approaches to health security systems is vital, as they allow for the secure management of patient data despite any errors or missing data. However, algorithmic design remains a challenge due to variables, such as inaccurate demographic information and data heterogeneity, which can reduce accuracy [8].

This article aims to highlight the current situation regarding the security of healthcare systems and to improve existing systems to enhance the quality of care for patients.

The article is organized as follows: In Section 2, a detailed analysis of the 31 identified security systems is presented. In Section 3, the methods used to identify and evaluate these systems are described, including an analysis of the Inclusion and Exclusion Criteria. Section 4 presents the findings of our study, describing security systems based on blockchain approaches, discussing attack types and mitigation strategies, and analyzing ransomware. Section 5 provides the discussion and conclusions, while Section 6 outlines future work.

2. Overview of Health Security Systems

In the era of digitalization, threats to the security of healthcare systems have significantly increased. Examples such as the creation of fake medical data, such as the introduction of fictitious conditions (e.g., fake tumors) or high-profile diseases (AIDS, SARS, Ebola) into diagnostic records, are serious threats that can mislead the medical community and lead to incorrect treatments. Researchers in Israel have developed a virus that can insert fake tumor data into Computed Tomography (CT) and Magnetic Resonance Imaging (MRI) scans, misleading doctors into erroneous diagnoses [5]. This threat is particularly alarming, as the security of medical data, including images and associated records, is critical for the accuracy of diagnoses and the effectiveness of treatment. The PACS (Picture Archiving and Communication System), which is used to store and manage medical data, exhibits vulnerabilities since it is connected to various networks and systems. This creates a large attack surface, allowing malicious users to compromise data and gain access to other critical health information. This makes the security of medical data essential for maintaining the integrity of diagnoses and patient care. An extensive literature review follows, documenting various security systems developed to protect against such threats (Table 1). Through a detailed examination of these systems, their descriptions, summaries, and the attacks they mitigate, we demonstrate how security remains paramount to the integrity of diagnoses and safe patient care.

Table 1. Comprehensive Analysis of Health Security Systems.

Author(s)	Security System	Synopsis	Mitigated Attacks	Evidence Type
[1]	LRO-S encryption method	It combines lion and remora optimization with serpent encryption to secure medical data, offering enhanced protection against cyber-attacks and privacy breaches, with improved encryption/decryption time and performance compared to existing methods.	Privacy Breaches, Unauthorized Access	Cryptographic, Algorithmic, Mathematical
[9]	WMSNs (Wireless Medical Sensor Networks)	It operates using three-factor authentication to securely verify remote users in WMSN environments. Additionally, it has been validated using Burrows–Abadi–Needham (BAN) logic and the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool.	Unauthorized Access, Offline Password Guessing Attacks	Simulation
[10]	IDS (Intrusion Detection System)	The proposed IDS is designed to detect network intrusions while minimizing the load on resource-constrained sensors, enhancing security without overburdening limited-capacity devices.	Man-in-the-middle	Empirical
[11]	Modified deep learning approach based on Cyber–Physical Systems (CPS)	The system uses deep learning and CPS for the secure processing of IoT data, protecting against DoS and DDoS attacks, with 98.2% accuracy and improved performance compared to existing models such as LSTM and CNN.	DoS (Denial of Service), DDoS (Distributed Denial of Service)	Algorithmic, Performance
[12]	BioCryptosystem	It enhances the security of biometric data by using FaceHashing with BioCrypto-Circuit and BioCrypto-Protection techniques, offering robust protection against external attacks and misuse.	Unauthorized Access	Empirical, Algorithmic
[13]	Energy-Efficient Routing Protocol (ECC-EERP)	This protocol enhances security and energy efficiency in Internet of Medical Things (IoMT) applications by employing elliptic curve cryptography for secure data transmission while minimizing energy consumption and communication overload.		Empirical, Algorithmic

