Review

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

Constantinos Koutsojannis *, Savina Mariettou, Vassilios Triantafillou

Posted Date: 8 November 2024

doi: 10.20944/preprints202411.0526.v2

Keywords: Health Security; Data Protection; Cybersecurity in Healthcare; Algorithmic; Artificial Intelligence; Approaches

 doi:10.20944/preprints202411.0526.v2

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, Patras, Greece
[2] Professor of Medical Physics & Electrophysiology, Director of Health Physics & Computational Intelligence Laboratory, Physiotherapy Department, School of Health Rehabilitation Sciences, University of Patras, Patras, Greece
[3] Professor of Network Technologies, Health Physics & Computational Intelligence Laboratory, Physiotherapy Department, School of Health Rehabilitation Sciences, University of Patras, Patras, Greece
* Correspondence: ckoutsog@upatras.gr

Abstract: This paper explores the overall picture regarding security systems in healthcare through an extensive review of the literature. 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-three 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 attack.

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

1. Introduction

The security of health systems and patient data is now one of the most critical issues in modern medical technology [1]. The main reason why the healthcare sector is a target for cyber-attacks is the constant movement of sensitive information and data [2]. The digitization of medical information, 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 [1]. Data breaches in healthcare are a serious issue regulated by the 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 at high levels [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 cyberattacks 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

 doi:10.20944/preprints202411.0526.v2

motivated many companies to test more innovative mechanisms and technologies to secure their information systems such as Blockchain and Algorithmic Approaches.

Delving a little deeper into these technologies, we have that Blockchain is a technology that uses public key encryption for authentication and records every transaction on a network. Every transaction that takes place cannot be modified once it is completed. Each network has nodes. All nodes record transaction information in blocks in chronological order, and each new block is connected to the previous one, thus creating a chain. This structure allows data to be kept secure. This security serves the system well as if an attacker who would like to compromise one block would have to compromise the entire chain. The blockchain uses hashing algorithms, which make any attempt to tamper or 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. The public blockchain, due to its complete decentralization, uses cryptography and consensus mechanisms, such as proof of work or proof of ownership, to ensure the reliability and security of its data [6]. All the above can be seen in Figure 1 which represents a Blockchain transaction. The nodes or users agree to a transaction [7].

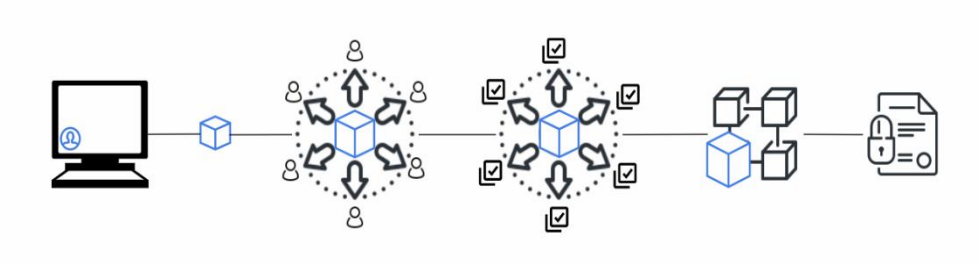

Figure 1. Visual representation of a blockchain transaction.

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, that can reduce accuracy [8].

The aim of this article is to highlight the current situation regarding the security of healthcare systems, with the goal of improving existing systems to enhance the quality of care for patients.

The article is organized as follows: in Section 2, a detailed analysis of the 33 identified security systems is performed. In Section 3, the methods used to identify and evaluate these systems are described. In Section 4, we present the findings of our study, while Section 5 presents the main conclusions and recommendations for future research.

