symmetry

MDPI

Review

Security and Privacy in Cloud-Based E-Health System

Remya Sivan * and Zuriati Ahmad Zukarnain *

Department of Information Security, Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan 43400, Malaysia

* Correspondence: gs59108@student.upm.edu.my (R.S.); zuriati@upm.edu.my (Z.A.Z.)

Abstract: Cloud based healthcare computing have changed the face of healthcare in many ways. The main advantages of cloud computing in healthcare are scalability of the required service and the provision to upscale or downsize the data storge, collaborating Artificial Intelligence (AI) and machine learning. The current paper examined various research studies to explore the utilization of intelligent techniques in health systems and mainly focused into the security and privacy issues in the current technologies. Despite the various benefits related to cloud-computing applications for healthcare, there are different types of management, technology handling, security measures, and legal issues to be considered and addressed. The key focus of this paper is to address the increased demand for cloud computing and its definition, technologies widely used in healthcare, their problems and possibilities, and the way protection mechanisms are organized and prepared when the company chooses to implement the latest evolving service model. In this paper, we focused on a thorough review of current and existing literature on different approaches and mechanisms used in e-Health to deal with security and privacy issues. Some of these approaches have strengths and weaknesses. After selecting original articles, the literature review was carried out, and we identified several models adopted in their solutions. We arrived at the reviewed articles after comparing the models used.

Keywords: e-Health; cloud computing; security; privacy in health system

check for updates

Citation: Sivan, R.; Zukarnain, Z.A. Security and Privacy in Cloud-Based E-Health System. *Symmetry* **2021**, *13*, 742. https://doi.org/10.3390/sym13050742

Academic Editor: Debiao He and Sergei D. Odintsov

Received: 29 January 2021
Accepted: 7 March 2021
Published: 23 April 2021

1. Introduction

Innovative changes have permitted progressive answers for be actualized to upgrade the nature of human existence. Analysts considering the development of innovation have identified and assessed wellbeing data from these sources to acquire information and take care of wellbeing-related issues. In this manner, the advancement of incorporated medical care innovation has the likelihood to enhance efficiency and improve understanding of the results at each level of the medical care framework. Long-term care (LTC) facilities are a crucial a part of the health care industry, providing care to the fastest-growing group of the population. However, the adoption of electronic health records (EHRs) in LTC facilities lags behind other areas of the health care industry [1]. The advancement of new Electronic-Health (e-Health) application frameworks can take care of specific issues pertinent to conventional medical care frameworks by means of powerful patient wellbeing controls, pervasive information access, distant patient checking, quick clinical intercession, and decentralized electronic-medical care records. These frameworks can oversee wellbeing data and patient information, upgrade personal satisfaction, increase coordinated effort, improve results, decrease expenses, and increase the generally efficiency of e-medical care administrations [2]. For health care, EHRs are required to be shared among different healthcare organizations, medical drug manufacturers, pharmacists, medical insurance providers, researchers, and patients. This poses a significant challenge keep the patients' sensitive data secure [3]. In addition, Eisenach depicted e-Health as a tech industry that addresses the assembly of the Internet, systems administration, and medical services and incredibly benefits the framework clients and partners. E-wellbeing is a rising field at the convergence of clinical informatics, general wellbeing, and Internet wellbeing administrations that embrace and drive the overall advancement of new innovation to tackle profound issues, drive down expenses, and improve understanding [4] (Malluhi, 2020).

Along these lines, models, gadgets, and frameworks associated with the Internet of Things (IoT) have become universal. Besides, the broad appropriation of IoT has harmonized with the improvement of interrelated correspondence advances, for example, registering knowledge for medical care, business, industry, operational frameworks, etc. The efficient and safe usage of wellbeing data advancements, benefits, and all-encompassing e-Health frameworks requires exceedingly efficient and strong security frameworks to make such execution reasonable. The universality of IoT frameworks has driven the innovative work of IoT innovation, remembering assorted designs for use for wellbeing organizations. Connecting networks, gadgets, applications, and administrations with the IoT permits e-Health frameworks to share related data utilizing the most recent innovation [5] (Hassen 2020).