Table 1. *Cont.*

Author(s)	Security System	Synopsis	Mitigated Attacks	Evidence Type
[14]	N-IDS (Network-Intrusion Detection System)	This system detects intrusions and attacks in a smart healthcare system using a deep learning approach that combines CNN (Convolutional Neural Networks) and LSTM (Long Short-Term Memory) to extract optimal features from network data and detect attacks with high		Empirical, Algorithmic
[15–26]	Blockchain	Modern security systems enhance medical data privacy, integrity, and access control in healthcare, enabling secure management of patient records, IoT (Internet of Things) devices, and remote healthcare systems.	Man-in-the-middle, DDoS (Distributed Denial of Service), Single Point of Failure, Data Tampering, Unauthorized Access, Tampering Attacks, Data Breach, Counterfeit Product Attacks	Survey, Algorithmic, Statistical, Cryptographic
[27]	QP-CNN (Quantum Photonic Convolutional Neural Network)	The QP-CNN enhances the security of AI-based healthcare systems by utilizing quantum photonic computation for the encryption and protection of patient data during transmission and storage. The study demonstrates its effectiveness through simulations, achieving high accuracy and various performance metrics.	DoS (Denial of Service), Stolen Device, Untraceability/Anonymity, Replay, Man-in-the-Middle, Impersonation, Temporary Secret Leakage Attack	Empirical
[27]	CMTL (Centralized Multi-Source Transfer Learning)	The "EoT-TL Healthcare" system combines edge computing, Internet of Things, blockchain, and cloud technologies for cyberattack detection and data security optimization in healthcare, with high performance evaluated using three datasets.	DoS (Denial of Service), DDoS (Distributed Denial of Service), Malware, Injection, Man-in-the-Middle	Empirical, Mathematical, Algorithmic
[28]	Cryptosystem with SHA-256 and Hyper Chaotic Multi Attractors Chen System	It uses DNA encoding, SHA-256, and HCMACS for secure medical image encryption, protecting statistical, differential, and brute-force attacks, while ensuring the confidentiality, integrity, and availability of data.	Statistical, Differential, Chosen-Plaintext	Algorithmic, Simulation, Cryptographic
[29]	Encryption technique	It uses genetic encryption for the secure transmission of health data via wireless sensors while incorporating an authentication process for user verification and preventing malicious attacks.	Blackhole, Selective Forwarding, Sybil, Hello Flood	Algorithmic, Simulation

Table 1. *Cont.*

Author(s)	Security System	Synopsis	Mitigated Attacks	Evidence Type
[30]	Zero-watermarking	Uses deep learning and specialized image processing techniques to secretly embed a distinguishing mark in medical images. This prevents unauthorized access or distribution, ensuring the protection and integrity of healthcare records.	Signal Interference, Spatial Manipulation, Communication Protocol Vulnerabilities	Algorithmic, Simulation, Cryptographic
[31]	PAAF-SHS (Physical Unclonable Authentication Function-Smart Healthcare Systems)	The PAAF-SHS provides secure encrypted communication between users and medical servers using mutual authentication and PUF technology.	Stolen Device, DoS (Denial of Service), Replay Attack, Man-in-the-Middle, Phishing, Impersonation, Key Compromise, Insider Threats	Algorithmic, Simulation, Cryptographic
[32]	CLM-based ECG Encryption System	The system utilizes the Chaotic Logistic Map (CLM) and fingerprint data to encrypt ECG signals, thereby ensuring secure transmission over the internet.	Noise-based attacks, Hacking attacks	Mathematical, Algorithmic
[33]	Encryption Framework for Secure Telehealth and Electronic Health Records (EHR)	The system utilizes ECG signals and a lightweight encryption algorithm to securely transmit electronic health records (EHR) in telehealth applications, ensuring enhanced data privacy, confidentiality, and access control.	-	Algorithmic, Simulation, Cryptographic
[34]	IEDF (Intelligent Encryption and Decryption Framework)	It combines the Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA), and Modified Blowfish (MBF) algorithms for cloud data security, using Automatic Sequence Cryptography (ASC) for efficient and secure data block encryption.	Data Breaches	Algorithmic, Simulation
[35]	WSNs (Wireless Healthcare Sensor Networks)	This protocol enhances the security of wireless sensor networks used in healthcare by implementing a three-factor authentication strategy that incorporates user identity, password, and biometric data. It ensures robust mutual authentication and protects against various potential attacks. Formally verified using the ProVerif tool.	User Impersonation, Offline Password Guessing Attack, Insider Attack, Device Stolen, GWN Bypassing Attack, DoS (Denial of service),	Algorithmic, Simulation

