applied sciences

MDPI

Article

Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis

Abdulatif Alabdulatif [1,*], Ibrahim Khalil [2] and Mohammad Saidur Rahman [2]

[1] Department of Computer Science, College of Computer, Qassim University, Buraydah 52571, Saudi Arabia
[2] Computer Science and Software Engineering, School of Science, RMIT University, Melbourne, VIC 3000, Australia
* Correspondence: ab.alabdulatif@qu.edu.sa

Abstract: A smart device carries a great amount of sensitive patient data as it offers innovative and enhanced functionalities in the smart healthcare system. Moreover, the components of healthcare systems are interconnected via the Internet, bringing significant changes to the delivery of healthcare services to individuals. However, easy access to healthcare services and applications has given rise to severe risks and vulnerabilities that hamper the performance of a smart healthcare system. Moreover, a large number of heterogeneous devices accumulate data that vary in terms of size and formats, making it challenging to manage the data in the healthcare repository and secure it from attackers who seek to profit from the data. Thus, smart healthcare systems are susceptible to numerous security threats and risks, such as hardware and software-based attacks, system-level attacks, and network attacks that have the potential to place patients' lives at risk. An analysis of the literature revealed a research gap in that most security surveys on the healthcare ecosystem examined only the security challenges and did not explore the possibility of integrating modern technologies to alleviate security issues in the smart healthcare system. Therefore, in this article, we conduct a comprehensive review of the various most recent security challenges and their countermeasures in the smart healthcare environment. In addition, an artificial intelligence (AI) and blockchain-based secure architecture is proposed as a case study to analyse malware and network attacks on wearable devices. The proposed architecture is evaluated using various performance metrics such as blockchain scalability, accuracy, and dynamic malware analysis. Lastly, we highlight different open issues and research challenges facing smart healthcare systems.

Keywords: smart healthcare systems; security; data privacy; Internet of things; blockchain; wearable devices; medical devices

check for updates

Citation: Alabdulatif, A.; Khalil, I.; Saidur Rahman, M. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. *Appl. Sci.* **2022**, *12*, 11039. https://doi.org/10.3390/app122111039

Academic Editors: Chunhua Su, Keping Yu, Celestine Iwendi and Thippa Reddy Gadekallu

Received: 28 September 2022
Accepted: 26 October 2022
Published: 31 October 2022

1. Introduction

The healthcare sector has seen a tremendous transformation by embracing key-enabler technologies, such as the Internet of Things (IoT), artificial intelligence (AI), blockchain, and next-generation wireless network (5G/6G). The adoption of these technologies in the healthcare industry has improved healthcare services and the quality of life of individuals. The integration of IoT technology in the healthcare sector strengthens the relationship between patients and healthcare providers. It enables lightweight devices (sensor node) to collect biometric data (e.g., temperature, blood pressure, oxygen rate, etc.) from the patient body and quickly transmit it to the other sensor nodes or directly relay it to healthcare providers, such as health professionals, pharmacies, and laboratories. The sensors comprise attribute and data profiles, processor, and memory. The attribute profile specifies the sensor's manufacturer, type, measurement range, date of manufacture, and location. The data profile handles the data format that the sensors are generating.

Sensors use various interfaces to transmit data, such as ZigBee, IEEE 802.11, general radio packet radio service (GPRS), Bluetooth, and cellular networks. Moreover, they transform the conventional healthcare system into a smart one for optimizing operational costs, remotely monitoring patients, smart applications for patients and caregivers, employee management, and the care of critical patients. However, smart healthcare systems are hindered by the security challenges that threaten the regular operations of a medical infrastructure. An adversary can discover security vulnerabilities in the hospital infrastructure (e.g., defibrillator, patient monitor, central server, etc.) that can be exploited using a malicious payload (e.g., ransomware, trojans, etc.) to put the patient's life at risk. A recent report by Fortified Health Security stated that, at the beginning of 2022, the healthcare sector reported 337 data breaches [1]. Figure 1 shows the financial loss due to cyberattacks on the healthcare industry from 2006–2026. The data were acquired from [2,3], and shows the average financial loss to the US organizations due to the data breaches. The report shown in [3] explains that the healthcare industry is the most affected sector according to the number of breaches that occurred in 2022. In Figure 1, the data from 2006–2022 are real-time data acquired from the [3]; further, the data are forecasted from 2022–2026 using an exponential smoothing algorithm (ESA) that takes time series or year data to predict the forecasted value. The forecasted value is our prediction value based on the previous year's value (it is acquired by the ESA algorithm). From Figure 1 it is clear that the healthcare sector is strongly affected by the lucrative business of the attacker that cost 8.7 million in the current year. This financial loss is detrimental to the nation's economy. The attackers leverage the security vulnerabilities either from the communication protocol or from hardware/software services, and exploit the vulnerability using nefarious attacks (e.g., Denial-of-Service (DoS), Man-in-the-Middle (MiTM), software-based attacks, data integrity attacks, and hardware-based attacks) and attempt to gain access to the legitimate healthcare resources. Therefore, it has become imperative to amalgamate different technologies and integrate them into the first line of defence (e.g., firewalls, access controls) in order to detect and mitigate or prevent security threats efficiently before they jeopardize the smart healthcare system.

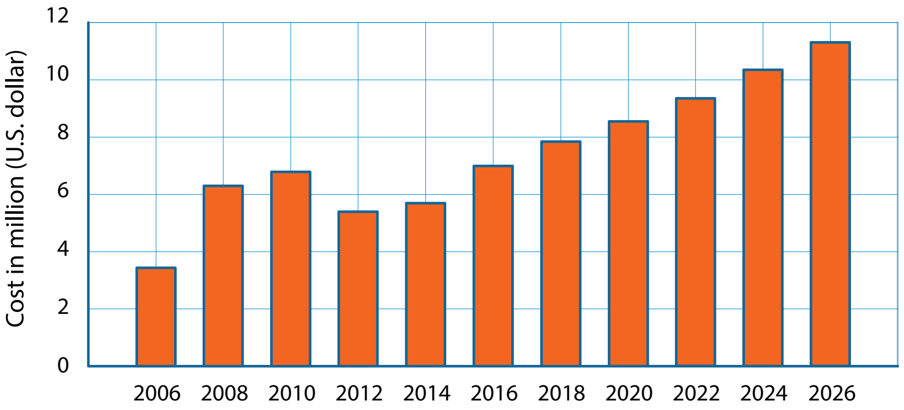


Figure 1. Total financial loss due to cyberattacks on the healthcare industry (2006–2026) [3].

The application of AI technology in smart healthcare systems is an effective means of addressing the increasing number of cyber-attacks proliferating in the healthcare ecosystem [4]. The AI plays a prominent role in analysing the attacker's malicious behavior, providing an endogenous security solution. Several researchers have proposed robust and concrete security solutions using AI in the smart healthcare system. For instance, the authors of [5] explored the security solutions of [6] on mutual authentication and patient anonymity for telecare medical information systems. They improved the results of [6] by examining the session keys between the communication entities of the healthcare system. Their proposed framework effectively addresses the forgery and spoofing attacks. Further, Wazid et al. in [7] proposed an AI-based lightweight and secure communication scheme to tackle protocol-based security threats. First, the patient's sensor collects data and forwards it to the personal server attached to the access points. At the receiving side, the healthcare providers (intended recipients of the data) are associated with the trusted authority for registration and authentication purposes. Then, the data are processed (i.e., prediction and classification using AI algorithms),and this step is overseen by the trusted authority. Their proposed scheme outperforms others in terms of delay, throughput, computation time, and accuracy with other baseline works.

However, AI algorithms cannot deal with data integrity attacks, where an attacker intercepts the communication in order to fetch and inject the malicious code into the legitimate data. In addition, the attacker passively (covertly) listens to the network communication to find sensitive information about the healthcare resources, which includes the number of patients are in critical conditions, what the thresholds of implant devices are, and login credentials of patient information systems [8]. This information is crucial from the security perspective because if the information gets into the wrong hands, severe privacy-related issues can threaten the smart healthcare system. Hence, the researcher has adopted blockchain technology characterised by decentralization, immutability, transparency, and security [9,10]. Pinto et al. in [11] explored the benefits of blockchain technology in the smart healthcare system, as it resolves the issue of data integrity, transparency, and security. They proposed a traceable system for electronic health records, whereby a patient and user can securely exchange their data. They used a private blockchain by implementing it in the HyperLedger Fabric, where two separate databases are maintained for data traceability. Further, the authors in [12] studied the heterogeneity problem of the smart healthcare system resulting from the variety of devices and data formats, which makes data management difficult. To address this issue, the authors presented a blockchain and cloud-based secure and efficient framework for better interoperability in smart healthcare systems. The integration of blockchain with cloud computing reduces the computational cost and increases the security and privacy of the smart healthcare system. Gohar et al. in [12] discusses the benefits of amalgamating blockchain and cloud technology to offer cost-effective and secure data storage of medical data. They proposed a five-tier secure and reliable framework for better interoperability between different healthcare providers. Next, Dhairya et al. in [13] proposed an AI and blockchain-based secure approach to securely transmit securely a patient's medical data to the medical staff. Firstly, they applied machine learning models to classify malicious data obtained by wearables and remove them from the healthcare systems. Then, they used blockchain technology to store the non-malicious wearable data to confront data integrity attacks. Similarly, the authors of [14] presented a collaborative framework comprising a deep learning model, blockchain, and 6G network interface. In their proposed framework, the predicted data from the deep learning models is stored inside the public blockchain to offer secure data storage. Moreover, the communication between each entity of their proposed framework is provided by the 6G network that offers low latency communication.

Despite applying the above-mentioned technologies in the smart healthcare system, numerous modern attacks still pose a threat to data security. Hence, the purpose of this current study is to examine various security attacks and their countermeasures for the smart healthcare ecosystem. First, we describe the emerging technologies and their impact on the smart healthcare system. Then, we examine recent security attacks on the healthcare environment, which includes smart healthcare systems, electronic health records, and patient information systems. Then a security solutions taxonomy is proposed to illustrate the different solutions proposed by the scientific community across the globe. Then, a comprehensive case study is conducted to mitigate cyber attacks on the smart healthcare system, which is evaluated using different performance metrics, such as accuracy, scalability, and malware dynamic analysis. Finally, we discuss several open issues and research challenges (in line with security) that still hinder the smart healthcare system's performance.

1.1. Scope of the Survey

In this section, we discuss the current state-of-the-art literature and present a comparative analysis of the existing solutions for security and privacy in smart healthcare systems. Researchers have proposed many surveys on security and privacy prospects for the smart healthcare system, but most of the surveys target electronic healthcare record databases, AI-based healthcare systems, and body area networks, where not all security attacks and their countermeasures are explored. For instance, Usman et al. in [15] presented a layered architecture for a body area network; then, at each layer, its security requirements are investigated. The study investigated various security threats and challenges, particularly for nano-networks and medical devices in body area networks. The authors of [16] explored security and privacy concerns for network-based medical devices. This exhaustive survey includes various medical devices, such as implantable, in and out body sensors, and remote healthcare monitoring interfaces with their regulatory standards and security challenges. The authors describe each security attack vector, such as eavesdropping, information disclosure, DoS, replay, sniffing attacks, etc., and its impact on medical devices. Further, they reveal the shortcomings of the existing regulations and countermeasures applied to address the security issues in network-based medical devices.

Then, Sun et al. in [17] studied the security and privacy vulnerabilities of IoT-based healthcare devices. They first proposed an architecture where each level of the architecture is endogenously explored for security and privacy challenges. They discuss attacks, such as authentication, data integrity, access control, key management, and DoS attack with their security solutions. The authors of [18] conducted a comprehensive study of security requirements of Healthcare 4.0, and elaborated on the requirements such as mutual authentication, anonymity, untraceability, perfect forward secrecy, and attack resistance [19]. Further, a taxonomy is presented comprised of various components of Healthcare 4.0, feasible security solutions are proposed. The authors of [20] explored the benefits of blockchain technology in tackling security and privacy attacks in electronic health record systems. They reviewed different blockchain-based schemes used to secure data storage, data sharing, and data audit of healthcare systems. Next, Bhuiyan et al. in [21] presented an exhaustive survey of IoT-based healthcare systems, where they focused on IoT-enabled healthcare infrastructure, standard protocols, IoT healthcare security challenges, and market opportunities. In regard to security issues, they reviewed device compromisation, information disclosure, and authentication attacks. Furthermore, a threat model is discussed where they emphasise the importance of having a risk management process to counter the security challenges. Jagatheesaperumal et al. in [22] reviewed the emerging technologies to offer security solutions in the healthcare environment. They discussed technologies such as IoT, futuristic networks, AI, and big data analytics and the role of these technologies in providing effective healthcare security solutions. However, most of the aforementioned studies explore general security attacks on a specific component of healthcare, such as smart devices, electronic healthcare records, and remote patient monitoring systems; but none of them gives a comprehensive details of those attacks and how they influence healthcare organization and the patient's life. Besides, a few surveys have not explored possible modern-day attacks, and their countermeasures. For instance, the authors of [20] reviewed only blockchain-based security solutions for the healthcare environment. In addition, the study did not investigates the recent attacks lunched on the smart healthcare system and how they impacts on the healthcare organization. Therefore, a comprehensive study is required that investigates recent security and privacy issues in smart healthcare systems. Moreover, this study would examine the role of modern technologies in confronting traditional and modern-day security attacks. Table 1 shows the comparative analysis between the existing and presented studies.

Table 1. Comparative analysis of the existing state-of-the-art studies and the proposed studies.

Author	Year	Contributions	Open Issues	Taxonomy	Case Study	Cons
Usman et al. [15]	2018	Concise survey on security and privacy issues of wireless body area network	Yes	No	No	Only body area network-based security attacks were considered
Yaqoob et al. [16]	2019	Studied security threats in network-based medical devices	Yes	Yes	No	Security solutions are not resistant towards modern security attacks

Table 1. *Cont.*

Author	Year	Contributions	Open Issues	Taxonomy	Case Study	Cons
Sun et al. [17]	2019	Survey on security requirements for Internet of medical things	Yes	No	No	Very consice security attacks are studied
Hathaliya et al. [18]	2020	Comprehensive survey on security and privacy issues of healthcare 4.0	Yes	Yes	No	Most of the security solutions are based on authentication schemes
Shi et al. [20]	2020	Review of blockchain-based security solutions for electronic healthcare systems	Yes	No	No	Only blockchain-based security solutions are explored
Bhuiyan et al. [21]	2021	Review of healthcare applications, security, protocols and market opportunities of IoT-based healthcare system	Yes	Yes	No	Solutions are not operable with advance security vulnerabilities
Jagathee saperumal et al. [22]	2022	Explored emerging technologies to offer security solutions in healthcare systems	Yes	No	Yes	Security attacks are partially explored
The proposed review	2022	Explored security and privacy solutions with their countermeasures in smart healthcare systems	Yes	Yes	Yes	-

1.2. Research Contributions

Following are the major contributions of this article.