IoT and distributed computing are progressive innovations that supplement each other's capacities when incorporated as flexible, versatile, and efficient tolerant medical service frameworks. The blend provides benefits, including simplicity of execution contrasted with regular organizations, improved data security during correspondence, speedy admittance to records, and energy investment funds over customary modalities. IoT-cloud-based e-Health frameworks can significantly improve medical care benefits and advance persistent efficient development. In IoT-cloud-based e-Health frameworks, hidden IoT networks empower correspondence between clients, administrations, and workers, with clinical information stored in the cloud. With new improvements in distributed computing proceeding to push past business as usual, different security dangers to be discussed or when storing data should be considered [6].

Distributed computing is an innovation that changed the medical care industry. Distributed computing's significant advantages are innovation adaptability, savvy, energy investment funds, processing and sharable assets, and quicker sending. This paper will walk through distributed computing identified within the medical service industry and other diverse cloud-related security and significant protection challenges. Additionally, we will discuss the plausible security arrangements. Coordinated effort of information in the cloud brings serious security and protection worries for medical service suppliers. Therefore, endeavored security, effectiveness, security, and versatility are primary worries in the reception of cloud-related innovation administrations [7].

Mists are piles of virtualized assets of actual workers, organized, virtualized workers, applications or potential benefits. Figuring assets can be arranged in clusters or individually to provide the need of the end client of the shopper. The up-time is itemized among arrangements, for example, Service-Level Agreement, SLA (Sandy 2011)

Distributed computing is an innovation that is intended to give and oversee application and information, Server accessibility, and end client figuring (EUC) conveyance. Cloud computing permits staff or workers to obtain and deal with their application and information continuously on any gadget, from any area. [8] A fruitful distributed computing arrangement should give rearranged or brought together, logical, and secure insight for infrastructure and end clients. Since all advances have a particular issue, distributed computing likewise has its own highlights, for example, the board, innovation, security, and legitimate issues. [9] The fundamental motivation behind this paper is to challenge the idea of cloud-based figuring, the current utilization of medical care and the difficulties, openings, and ways to deal with arranging where medical care has settled on another cloud-based help model (Steve 2019).

2. Methods and Materials

All the open writing that is identified with e-Health security and safety is essentially hard to survey. Therefore, in terms of reviewing selected posts, we dominate. Following the collection of more than one hundred and ten (1 1 0) specific posts, the writing audit was completed, and a few templates that followed their responses were sorted. We downloaded more than forty (40) papers from the ACM advanced library, 57 articles from the IEEE computerized library, and 43 from the IEE Explore advanced library to provide a fair and calculable number of articles surveyed. Different articles were accessed from the specialized repositories of Springer, Elsevier, and Science Direct. There were hardly any papers downloaded from numerous diaries that are not known and respected as those cited. We obtained 110 surveyed publications in the face of conflicting models and methods used by many analysts. Due to the similarities found in the models obtained by some scientists, the analyzed papers were restricted to the momentum number.

Besides that, by looking at and dissecting the strengths of each of the approaches obtained in seeking a solution to the protection problem in e-Health, we directly analyzed the papers. In addition, we identified numerous shortcomings of both of these techniques that eventually indicated the way forward to mitigate e-Health security and safety slips. E-wellbeing is a developing area at the crossroads of clinical informatics, general well-being, and industry, relating to well-being administrations and knowledge communicated or enhanced through the Internet and related technologies. [10–13] The word represents a specialized turn of events from a more detailed viewpoint, but also a perspective, a demeanor, and a duty for coordinated, national speculation to enhance patient care through the use of information and communication technologies locally, territorially, and internationally [14].

2.1. Research Strategy

As this a comprehensive review, we aim to update the findings of previous studies (54) regarding the same matter. We retrieved eligible studies from late 2013 to December 2020. The study selection searched for publications from Symmetry Journals in MDPI, other Journals in MDPI, IEEE Access journal, and other IEEE Journals. The first step involved including the relevant articles with related keywords in the title or abstract based on the inclusion criteria. Papers not related to our study were excluded. The second step consisted of a full-text screening of the relevant studies to select the most eligible articles.