Table 1. *Cont.*

Author(s)	Security System	Synopsis	Mitigated Attacks	Evidence Type
[36]	Image Encryption Framework	The Deep Learning-Based Image Encryption Framework employs ResNet-50 to secure medical images through encryption and decryption, effectively addressing cyber threats and ensuring the confidentiality and integrity of sensitive patient data.	Unauthorized Access, Data Breaches, DoS (Denial of Service), Impersonation Attacks, Replay Attacks	Algorithmic, Simulation, Cryptographic
[37]	Chaos-Based Lightweight Encryption Scheme	Its 4-scroll chaotic attractor securely encrypts health data, particularly from wearable devices. It ensures confidentiality and integrity while maintaining real-time processing. The method has demonstrated strong resistance to known and chosen plaintext attacks, supported by a large key space and adequate throughput.	Unauthorized Access, Data Breaches, Known-Plaintext, Chosen-Plaintext Attacks	Algorithmic, Simulation, Cryptographic
[38]	Standard-Based Approach	It utilizes standards such as COSMIC ISO/IEC 19761 to design a secure healthcare system architecture. This method combines system and software security requirements, employing features like access control, data encryption, and auditability to mitigate vulnerabilities and protect against unauthorized access.	Unauthorized Access, Data Breaches, Ransomware, Tampering, Data Corruption	Simulation

3. Materials and Methods

A comprehensive literature review was conducted for this review article between 1 February 2024 and 30 September 2024. The search was performed in major electronic databases, including PubMed, Google Scholar, MDPI, IEEE, and ScienceDirect, focusing on the published medical literature. The research used keywords such as health security system, artificial intelligence in healthcare, health data protection, cybersecurity in healthcare, and cyber-attacks in healthcare.

The selection process for the articles was based on predefined inclusion and exclusion criteria. Specifically, articles were included if they examined health system security using technologies such as Artificial Intelligence (AI), blockchain, Internet of Things (IoT), and other algorithmic or innovative approaches to data protection. On the other hand, articles focusing on non-healthcare applications or lacking sufficient documentation were excluded. More specifically, studies relying solely on theoretical models or proposing systems without experimental evaluation or practical evidence were not considered.

As illustrated in the Flowchart (Figure 2), an initial 550 articles were identified, from which 77 duplicate records were removed. The duplicate records resulted from the overlap of identical studies appearing in different repositories due to the coverage of multiple databases. Subsequently, the titles and abstracts of the remaining articles were assessed, leading to the exclusion of 299 articles that did not meet the predefined criteria. These

articles included material that, while related either to healthcare or to system security, did not establish a clear connection between the two topics.