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 CT and MRI scans, misleading doctors into erroneous diagnoses [5]. This threat is particularly alarming, as the security

 doi:10.20944/preprints202411.0526.v2

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. 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
[9]	WMSNs (Wireless Medical Sensor Networks)	It operates using three-factor authentication to securely verify remote users in WMSNs 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
[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
[11]	Modified deep learning approach based on Cyber Physical Systems (CPS)	The system uses deep learning and CPS for secure processing of IoT data, providing protection 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)
[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
[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.	-
[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 accuracy.	KISTI Network Payload Dataset, KDDCup-99, UNSW-NB15, CICIDS-2017, WSN-DS
[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,

 doi:10.20944/preprints202411.0526.v2

			Tampering Attacks, Data Breach, Counterfeit Product Attacks
[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
[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
[28]	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
[29]	Cryptosystem with SHA-256 and Hyper Chaotic Multi Attractors Chen System	It uses DNA encoding, SHA-256, and HCMACS for secure medical image encryption, providing protection against statistical, differential, and brute-force attacks, while ensuring the confidentiality, integrity, and availability of data.	Statistical, Differential, Chosen-Plaintext
[30]	Encryption technique	It uses genetic encryption for 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
[31]	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
[32]	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
[33]	Decentralized Adaptive Security Architecture	Dynamically adapts security solutions in real-time to address the constraints of Internet of Medical Things (IoMT) devices, ensuring the protection of data through the implementation of the edge-cloud continuum.	-
[34]	CLM-based ECG Encryption System	The system utilizes the Chaotic Logistic Map (CLM) and fingerprint data to encrypt ECG	Noise-based attacks, Hacking attacks

 doi:10.20944/preprints202411.0526.v2

		signals, thereby ensuring secure transmission over the internet.	
[35]	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.	-
[36]	IEDF (Intelligent Encryption and Decryption Framework)	It combines the AES, DES, RSA, and Modified Blowfish (MBF) algorithms for cloud data security, using Automatic Sequence Cryptography (ASC) for efficient and secure data block encryption.	Data Breaches
[37]	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),
[38]	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 ser-vice), Impersonation Attacks, Replay Attacks
[39]	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
[40]	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

3. Materials and Methods

For this review article, a comprehensive search was conducted covering the period from 01/02/2024 until 30/09/2024 in major databases, on published medical literature using several electronic databases including Pubmed, Google Scholar, MDPI, IEEE, ScienceDirect. The research used keywords such as health security system, artificial intelligence in healthcare, health data protection, cybersecurity in healthcare, cyberattacks in healthcare.

 doi:10.20944/preprints202411.0526.v2

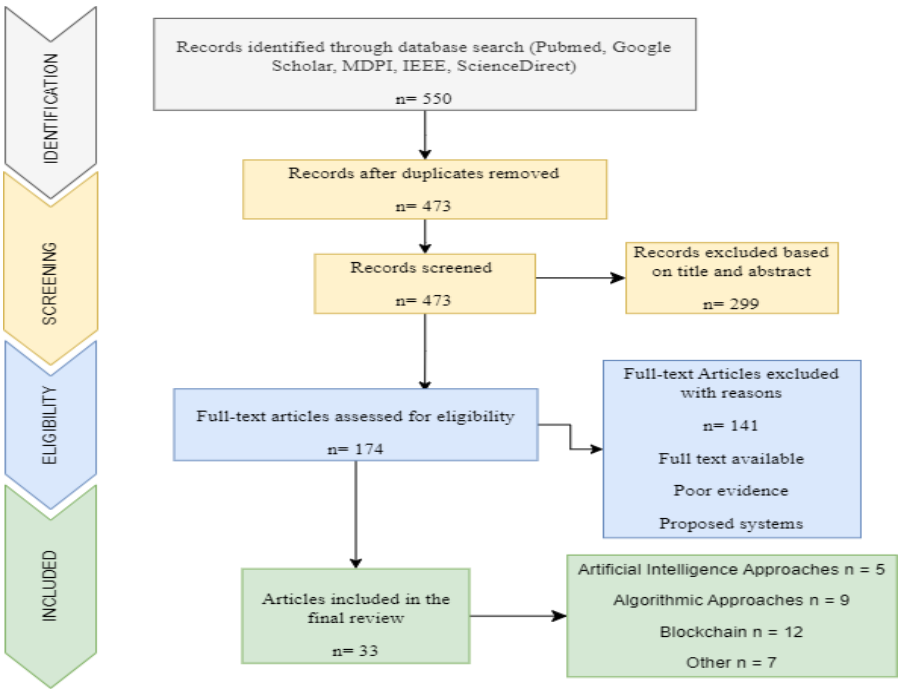

Figure 2. Flowchart of our research approach.