- We discuss emerging technologies (i.e., AI, IoT, cloud computing, and blockchain) and emphasise the important role they play in the smart healthcare systems as a means of offering predictive, automated, computationally inexpensive, and reliable security services.
- We discuss the security challenges associated with the healthcare ecosystem (i.e., patient information systems, wearable systems, implantable and electronic health records) to encourage researchers from industry and academia to provide endogenous security solutions.
- We design a comprehensive taxonomy of existing security countermeasures to mitigate security threats in the smart healthcare environment.
- We proposed a real-world case study by designing an AI and blockchain-based secure architecture that confront malware samples and network attacks for smart healthcare systems. The proposed architecture is evaluated using various performance metrics, such as accuracy, scalability, and dynamic malware analysis.

1.3. Organization

This article comprises the following sections: Section 2 discusses the emerging technologies being applied in smart healthcare systems. Section 3 explores various security threats to and vulnerabilities of the smart healthcare system. Section 4 presents a taxonomy of security countermeasures that can ensure security. Section 5 proposes a secure architecture to mitigate the security risks in smart healthcare systems. Section 6 discusses the open issues and research challenges of smart healthcare systems. Finally, Section 7 concludes the paper.

2. Overview of Modern Technologies and Frameworks in Smart Healthcare Systems

Traditional healthcare systems consist of doctors, patients, clinical observatories, laboratories, hospitals, electronic health record systems, and patient information systems. In addition, they can include various healthcare services associated with healthcare monitoring, diagnosis and medical treatment, medical research, decision-making, and hospital management that require key-enabler technologies to control and manage the aforementioned healthcare services. The integration of various modern technologies, such as AI, IoT, blockchain, edge computing, and cloud computing, can offer the automation, intelligence, security, and inexpensive computational ecosystem that constitute the cornerstone of healthcare and improve the performance of the traditional healthcare system. The following are the key technologies adapted by the smart healthcare systems. Figure 2 illustrates key-enabler technologies with their essential characteristics in the smart healthcare system. Moreover, Table 2 shows the comparative analysis of various services offered by the modern technologies such as blockchain, IoT, AI, and cloud computing. Then, Table 3 presents a comprehensive analysis of the aforementioned modern technologies in the smart healthcare systems comprehensively.

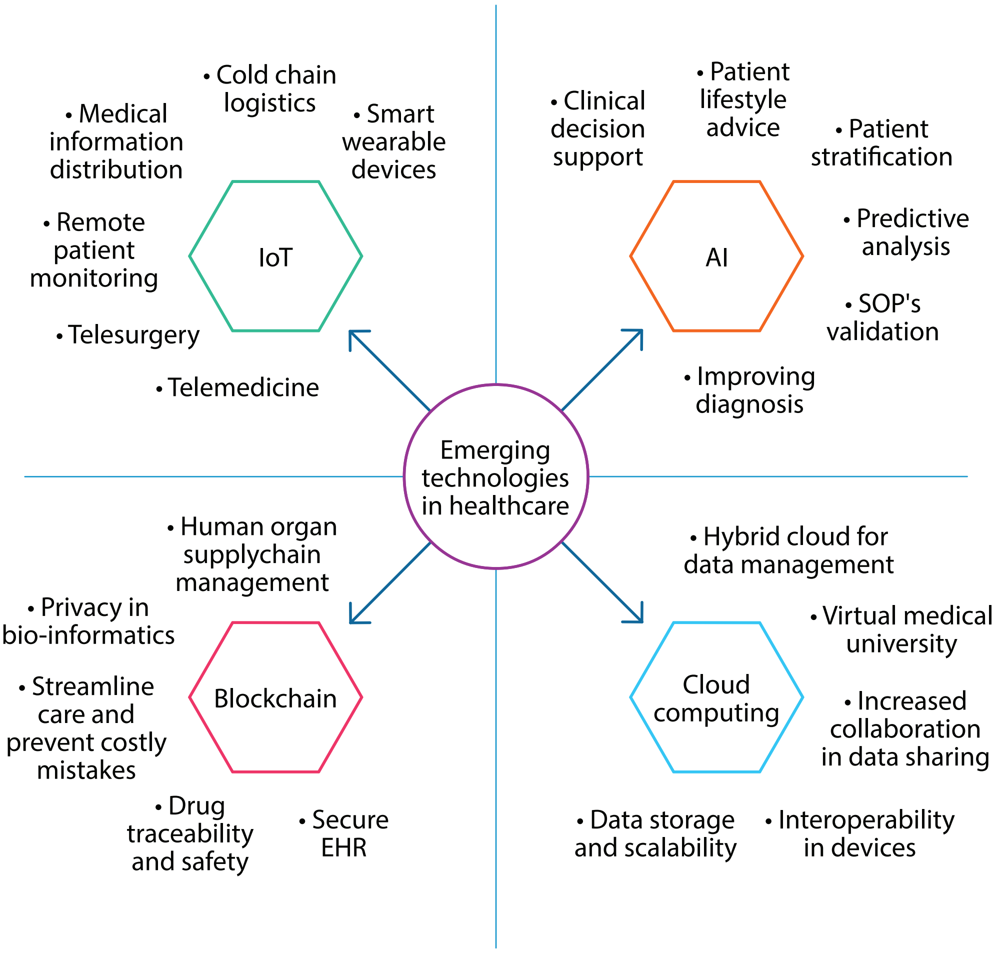

Emerging technologies in healthcare
IoT
• Cold chain logistics
• Medical information distribution
• Smart wearable devices
• Remote patient monitoring
• Telesurgery
• Telemedicine
AI
• Clinical decision support
• Patient lifestyle advice
• Patient stratification
• Predictive analysis
• SOP's validation
• Improving diagnosis
Blockchain
• Human organ supplychain management
• Privacy in bio-informatics
• Streamline care and prevent costly mistakes
• Drug traceability and safety
• Secure EHR
Cloud computing
• Hybrid cloud for data management
• Virtual medical university
• Increased collaboration in data sharing
• Data storage and scalability
• Interoperability in devices

Figure 2. Emerging technologies and framework of smart healthcare systems with their essential characteristics.

Table 2. Comparison analysis of various services offered by modern technologies.

Modern Technologies	Advantages	Challenges
Blockchain	High security, decentralized, high latency, transferable identity, high reliability, anonymity	security issues with private owner, high bandwidth consumption, poor scalability with large network, high resource consumption
AI	High availability, dynamic compatibility with all other platforms, and better efficiency	Low efficiency, high communication and computation costs, need to focus on protecting data
Cloud computing	High computational capacity, efficient, improved data storage, improved flexibility and mobility	High communication costs, security concern, reliability, portability, and interoperability issues
IoT	Requires low latency, lightweight algorithms, greater heterogeneity	Low computational capacity, data storage, and privacy challenges

2.1. Internet of Things-Based Smart Healthcare Systems

Previously, because the separate components of the healthcare system were not interconnected, the system was not capable of continuously delivering medical services to patients. Hence, it was challenging for medical practitioners to continue monitoring their patient's health and give recommendations accordingly. The incorporating of IoT technology in the healthcare sector allows doctors to remotely diagnose and treat their patients and enables medical staff to provide high-level care to their patients. This is accomplished by lightweight IoT devices (sensors) that are deployed in the healthcare environment, where each sensor has the potential to accumulate data from the surrounding environment (e.g., patient's body) and forward it to various healthcare applications via the Internet. IoT allows patients to send their real-time medical data, such as blood pressure, oxygen levels, calorie consumption, and heart rate, using wearable sensors attached to the body. With the help of sensors placed on the body, the doctors can pervasively monitor them (continuous monitoring) and suggest recommendations as per their live medical data. Here, the patients do not have to come to the hospital; instead, it directly connects to the doctor via a remote connection from their home. Due to this, the vital bed is free for other patients who need emergency intensive care.

Moreover, the healthcare system has many physical assets, such as oxygen cylinders, nebulizers, wheelchairs, oxygen meters, heart monitors, personal protective equipment, and surgical tools that must be properly managed so that one can easily track down their numbers and locations in the emergency situations [23,24]. IoT-based healthcare asset management helps to track these assets in no time. For example, in [25], the authors discuss the COVID-19 global pandemic that requires advanced medical facilities in a short span of time. To this end, they proposed an IoT-based healthcare monitoring architecture that offers hybrid communication, colossal medical screening, and cloud-based data centres to help hospitals, rescue teams, and first aid units. Further, Subhai et al. in [26] presented an edge-enabled IoT healthcare management system intended to improve the performance of the monitoring, diagnosis, and management of the patient's data. They proposed a system that monitors different medical tasks and manages various healthcare activities using database systems. However, because of the system's centralized storage, the attacker can breach its security.

Table 3. Comparative analysis of various modern technologies in smart healthcare systems.

Authors	Year	Objective	Modern Technology	Pros	Cons
Subahi et al. [26]	2019	IoT edge-enabled medical management system for better recommendation in healthcare systems	IoT	Performance of system needs to be improved	Anonymity, scalability, and efficiency parameters are not considered
Gupta et al. [27]	2020	Presented a UAV and blockchain-based outdoor delivery scheme for healthcare 4.0	UAV	Improved scalability, latency, and network bandwidth	Communication and computation overhead is not focused
Ray et al. [28]	2021	Proposed an EHR scheme in IoT-based blockchain system	Blockchain	Anonymous, high interoperability, low cost	Should be implemented in real-time environment
Gourob et al. [29]	2021	Studied a vision-based gesture recognition system for controlling robotic hand	Wearable technology	Real-time execution	Need to consider latency and reliability parameters
Subramanian et al. [30]	2021	Presented a consortium blockchain-based system to secure the data of diabetic patients	Blockchain	Authenticated and improved transaction speed	Need to minimize transaction fee and power consumption
Tomasicchio et al. [25]	2022	Discussed a healthcare emergency management to monitor wide epidemics	IoT	High robustness and quality of service	Communication and computation overhead is not discussed

Table 3. *Cont.*

Authors	Year	Objective	Modern Technology	Pros	Cons
Parra et al. [31]	2022	Presented an AI-based recommendation system in a healthcare scenario	AI	Fair and preserve data screening	Not focused security attacks such as data modification and spoofing
Elayan et al. [32]	2022	Performed healthcare data analysis using deep federated learning	AI	Reduced operational costs	Need to ensure security against cyber and privilege attacks
Costa et al. [33]	2022	A Fog and blockchain-based architecture to manage the global vaccination	Cloud computing	Low latency, high scalability, and feasibility	Need to check feasibility in a virtual environment

2.2. Artificial Intelligence in Smart Healthcare Systems

The healthcare industry requires intelligent and predictive services, providing endless opportunities for precise and impactful patient care and administrative processes [34]. Moreover, with the incorporation of IoT devices, a colossal amount of data are generated and transmitted from different entities in the healthcare industry. The generated data needs efficient management and data improvisation by incorporating AI technology in the healthcare sector. The application of AI technology in the healthcare sector offers numerous advantages over the conventional healthcare system that uses cumbersome data analytics and decision-making techniques. It interacts with medical data (training data) to provide valuable insights into medical diagnosis, treatment, and clinical decision support. For example, in [35], the researchers explored osteoporosis disorder (porous bones), which is generally detected by standard X-rays and magnetic resonance imaging (MRI) scans. The authors aimed to improve classification of osteoporosis patients over the ultrasound features using an AI-based feature selection technique. As a result, they achieved 71% accuracy in classifying the osteoporosis patients according to the risk of fracture. Further, the studies [36,37] proposed an AI-based remote patient monitoring system (especially for intensive care unit (ICU) patients) that provides readmission, vital sign assessment (body temperature, pulse rate, respiratory rate), and any abnormality in the patient routine care. Their proposed model outperforms others in terms of accuracy, i.e., 67.53% for readmission and 67.40% for abnormality.

Wazid et al. [7] presented the essential characteristics of AI in healthcare sector, where they use AI models to efficiently predict the chances of heart attacks and likelihood of getting tumours, and finding intelligent patterns from the healthcare data. They presented an AI-based lightweight and secure communication scheme for the healthcare ecosystem. They evaluated their scheme using various performance parameters, such as end-to-end delays and throughput with different simulation scenarios. They concluded that the decision tree algorithm outperforms other algorithms in terms of computation time and SVM outperforms in terms of accuracy over the existing algorithms. Then, Parra et al. in [31] studied the application of AI algorithms for sustainable development. Here, they examined the individuals who are in need of an AI-based question recommender system for different scenarios. The sole purpose of their study was to strengthen the AI-based question recommendation to not only for security screening and financial services, but also for incorporation in the healthcare sector where it has potential for a number of applications. Recently, federated learning has received much attention in order to data offloading and preserving privacy in the healthcare sector [32,38]. From this perspective, the authors of [32] proposed a federated learning-based healthcare data monitoring framework to address the problem of local data acquisition. Their framework also helps medical professionals to detect skin diseases effectively. The empirical results show that their proposed framework preserves patients' data privacy and reduces the operational cost of the medical providers. Similarly, ref. [39] reviewed the problem associated with the diverse data of healthcare, where machine learning models do not have the capability to train on the data. Therefore, they adopted the decentralized algorithm, i.e., federated learning to develop a message queuing telemetry transport (MQTT)-based distributed networking framework for brain tumour segmentation. Their results show that their proposed framework has better accuracy and latency performance in the regular operations of the healthcare systems.

2.3. Blockchain-Enabled Healthcare Systems

One of the imperative requirements of the healthcare sector is to secure medical data (patient data) and efficiently manage different supply chains, such as pharmaceuticals, human organ donation, and medical appliances or infrastructure of smart healthcare ecosystems. Blockchain is a prominent technology that provides security, reliability, privacy, and interoperability, thereby transforming the healthcare system [40]. Blockchain has an immutable and decentralized ledger, where medical data are securely stored and safeguarded from data integrity attacks. The ledger is protected from cryptographic features, such as asymmetric keys, hashing, and digital signatures, making the data are tampered-proof [41]. Moreover, the ledger is decentralized, so if any small change occurs in the data transaction, it will be known by each blockchain member, thereby improving improving the transparency of the overall system. As the healthcare domain is always at a high risk of being exploited by attackers, leveraging blockchain technology facilitates secure patient data exchange, prevents disruptions, and efficiently manages medical resources. The authors of [42] presented a blockchain-based smart healthcare system to protect the data privacy of various healthcare system users. They developed different types of smart contracts to validate data transactions, access control, and decision-making in an open network. In addition, they utilized differential privacy mechanisms to preserve users' privacy. Their results show that the proposed scheme outperforms others in terms of reliability, stability, and system-level traceability [43].