2.2. Research Questions

In this paper, we will be discussing the three main areas in ehealth system, such as:

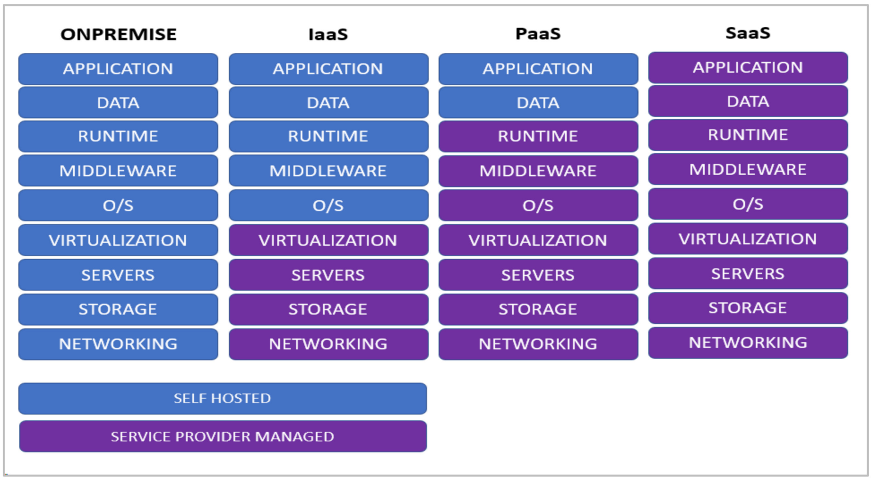
1. What is the cloud computing scheme and state-of-the-art of the cloud-based computing solutions commonly used in healthcare systems?
2. What are the security concerns or challenges in Cloud-based computing in Healthcare systems?
3. How are the current Cloud computing-based ehealth systems being protected?
4. What is the best solution for security in cloud-based E-health systems?

3. State-of-the-Art Cloud Computing-Based E-Health Systems

Cloud computing schemas are mainly divided into three (3) types: Infrastructure as a Service (IaaS): Infrastructure as a Service is a cloud-computing technology that delivers computing resources, networking, and storage to consumers on-demand, over the internet. It enables end customer or end users to upscale or downsize resources on an as-when needed basis, reducing the need for upscaling, up-front capital expenditures or unnecessary infrastructure. [15,16]

Platform as a Service (PaaS): Platform as a Service (PaaS) is termed as a development and deployment environment provided by a cloud partner. PaaS provides a platform on which software is developed and deployed. IaaS platforms handle the complexity around operating systems and servers and leaves application developers liberally to focus the business requirements of the software.

Software as a Service (SaaS): Software as a service (SaaS) is the option for businesses in the cloud market. It is easily accessible—all you need is an internet connection and a browser—and it is hands-off. The SaaS delivery model requires vendors to manage all the technical issues—meaning customers do not need to lean on their in-house IT expertise. Figure 1 shows the High-Level Architecture of the Cloud Infra-structure.



ONPREMISE	IaaS	PaaS	SaaS
🟦 APPLICATION	🟦 APPLICATION	🟦 APPLICATION	🟪 APPLICATION
🟦 DATA	🟦 DATA	🟦 DATA	🟪 DATA
🟦 RUNTIME	🟦 RUNTIME	🟪 RUNTIME	🟪 RUNTIME
🟦 MIDDLEWARE	🟦 MIDDLEWARE	🟪 MIDDLEWARE	🟪 MIDDLEWARE
🟦 O/S	🟦 O/S	🟪 O/S	🟪 O/S
🟦 VIRTUALIZATION	🟪 VIRTUALIZATION	🟪 VIRTUALIZATION	🟪 VIRTUALIZATION
🟦 SERVERS	🟪 SERVERS	🟪 SERVERS	🟪 SERVERS
🟦 STORAGE	🟪 STORAGE	🟪 STORAGE	🟪 STORAGE
🟦 NETWORKING	🟪 NETWORKING	🟪 NETWORKING	🟪 NETWORKING

🟦 SELF HOSTED

🟪 SERVICE PROVIDER MANAGED

Figure 1. Cloud Infrastructure Architecture.

The E-health system is a newly developed space that contains electronic processes and communications. EHR or EMR is a compilation of patient health data. EHR or EMR is digital information that contains data, diagrams, patient medical information, medications, hospital or clinic reports, radiology photographs, billing information, and other sensitive patient information. Cloud computing offers the cost of effectively storing, processing, and updating data with efficiency and quality [17].

Cloud computing offers the advantage of access to hosted services from multiple lo-cations with a number of multiple users. E-health systems promise faster, robust, and sought-after access to medical records, fewer medical regulations, and improved health care quality, but equally reflect patient privacy, improper authorization, and misuse of EHR data. Cloud security and privacy are critical requirements when sharing or accessing patient data. An overview of e-health structures is shown in Figure 2.