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. 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 use algorithmic technology approaches. In terms of key threats, Selvarajan & Mouratidis (2023) highlight unauthorized access, where attackers attempt to gain access to 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), and many other researchers, ransomware attacks are widely prevalent. However, only in the study by Abusal et al. (2024) were they considered a significant threat and thoroughly analyzed within the context of overall security threats. Anand et al. (2024) analyzes the resilience of the proposed system through three main attack categories: Noise Removal, Geometry, and Protocol. 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) presents the performance of the N-IDS intrusion detection system on various 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. At this point, we would like to add some additional information that was considered important for a better understanding and evaluation of these systems.

The security system proposed by Tariq et al. (2020), known as Blockchain-based Security Solution for IoT-enabled Smart Healthcare Systems, uses blockchain for distributed, scalable, and efficient management of medical transactions, with immutable records. The system by Puri et al. (2021) offers decentralized patient data management using AI and blockchain. It targets transparency through smart contracts and includes mechanisms to detect malicious IoT devices, improving energy consumption, response time, and transaction delays. The system proposed by Abid et al. (2022) offers decentralized access for IoT devices using smart contracts and the Generalized Temporal Role Based Access Control (GTRBAC) model for detailed access policy with time constraints. Experimental evaluation showed low gas cost and low latency. The application developed by Sharma et al. (2023)

 doi:10.20944/preprints202411.0526.v2

uses blockchain to manage medical certificates via smart contracts. The system, deployed on Ethereum, offers transaction cost and efficiency analysis, including gas consumption and processing time. Consultative Transaction Key Generation and Management (CTKGM), proposed by Selvarajan & Mouratidis (2023), uses blockchain to generate cryptographic key pairs and the Quantum Trust Reconciliation Agreement model (QTRAM) for trust evaluation. The Tuna Swarm Optimization (TSO) method verifies nonce messages, ensuring authenticity and efficient data transmission. The IoT-based Distributed Healthcare Framework with Blockchain and AI-based Smart Contracts, proposed by Rani et al. (2023), offers a distributed framework for remote healthcare services, using Distributed Database Management System (DDBMS) and blockchain for data storage and processing, with high-performance evaluation. The solution proposed by Akinola et al. (2024) integrates blockchain with cryptographic techniques such as hashing and digital signatures for medical devices, using Proof-of-Work and Proof-of-Stake consensus mechanisms. The system complies with HIPAA and GDPR standards. Mohammed et al.'s (2024) Pattern-Proof Malware Validation (PoPMV) is a blockchain-based system for malware validation in microservice flows. No specific attack scenarios were reported in the experimental evaluation. The system proposed by Liu et al. (2024) is based on blockchain and 6G and consists of two layers: the Sensing Communication Layer (SenCom-Layer) and the Blockchain Layer (BlockC-Layer). An energy-efficient algorithm is applied to the SenCom-Layer, while the BlockC-Layer uses cooperative gaming for energy efficiency. The system developed by Wu et al. (2024) uses the Hyperledger Composer platform to manage the implant supply chain. Although no specific attacks were tested, the use of blockchain and hybrid encryption offers increased security. The IoMT-Fog-Blockchain with IPFS Framework, proposed by Mallick et al. (2024), integrates IoMT, Fog Computing, Blockchain, and IPFS for decentralized medical data management. The system offers scalable searches and stores data hashes on the blockchain, while the use of Elliptic Curve Digital Signature Algorithm (ECDSA) protects against forgery. Blockchain-based Attribute-Based Access Control (ABAC) with anonymous authentication, developed by Idrissi & Palmieri (2024), combines mobile agents and blockchain for mutual authentication and access control (ABAC) in IoT-based healthcare systems. Elliptic Curve Cryptography (ECC) encryption offers fast key agreement, while the system has low communication costs and reduced computational load.