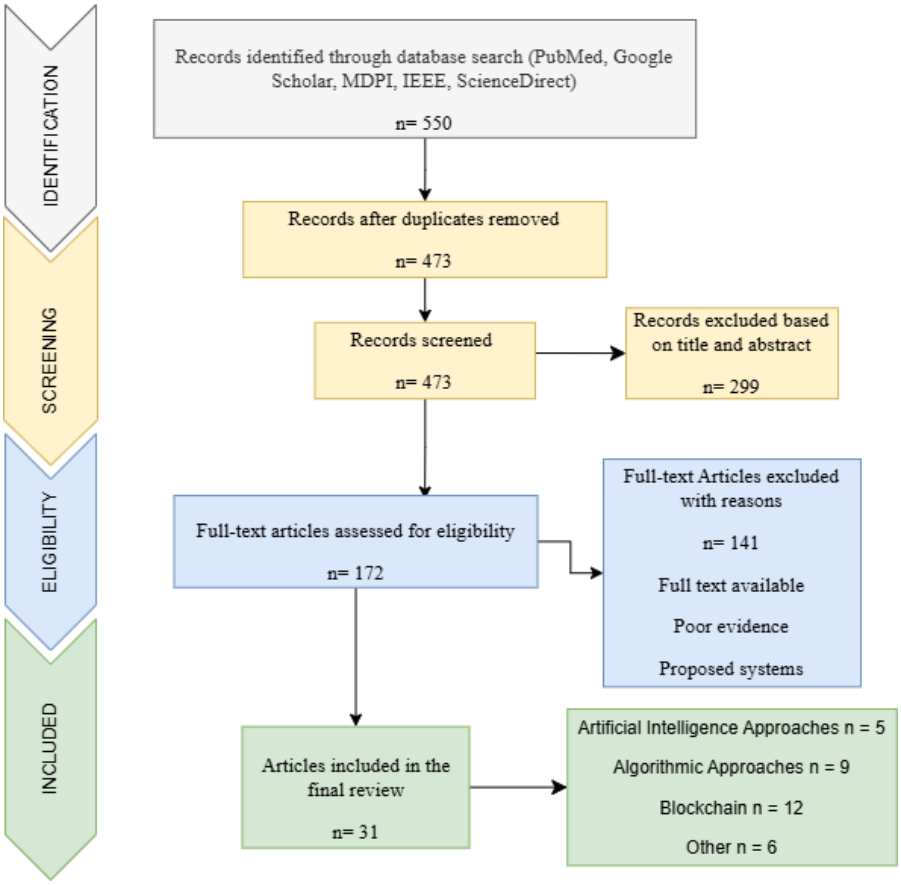


Figure 2. Flowchart of our research approach.

In the next stage, 172 articles underwent full-text evaluation, of which 141 were excluded due to insufficient evidence or non-implemented proposals. Although these articles addressed both security systems and healthcare, they did not practically demonstrate the functionality and effectiveness of these systems in real-world healthcare settings.

Ultimately, 31 articles were selected and categorized into four main groups: artificial intelligence approaches (n = 5), algorithmic methods (n = 9), blockchain technologies (n = 12), and other approaches (n = 7).

Although the study covers the period from 2018 to 2024, most of the collected articles are from 2023 and 2024. Notably, no studies were identified for the year 2019, while 2018 is represented by only one study. The time frame was deliberately set to include studies from the last 5–6 years, ensuring a focus on recent advancements while avoiding overly dated material.

Inclusion and Exclusion Criteria

The inclusion criteria for selecting articles for the study were designed to ensure that the review focused on recent, high-quality research addressing healthcare system security through advanced technologies. The criteria were as follows:

- Publications from 2018 to 2024.
- Studies explored healthcare system security using proven technologies, including artificial intelligence (AI), blockchain, Internet of Things (IoT), or other algorithmic and innovative data protection methods.

- Articles that demonstrated practical applications of these technologies, with experimental validation conducted under controlled test conditions.
- Studies that addressed security issues, whether related to network security or software security.

Similarly, the studies and publications that were not included in this review were based on the following exclusion criteria:

- Studies focus solely on non-healthcare applications.
- Articles lacking sufficient documentation or relying exclusively on theoretical models without experimental evaluation or practical evidence.
- Case studies or reports in which the proposed system was not tested under controlled conditions, such as simulated cyber threats.

However, it is important to clarify that experimental evaluation in this context does not equate to experimental evaluation as is understood in medical research, where clinical trials and patient safety are paramount.

4. Results

After a thorough study of modern security systems, as presented in Table 1, all systems focus on security in the collection and transmission of patient data, with the main objective of protecting against attacks in the healthcare sector. For all the systems examined, the common types of evidence identified were the system design and the security evaluation, both aimed at enhancing protection and mitigating threats. The technologies used in this area focus on maintaining data privacy and integrity without affecting the performance of devices or networks. Most of the research analyzed uses algorithmic technology approaches. In terms of key threats, Selvarajan and Mouratidis, (2023), highlight unauthorized access, where attackers attempt to gain access to medical data without permission. DoS attacks, which disrupt services by overloading the network with fake requests, and man-in-the-middle attacks, in which the attacker gains control of the communication, are also critical [26]. As noted by Javaid et al. (2023) [2], and many other researchers, ransomware attacks are widely prevalent. However, only in the study by Abuasal et al. (2024) [38], were they considered a significant threat and thoroughly analyzed within the context of overall security threats. Anand et al. (2024) [30], analyze the resilience of the proposed system through three main attack categories: Noise Removal, Geometry, and Protocol in medical images. In the Noise Removal category, the attacks include various types of noise such as gaussian noise, while in the geometry category, attacks such as JPEG compression, zoom, and rotation are considered. Finally, Ravi, (2023) [14] presents the performance of the N-IDS intrusion detection system on various medical datasets.

4.1. Security Systems Based on Blockchain Approaches

We note in Table 1 that blockchain-based systems have been extensively studied by many authors. To provide a more comprehensive understanding, we include additional information about key systems that highlight their unique features, applications, and contributions.