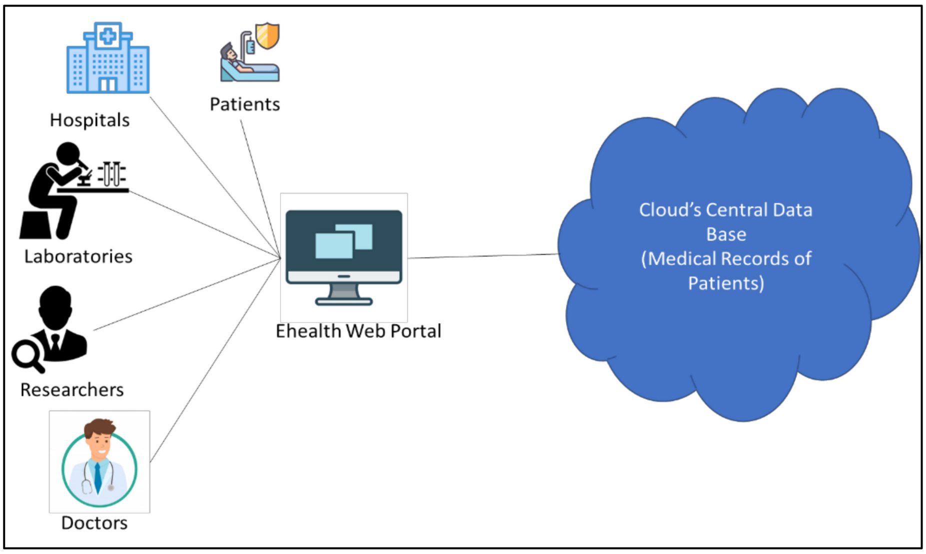


Figure 2. E-health architecture in the cloud.

There are many ways to achieve the use of the cloud platform. A few of them are as mentioned below.

Public Cloud: A cloud service provider will make resources available to private and public users via the Internet for free on-going or demand purposes that allow clients to pay only for what they use without lower fees. Instead of purchasing a physical server and switching, the company can purchase a virtual server and network. A virtual server can be turned on or off for minutes and can be accessed anywhere. The public cloud relies on a customized environment to provide corporate infra-structure expansion, allowing the company to host certain aspects of its infra structure and services on virtual and identifiable third-party servers. Public cloud service providers have unique capabilities, and they offer excellent types of services and price models. Companies considering migration have carefully considered their options when it comes to choosing a provider, especially if they are to be terminated in a long-term contract. Careful planning can help reduce costs in monthly payments for cloud services, but organizations with unexpected age of the us-age community may find it difficult to avoid spending large sums on public cloud services under unforeseen use. [18]

Independent cloud: A public cloud is an infrastructure that uses a single organization and defines a single network or datacenter that provides services hosted to a specific group of people. The public cloud service offers easy access. Although a private cloud is less expensive than using a public cloud, it is not easily measured. The development or growth of infrastructure will require the purchase of additional equipment. Similarly, when the need for a private cloud decreases, expensive resources and equipment are misused [19,20].

Hybrid Cloud: A cloud infrastructure that is a combination of two or more clouds that can be a combination of a private, or public cloud. In hybrid cloud infrastructure, the organization provides and manages resources within the private data center and provides outsourced services such as VMware that works with Fortinet Networks to provide hybrid cloud infrastructure to businesses to lighten their private cloud to remote servers while the public cloud is secure.

The Hybrid model cloud is usually an excellent deal for those looking at a public cloud vs. private cloud. Hybrid Cloud refers to any integration of personal and public cloud solutions. The hybrid cloud environment allows organizations to take advantage of both types of cloud platforms and choose which cloud will provide the specific data needs. For example, the hybrid cloud provides another way to store sensitive data company information that can provide services through the public cloud while maintaining sensitive configuration in the private cloud [21,22].

Advantages of Cloud-Based Ehealth Systems

The more a healthcare center connects system information to a global computer network such as the Internet, the more it opens up access from around the world and facilitates data leaks. The need for an electronic health record should be protected from illegal users who may misuse this for a variety of purposes. Identity-based encryption is one of the best security solutions to protect eHealth record data [23,24]. The algorithm deals with problems found in common cryptographic techniques using any thread as a public key. The system can enhance the security of health records by adding authentication procedures to three connected servers. In this system, communication between three servers uses encrypted data using IBE, so that each server can perform the encryption and decryption process during the data exchange. Only servers with IDs can access and extract health record data. Currently, test results show performance relative to the speed of the algorithm used in the system [25,26].