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]. Regarding the Decentralized Adaptive Security Architecture scheme, no specific details on experimental studies or results confirming the effectiveness of the proposed security architecture are provided. Instead, the emphasis is on describing the architecture and the challenges faced by digital healthcare systems, elements that provide important insights relevant to this work [33]. 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 [35].

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.

 doi:10.20944/preprints202411.0526.v2

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 [32].
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 [30].
4. Selective Forwarding Attack: during this attack, selected data packets - often of a sensitive nature - are dropped by sensors, disrupting the information flow [30].
5. Sybil Attack: a malicious node pretends to be multiple different nodes, illegally gaining access to the network and causing a security risk [30].
6. Hello Flood Attack: this is an attack where a node sends fake Hello packets, disrupting the communication flow and causing confusion in data transmission [30].
7. Privacy Leakage: It 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: they 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 [36].
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 [41].
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 [42].

Other types of attacks can be identified, but the most important thing is that research should focus on the effectiveness against different attacks. It is also important that the functionality of hospital information systems is tested and adapted to new data.

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 the 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 [43].

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

 doi:10.20944/preprints202411.0526.v2

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 [44]. The analysis of the attack is graphically depicted in the image below, offering a visual representation of the path.

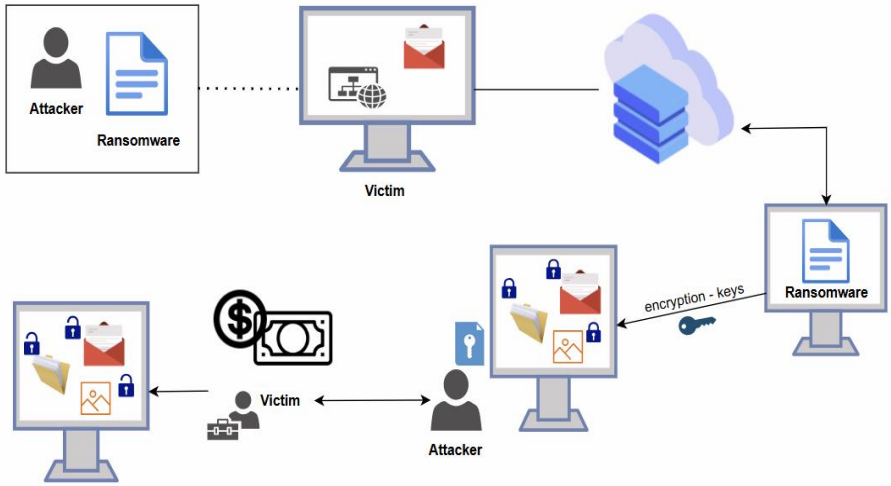

Figure 3. Ransomware Attack Lifecycle.

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. Cybercriminals can use the stolen data for extortion or 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 [45].

5. Discussion and Conclusions

In summary, this study has highlighted the importance of cutting-edge technologies, such as blockchain, multi-factor authentication methods, as well as artificial intelligence techniques and algorithmic approaches, which contribute to enhanced protection against attacks and ensuring data confidentiality in the healthcare sector [40]. 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 [39]. 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

 doi:10.20944/preprints202411.0526.v2

As future work, it is proposed to further extensive 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 [40]. 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].