A noteworthy security system proposed by Tariq et al. (2020) [15], known as the blockchain-based Security Solution for IoT-enabled Smart Healthcare Systems, utilizes blockchain for distributed, scalable, and efficient medical transaction management with immutable records. This system enhances the secure transmission of medical information between providers, restores data ownership to patients, and ensures protection and transparency.

Similarly, the decentralized system by Puri et al. (2021) [16], integrates AI and blockchain to manage patient data. Through smart contracts, it ensures transparency,

detects malicious IoT devices, and optimizes energy consumption, response times, and transaction delays. Its primary aim is to safeguard personal health records (PHR) while addressing malicious network threats with a rule-based AI layer embedded in smart contracts.

Abid et al. (2022) [17], introduced a decentralized access model using smart contracts and the Generalized Temporal Role-Based Access Control (GTRBAC) framework, which incorporates time-constrained policies. Experimental results indicate low gas costs and latency, showcasing its effectiveness in enhancing security and privacy in IoT-enabled healthcare systems.

Sharma et al. (2023) [18], developed an application leveraging blockchain to manage medical certificates using Ethereum smart contracts. The system provides insights into transaction costs and processing efficiency, offering a secure and transparent solution for certificate management while improving trust between patients and healthcare providers.

The Consultative Transaction Key Generation and Management (CTKGM) system by Selvarajan and Mouratidis, (2023) [19], employs blockchain to generate cryptographic key pairs and evaluate trust using the Quantum Trust Reconciliation Agreement model (QTRAM). Additionally, the Tuna Swarm Optimization (TSO) method validates nonce messages, ensuring authenticity and efficient data transmission for secure healthcare operations.

Another innovative approach by Rani et al. (2023) [20], the IoT-based Distributed Healthcare Framework, uses blockchain and AI-based smart contracts to deliver remote healthcare services. Integrating a Distributed Database Management System (DDBMS) protects against single points of failure while enhancing transparency, security, and reliability in medical data management.

Akinola et al. (2024) [21] designed a system combining blockchain with cryptographic techniques, such as hashing and digital signatures, utilizing both Proof-of-Work and Proof-of-Stake consensus mechanisms. Compliant with HIPAA and General Data Protection Regulation (GDPR) standards, the system ensures the security and integrity of medical device data.

Mohammed et al.'s (2024) [22], Pattern-Proof Malware Validation (PoPMV) framework focuses on malware validation in distributed cloud fog systems for healthcare. Though no specific attack scenarios were tested, the system demonstrates robust security and performance in managing threats to healthcare workflows.

Wu et al. (2024) [24] utilized the Hyperledger Composer platform for managing the implant supply chain. While specific attacks were not tested, the integration of blockchain with hybrid encryption enhances overall security and efficiency in supply chain operations.

Mallick et al.'s (2024) [25], IoMT-Fog-blockchain with InterPlanetary File System (IPFS) Framework integrates the Internet of Medical Things (IoMT), Fog Computing, blockchain, and IPFS for decentralized medical data management. The use of scalable data searches and the Elliptic Curve Digital Signature Algorithm (ECDSA) ensures security and protects against forgery.

Finally, the blockchain-based Attribute-Based Access Control (ABAC) system by Idrissi and Palmieri, (2024) [26] combines mobile agents and blockchain for mutual authentication and access control in IoT healthcare. Utilizing Elliptic Curve Cryptography (ECC), the system achieves fast key agreement with reduced communication costs and computational load.

To contextualize these findings, it is essential to address the challenges and limitations encountered during the development, deployment, and performance evaluation of these systems. This analysis can offer valuable insights for future research and innovation in blockchain-based healthcare solutions.

Challenges and Risks of Blockchain

While offering numerous advantages, blockchain faces significant challenges and risks, particularly in critical sectors such as healthcare. These challenges must be addressed to enhance the security, scalability, and efficiency of blockchain-based systems.

A key issue, as noted by Akinola et al. (2024) [21], is the scalability of blockchain systems. Although scalability is theoretically achievable, realizing it in practice requires the development of more efficient artificial intelligence (AI) algorithms. The performance of blockchain systems in real-world applications, especially in healthcare, remains a critical hurdle, as it must handle high transaction volumes and large-scale data efficiently.