Ray et al. in [28] proposed a secure and reliable blockchain-based scheme to counter security attacks on electronic healthcare record systems. They used private blockchain and swarm intelligence approaches to ensure secure data exchange across the IoT network. Further, Subramanian et al. in [30] explored the use-case of blockchain technology in tackling diabetes disorder, especially during the COVID-19 pandemic. Using blockchain technology, they prioritized healthcare resources, such as medical beds, oxygen, insulin pumps, telemedicine, and a constant monitoring system for diabetic patients who were mostly affected by the pandemic. They applied blockchain-based technologies, such as interplanetary file systems, smart contracts, and the new economy movement, to encrypt and authenticate patient data and develop a proof-of-concept model. Their proposed system shows notable outcomes in terms of transaction speed, transaction fees, and power consumption.

2.4. Cloud Computing Technology for Healthcare

Cloud computing and its various domains, such as edge and fog computing, offers a collaborative and connected environment for different sectors of the healthcare industry [44]. The smart healthcare ecosystem is vast and faces many critical challenges, including high operational costs, security, privacy, and centralized data storage. The use of cloud technology strengthens the overall workflow of the healthcare sector in terms of accessibility, quicker response time and better-personalized care, and resolves load balancing issues. Furthermore, fog and edge computing are versatile cloud computing techniques that reduce the latency between wearable devices and doctors. This is imperative because an ICU patient requires critical care without any data transmission delay; if his wearable device cannot relay the data quickly to the medical practitioners, his life can be at risk. The fog and edge computing allow the medical devices to process their data locally rather than transmitting it from the global model, resulting in less delay (quick response time), which improves the performance of remote monitoring and strengthens the patient engagement process.

Researchers have adopted many solutions by employing on-demand computing services [12,45]. For instance, Wang et al. in [46,47] presented the problem of delayed response time in the safety-critical system of healthcare. To tackle the issue, they utilized fog computing for reliable data exchange and rapid data processing. However, they observed that fog devices generate an enormous amount of data which is difficult to manage, so they used neighbourhood optimization that enhances the data transmission and fault tolerance of the smart devices of the smart healthcare systems. Costa et al. in [33] proposed a fog and blockchain-based global vaccination scheme to offer a quick and efficient decision-making strategy for vaccination during the COVID-19 pandemic. The proposed prototype was implemented and evaluated using different performance metrics, such as response time, throughput, and data rates where the global vaccination campaign was organized. Then, [48] studied task scheduling challenges (time delay) facing healthcare services, where if the transmission of data to the healthcare providers is delayed, this directly influences the quality of service delivery and patient's life. To address the issue of delayed communication, the authors used cloud computing in the IoT-based healthcare system. They used swarm intelligence algorithms to optimize the data communication between healthcare providers and the patients. Their proposed model outperforms the baseline models in terms of waiting time, makespan, and resource utilization. Then, Itoo et al. in [49] discuss the security and privacy issues associated with the traditional medical system that uses precarious communication link between different entities of the healthcare system. Further, they also examined the inefficiency of blockchain technology in terms of computational complexity and its ability to store massive amounts of data. They used cloud computing to store the medical data and blockchain technology to offer privacy and security to the stored medical data. In addition, the authors validated their work using AVISPA tool against different security attacks (e.g., replay attacks). Ansari et al. in [50] studied the sensitive nature of medical data targeted by attackers. To overcome this issue, the authors presented a privacy-enabled secure communication framework for a smart healthcare system. Using cloud-based authentication, they provides a robust anonymity to the doctors, patients, and communication between doctors and patients.

2.5. Wearable Sensing Technology for Healthcare

Wearable sensing technologies have a huge impact on people quality of life, with the advancement of innovative technologies such as Artificial Intelligence (AI), big data analytics (BDA), and blockchain. Wearable sensing technologies such as smart watch, smart shoes, tracking sensors, smart eye-wear, help to track and manage the patient's health data remotely by utilizing either the wireless sensor network or the conventional network [51]. These wearable sensing technologies have proves to be beneficial for the treatment of patients suffering from life-threatening diseases. Basically, these sensing devices can be attached to the patient's body or their clothing to gather and process data that can indicate the patient's health status. Moreover, these wearable technologies are made to be versatile and comfortable to wear, especially for elderly people. Thus, wearable sensing devices have completely transformed the working environment of hospitals because some patients can now be treated remotely. Moreover, the remote monitoring of patient's health overcomes the high cost and efficient treatment challenges associated with traditional patient care. This has motivated people to opt for wearable sensing technology, accounting for the increasing use of these technologies over the years. Considering the outlook and usage of wearable sensor technologies for healthcare, many researchers have considered the advantages of these wearable technologies for benefit of the healthcare system. For instance, Gourob et al. [29] developed a vision-based hand gesture recognition system for controlling the robotic hand. They have improved the performance of gesture recognition system to implement it in real-time scenarios. Further, by means of an implantable fluorescence image sensor the authors of [52] performed the real-time monitoring of immune response in cancer therapy. They have designed a prototype to improve the response time for 50% of cancer patients who were undertaking immunotherapy. However, the aforementioned authors did not consider the scenario where elderly people are being treated with the help of wearable sensor technologies. Thus, Mansour et al. [53] applied an AI and Internet of Things (IoT)-based disease diagnosis model for smart healthcare systems. They have considered the Cascaded Long Short Term Memory model for an efficient heart and diabetes diagnosis, achieving the improved accuracy.

2.6. Unmanned Aerial Vehicles in Healthcare

With the evolution of Information and Communication Technology (ICT), the hospital management have adopted the smart wearable technologies for the timely and efficient treatment of patients. However, various innovative technologies such as DL, AI, swarm intelligence, unmanned aerial vehicle (UAV) have been exploited to combat the severe medical conditions of patients. For example, we can consider the scenario of coronavirus disease which has had sever impacts on the people's health, can be tackled using the usage of aforementioned promising technologies. However, the main reason for for widespread incidence of coronavirus is the increase in human interaction which occurs other during, and which can be reduced with the help of drone (unmanned aerial vehicles—UAV) technology. The usage of UAV minimizes the human contact and helps with clinical treatment by providing the medical equipment and medicines within the threshold time required for the patient's early treatment. For example, the authors of [54] studied the role of drone technology in tackling the surge of coronavirus disease worldwide. The authors analysed various promising technologies such as IoT, edge computing, DL, and virtual reality (VR) to mitigate the effect of coronavirus disease. Moreover, they have focused on the advantages and limitations of adopting the drone technology in healthcare. Next, Gupta et al. [27] utilized the blockchain technology to enable a secure and preserve outdoor delivery scheme for Healthcare 4.0 with the help of UAVs. They mainly focused on securing the medical supplies during the outdoor delivery process by performing a security analysis using the on MyThril security tool. Further, the authors of [55] implemented the IoT and UAV-enabled wireless body area networks (WBAN) for healthcare applications. They have considered various sensors to ensure the smooth and faster interaction between patient and healthcare professionals with the usage of UAVs, especially in cases of emergency.

3. Security Attacks in Smart Healthcare Systems

Nowadays, most traditional healthcare systems are connected with each other via the Internet to offer ubiquitous medical services, such as telemedicine, remote diagnosis, and patient information systems. Consequently, today's healthcare system saves many patients' lives before their conditions become exacerbated, and reduces the expense of medical treatment across the globe, thereby improving the individual's quality of life. However, connecting the medical services or devices through the open-access network, i.e., the Internet, have inevitable consequences for security and privacy, as these devices are susceptible to denial-of-service (DoS) attack, data modification attacks in the patient information system, malware attacks to thwart the entire operation of the healthcare system, and implantable (smart devices) controlled by the master node, which can be exploited using IoT-based attacks [56]. Below, a detailed explanation is provided of each attack that could be launched on a healthcare system. Figure 3 shows various security threats associated with a smart healthcare system.

3.1. Denial-of-Service Attacks

Healthcare systems are most vulnerable to voluminous attacks (e.g., DoS and flooding), where hackers or cybercriminals make the network resource inoperable by flooding the network with a massive number of packets. As a result, several critical services in healthcare systems, such as data sharing, appointment scheduling, and patient reports, cannot be accessed by medical personnel. The attack could be more severe when multiple machines are connected with each other to target a specific machine or resource in the healthcare systems, commonly known as distributed denial-of-service (DDoS) attack. The traditional

DoS attack sends multiple packets from a single machine; conversely, in a DDoS attack, the attackers use previously-hijacked machines and interconnect them (botnets) so that each machine sends multiple packets to the target machine simultaneously, thereby harming the healthcare ecosystems. Several cases have been reported in the past where DDoS has been considered one of the most significant attack vectors in the healthcare environment. For example, in 2014, attackers unleashed a DDoS attack on the Boston Children's Hospital, where $\approx$ 40,000 network resources were manipulated and controlled by the attacker's home computer [57]. This attack was so massive that the Boston hospital not the only facility to be affected; the attack also had severe effects on other hospitals connected to the same network interface. Furthermore, the impact of DDoS attacks become more severe when integrated with other passive or active attacks, such as malware and injection attacks, leading to huge losses to healthcare infrastructure. Cybersecurity and Infrastructure Security Agency (CISA) recently disclosed a new vulnerability in patient monitoring systems (CME8000 devices) that could cause a massive DDoS attack [58]. The attacker can craft multiple user datagram protocol (UDP) packets to crash the CME8000 devices and to gain momentary access to the system setting, where they can install malicious firmware. Consequently, CME8000 devices' functionality is permanently changed, which places the patient's life at risk. The authors of [59] designed a device authentication mechanism for IoT-enabled healthcare systems. They have adopted the authentication mechanism to secure the IoT-based healthcare system against DoS attack along with the other attacks such as MITM and eavesdropping attacks.

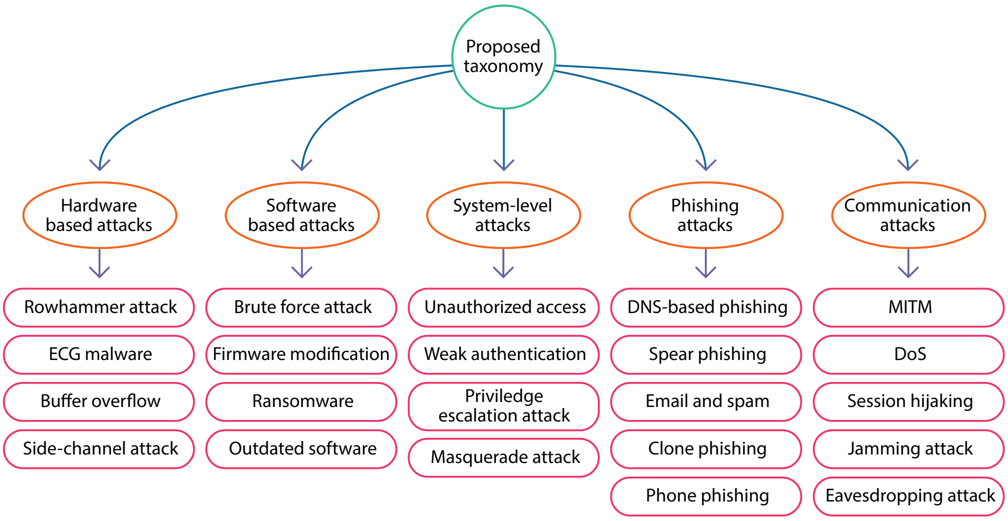


Figure 3. Taxonomy of different security attacks on a smart healthcare system.

3.2. Data Breach Attacks

A data breach is a coordinated security incident where a cognizant insider or external malicious user obtains unauthorized access to the authorized information (e.g., confidential or protected data). This attack could be an accidental event, where an insider (employee) accidentally reveals the sensitive information, or it could be a nefarious event, where an attacker explicitly performs the privilege escalation approaches to extract the sensitive information. In the context of smart healthcare systems, patients' medical records, personal information, social security number, and financial information is the most sensitive information that an attacker attempts to acquire. Most healthcare facilities have electronic healthcare record databases where the patient's information is centrally stored; these are the prime target of cybercriminals. Once they acquire the central databases, they extract patients' critical information and sell it to third-party intermediaries, resulting in the healthcare sector having to sustain financial loss and reputational damage loss. In May 2022, Partnership HealthPlan and Shields Health Care Group organizations of California and

Quincy disclosed a data breach that affected ≈2 million individuals and 50 small facilities. In a cyberattack, individuals' data, such as date of birth, patient medical data, addresses, patients health insurance, and social security numbers, where accessed by the attackers [60]. Later, in August 2022, Yuma Regional Medical Center was exposed to a ransomware attack that stole the social security numbers of ≈700,000 individuals [61]. Sharma et al. [62] proposed a blockchain-based architecture to secure and preserve the patient's electronic health records by executing a smart contract. Furthermore, they focused on confirming the user's identity utilizing the zero-knowledge proof and proxy re-encryption safeguard the healthcare systems against data breaches.

3.3. Phishing Attacks

A phishing attack is an attempt to acquire the victim's valuable information, such as login credentials (e.g., username and password), bank details, credit card numbers, company data, and other personal information that potentially has value. In a smart healthcare system, phishing is performed by creating a fake web link with malicious code running in the backend. So, when a user clicks on the link, the malicious code silently installs the malware on the healthcare system, which will spread rapidly to various medical devices. The attackers use social engineering techniques (e.g., baiting, pretexting, scareware, etc.) to create fake web links, which encourage the hospital staff or patients to deliberately click on them. In April 2022, three medical institutions, i.e., Charleston Area Medical Center, Central Minnesota Mental Health Center, and Christie Clinic were targeted by phishing attacks and email security incidents. The attackers have collected many employees' login credentials, and social security numbers, which impacted 54,000 individuals [63]. Another incident oocrred in August 2022, when Allegheny Health Network was compromised by a phishing attack that affected ≈8000 patients, causing them to lose their login accounts. To respond to this attack, the organization immediately shut down (temporarily disabled) the compromised accounts, reset login credentials, and applied monitoring controls [64]. In addition, the Health Sector Cybersecurity Coordination Center reported that attackers have developed a new phishing scheme that lures the victims to redirect to a phishing web page (containing malicious Trojans) that steals your valuable information. Mostly, the phishing attack is launched via emails, where catchy phrases are framed to manoeuvre the human brain to click the malicious web page [65]. Therefore, to protect the smart healthcare system from fraud and phishing detection, Mehbodniya et al. [66] applied ML and DL models such as Random Forest, K-nearest Neighbor (KNN), Decision Tree, Naive Bayes to identify the financial fraud detection in modern healthcare systems. Finally, the KNN model yielded the best accuracy compared with the other conventional models used for mitigate the phishing detection in healthcare.

3.4. Malware Attacks

Smart healthcare systems are susceptible to malware attacks. Particularly, electronic healthcare record systems are at a high risk of being exploited by malware. This is because these systems have up-to-date information about their patients (e.g., patient medical data, patient health insurance, patient billing information), collected by the smart healthcare system for the purpose of providing patient care. The attackers use modern tools, tactics, and procedures to deploy different malware variants in the healthcare infrastructure to compromise the electronic healthcare record systems. Formally, trojans are the widely used malware in the healthcare industry, which deliberately target the infrastructure and propagate their impact via the internet. Trojans are remotely controlled by attackers who can perform undesired operations on the victim's computers, such as modifying or deleting the patient's data from the electronic healthcare record system. Furthermore, ransomware is the type of malware that makes the system and its files inaccessible to authentic users until the ransom is paid.