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, doi:10.3390/s23073612.
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 Security and Applications* **2023**, *1*, 100016, doi:10.1016/j.csa.2023.100016.
3. Lee, I. Analyzing Web Descriptions of Cybersecurity Breaches in the Healthcare Provider Sector: A Content Analytics Research Method. *Computers & Security* **2023**, *129*, 103185, doi:10.1016/j.cose.2023.103185.
4. Mariettou, S., Koutsojannis, C., Triantafillou V., (2023). Security Systems in Greek Health Care Institutions: a Scoping Review Towards an Effective Benchmarking Approach, International Conferences e-Society 2024 and Mobile Learning 2024, 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. *Computers & Security* **2023**, *129*, 103189, doi:10.1016/j.cose.2023.103189.
6. 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, doi:10.3390/s22041371.
7. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities. Renewable and Sustainable Energy Reviews **2018**, 100, 143–174, doi:10.1016/j.rser.2018.10.014.
8. Riplinger, L.; Piera-Jiménez, J.; Dooling, J.P. Patient Identification Techniques – Approaches, Implications, and Findings. Yearbook of Medical Informatics **2020**, 29, 081–086, doi:10.1055/s-0040-1701984.
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. *Journal of Ambient Intelligence and Humanized Computing* **2018**, *15*, 1165–1186, doi:10.1007/s12652-018-1015-9.
10. Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. *IEEE Access*, *8*(1), 106576–106584. https://doi.org/10.1109/access.2020.3000421
11. Kanagala, P. Effective Cyber Security System to Secure Optical Data Based on Deep Learning Approach for Healthcare Application. *Optik* **2022**, *272*, 170315, doi:10.1016/j.ijleo.2022.170315.
12. Sardar, A.; Umer, S.; Rout, R.Kr.; Wang, S.-H.; Tanveer, M. A Secure Face Recognition for IoT-Enabled Healthcare System. *ACM Transactions on Sensor Networks* **2022**, *19*, 1–23, doi:10.1145/3534122.
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, doi:10.3390/infrastructures8020022.
14. Ravi, V. Deep Learning-Based Network Intrusion Detection in Smart Healthcare Enterprise Systems. *Multimedia Tools and Applications* **2023**, doi:10.1007/s11042-023-17300-x.
15. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and Smart Healthcare Security: A Survey. *Procedia Computer Science* **2020**, *175*, 615–620, doi:10.1016/j.procs.2020.07.089.
16. Puri, V.; Kataria, A.; Sharma, V. Artificial Intelligence-powered Decentralized Framework for Internet of Things in Healthcare 4.0. *Transactions on Emerging Telecommunications Technologies* **2021**, doi:10.1002/ett.4245.
17. Abid, A.; Cheikhrouhou, S.; Kallel, S.; Tari, Z.; Jmaiel, M. A Smart Contract-Based Access Control Framework for Smart Healthcare Systems. *The Computer Journal* **2022**, *67*, 407–422, doi:10.1093/comjnl/bxac183.
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. *Information Sciences* **2023**, *629*, 703–718, doi:10.1016/j.ins.2023.01.148.