Performance degradation is another significant challenge. The exponential growth of connected medical devices and the vast data they generate reduce blockchain performance, causing lower transaction throughput and higher latency. Such delays can be critical in real-time healthcare environments. Akinola et al. (2024) [21], emphasize that while blockchain can be enhanced to handle scalability, performance issues, such as reduced throughput, require innovative solutions to remain viable in high-demand medical contexts.

Moreover, increased failed workflow tasks raise computation time at decision nodes. This highlights the need for enhanced methodologies to improve decision-making efficiency in blockchain systems. Mohammed et al.'s (2024) [22], study illustrates how distributed cloud fog systems in healthcare can face computational delays, adversely impacting workflow efficiency. Addressing these issues through federated AI analysis presents a promising direction for future improvements. By distributing computational tasks across edge devices, federated AI reduces the load on central nodes, minimizes energy, time, and storage costs, and enhances both system scalability and data privacy.

Lastly, the diversity of healthcare settings demands optimized user interfaces and performance adjustments to ensure efficient resource utilization and a seamless user experience. Wu et al. (2024) [24], point out that although blockchain systems with hybrid encryption can enhance data security in healthcare supply chains, the challenge of maintaining usability and performance in varied healthcare environments remains.

This analysis highlights areas requiring innovation to fully realize the potential of blockchain in healthcare. The continued development of AI integration, performance optimization, and user-centric design will be essential to overcoming these challenges and ensuring the practical implementation of blockchain technology in the healthcare sector.

4.2. Attack Types and Mitigation Strategies

At this point, it is necessary to describe the types of attacks listed in Table 1, to facilitate the understanding of their nature and the data they seek to intercept through specific methods. However, before being analyzed in detail, it is worth noting that systems that do not include specific information in the Mitigated Attacks field were examined separately, to clarify their effectiveness and the attacks they can mitigate more accurately.

Initially, the ECC-EERP system has been evaluated against other existing methods, showing improved security, high encryption efficiency (99%), increased energy efficiency, longer network lifetime, and lower computational cost. The present scheme demonstrates significant superiority in critical parameters such as security, encryption performance, communication overload reduction, and processing time efficiency, outperforming other existing methods [13]. Finally, the Encryption Framework for Secure Telehealth and Electronic Health Records (EHR) system was not specifically tested for more complex attacks, such as DDoS or man-in-the-middle, but focused on Functional Testing and performance testing. Despite limited security testing, it was deemed worthy of inclusion in this work due to its overall performance evaluation [33].

Completing the analysis of the security systems that did not have a specific attack, the terminology of the others follows to better understand the potential risks that threaten health systems and patient data.

1. Man-in-the-middle (Middleman Attack): The attacker interferes with the communication between two parties, trying to obtain or alter information. The security of key agreement and authentication protocols is verified through the AVISPA tool [26].
2. DoS (Denial of Service): Attackers flood the medical server with numerous requests, overwhelming its resources and substantially slowing down or crashing the system, which compromises the availability of medical services [31].
3. Blackhole Attack: In this attack, a malicious node interferes with the flow of data by redirecting it to a blank spot and preventing proper transmission in the network [29].
4. Selective Forwarding Attack: During this attack, selected data packets—often of a sensitive nature—are dropped by sensors, disrupting the information flow [29].
5. Sybil Attack: A malicious node pretends to be multiple different nodes, illegally gaining access to the network and causing a security risk [29].
6. Hello Flood Attack: An attack where a node sends fake Hello packets, disrupting the communication flow and confusing data transmission [29].
7. Privacy Leakage: This involves the loss of sensitive data, mainly due to inadequate protection measures [15].
8. Tampering (Data Tampering): Malicious users tamper with medical records, affecting the reliability of the data [15].
9. Forgery: Malicious attempts to create fake medical data or transactions for fraudulent purposes [15].
10. Single Point of Failure: In traditional systems, there is a central point of vulnerability that can cause total system failure [15].
11. Data tampering attacks: Attackers focus on data tampering. The blockchain ensures integrity by preventing tampering [26].
12. Forgery attacks: Attempts to create false data. ECC and mobile agents offer protection [26].
13. Privacy violation attacks: Revealing personal data. Anonymous authentication protects the personal data of patients and professionals [26].
14. Data breach: Unauthorized individuals gain access to sensitive information through attacks such as hacking or phishing, causing damage to personal and financial data [34].
15. DDoS (Distributed Denial of Service): Coordinated attacks by multiple compromised devices, or a botnet, flood a system with excessive traffic, rendering it inoperative and denying service to legitimate users. This widespread disruption critically affects the availability of medical services [39].
16. Ransomware: A type of malware that encrypts a victim's files, demanding a ransom payment for the decryption key. This malware exploits the critical nature of personal and business data, forcing victims to pay to regain access. Ransomware attacks can severely disrupt operations and result in substantial financial and data losses, underlining the importance of robust cybersecurity measures to protect sensitive information [40].