Here, a trojan acts as a carrier that carries ransomware as a payload, and once installed in the healthcare system, it encrypts the patient's information. It uses asymmetric cryptography to generate public-private key pairs that encrypt and decrypt all files associated with the system. Here, the attackers only publicize the private key only when the victim pays the ransom. Such malware compromises the entire healthcare organization in terms of finance and reputation. For instance, the Karakurt ransomware group extended its cyberattacks and impacted thousands of lives. First, it performs scanning and reconnaissance to gather information about its targets; then, it attempts to acquire sensitive patient information. Once the information is acquired, it encrypts the files until the ransom is paid [67]. Further, North Korean-based Maui ransomware is targeting US-based healthcare sectors, especially electronic health records, imaging, and diagnostic services [68]. It is designed to remotely control and encrypt a particular file on an infected machine; it uses advanced encryption standard (AES) 128-bit encryption standard with unique public-private key pairs, here the key pairs are further encrypted using the Rivest Shamir Adleman (RSA) algorithm. Moreover, the authors of [69] explored different types of ransomware attacks and their possible countermeasures in smart healthcare systems. They discussed the significant benefits of modern technologies, such as AI, blockchain, software-defined networks, and IoT, safeguarding the smart healthcare ecosystem against malicious attacks.

3.5. Man-in-the-Middle (Sniffing, Eavesdropping, Data Integrity) Attacks

MiTM attacks, where a preparatory (attacker) interferes with the conversation between two legitimate users. The preparatory (attacker) either intercepts (eavesdrop) the communication or uses impersonation (using address resolution protocol (ARP) spoofing) to jeopardize the communication between two parties. The sole purpose of this attack is to passively listen to ongoing communication and steal personal information for their own benefit. In a smart healthcare system perspective, the MiTM attacker hijacks the communication between healthcare providers, wearables, or patients and doctors, whereby they unethically alter or copy healthcare data. Further, with MiTM attacks, the attacker inserts malicious payloads that disrupt the patient's monitoring system. The smart healthcare system consists of different portable sensor nodes, which require short-range communication (with low bandwidth) to relay their information to other sensors. Formally, they use conventional Bluetooth technology (with low energy) to exchange data with local servers; however, intruders launch MiTM attacks by leveraging the precarious communication link between sensors and local servers [70]. The attackers either uses publicly available tools, such as Hetty, Bettercap, MiTMproxy, and Proxy.py, or they develop their own sophisticated MiTM tool that the first line of defense (e.g., firewalls) cannot detect. Using the tools mentioned above, an attacker can successfully intercept (sniff) the communication (both HTTP and HTTPS) between sensors and local servers; then, it conducts traffic analysis to find the sensitive information. As a result, the attacker can insert the healthcare emergency or abnormal medical data into normal data and send it back to the local servers. For example, in [71], a security expert from McAfee shows a MiTM attack on insulin pumps, where a modified antenna and software are designed to wirelessly control the device. They show how an attacker can remotely control the insulin dosage of a diabetic patient. Further, two researchers, Billy Rios and Jonathan Butts from QED security, improved the detection of attacks by determining the radio frequencies between the insulin pump and its controller known as "boluses". They stated that the communication between implant device and controller is entirely unencrypted and that it is relatively easy for an attacker to perform a coordinated MiTM attack [72]. Furthermore, the authors of [73] considered a smart healthcare communication environment along with an elliptic curve-based secure and preserve protocol to maintain the data authentication and integrity during the wireless communication between patient and healthcare experts.

3.6. Software-Based Attacks

The smart healthcare system consists of various hardware and software that provide necessary services to the medical staff, patients, and other sectors of the healthcare ecosystem. One of the main critical weaknesses of a large technological organization is that it cannot adequately maintain its resources and infrastructure properly. This is one reason that the attacker first uses reconnaissance, i.e., scans the entire organization's network to find strong and weak vulnerabilities, either in software or in hardware. Software-based attacks can occur where the administrator does not update their software, tools, operating system, utility, and firmware. Outdated and obsolete software poses a severe threat to the healthcare infrastructure; for example, old bugs are not patched in the updated version of the software. Recently, four vulnerabilities have been found in healthcare services, such as CVE-2020-11022, 2020-11023, 2015-9251, and 2019-11358 are the basic jQuery-based vulnerabilities [74]. Another vulnerability, i.e., CVE-2020-0601, was found in the Biomerieux product, where an attacker signed a malicious executable using a spoofed code-signing certificate to proliferate ransomware attack [75]. Further, healthcare providers are not updating their firmware, which opens up the gate for attackers to counterfeit firmware that gains access to the medical devices and makes fake copies of the healthcare firmware. Argaw et al. [76] proposed a risk-based approach to maintain the cybersecurity between healthcare professionals, staff, patients, vendors, academics, and manufacturers in the modern healthcare systems. Further, they have discussed about the recent security and privacy research challenges to the healthcare systems due to the involvement of medical devices during the remote monitoring of patient's health.

3.7. Side-Channel (Information Gathering, Reconnaissance) Attacks

Before any cybersecurity attack, an attacker must scan and extract sensitive information from the victim's infrastructure, such as encryption methods, open service ports, software version numbers, and network information. In a smart healthcare system, the attackers have a wide opportunity to propagate their attacks due to the many heterogeneous devices involved in an ongoing task. Here, attackers first discover how the medical device's circuit works, how data are exchanged between devices, their communication protocols, and much more. For example, attackers can exploit the electromagnetic interference that intercepts or jams the communication to infer/extract the patient's sensitive information. In addition, the attackers can manoeuvre the medical devices that show forged sensor readings to trick the medical staff and practitioners. Also, an attacker alters the physical resources (network) to passively disrupt the performance of medical devices (e.g., sensor spoofing). By means of this attack, an adversary can easily find the cryptography keys and digital certificates that are essentially as protection from cyber-attacks. The authors of [77] show the impact of side-channel attacks in the smart healthcare sector, where an attacker can compromise the smartphone-based personal health records consisting of patient medical reports, family medical history, mental health data, fitness data, physical activity data, and other information. Furthermore, attackers can use more sophisticated side-channel attacks, such as statistical and differential power analysis attacks. These are statistical attacks that measure the power consumption of two samples to analyse the correlations between them [78]. For instance, an adversary can analyse the RSA keys by averaging the two samples, where '1' is displayed as a taller bump, and '0' has a shorter bump.

4. Taxonomy of Smart Healthcare Security Solutions

In this section, we present a solution taxonomy for different security solutions adopted by researchers across the globe. The taxonomy is categorized according to various security attacks, such as hardware, software, network, system-level, and side-channel, and their countermeasures given by the scientific community and cyber experts for smart healthcare systems. Table 4 shows the comparative analysis of different security solutions proposed by the researchers across the globe. A summarized explanation of each security solution is given below.

4.1. Hardware-Based Attacks

Hardware attacks are those where attackers manipulate medical devices to forge medical data, thereby placing the patient's life at risk. In order to address this security issue, Gountia et al. in [79] studied a vulnerability in the design flow of biochip devices where an attacker can manipulate the samples by leveraging attacks, such as DoS, hardware malware, and counterfeiting. To respond to these security issues, the authors developed a user-defined algorithm that efficiently assigns a checkpoint for error recovery to improve the security of microfluidic biochips. Their results show that the proposed algorithm outperforms other baseline approaches in terms of computational complexity and error detection rate. Further, the authors of [80,81] explored security issues (IoT device attacks) in IoT-based healthcare systems. They proposed a multi-layered scheme where they integrate programmable gate arrays consisting of hardware-based cipher algorithms to optimize the security and privacy of the IoT-based healthcare ecosystem. Their results show that the proposed scheme outperforms others in terms of energy consumption, computation time, and frequency rate towards tackling security threats of IoT healthcare systems.

4.2. Software-Based Attacks

Software-based attacks directly impact healthcare resources, where an outdated software/firmware/tool/utility/operating system leads to propagating security attacks in smart healthcare systems. They are categorized as malware, outdated software, fake firmware updates, and phishing; their countermeasures are explained below.

- Malware—These are malicious executable, files, or code that disrupts the behaviour of the smart healthcare system. Thus, to counter such attacks on the healthcare ecosystem, ref. [82] presented attention and deep learning (DL)-based detection and classification approach to find IoT-based malware in healthcare devices. The authors extract the byte sequence from the malware executable and automate the feature selection. Their proposed approach was evaluated using malware detection and classification accuracy, achieving 95% and 94%, respectively, compared to the existing approaches. Recently, the android-based smartphone and wearables have been popularized by integrating predictive and intelligent services, such as AI-based diet planning recommendations, digital well-being, and tracking vital signs for any particular diseases. Nevertheless, the wearables are susceptible to malware attacks that diminish the performance of predictive services. Kong et al. in [83] designed a secure analysis system for medical wearables. It first performs a matching analysis between smartphones and wearables to ensure that a safe application is installed. Further, they conduct similarity analysis of malicious applications using the oversampling method. Finally, their proposed work is evaluated on the Google play store, where they found 44 applications that have permission mismatches.
- Ransomware—Ransomware is a special type of malware that is installed from backdoors or by clicking on an illegitimate web link. It encrypts the sensitive files using asymmetric key encryption, which is decrypted using a private key that the victims can obtain after the ransom is paid. Researchers have adopted AI-based algorithms to tackle ransomware in the smart healthcare sectors. For instance, Almashhadani et al. in [84] stated that modern detection systems are not capable of detecting the anomalies and malware signatures promptly, and by the time these are detected, the ransomware has already infected and exfiltrated a large number of healthcare resources. They studied the behavioural properties (e.g., network activities) of ransomware, especially “Locky” ransomware which is one of the most rampant families of ransomware. Subsequently, they developed an intrusion detection system that analyses the packet and flow levels of the network, and based on that; they analysed the ransomware behaviour. Their detection system has better accuracy and low false positive rates and efficiently tracks ransomware network activities. Further, Butt et al. in [85] studied control systems and their security vulnerabilities, especially in terms of ransomware. Smart healthcare systems also use control systems, such as supervisory control and data acquisition (SCADA), to control various items of medical equipment. Ransomware targets different operations performed by the SCADA system to jeopardize the overall performance of the healthcare ecosystem. The authors

highlighted various security loopholes in SCADA systems where the ransomware can be directly attacked; also, it shows different countermeasures to tackle the attack. The authors of [86] proposed a blockchain-based ransomware defence system, where all healthcare devices are associated with the blockchain network. Here, if the attackers lock the system and personal files, the locked system can fetch the data from the blockchain node (data recovery using blockchain backups). The proposed system also saves the ransomware signatures in the blockchain to detect it and prevent it from attacking the smart healthcare systems.

- Outdated software—Most smart healthcare systems still rely on old legacy systems running on outdated operating systems and software easily accessible by the attacker. This outdated software leaves many footprints (sensitive data), such as X-rays, MRI scans, and doctor-patient conversations, that can raise several privacy concerns if they fall into the wrong hands. Recently, security experts explored key-enabler technologies to integrate endpoint detection [87], reputational analysis [88], and real-time behavioural analysis to detect any suspicious activities in smart healthcare systems. In addition, the researchers also suggest using different vulnerability management tools (e.g., Nessus, Nexpose, Tenable, Qualys, etc.) [89] that show device and software vulnerabilities and software configurations in order to reduce the attack surface and protect the healthcare resources from any security attacks.
- Fake firmware update—Smart healthcare systems are facing a major challenge in regularly patching the firmware of their medical devices firmware. T. It is left to the device manufacturer and maintenance vendor to update and patch the devices and their associated firmware. Nonetheless, with modern security attacks, the attackers can easily lure the old patched firmware and convert it into counterfeit firmware using remote attacks, physical tampering, and indirect modification that helps the attacker to propagate their attack surface and impact a large number of healthcare resources. To secure the healthcare device's firmware from the fake firmware update, a maintenance vendor must analyse the firmware using the firmware security testing methodology. The methodology is composed of nine consecutive steps, such as reconnaissance, securely obtaining the firmware copy, analysing firmware using firmware characteristics, analysing the firmware filesystem, performing static analysis on the firmware to find code-based vulnerabilities, emulating the firmware, analysing the binaries of firmware, performing dynamic analysis on firmware, and exploiting the previously-identified firmware vulnerabilities [90].

4.3. Phishing Attacks

To address the security challenge posed by phishing attacks, ref. [91] proposed a novel phishing detection system by incorporating equilibrium optimization, transfer function, and AI models. The optimizer has exploration and exploitation capabilities that help with feature selection, where a transfer function is used to optimize the algorithm's exploration ability. As a result, their system outperforms others in terms of accuracy and feature selection compared to the existing state-of-the-art techniques. Further, Alshehri et al. in [92] presented a DL-based phishing detection scheme to prevent the attacker from proliferating their attack surface. For this, they used character-level decoding to analyse the phishing uniform resource locator (URL). First, they created a standard dataset of labelled and unlabelled URLs that is processed using data sanitization techniques; then, it is forwarded to tokenization, where the URLs are separated into smaller units to achieve better inferences. Then, both inferences and token data are fed as input to the DL model to detect the phishing URLs. As a result, they achieved a detection rate of 98.13% in an energy-constrained environment. Additionally, the researchers also used fuzzy logic and data mining techniques to alleviate the risk of phishing attacks; for instance, Zahra et al. in [93] employs fuzzy logic, which takes specially crafted (COVID-19 themed) URL of the web page as an input. The fuzzy system has a rule-based approach where it first checks the authenticity, content, address bar, and social criteria of the URL; then it forwards it to the inference engine, which output the severity of the URL, i.e., very low, low, medium, and very high.

4.4. System Level Attacks

System-level attacks are those attacks where an attacker explicitly targets the system-level resources by discovering loopholes in the authentication schemes, authorization, and cryptographic key management infrastructure. In the smart healthcare sector, the patient's medical data have to be transmitted from various devices and services to reach their intended recipients. An attacker finds the system-level vulnerability to gain access to the patient's data and disrupts the performance of smart healthcare systems. Several researchers have proposed robust authentication schemes to overcome the aforementioned issues and reduce the impact of system-level attacks. For example, Le et al. in [94] proposed a three-stage authentication mechanism consisting of a smart card, password, and biometrics to ensure secure authentication between patients and healthcare providers. Then, they evaluated their proposed protocol using standard verification tools, i.e., real-or-random model, automated validation of internet security protocol, and Burrows–Abadi–Needham logic, wherein they outperform in terms of cost and secure functionalities compared to other baseline works. A two-stage authentication mechanism was proposed in [95] which involved hardware security, i.e., physical unclonable functions for IoT-based healthcare systems. Since the physical unclonable functions do not use cryptographic solutions, they can easily be integrated into the resource-constrained devices to offer lightweight authentication schemes. The proposed mechanism provides better computation time and offers robust security against system-level attacks in the smart healthcare ecosystem. Another system-level attack can be launched via privilege escalation techniques, where the attacker first carries out a reconnaissance of a victim's system to find hardware or software-related vulnerabilities that can be exploited at a later stage. Yin et al. in [96] presented a novel static analysis framework that detects privilege escalation attacks in a unified extensible firmware interface (UEFI). The authors used a callback programming procedure to find malicious callable functions in the UEFI firmware. They collected 1148 UEFI binaries from different vendors, and discovered 36 privilege escalation vulnerabilities. Those vulnerabilities can cause random code execution and allow an attacker to modify the writing operation of the physical device.