 doi:10.20944/preprints202411.0526.v2

19. Selvarajan, S.; Mouratidis, H. A Quantum Trust and Consultative Transaction-Based Blockchain Cybersecurity Model for Healthcare Systems. *Scientific Reports* **2023**, *13*, doi:10.1038/s41598-023-34354-x.
20. Rani, S.; Chauhan, M.; Kataria, A.; Khang, A. IoT Equipped Intelligent Distributed Framework for Smart Healthcare Systems. In *Studies in big data*; 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. *International Journal of Scientific Research and Modern Technology* **2024**, 1–13, doi:10.38124/ijsrmt.v3i4.27.
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. *Engineering Applications of Artificial Intelligence* **2023**, *129*, 107612, doi:10.1016/j.engappai.2023.107612.
23. Liu, Y., Wang, X., Zheng, G., Wan, X., & Ning, Z. (2024). An AOI-Aware data transmission algorithm in Blockchain-Based intelligent healthcare systems. *IEEE Transactions on Consumer Electronics*, 1. https://doi.org/10.1109/tce.2024.3365198
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. *International Journal of Medical Informatics* **2024**, *186*, 105415, doi:10.1016/j.ijmedinf.2024.105415.
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 Computer Science* **2024**, *5*, doi:10.1007/s42979-023-02511-8.
26. Idrissi, H.; Palmieri, P. Agent-Based Blockchain Model for Robust Authentication and Authorization in IoT-Based Healthcare Systems. *The Journal of Supercomputing* **2023**, *80*, 6622–6660, doi:10.1007/s11227-023-05649-7.
27. Kumari, K.S.; Shivaprakash, G.; Arslan, F.; Alsafarini, M.Y.; Ziyadullayevich, A.A.; Haleem, S.L.A.; Arumugam, M. Research on the Quantum Photonic Convolutional Neural Network for Artificial Intelligence-Based Healthcare System Security. *Optical and Quantum Electronics* **2023**, *56*, doi:10.1007/s11082-023-05574-2.
28. 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 Transactions on Sensor Networks* **2023**, doi:10.1145/3597210.
29. Banu, S.A.; Al-Alawi, A.I.; Padmaa, M.; Priya, P.S.; Thanikaiselvan, V.; Amirtharajan, R. Healthcare with Datacare—a Triangular DNA Security. *Multimedia Tools and Applications* **2023**, doi:10.1007/s11042-023-16303-y.
30. 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, doi:10.3390/s23115055.
31. Anand, A.; Bedi, J.; Aggarwal, A.; Khan, M.A.; Rida, I. Authenticating and Securing Healthcare Records: A Deep Learning-Based Zero Watermarking Approach. *Image and Vision Computing* **2024**, 104975, doi:10.1016/j.imavis.2024.104975.
32. Aldosary, A.; Tanveer, M. PAAF-SHS: PUF and Authenticated Encryption Based Authentication Framework for the IoT-Enabled Smart Healthcare System. *Internet of Things* **2024**, 101159, doi:10.1016/j.iot.2024.101159.
33. Ahmad, I.; Ahmad, I.; Harjula, E. Adaptive Security in 6G for Sustainable Healthcare. In *Communications in computer and information science*; 2024; pp. 38–47.
34. Gopalakrishnan, N.R.; Kumar, N.R.M.S. Cloud Security System for ECG Transmission and Monitoring Based on Chaotic Logistic Maps. *Journal of Advanced Research in Applied Sciences and Engineering Technology* **2024**, *39*, 1–18, doi:10.37934/araset.39.2.118.
35. 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. *Computers in Human Behavior* **2024**, *153*, 108134, doi:10.1016/j.chb.2024.108134.
36. 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 Systems With Applications* **2024**, *255*, 124479, doi:10.1016/j.eswa.2024.124479.
37. Saini, K.K.; Kaur, D.; Kumar, D.; Kumar, B. An Efficient Three-Factor Authentication Protocol for Wireless Healthcare Sensor Networks. *Multimedia Tools and Applications* **2024**, doi:10.1007/s11042-024-18114-1.
38. Nadhan, A.S.; Jacob, I.J. Enhancing Healthcare Security in the Digital Era: Safeguarding Medical Images with Lightweight Cryptographic Techniques in IoT Healthcare Applications. *Biomedical Signal Processing and Control* **2024**, *88*, 105511, doi:10.1016/j.bspc.2023.105511.
39. Clemente-Lopez, D.; De Jesus Rangel-Magdaleno, J.; Muñoz-Pacheco, J.M. A Lightweight Chaos-Based Encryption Scheme for IoT Healthcare Systems. *Internet of Things* **2023**, *25*, 101032, doi:10.1016/j.iot.2023.101032.

40. Abuasal, S.; Alsarayra, K.; Alyabroodie, Z. Designing a Standard-Based Approach for Security of Healthcare Systems. *Journal of Statistics Applications & Probability* **2024**, *13*, 419–434, doi:10.18576/jsap/130129.
41. Snehi, M.; Bhandari, A. Vulnerability Retrospection of Security Solutions for Software-Defined Cyber–Physical System against DDoS and IoT-DDoS Attacks. *Computer Science Review* **2021**, *40*, 100371, doi:10.1016/j.cosrev.2021.100371.
42. Ali, A. Ransomware: A Research and a Personal Case Study of Dealing with This Nasty Malware Available online: https://www.informingscience.org/Publications/3707.
43. Patyal, M.; Sampalli, S.; Qiang, Y.; Rahman, M. Multi-Layered Defense Architecture against Ransomware. International Journal of Business and Cyber Security (IJBCS), **2017**, 1, 2.
44. Qartah, A.A. Evolving Ransomware Attacks on Healthcare Providers. *Utica College* **2020**, doi:10.13140/RG.2.2.23202.45765.
45. Treadwell, G.W. Preventing Employee Frauds in Small Businesses with Low-Cost Methods. Journal of Business & Accounting **2021**, 14, 3.