Other types of attacks (Untraceability/Anonymity, Stolen Devices, Malware, Communication Protocol Vulnerabilities, Offline Passwords, etc.) can be identified, but are very close to the described so the most important thing is that research should focus on the effectiveness of different major attacks. It is also important that the functionality of hospital information systems is tested and adapted to change parameters continuously.

4.3. Ransomware

Ransomware (ransom + malware) is a form of malware that aims to encrypt user or organization files, demanding payment to restore access to them. This attack has been described as the most common in the healthcare sector. The attack starts when the user opens a malicious link or attachment in an email, installing ransomware on their system. As the files are encrypted, a warning appears asking for a ransom, threatening to delete the data or increase the required amount if payment is not made within a certain deadline. Through this digital extortion tactic, many users are forced to pay to recover their data [41].

From the analysis of the lifecycle of ransomware attacks, seven main stages can be observed: Planning, Proliferation, Arrival, Control Communication, User Information Retrieval, Encryption and Extortion, and Financial Claims. The cycle begins with the creation and deployment of ransomware, leveraging tools such as Ransomware-as-a-Service (RaaS). This is followed by propagation through various social engineering attacks. Once the malware reaches the victim's device, it communicates with a remote-control server to obtain the encryption key. It then seeks critical files for encryption and, in the final stage, demands a ransom from the victim to restore the files [42]. The analysis of the attack is graphically depicted in the image below, offering a visual representation of the path.

We focused on the ransomware attack as the healthcare industry is particularly vulnerable to attacks of this type due to the retention of high-value sensitive data, such as medical and personal records, making organizations high-value targets (Figure 3).

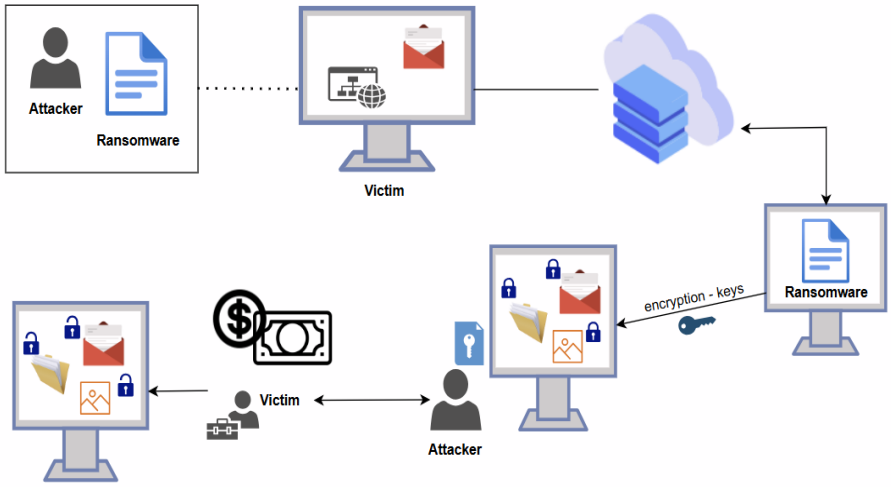


Figure 3. Ransomware attack lifecycle.

Cybercriminals can use the stolen data for extortion, or they can resell it on the black market, where it is more lucrative than financial data. In addition, inadequate training of employees in threat detection and generally poor cybersecurity infrastructure exacerbates the problem, while the widespread use of Internet of Medical Things (IoMT) devices increases network vulnerabilities, making them easier targets [43].

5. Discussion and Conclusions

In summary, this study has highlighted the importance of cutting-edge technologies, such as blockchain, artificial intelligence techniques, and algorithmic approaches, which contribute to enhanced protection against attacks and ensure data confidentiality in the healthcare sector [38].