Table 4. Comprehensive analysis of existing state-of-the-art work for security solutions in smart healthcare systems.

	Author	Year	Objective	4	5	6	7	8	Security Approach	OSI Layer Secured
Hardware-based attack solutions	[79]	2019	To detect trojan attacks on medical hardware devices	Yes	No	No	Yes	No	Checkpoint assignment	Physical layer
	[80]	2018	To develop a secure data collection scheme for smart healthcare system	Yes	No	No	Yes	Yes	Field programmable gate array (FPGA)	Physical layer, network layer
	[81]	2021	To improve the security performance of IoT devices	Yes	No	No	Yes	No	IoT Hardware Platform Security Advisor (IoT-HarPSecA) framework	Physical and network layer

Table 4. *Cont.*

	Author	Year	Objective	4	5	6	7	8	Security Approach	OSI Layer Secured
Software-based attack solution	[82]	2022	Detect malware in medical devices	No	Yes	No	No	No	Attention-based AI technique	Physical layer, network layer
	[83]	2022	Improve the security of android wearable applications	No	Yes	Yes	No	No	Oversampling with AI models	Application layer
	[84]	2019	Case study on Ransomware detection	No	Yes	Yes	No	Yes	Dynamic malware analysis	Network layer
	[85]	2019	Critical analysis of ransomware on SCADA systems	No	Yes	Yes	No	No	Provide a comprehensive analysis on ransomware	Network layer
	[86]	2022	To develop a secure framework to detect ransomware in smart healthcare systems	No	Yes	Yes	No	Yes	Blockchain and machine learning-based secure framework	Network and Application layer
Phishing security solutions	[91]	2022	Detect and defend the phishing attacks	No	No	No	No	Yes	Equilibrium optimization with transfer function	Network layer
	[92]	2022	Energy-Efficient phishing URL detection	No	No	No	No	Yes	AI and Character-level word encoding	Network layer
	[93]	2022	Study the impact of COVID1-19 against the malicious URL attacks	No	No	No	No	Yes	Fuzzy logic and data mining approaches	Application and network layer
System-based attack solution	[94]	2022	Develop a three factor authentication mechanism for smart healthcare system	No	No	No	Yes	Yes	Centreless user controlled single sign on authentication mechanism	Application and network layer
	[95]	2020	Two stage authentication scheme for IoT healthcare systems	No	No	No	Yes	Yes	Physical unclonable functions	Physical, application and network layer
	[96]	2022	To develop a static detection framework to detect privilege escalation attack	No	No	No	Yes	Yes	Static analysis using callback-based programming	Physical, application and network layer
Communication-based attack solutions	[97]	2020	Proposed a self anomaly detection system for IoT-based devices	No	No	No	Yes	Yes	Proof-of-concept for anomaly detection	Network layer
	[98]	2021	Proposed an energy-efficient and privacy preserving framework to detect MiTM attack for smart healthcare system	No	No	No	Yes	Yes	Cryptographic mechanisms	Application and network layer
	[99]	2022	Proposed an authentication mechanism for wearable devices	No	No	No	Yes	Yes	Lightweight authentication scheme using different security phases	Application and network layer

Parameters- 4: DoS, 5: Malware, 6: Ransomware, 7: Data integrity, 8: Communication attack.

4.5. Communication Attacks

A smart healthcare system is comprised of different IoT-enabled devices that interconnect with each to other to accomplish the shared objective. For interconnection the IoT devices have to utilize different communication protocols, such as MQTT, constrained application protocol (CoAP), hypertext transfer protocol (HTTP), extensible messaging and presence protocol (XMPP), and an advanced message queuing protocol (AMQP) that have rules and regulations that allow different IoT-based medical devices to exchange their data. However, the communication protocols are exposed to numerous security vulnerabilities, such as including SYN, flooding, and fragmentation attacks [21,94]. In this subsection, we discuss the countermeasures for different communication attacks, such as MiTM, eavesdropping, impersonation, and replay attacks. A detailed explanation of each countermeasure is given below.

- **MiTM—**These attacks exploit the communication channel between two legitimate users (healthcare components) in order intercept or inject malicious data into the communication channel [95]. To counter this attack, Gong et al. in [97] studied channel-based MiTM attacks on healthcare devices. The authors of [97] adopted self-anomaly detection using access point scans to detect the MiTM attacks. The self-anomaly detection allows Wireless-Fidelity (Wi-Fi) devices to authenticate themselves without needing access points. With this advantage of self-anomaly detection, they achieved a 99% of detection accuracy. Further, Salem et al. in [98] proposed a secure framework to detect the MiTM attack on IoT-based medical devices. Here, they transmit a small-size signature and message authentication code along with the patient data to detect any MiTM attack. They achieved an excellent detection rate with a low false positive rate (3%).
- **Eavesdropping—**To tackle eavesdropping, the authors of [100] examined the effect of eavesdropping in multiple input and single output (MISO)-based wireless channels for image transmission. They segmented the image into two parts: an image consisting of important diagnostic information (requiring high level of reliability and confidentiality) and the image's background (requires less security). Then, the authors observed the link quality of both image segments to control and monitor the eavesdropper interception. Further, in [101], the authors discussed the essential benefits of implantable devices that sends patient's critical healthcare data to the hospital staff. However, they emphasize the risk of security attacks, especially eavesdropping attack on implantables that place the patient's life risk [102]. In their study, they revealed a proper trade-off between information rate and eavesdropping while transmitting sensitive healthcare data. Their study helps the implantable manufacturers to design their devices in a more secure way, i.e., with less security-associated vulnerability.
- **Replay attack—**Data integrity is one of the significant challenges in the healthcare industry, since the data can be intercepted and forged by attackers. To prevent this type of attack, Rughoobur et al. in [103] proposed a lightweight framework by utilizing different attributes, such as timestamps, unique identifiers, and self-learning, to detect any replay attacks on IoT devices. The authors of [104] presented a reliable and lightweight framework to tackle replay attacks in the smart healthcare system. Their framework uses unique registration identifiers, timestamps, and authentication phases that improve the data rate and security of the medical data. Their results shows that the proposed framework outperforms current baseline works in terms of computational and communication overhead.
- **Protocol-based attack—**IoT-based medical devices communicate with each other using IoT and communication-based protocols, such as HTTP, MQTT, and CoAP. However, these protocols are prone to various security threats. To overcome that, several authors have proposed solutions; for example, The authors in [105] presented a proximity-based secure protocol for smart healthcare systems. This offers a seamless balance between security, privacy, and scalability. Their protocol first verifies the users interacting with the healthcare interface using registration identifier, then it is authenticated using digital signatures. The result shows that the proposed protocol offers acceptable computational complexity and communication overhead. Further, Zia et al. in [99] explored the security challenges of wireless body area network in patient healthcare information system. To confront the potential security threats, they proposed a secure and lightweight authentication protocol that securely exchanges the data between sensors and controller. Their result shows that the proposed protocol has better computation and communication costs, i.e., 20.3% and 12.3%, respectively.

5. Case Study for Mitigating Security Attacks in Smart Healthcare System

This section presents a case study of how security attacks can be mitigated in the smart healthcare system. The proposed architecture consists of five-layers: data, malware analysis, intelligence, blockchain, and application layers as shown in Figure 4. A detailed description of each layer is given below.

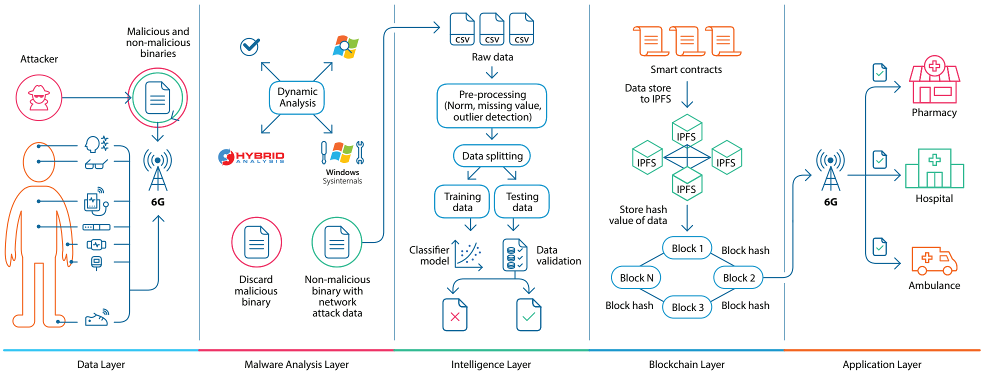


Figure 4. Smart healthcare architecture for mitigating security attacks.

5.1. Data Layer

This section discusses various wearables devices (sensors) associated with an individual or critical patient. The sensors collect the data, such as blood pressure, oxygen rate, heartbeat, temperature, from the patient's body and transmit the data to various the healthcare providers such as pharmacies, hospitals, ambulances, and government organizations via the traditional Internet. However, the precarious link between the sensor node and its recipient is impeded by different security attacks, such as malware, communication, and software-based attacks, which disrupt the performance of different healthcare services (e.g., medicine, nursing, telesurgery). Therefore, there is a need for a robust system that detects and alleviates the security threats from the smart healthcare system. Here, the data layer collects the malware samples (malicious and non-malicious binaries) and forwards them to the malware analysis layer.

5.2. Malware Analysis Layer

The malware samples collected at the data layer are forwarded in this layer, where we utilized dynamic malware analysis techniques to find intuitive features associated with the malware. For that, Pestudio, process explorer, Sysinternal tools, and Hexeditors are used to analyse the runtime behaviour of the malware. Dynamic analysis helps in bifurcating the malware and non-malware files by their specific signatures shown in the dynamic analysis tools. Few binaries are analysed using an automated malware analysis tool, like a Hybrid analysis web-based tool that gives information, such as hash signatures, threat score, risk assessment, and scope of the MiTM attack. This layer discards all the malware samples from the proposed architecture; only the non-malware sample is forwarded to the intelligence layer.

5.3. Intelligence Layer

The non-malware samples acquired from the previous layer (malware analysis layer) still have network-related vulnerabilities that, if they fall into the wrong hand (attacker), will have severe consequences on the healthcare sector. Therefore, in this layer, we utilize AI algorithms' significant benefits to efficiently classify non-malware samples, according to whether that contain malicious or non-malicious data. AI algorithms, such as logistic regression (LR), support vector machine (SVM), random forest (RF), perceptron, and Naive Bayes (NB), are used for classification purposes [106]. Initially, the AI algorithms are trained using a standard wearable security dataset, i.e., ICU dataset, that has network-related features and a binary class label (0-non-attack and 1-attack) [107]. Here, the standard dataset is first analyzed using a statistical test to observe the distribution of the feature space. For that, a parametric test is applied to the feature space (e.g., tcp.srcport, tcp.dstport, tcp.windows, tcp.checksum, etc.) of the dataset to analyze the normal distribution. Figure 5 show that the dataset feature space does not follow a normal distribution. Therefore, we used a non-parametric test, i.e., the Mann–Whitney U test, to analyse the dependency between dependent and independent features.

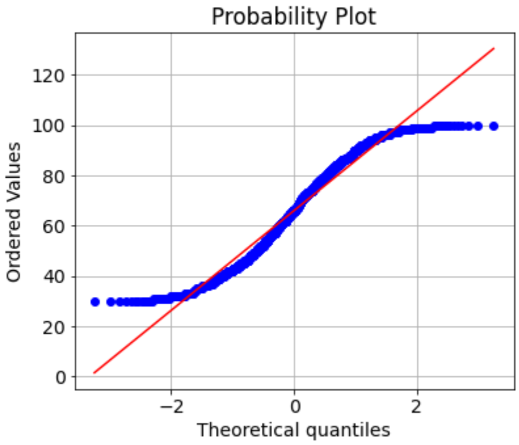


Figure 5. Parametric test to observe the normal distribution of the dataset.

A null hypothesis is created, i.e., a significant correlation between two features. The null hypothesis is rejected if the p-value is smaller than the significance value, i.e., 0.05. We used different features, i.e., mqtt.client and mqtt.conack.flags, to the Mann-Whitney U Test that gives the *p*-value of 0.04, which is smaller than the significance. Hence, it rejects the null hypothesis is rejected as there is no strong correlation between mqtt.client and mqtt.conack.flags.

```
stat, p_value = mannwhitneyu(data.mqtt.client,
data.mqtt.conack.flags)
sign = 0.05
if p_value < sign:
    print('No significant correlation between two features)')
else:
    print('Significant correlation between two features)')
```

Further, the dataset is preprocessed using various data preprocessing techniques, such as missing values, normalization, and datatype casting. Then, the processed data are forwarded to the AI models, where it is trained and validated using the real-time network data extracted from the non-malware samples. Finally, the non-malware samples containing malicious data are discarded from the proposed architecture, and only the non-malware sample containing non-malicious data is forwarded to the next layer.

5.4. Blockchain Layer

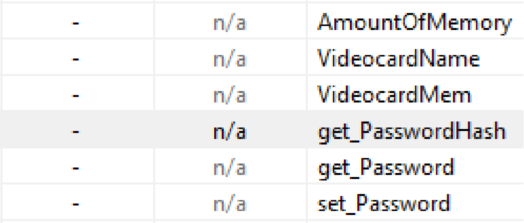
The data or file which is forwarded from the intelligence layer is still at a high risk of being exploited by the attackers; usually, they can perform data modification attacks in order to jeopardize healthcare operations. For example, an attacker can launch an MiTM attack to change the emergency alert of the patient data into non-emergency, thereby placing the patient's life at risk. Thus, there is an urgent need for technology, such as a blockchain that can securely store non-malicious data or files in a decentralized and immutable ledger [108]. Here, the ledger is distributed among all the blockchain members (all the entities of hospitals), so if any change is made to the stored data by attackers, this will be known to all the blockchain members. This builds robust transparency in smart healthcare systems. Initially, the healthcare data (non-malicious data) is validated using a smart contract, which has predetermined conditions; upon meeting those conditions, the data are validated [109]. Then, the data are received by the interplanetary file system (IPFS), which hash the raw data to improve the response time of the blockchain network. Finally, the hashed data are stored inside the public blockchain, where it is safeguarded from data integrity attacks.