The protection of medical data is critical not only because of its nature—as it includes sensitive personal information that, if leaked, can lead to serious consequences—but also because it contributes to improving the quality of patient care. An information system that

works efficiently and with enhanced security measures offers significant benefits to the overall improvement of patients' quality of life.

Despite the plethora of proposed security systems, we observed that many of them have not undergone experimental testing to assess their resilience against insider attacks. In our study, we excluded all systems that had not been experimentally evaluated, except for three publications that stood out due to the complexity and novelty of their architecture [37]. These cases deserve further analysis and evaluation of their security performance in the future.

It is also important to note that while ransomware attacks have been identified as one of the most frequent and serious threats, only one publication evaluated the resilience of the proposed architecture against this threat. More work is needed in this direction.

6. Future Work

As future work, it is proposed to further study the effectiveness of security systems, with a focus on threats such as ransomware. In addition, it is proposed to develop a simulated intelligence system that will be subjected to controlled attacks, including ransomware attacks. Data security solutions will enable deeper visibility and effective threat detection and response while ensuring real-time compliance. The integration of both artificial intelligence and algorithmic approaches into healthcare security systems offers a new level of dynamism, enabling real-time threat detection and threat response with accuracy and efficiency [38]. The superiority of either approach is too early to measure. An effective benchmarking approach for these systems needs longer periods of use and extensive operational data [4].

Author Contributions: Conceptualization, C.K. and V.T.; methodology, S.M. and V.T.; formal analysis, S.M.; writing—original draft preparation, S.M.; writing—review and editing, S.M. and C.K.; supervision, V.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

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. [CrossRef] [PubMed]
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. [CrossRef]
3. Lee, I. Analyzing Web Descriptions of Cybersecurity Breaches in the Healthcare Provider Sector: A Content Analytics Research Method. *Comput. Secur.* **2023**, *129*, 103185. [CrossRef]
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. [CrossRef]
6. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology. *Circ. Cardiovasc. Qual. Outcomes* **2017**, *10*, e003800. [CrossRef] [PubMed]
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. [CrossRef]
8. Riplinger, L.; Piera-Jiménez, J.; Dooling, J.P. Patient Identification Techniques—Approaches, Implications, and Findings. *Yearb. Med. Inform.* **2020**, *29*, 81–86. [CrossRef]
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. [CrossRef]
10. Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. Available online: https://ieeexplore.ieee.org/document/9109651 (accessed on 3 September 2024).

11. Kanagala, P. Effective Cyber Security System to Secure Optical Data Based on Deep Learning Approach for Healthcare Application. *Optik* **2022**, *272*, 170315. [CrossRef]
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. [CrossRef]
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. [CrossRef]
14. Ravi, V. Deep Learning-Based Network Intrusion Detection in Smart Healthcare Enterprise Systems. *Multimed. Tools Appl.* **2023**, *83*, 39097–39115. [CrossRef]
15. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and Smart Healthcare Security: A Survey. *Procedia Comput. Sci.* **2020**, *175*, 615–620. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
19. Selvarajan, S.; Mouratidis, H. A Quantum Trust and Consultative Transaction-Based Blockchain Cybersecurity Model for Healthcare Systems. *Sci. Rep.* **2023**, *13*, 7107. [CrossRef]
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. [CrossRef]
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. [CrossRef]
23. An AOI-Aware Data Transmission Algorithm in Blockchain-Based Intelligent Healthcare Systems. Available online: https://ieeexplore.ieee.org/document/10433851 (accessed on 3 September 2024).
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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**. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]

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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
40. Ali, A. Ransomware: A Research and a Personal Case Study of Dealing with This Nasty Malware. Available online: https://www.informingscience.org/Publications/3707 (accessed on 3 October 2024).
41. Patyal, M.; Sampalli, S.; Qiang, Y.; Rahman, M. Multi-Layered Defense Architecture against Ransomware. *Int. J. Bus. Cyber Secur.* **2017**, *1*, 2.
42. Qartah, A.A. Evolving Ransomware Attacks on Healthcare Providers. Master's Thesis, Utica College, Utica, NY, USA, 2020. [CrossRef]
43. Treadwell, G.W. Preventing Employee Frauds in Small Businesses with Low-Cost Methods. *J. Bus. Account.* **2021**, *14*, 3–15.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.