5.5. Application Layer

This layer comprises all the recipients for whom the healthcare data are intended. It consists of a destination sensor, medical device, hospitals, pharmacy, laboratories, ambulances, and the government healthcare organization that collects the data from the secure pipeline (data layer to blockchain layer). Here, all the components are connected to a next-generation wireless network, i.e., a 6G network interface, which offers several advantageous features such as high data rates, low latency, high reliability, and availability. Furthermore, incorporating a 6G network interface improves the latency (response time); therefore, one can quickly send the data to the intended recipient who can use it for patient care.

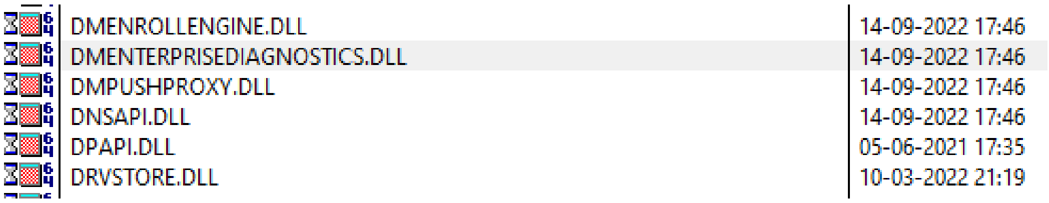
5.6. Performance Evaluation of the Proposed Architecture

This section discusses the evaluation of the proposed architecture's performance evaluation by applying different metrics, such as accuracy, scalability, and internal details of the malware from the dynamic analysis. For dynamic malware analysis, we utilized PEstudio, which provides an initial malware assessment that consists of malware indicators, important strings, directories, sections, resources, file headers, manifest files, and certificates. Here, we analysed various malware samples of smart healthcare systems that target web-based resources and patient data. For example, one malware sample (md5-584B853E5F597883FB56CC5E879D8A3D), written in C++, specifically targets the web-based login credentials using functions, such as $get\_Browser()$, $GetSavedPassword()$, $GetSavedCookies$, $GetValueNames()$, $urlHistroy()$, $get_passwordHash()$, and many more (as shown in Figure 6). Further, they imported different malicious and illegitimate dynamic link libraries (DLL) and application programming interfaces (API), such as $dmpushproxy.dll$, $dmenterprisediagnostics.dll$ to spoof the user into installing malicious executable files as shown in Figure 7. In addition, it contains another graphical user interface (GUI) executable file that propagates its attack surface once installed on the victim's physical device.



-	n/a	AmountOfMemory
-	n/a	VideocardName
-	n/a	VideocardMem
-	n/a	get_PasswordHash
-	n/a	get_Password
-	n/a	set_Password

Figure 6. Malicious functions used in malware sample.



DMENROLLENGINE.DLL	14-09-2022 17:46
DMENTERPRISEDIAGNOSTICS.DLL	14-09-2022 17:46
DMPUSHPROXY.DLL	14-09-2022 17:46
DNSAPI.DLL	14-09-2022 17:46
DPAPI.DLL	05-06-2021 17:35
DRVSTORE.DLL	10-03-2022 21:19

Figure 7. Malicious DLL used in malware sample.

Further, Figure 8 shows the evaluation of the intelligence layer, where different AI-based algorithms are trained using a standard dataset and validated using a generated dataset from the malware samples. Here, the RF outperforms other algorithms in terms of accuracy, i.e., 93.14%, because RF splits the entire dataset into small samples (as a decision tree) by using split node criteria. Then, each sample is individually trained, and the best decision tree is chosen using majority voting (highest accuracy). Nevertheless, the other AI algorithms are not optimized compared to RF because they need a few hyperparameters so as to achieve good accuracy. Table 5 shows the performance analysis of the proposed architecture in terms of precision, recall, log-loss score, and F1 score. Here, RF outperforms in terms of precision, recall, log-loss score, and F1 score, i.e., 93.24%, 92.99%, 6.34%, and 93.67%, respectively compared to other AI models. Specifically, the accuracy parameter shows how efficiently an AI model predicts the output. The higher the accuracy score, the higher the AI model's prediction performance. Conversely, the log-loss score shows an error in the prediction output, i.e., the higher the log-loss score, the lower the AI model's prediction performance and vice-versa. Figure 9 illustrates the scalability comparison of the blockchain network. The proposed architecture applies an IPFS-based blockchain that uses hash data to store in the immutable ledger, unlike the conventional blockchain, which uses raw data. The incorporation of IPFS improves the response time of the blockchain network because one can more easily fetch the hash data from the blockchain network compared to the raw data, resulting in a quick response time. This implies the higher the response time, the higher the scalability of the proposed architecture. It is clear from the Figure 9 that the IPFS-based blockchain has greater scalability than the conventional blockchain.

Table 5. Performance parameters of the proposed architecture.

Algorithm	Precision	Recall	Log-Loss Score	F1 Score
Random Forest	93.24%	92.99%	6.34%	93.67%
Support Vector Machine	82.13%	82.78%	14.19%	82.90%
Naïve Bayes	66.89%	65.13%	32.84%	67.12%
Logistic Regression	42.56%	43.60%	48.67%	44.02%
Perceptron	32.90%	33.53%	69.89%	33.19%

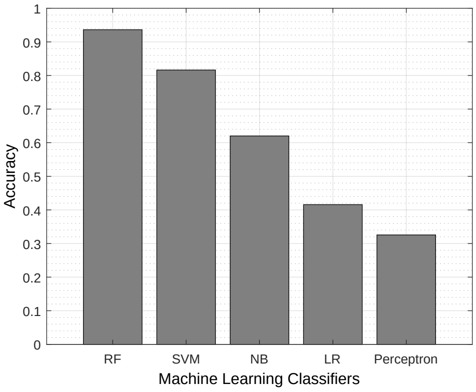


Figure 8. Evaluation of the intelligence layer where different AI-based algorithms are trained using a standard dataset and validated using a generated dataset from the malware samples.

The proposed architecture achieves a better performance compared to the existing state-of-the-art models. For instance, [7] proposed a lightweight and intelligent framework to protect medical devices from security threats, and they achieved an accuracy of 87.57% to predict the network-based attack. Conversely, the proposed architecture uses different AI models, wherein the RF achieves an accuracy of 93.14% compared to [7] in detecting attacks on smart healthcare systems. Moreover, the proposed architecture uses malware analysis, i.e., dynamic analysis, to discard malicious malware from the regular operations of the smart healthcare system. However, most of the previous studies do not conduct malware analysis in their proposed solutions. Furthermore, the authors of [11] used a private blockchain to store their data, although most of the private blockchain has a central repository to maintain and control the private data of the healthcare ecosystem. The private blockchains are severely affected by network-related attacks; therefore, the blockchain is useful only for critical applications, such as covert military applications, where they can integrate more sophisticated solutions at the cost of latency to strengthen the security of the central repository of private blockchain. However, in smart healthcare systems, maintaining the latency is challenging; hence, it is advisable not to use it. In our proposed work, we have two security filters, i.e., malware and network-related attacks; both malware and intelligence layers discard the malicious data from the proposed architecture. Only non-malicious data are forwarded to the public blockchain; further, to improve the latency of the smart healthcare system, we utilize the significant benefits of IPFS that improve the response time of the blockchain network, resulting in greater scalability. As a result, the proposed work is better and more robust than the existing work [11] in terms of accuracy, scalability, and security.

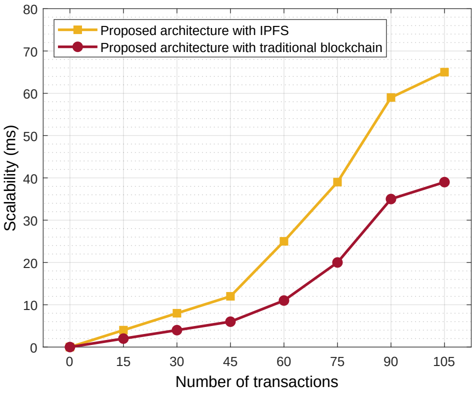


Figure 9. Evaluation of the scalability comparison of the blockchain network.

6. Open Issues and Research Challenges

This section discusses the open issues and research challenges associated with the smart healthcare systems which eventually have a detrimental effect on the patients' health during the remote monitoring of their health status.

- There is a lack of security standardization in smart healthcare—current health safety standards are too conventional and have become obsolete. Neither are they robust enough to sustain modern security attacks. The need for standardization, particularly in health care, can minimize the risk of mistakes, increase patient safety, and make a real difference to the patients experience. Moreover, arising security issues arising from the remote monitoring of patients can have a deleterious impact on their health, and can discourage them from taking medication from that particular healthcare provider. Thus, it can affect the reputation of the hospital's management which can reduce their overall revenue [110];
- Inefficient first line of defence—The spectrum of security risks and newly discovered security vulnerabilities for intelligent health systems keeps expanding. Security threats have less of an impact on smart healthcare environments when a variety of defences, including firewalls and intrusion detection systems, are used effectively and efficiently. However, despite the fact that they offer a number of advantages that can safeguard health systems, they are ineffective at spotting contemporary security threats; hence they continue to be open to assault [111];
- Non-availability of physical layer access control—The basis of all security measures is the physical security layer. The access control restrictions imposed by the existing security measures apply only to the application layer. Because the wireless communication in the physical layer is unprotected, the new security threats target it. The loss of physical security typically leaves the smart healthcare system completely exposed. Further, an adversary can easily modify the data extracted from implantable medical

devices such as pacemaker, artificial joints, cardiac implants., attached to the patient's body, which gives rise to security issues in wireless communication between patient and healthcare professionals during the remote treatment [112];

- Modern security attacks on smart healthcare systems—In addition to the typical attacks such as DDoS, MITM, ransomware., the attackers have discovered new methods of system attacking a system. The latest attacks include: software supply chain attacks; attackers take advantage of the supplier network of a healthcare institution and capitalize on the system's vulnerability. Internet of Things (IoT) attacks, A wide variety of endpoint devices is now remotely connected to the Internet. The malware interprets the changes caused by the system and manipulates the signals it receives to carry out destructive activities [113];
- Accessibility of advanced technology in smart healthcare—With the modernization of smart healthcare systems, healthcare professionals and staff have to manage advanced technologies to handle the medical equipment for the remote monitoring of patients. However, not all the healthcare professionals have had sufficient experience and training enabling them to tackle the patient's health symptoms through the usage of innovative technologies. Thus, hospital management should train their professionals or staff so that they become familiar with these technologies, although this can be costly for hospitals [111,114];
- Scalability: Scalability is one of the major concerns that needs to be managed during the wireless communication between patient and doctor in the remote treatment set up. Depending on the patient's health symptoms, healthcare professionals may require several items of medical equipment and various implantable sensors to gather the health data of patients and determine further treatment. Therefore, network bandwidth needs to be optimized in smart healthcare systems for the reliable and timely treatment of patients, since, low scalability communication between patient and healthcare professionals can delay their treatment which can exacerbate a health condition or even lead to the death or severe condition of patients [115].

7. Conclusions

The adoption of noteworthy catalyzers of innovations, such as AI, blockchain, IoT, and cloud computing, will reshape the future of healthcare systems. However, the integration of these innovations of healthcare ecosystems comes with associated security threats, including the manipulation of the patient monitor, exploitation of the healthcare data repository, and interception of the communication between the healthcare provider and the patient, all of which can jeopardize healthcare operations. Therefore, there is a need to study different security challenges associated with smart healthcare systems along with their security countermeasures. Hence, in this study, we first reviewed emerging technologies and frameworks that offer automation, quality-of-service, fault tolerance, and intelligent healthcare functionalities to patients. Then, we explored the various security and privacy challenges facing the smart healthcare system, such as DoS, MiTM, data integrity attacks, phishing, and hardware-based attacks. Further, based on the security challenges of the healthcare industry, we reviewed prominent security solutions intended to strengthen the security and privacy of smart healthcare systems. Another contribution to this study is our proposal of an AI and blockchain-based secure architecture (as a case study) that analyses the malware and network attacks on the smart healthcare system. First, medical data are acquired from the data layer, which consists of different healthcare providers and patients. Then, dynamic malware analysis is used to remove the data associated with the malware by analysing its different characteristics, such as DLL, file size, hidden strings, and signatures. Further, a standard dataset is used to train AI models for network-related attacks in smart healthcare systems. The data are first preprocessed using data preprocessing steps, such as the insertion of missing values, data normalization, and datatype casting. Then, the preprocessed data are forwarded to the different AI models, such as RF, NB, LR, and perceptron. The RF outperforms other existing AI algorithms in terms of accuracy, i.e., 93.14%. Further, the non-malicious data (classified from AI models) are passed to the blockchain layer for secure data storage from data integrity attacks. Then, the proposed architecture is evaluated using performance parameters, such as blockchain scalability, accuracy, and dynamic malware analysis. Lastly, we discussed open issues and research challenges associated with smart healthcare systems in order to encourage other researchers and youngsters to offer better security solutions.

In future work, we intend to strengthen the security and privacy of AI and blockchain-based smart healthcare systems by considering the various security attacks such as rowhammer, buffer overflow, masquerade, clone phishing, and phone phishing attacks, and the mechanism to tackle the aforementioned security attacks to further maintain the security of smart healthcare systems.

Author Contributions: Conceptualization, A.A.; Data curation, A.A. and I.K.; Funding acquisition, A.A.; Investigation, A.A.; Software, A.A. and I.K.; visualization, M.S.R.; Writing—original draft, A.A.; Writing—review & editing, M.S.R. All authors have read and agreed to the published version of the manuscript.

Funding: The authors gratefully acknowledge Qassim University, represented by the Deanship of Scientific Research, on the financial support for this research under the number (10118-coc-2020-1-3-I) during the academic year 1441 AH/2020 AD.

Data Availability Statement: Not applicable.

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

References

1. Top Mid-Year Healthcare Cybersecurity Trends. Available online: https://healthitsecurity.com/features/top-mid-year-healthcare-cybersecurity-trends (accessed on 11 September 2022).
2. Average Cost of a Data Breach in the United States from 2006 to 2022. Available online: https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/ (accessed on 21 September 2022).
3. Cost of a Data Breach 2022. Available online: https://www.ibm.com/reports/data-breach (accessed on 12 September 2022).
4. Patel, K.; Mehta, D.; Mistry, C.; Gupta, R.; Tanwar, S.; Kumar, N.; Alazab, M. Facial Sentiment Analysis Using AI Techniques: State-of-the-Art, Taxonomies, and Challenges. *IEEE Access* **2020**, *8*, 90495–90519. https://doi.org/10.1109/ACCESS.2020.2993803. [CrossRef]
5. Deebak, B.D.; Al-Turjman, F. Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 346–360. https://doi.org/10.1109/JSAC.2020.3020599. [CrossRef]
6. Chiou, S.Y.; Ying, Z.; Liu, J. Improvement of a privacy authentication scheme based on cloud for medical environment. *J. Med. Syst.* **2016**, *40*, 101. [CrossRef]
7. Wazid, M.; Singh, J.; Das, A.K.; Shetty, S.; Khan, M.K.; Rodrigues, J.J.P.C. ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. *IEEE Access* **2022**, *10*, 57990–58004. https://doi.org/10.1109/ACCESS.2022.3179418. [CrossRef]
8. Li, C.; Raghunathan, A.; Jha, N.K. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In Proceedings of the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, MO, USA, 13–15 June 2011; pp. 150–156. https://doi.org/10.1109/HEALTH.2011.6026732. [CrossRef]
9. Aggarwal, S.; Kumar, N.; Tanwar, S. Blockchain-Envisioned UAV Communication Using 6G Networks: Open Issues, Use Cases, and Future Directions. *IEEE Internet Things J.* **2021**, *8*, 5416–5441. https://doi.org/10.1109/JIOT.2020.3020819. [CrossRef]
10. Gupta, R.; Shukla, A.; Tanwar, S. AaYusH: A Smart Contract-Based Telesurgery System for Healthcare 4.0. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6. https://doi.org/10.1109/ICCWorkshops49005.2020.9145044. [CrossRef]
11. Pinto, R.P.; Silva, B.M.C.; Inácio, P.R.M. A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain. *IEEE Access* **2022**, *10*, 92760–92773. https://doi.org/10.1109/ACCESS.2022.3203193. [CrossRef]
12. Gohar, A.N.; Abdelmawgoud, S.A.; Farhan, M.S. A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT. *IEEE Access* **2022**, *10*, 92137–92157. https://doi.org/10.1109/ACCESS.2022.3202902. [CrossRef]
13. Jadav, D.; Patel, D.; Gupta, R.; Jadav, N.K.; Tanwar, S. BaRCODe: A Blockchain-based Framework for Remote COVID Detection for Healthcare 5.0. In Proceedings of the 2022 IEEE International Conference on Communications Workshops (ICC Workshops), Seoul, Korea, 16–20 May 2022; pp. 782–787. https://doi.org/10.1109/ICCWorkshops53468.2022.9814593. [CrossRef]
14. Mistry, C.; Thakker, U.; Gupta, R.; Obaidat, M.S.; Tanwar, S.; Kumar, N.; Rodrigues, J.J.P.C. MedBlock: An AI-enabled and Blockchain-driven Medical Healthcare System for COVID-19. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6. https://doi.org/10.1109/ICC42927.2021.9500397. [CrossRef]

15. Usman, M.; Asghar, M.R.; Ansari, I.S.; Qaraqe, M. Security in Wireless Body Area Networks: From In-Body to Off-Body Communications. *IEEE Access* **2018**, *6*, 58064–58074. https://doi.org/10.1109/ACCESS.2018.2873825. [CrossRef]
16. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. https://doi.org/10.1109/COMST.2019.2914094. [CrossRef]
17. Sun, Y.; Lo, F.P.W.; Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access* **2019**, *7*, 183339–183355. https://doi.org/10.1109/ACCESS.2019.2960617. [CrossRef]
18. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018. [CrossRef]
19. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Park, Y.; Tanwar, S. Design of an Anonymity-Preserving Group Formation Based Authentication Protocol in Global Mobility Networks. *IEEE Access* **2018**, *6*, 20673–20693. https://doi.org/10.1109/ACCESS.2018.2827027. [CrossRef]
20. Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput. Secur.* **2020**, *97*, 101966. https://doi.org/10.1016/j.cose.2020.101966. [CrossRef]
21. Bhuiyan, M.N.; Rahman, M.M.; Billah, M.M.; Saha, D. Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities. *IEEE Internet Things J.* **2021**, *8*, 10474–10498. https://doi.org/10.1109/JIOT.2021.3062630. [CrossRef]
22. Jagatheesaperumal, S.K.; Mishra, P.; Moustafa, N.; Chauhan, R. A holistic survey on the use of emerging technologies to provision secure healthcare solutions. *Comput. Electr. Eng.* **2022**, *99*, 107691. https://doi.org/10.1016/j.compeleceng.2022.107691. [CrossRef]
23. Mezghani, E.; Exposito, E.; Drira, K. A Model-Driven Methodology for the Design of Autonomic and Cognitive IoT-Based Systems: Application to Healthcare. *IEEE Trans. Emerg. Top. Comput. Intell.* **2017**, *1*, 224–234. https://doi.org/10.1109/TETCI.2017.2699218. [CrossRef]
24. Haghi, M.; Neubert, S.; Geissler, A.; Fleischer, H.; Stoll, N.; Stoll, R.; Thurow, K. A Flexible and Pervasive IoT-Based Healthcare Platform for Physiological and Environmental Parameters Monitoring. *IEEE Internet Things J.* **2020**, *7*, 5628–5647. https://doi.org/10.1109/JIOT.2020.2980432. [CrossRef]
25. Tomasicchio, G.; Ceccarelli, A.; Matteis, A.D.; Spazzacampagna, L. A space-based healthcare emergency management system for epidemics monitoring and response. In Proceedings of the 38th International Communications Satellite Systems Conference (ICSSC 2021), Arlington, VA, USA, 27–30 September 2021; Volume 2021, pp. 195–199. https://doi.org/10.1049/icp.2022.0571. [CrossRef]
26. Subahi, A.F. Edge-Based IoT Medical Record System: Requirements, Recommendations and Conceptual Design. *IEEE Access* **2019**, *7*, 94150–94159. https://doi.org/10.1109/ACCESS.2019.2927958. [CrossRef]
27. Gupta, R.; Shukla, A.; Mehta, P.; Bhattacharya, P.; Tanwar, S.; Tyagi, S.; Kumar, N. VAHAK: A Blockchain-based Outdoor Delivery Scheme using UAV for Healthcare 4.0 Services. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 255–260. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162738. [CrossRef]
28. Ray, P.P.; Chowhan, B.; Kumar, N.; Almogren, A. BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. *IEEE Internet Things J.* **2021**, *8*, 10857–10872. https://doi.org/10.1109/JIOT.2021.3050703. [CrossRef]
29. Hossain Gourob, J.; Raxit, S.; Hasan, A. A Robotic Hand: Controlled With Vision Based Hand Gesture Recognition System. In Proceedings of the 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Rajshahi, Bangladesh, 8–9 July 2021; pp. 1–4. https://doi.org/10.1109/ACMI53878.2021.9528192. [CrossRef]
30. Subramanian, G.; Sreekantan Thampy, A. Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations. *IEEE Access* **2021**, *9*, 162459–162475. https://doi.org/10.1109/ACCESS.2021.3132302. [CrossRef]
31. Parra, C.M.; Gupta, M.; Dennehy, D. Likelihood of Questioning AI-Based Recommendations Due to Perceived Racial/Gender Bias. *IEEE Trans. Technol. Soc.* **2022**, *3*, 41–45. https://doi.org/10.1109/TTS.2021.3120303. [CrossRef]
32. Elayan, H.; Aloqaily, M.; Guizani, M. Sustainability of Healthcare Data Analysis IoT-Based Systems Using Deep Federated Learning. *IEEE Internet Things J.* **2022**, *9*, 7338–7346. https://doi.org/10.1109/JIOT.2021.3103635. [CrossRef]
33. De Moura Costa, H.J.; Da Costa, C.A.; Da Rosa Righi, R.; Antunes, R.S.; De Paz Santana, J.F.; Leithardt, V.R.Q. A Fog and Blockchain Software Architecture for a Global Scale Vaccination Strategy. *IEEE Access* **2022**, *10*, 44290–44304. https://doi.org/10.1109/ACCESS.2022.3169418. [CrossRef]
34. Rehman, M.U.; Shafique, A.; Ghadi, Y.Y.; Boulila, W.; Jan, S.U.; Gadekallu, T.R.; Driss, M.; Ahmad, J. A Novel Chaos-Based Privacy-Preserving Deep Learning Model for Cancer Diagnosis. *IEEE Trans. Netw. Sci. Eng.* **2022**, 1–17. https://doi.org/10.1109/TNSE.2022.3199235. [CrossRef]
35. Miranda, D.; Olivares, R.; Munoz, R.; Minonzio, J.G. Improvement of Patient Classification Using Feature Selection Applied to Bidirectional Axial Transmission. *IEEE Trans. Ultrason. Ferroelectr. Freq. Control.* **2022**, *69*, 2663–2671. https://doi.org/10.1109/TUFFC.2022.3195477. [CrossRef] [PubMed]
36. Alghatani, K.; Ammar, N.; Rezgui, A.; Shaban-Nejad, A. Precision Clinical Medicine Through Machine Learning: Using High and Low Quantile Ranges of Vital Signs for Risk Stratification of ICU Patients. *IEEE Access* **2022**, *10*, 52418–52430. https://doi.org/10.1109/ACCESS.2022.3175304. [CrossRef]

37. Tanwar, S.; Vora, J.; Kaneriya, S.; Tyagi, S.; Kumar, N.; Sharma, V.; You, I. Human Arthritis Analysis in Fog Computing Environment Using Bayesian Network Classifier and Thread Protocol. *IEEE Consum. Electron. Mag.* **2020**, *9*, 88–94. https://doi.org/10.1109/MCE.2019.2941456. [CrossRef]
38. Patel, V.A.; Bhattacharya, P.; Tanwar, S.; Gupta, R.; Sharma, G.; Bokoro, P.N.; Sharma, R. Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions. *IEEE Access* **2022**, *10*, 90792–90826. https://doi.org/10.1109/ACCESS.2022.3201876. [CrossRef]
39. Camajori Tedeschini, B.; Savazzi, S.; Stoklasa, R.; Barbieri, L.; Stathopoulos, I.; Nicoli, M.; Serio, L. Decentralized Federated Learning for Healthcare Networks: A Case Study on Tumor Segmentation. *IEEE Access* **2022**, *10*, 8693–8708. https://doi.org/10.1109/ACCESS.2022.3141913. [CrossRef]
40. Gupta, R.; Reebadiya, D.; Tanwar, S.; Kumar, N.; Guizani, M. When Blockchain Meets Edge Intelligence: Trusted and Security Solutions for Consumers. *IEEE Netw.* **2021**, *35*, 272–278. https://doi.org/10.1109/MNET.001.2000735. [CrossRef]
41. Kumari, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. When Blockchain Meets Smart Grid: Secure Energy Trading in Demand Response Management. *IEEE Netw.* **2020**, *34*, 299–305. https://doi.org/10.1109/MNET.001.1900660. [CrossRef]
42. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1917–1927. https://doi.org/10.1109/JBHI.2021.3123643. [CrossRef] [PubMed]
43. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. A Taxonomy of Blockchain-enabled Softwarization for Secure UAV Network. *Comput. Commun.* **2020**, *161*, 304–323. https://doi.org/10.1016/j.comcom.2020.07.042. [CrossRef]
44. Prasad, V.K.; Bhavsar, M.D.; Tanwar, S. Influence of montoring: Fog and edge computing. *Scalable Comput. Pract. Exp.* **2019**, *20*, 365–376. [CrossRef]
45. Xu, B.; Zhou, F. The Roles of Cloud-Based Systems on the Cancer-Related Studies: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 64126–64145. https://doi.org/10.1109/ACCESS.2022.3181147. [CrossRef]
46. Wang, K.; Shao, Y.; Xie, L.; Wu, J.; Guo, S. Adaptive and Fault-Tolerant Data Processing in Healthcare IoT Based on Fog Computing. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 263–273. https://doi.org/10.1109/TNSE.2018.2859307. [CrossRef]
47. Isa, I.S.B.M.; El-Gorashi, T.E.H.; Musa, M.O.I.; Elmirghani, J.M.H. Energy Efficient Fog-Based Healthcare Monitoring Infrastructure. *IEEE Access* **2020**, *8*, 197828–197852. https://doi.org/10.1109/ACCESS.2020.3033555. [CrossRef]
48. Hassan, K.M.; Abdo, A.; Yakoub, A. Enhancement of Health Care Services Based on Cloud Computing in IOT Environment Using Hybrid Swarm Intelligence. *IEEE Access* **2022**, *10*, 105877–105886. https://doi.org/10.1109/ACCESS.2022.3211512. [CrossRef]
49. Itoo, S.; Khan, A.A.; Kumar, V.; Alkhayyat, A.; Ahmad, M.; Srinivas, J. CKMIB: Construction of Key Agreement Protocol for Cloud Medical Infrastructure Using Blockchain. *IEEE Access* **2022**, *10*, 67787–67801. https://doi.org/10.1109/ACCESS.2022.3185016. [CrossRef]
50. Ansari, A.A.; Mishra, B.; Gera, P.; Khan, M.K.; Chakraborty, C.; Mishra, D. Privacy-Enabling Framework for Cloud-Assisted Digital Healthcare Industry. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8316–8325. https://doi.org/10.1109/TII.2022.3170148. [CrossRef]
51. Tanwar, S.; Kumar, N.; Niu, J.W. EEMHR: Energy-efficient multilevel heterogeneous routing protocol for wireless sensor networks. *Int. J. Commun. Syst.* **2014**, *27*, 1289–1318. https://doi.org/10.1002/dac.2780. [CrossRef]
52. Rabbani, R.; Najafiaghdam, H.; Ghanbari, M.M.; Papageorgiou, E.P.; Zhao, B.; Roschelle, M.; Stojanovic, V.; Muller, R.; Anwar, M. Towards an Implantable Fluorescence Image Sensor for Real-Time Monitoring of Immune Response in Cancer Therapy. In Proceedings of the 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Guadalajara, Mexico, 31 October–4 November 2021; pp. 7399–7403.
53. Mansour, R.F.; Amraoui, A.E.; Nouaouri, I.; Díaz, V.G.; Gupta, D.; Kumar, S. Artificial Intelligence and Internet of Things Enabled Disease Diagnosis Model for Smart Healthcare Systems. *IEEE Access* **2021**, *9*, 45137–45146. https://doi.org/10.1109/ACCESS.2021.3066365. [CrossRef]
54. Mohsan, S.A.H.; Zahra, Q.U.A.; Khan, M.A.; Alsharif, M.H.; Elhaty, I.A.; Jahid, A. Role of Drone Technology Helping in Alleviating the COVID-19 Pandemic. *Micromachines* **2022**, *13*, 1593. [CrossRef] [PubMed]
55. Ananthi, J.V.; Jose, P.S.H. Implementation of IoT and UAV Based WBAN for healthcare applications. In Proceedings of the 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2–4 September 2021; pp. 37–42. https://doi.org/10.1109/ICIRCA51532.2021.9545052. [CrossRef]
56. Chaudhary, S.; Kakkar, R.; Jadav, N.K.; Nair, A.; Gupta, R.; Tanwar, S.; Agrawal, S.; Alshehri, M.D.; Sharma, R.; Sharma, G.; et al. A Taxonomy on Smart Healthcare Technologies: Security Framework, Case Study, and Future Directions. *J. Sens.* **2022**, *2022*, 1863838. [CrossRef]
57. Boston Children's Hospital Ddos Attacker Convicted. Bank Information Security. Available online: https://www.bankinfosecurity.com/boston-childrens-hospital-ddos-attacker-convicted-a-11279 (accessed on 14 September 2022).
58. CISA Warns of Possible DDoS Risk in Contec Patient Monitor Medical Devices. Available online: https://www.scmagazine.com/analysis/device-security/cisa-warns-of-possible-ddos-risk-in-contec-patient-monitor-medical-devices (accessed on 2 September 2022).
59. Joshitta, R.S.M.; Arockiam, L. Device authentication mechanism for IoT enabled healthcare system. In Proceedings of the 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, India, 16–18 February 2017; pp. 1–6. https://doi.org/10.1109/ICAMMAET.2017.8186646. [CrossRef]

60. Notice of Data Security Incident. Available online: https://shields.com/notice-of-data-security-incident/ (accessed on 12 July 2022).
61. YRMC Experiences Ransomware Incident. Available online: https://www.yumaregional.org/For-The-Community/News/2022/May/YRMC-Experiences-Ransomware-Incident (accessed on 3 August 2022).
62. Sharma, B.; Halder, R.; Singh, J. Blockchain-based Interoperable Healthcare using Zero-Knowledge Proofs and Proxy Re-Encryption. In Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 7–11 January 2020; pp. 1–6. https://doi.org/10.1109/COMSNETS48256.2020.9027413. [CrossRef]
63. Phishing Attacks, Email Security Incidents Hit 3 Healthcare Orgs. Available online: https://healthitsecurity.com/news/phishing-attacks-email-security-incidents-hit-3-healthcare-org (accessed on 14 July 2022).
64. Phishing Attack at Allegheny Health Network Impacts 8K. Available online: https://healthitsecurity.com/news/phishing-attack-at-allegheny-health-network-impacts-8k (accessed on 12 July 2022).
65. Threat Actors Use Evernote-Themed Phishing Scheme to Attack Healthcare Organizations. Available online: https://healthitsecurity.com/news/threat-actors-use-evernote-themed-phishing-scheme-to-attack-healthcare-organizations (accessed on 12 July 2022).
66. Mehbodniya, A.; Alam, I.; Pande, S.; Neware, R.; Rane, K.P.; Shabaz, M.; Madhavan, M.V. Financial fraud detection in healthcare using machine learning and deep learning techniques. *Secur. Commun. Netw.* **2021**, *2021*, 9293877:1–9293877:8. [CrossRef]
67. HC3 Warns Healthcare Sector of Karakurt Ransomware Group. Available online: https://healthitsecurity.com/news/hc3-warns-healthcare-sector-of-karakurt-ransomware-group (accessed on 12 July 2022).
68. North Korean Maui Ransomware Actively Targeting U.S. Healthcare Organizations. Available online: https://thehackernews.com/2022/07/north-korean-maui-ransomware-actively.html (accessed on 7 July 2022).
69. Thamer, N.; Alubady, R. A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. In Proceedings of the 2021 1st Babylon International Conference on Information Technology and Science (BICITS), Babil, Iraq, 28–29 April 2021; pp. 210–216. https://doi.org/10.1109/BICITS51482.2021.9509877. [CrossRef]
70. Gupta, R.; Patel, M.M.; Tanwar, S.; Kumar, N.; Zeadally, S. Blockchain-Based Data Dissemination Scheme for 5G-Enabled Softwarized UAV Networks. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1712–1721. https://doi.org/10.1109/TGCN.2021.3111529. [CrossRef]
71. Blind Attack On Wireless Insulin Pumps Could Deliver Lethal Dose. Available online: https://threatpost.com/blind-attack-wireless-insulin-pumps-could-deliver-lethal-dose-102711/75808/ (accessed on 7 July 2011).
72. These Hackers Made an App That Kills to Prove a Point. Available online: https://www.wired.com/story/medtronic-insulin-pump-hack-app/ (accessed on 16 July 2019).
73. Nyangaresi, V.O.; Abduljabbar, Z.A.; Ma, J.; Al Sibahee, M.A. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In Proceedings of the 2022 4th Global Power, Energy and Communication Conference (GPECOM), Nevsehir, Turkey, 14–17 June 2022; pp. 569–574. https://doi.org/10.1109/GPECOM55404.2022.9815685. [CrossRef]
74. How Security Vulnerabilities Pose Risks for Healthcare Organizations. Available online: https://www.techrepublic.com/article/security-vulnerabilities-healthcare/ (accessed on 21 August 2019).
75. CVE-2020-0601 Detail. Available online: https://nvd.nist.gov/vuln/detail/CVE-2020-0601. (accessed on 10 June 2019).
76. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 146. [CrossRef]
77. Rehman, A.; Razzak, I.; Xu, G. Federated Learning for Privacy Preservation of Healthcare Data from Smartphone-based Side-Channel Attacks. *IEEE J. Biomed. Health Inform.* **2022**. https://doi.org/10.1109/JBHI.2022.3171852. [CrossRef]
78. Differential Power Analysis Countermeasures. Available online: https://www.silabs.com/security/differential-power-analysis (accessed on 19 August 2019).
79. Gountia, D.; Roy, S. Checkpoints Assignment on Cyber-Physical Digital Microfluidic Biochips for Early Detection of Hardware Trojans. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 16–21. https://doi.org/10.1109/ICOEI.2019.8862598. [CrossRef]
80. Tao, H.; Bhuiyan, M.Z.A.; Abdalla, A.N.; Hassan, M.M.; Zain, J.M.; Hayajneh, T. Secured Data Collection With Hardware-Based Ciphers for IoT-Based Healthcare. *IEEE Internet Things J.* **2019**, *6*, 410–420. https://doi.org/10.1109/JIOT.2018.2854714. [CrossRef]
81. Samaila, M.G.; Lopes, C.; Édi, A.; Sequeiros, J.B.; Simões, T.; Freire, M.M.; Inácio, P.R. Performance evaluation of the SRE and SBPG components of the IoT hardware platform security advisor framework. *Comput. Netw.* **2021**, *199*, 108496. https://doi.org/10.1016/j.comnet.2021.108496. [CrossRef]
82. Ravi, V.; Pham, T.D.; Alazab, M. Attention-Based Multidimensional Deep Learning Approach for Cross-Architecture IoMT Malware Detection and Classification in Healthcare Cyber-Physical Systems. *IEEE Trans. Comput. Soc. Syst.* **2022**, *2022*, 3198123. https://doi.org/10.1109/TCSS.2022.3198123. [CrossRef]
83. Kong, K.; Zhang, Z.; Guo, C.; Han, J.; Long, G. PMMSA: Security analysis system for android wearable applications based on permission matching and malware similarity analysis. *Future Gener. Comput. Syst.* **2022**, *137*, 349–362. https://doi.org/10.1016/j.future.2022.08.002. [CrossRef]

84. Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware. *IEEE Access* **2019**, *7*, 47053–47067. https://doi.org/10.1109/ACCESS.2019.2907485. [CrossRef]
85. Javed Butt, U.; Abbod, M.; Lors, A.; Jahankhani, H.; Jamal, A.; Kumar, A. Ransomware Threat and its Impact on SCADA. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 205–212. https://doi.org/10.1109/ICGS3.2019.8688327. [CrossRef]
86. Wazid, M.; Das, A.K.; Shetty, S. BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare. *IEEE Trans. Consum. Electron.* **2022**, *7*, 1. https://doi.org/10.1109/TCE.2022.3208795. [CrossRef]
87. What Is Endpoint Detection and Response (EDR)? Available online: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html (accessed on 20 August 2019).
88. What Is Reputation Analysis? Available online: https://vaultinfosec.com/service/next-gen-solutions/reputation-analysis (accessed on 15 September 2022).
89. Top Vulnerability Management Tools for 2022. Available online: https://www.esecurityplanet.com/products/vulnerability-management-software/ (accessed on 17 March 2019).
90. OWASP Firmware Security Testing Methodology. Available online: https://scriptingxss.gitbook.io/firmware-security-testing-methodology/ (accessed on 23 September 2019).
91. Minocha, S.; Singh, B. A novel phishing detection system using binary modified equilibrium optimizer for feature selection. *Comput. Electr. Eng.* **2022**, *98*, 107689. https://doi.org/10.1016/j.compeleceng.2022.107689. [CrossRef]
92. Alshehri, M.; Abugabah, A.; Algarni, A.; Almotairi, S. Character-level word encoding deep learning model for combating cyber threats in phishing URL detection. *Comput. Electr. Eng.* **2022**, *100*, 107868. https://doi.org/10.1016/j.compeleceng.2022.107868. [CrossRef]
93. Rameem Zahra, S.; Ahsan Chishti, M.; Iqbal Baba, A.; Wu, F. Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egypt. Inform. J.* **2022**, *23*, 197–214. https://doi.org/10.1016/j.eij.2021.12.003. [CrossRef]
94. Le, T.V.; Lu, C.F.; Hsu, C.L.; Do, T.K.; Chou, Y.F.; Wei, W.C. A Novel Three-Factor Authentication Protocol for Multiple Service Providers in 6G-Aided Intelligent Healthcare Systems. *IEEE Access* **2022**, *10*, 28975–28990. https://doi.org/10.1109/ACCESS.2022.3158756. [CrossRef]
95. Alladi, T.; Chamola, V.; Naren. HARCI: A Two-Way Authentication Protocol for Three Entity Healthcare IoT Networks. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 361–369. https://doi.org/10.1109/JSAC.2020.3020605. [CrossRef]
96. Yin, J.; Li, M.; Wu, W.; Sun, D.; Zhou, J.; Huo, W.; Xue, J. Finding SMM Privilege-Escalation Vulnerabilities in UEFI Firmware with Protocol-Centric Static Analysis. In Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–26 May 2022; pp. 1623–1637. https://doi.org/10.1109/SP46214.2022.9833723. [CrossRef]
97. Gong, S.; Ochiai, H.; Esaki, H. Scan-Based Self Anomaly Detection: Client-Side Mitigation of Channel-Based Man-in-the-Middle Attacks Against Wi-Fi. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 1498–1503. https://doi.org/10.1109/COMPSAC48688.2020.00-43. [CrossRef]
98. Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2053–2062. https://doi.org/10.1109/TII.2021.3089462. [CrossRef]
99. Zia, M.; Obaidat, M.S.; Mahmood, K.; Shamshad, S.; Saleem, M.A.; Chaudhry, S.A. A Provably Secure Lightweight Key Agreement Protocol for Wireless Body Area Networks in Healthcare System. *IEEE Trans. Ind. Inform.* **2022**, 1–8. https://doi.org/10.1109/TII.2022.3202968. [CrossRef]
100. Letafati, M.; Behroozi, H.; Khalaj, B.H.; Jorswieck, E.A. Content-Based Medical Image Transmission Against Randomly-Distributed Passive Eavesdroppers. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–7. https://doi.org/10.1109/ICCWorkshops50388.2021.9473492. [CrossRef]
101. Awan, M.; Kansanen, K. Estimating Eavesdropping Risk for Next Generation Implants: Technology, Communications and Computing. In *Advances in Body Area Networks I*; Springer: Berlin/Heidelberger, Germany, 2019; pp. 387–398. https://doi.org/10.1007/978-3-030-02819-0_29. [CrossRef]
102. Alkeem, E.A.; Shehada, D.; Yeun, C.Y.; Zemerly, M.J.; Hu, J. New secure healthcare system using cloud of things. *Clust. Comput.* **2017**, *20*, 2211–2229. [CrossRef]
103. Rughoobur, P.; Nagowah, L. A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, United Arab Emirates, 18–20 December 2017; pp. 811–817. https://doi.org/10.1109/ICTUS.2017.8286118. [CrossRef]
104. Chaudhary, R.R.K.; Chatterjee, K. A lightweight security framework for electronic healthcare system. *Int. J. Inf. Technol.* **2022**, *14*, 3109–3121 [CrossRef]
105. Masmoudi, S.; Kaaniche, N.; Laurent, M. SPOT: Secure and Privacy-preserving prOximiTy protocol for e-healthcare systems. *IEEE Access* **2022**, *10*, 106400–106414 https://doi.org/10.1109/ACCESS.2022.3208697. [CrossRef]
106. Verma, C.; Stoffová, V.; Illés, Z.; Tanwar, S.; Kumar, N. Machine Learning-Based Student's Native Place Identification for Real-Time. *IEEE Dataport* **2020**, *8*, 130840–130854. https://doi.org/10.1109/ACCESS.2020.3008830. [CrossRef]

107. Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. IoT Healthcare Security Dataset. *IEEE Dataport* **2021**. https://doi.org/10.21227/9w13-2t13. [CrossRef]
108. Reebadiya, D.; Rathod, T.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain-based Secure and Intelligent Sensing for Autonomous Vehicles Activity Tracking Beyond 5G Networks. *Peer-Peer Netw. Appl.* **2021**, *14*, 2757–2774 https://doi.org/10.1007/s12083-021-01073-x. [CrossRef]
109. Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and 5G Integrated Softwarized UAV Network Management: Architecture, Solutions, and Challenges. *Phys. Commun.* **2021**, *47*, 101–355 https://doi.org/10.1016/j.phycom.2021.101355. [CrossRef]
110. Ahad, A.; Tahir, M.; Yau, K.L.A. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. *IEEE Access* **2019**, *7*, 100747–100762. https://doi.org/10.1109/ACCESS.2019.2930628. [CrossRef]
111. Navaz, A.N.; Serhani, M.A.; El Kassabi, H.T.; Al-Qirim, N.; Ismail, H. Trends, Technologies, and Key Challenges in Smart and Connected Healthcare. *IEEE Access* **2021**, *9*, 74044–74067. https://doi.org/10.1109/ACCESS.2021.3079217. [CrossRef]
112. Wu, L.; Du, X.; Guizani, M.; Mohamed, A. Access Control Schemes for Implantable Medical Devices: A Survey. *IEEE Internet Things J.* **2017**, *4*, 1272–1283. https://doi.org/10.1109/JIOT.2017.2708042. [CrossRef]
113. Dofe, J.; Nguyen, A.; Nguyen, A. Unified Countermeasures against Physical Attacks in Internet of Things—A survey. In Proceedings of the 2021 IEEE International Symposium on Smart Electronic Systems (iSES), Jaipur, India, 18–22 December 2021; pp. 194–199. https://doi.org/10.1109/iSES52644.2021.00053. [CrossRef]
114. Chengoden, R.; Victor, N.; Huynh-The, T.; Yenduri, G.; Jhaveri, R.H.; Alazab, M.; Bhattacharya, S.; Hegde, P.; Maddikunta, P.K.R.; Gadekallu, T.R. Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions. *arXiv* **2022**, arXiv:2209.04160.
115. Algarni, A. A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems. *IEEE Access* **2019**, *7*, 101879–101894. https://doi.org/10.1109/ACCESS.2019.2930962. [CrossRef]