As discussed, and referred to in article [27], Cloud Storage is a computer model that stores data on the Internet or in the cloud. Cloud storage is delivered according to demand and capacity and costs that will leave the customer investing and managing their data storage infrastructure. This provides speed, scale, and durability.

Below are some of the general advantages of cloud computing; in our case, we focus on E-health systems.

Ease of access using a 'Web Browser' with integrated Single-Sign-On (SSO).

No requirement for VPN to access Cross Sites or Networks.

Simplified Management and On-demand Scalability.

No Overhead Cost to maintain the physical infrastructure.

No Hardware post warranty charges for the physical infrastructure.

No Power Consumption.

One of the major schemes in healthcare systems is attribute-based encryption for data. Encryption provides high-class access control for every user and revocation, scalability, dynamic user management, and traceability. Users have high-grade login access which can be integrated with 2FA authentication as well as OTP for every access. Similarly, users' access can be revoked from a centralized management console at any point in time by the administrator. The most important advantage is that every access is recorded and can be traced, and clipping implemented for each session [28]. Privileged Access Management (PAM) is one of the best technologies which can be used if there are many subsystems that a user needs to access at a single point in time.

Another scheme used in health care in cloud computing is robust and secure access control which resolves single-point performance bottle-neck problems. This solves the majority of the security access control issues as the certificate needs to be trusted and issued from a certified hosting platform. As we all know, the main disadvantage is that there is no process or mechanism for attribute revocation.

4. Cloud-Based E-Health Security Issues

As we all know, cloud computing has its own security challenges which emerge from time to time due to proper security technologies and because of a lack of security compliance, as discussed using the benchmark in research papers [29–33].

A few of them are mentioned below such as:

Confidentiality: Confidentiality is a process or mechanism of safeguarding patient health data from unauthorized access from public or internal users. Unauthorized access is dangerous and can potentially result in data leakage and can even cause serious damage to businesses. With respect to the data size, the number of patients on devices increases, and there is a huge potential threat to the data to expose these to external parties. Confidentiality is important in the healthcare industry as the patient can be reluctant to give personal details to doctors if they are not confident with the confidentiality. By implementing access control and using encryption techniques, confidentiality can be achieved.

Integrity: Integrity is important factor to make sure that the data are not changed at any single point in time. The HIPAA Security illustrates that covered entities must implement procedures and policies to protect electronic healthcare information from improper destruction or alteration.

Integrity can be achieved by a hashing mechanism or checksum for all the data. One of the best and accurate ways is by implementing block chain technology as it is merely impossible to change the hash of the data as it will change the entire chain if any of the hashes are changed.

Availability: The information must be available all the time. Business critical systems should be clustered or must have high availability to have maximum uptime without service interruptions.

Data Violations: Business Impact on Company Dignity and Trust for Customers or Partners. Degradation of intellectual property by competitors can lead to product outsourcing, financial discovery, and the occurrence of events and forensics.

Wrong fix: This is one of the most common cloud challenges.

As cloud computing is a shared resource, any misconfiguration of the datacenter will lead to complete exploration of all the customer data hosted within the same datacenter.

Lack of Security Technologies: The biggest challenge during the transition to cloud computing is the implementation of appropriate security architecture to withstand cyber-attacks. Unfortunately, this process remains a mystery for several organizations. Data are exposed to different threats when organizations assume that cloud migration is a "lift-and-shift" endeavor of simply porting their existing IT stack and security controls to a cloud environment. A lack of knowledge of the shared security responsibility is also a contributing factor.

Account hijacking: A key feature where attackers gain access to accounts, and serious or sensitive rights are exploited. Criminal attacks on sensitive data, cloud system exploits, or access to stolen signals can put these accounts at risk.

Insider Threat: Circumstances have been identified including malicious servers, employees saving sensitive data on their unprotected devices and programs, employees or other insiders who steal stolen emails exposed by malicious attacks on company assets.

Unsecured APIs: Cloud computing providers develop a range of user software and APIs to allow customers to manage and interact with cloud services. The security and availability of standard cloud services are linked to the security of those APIs. Poorly designed APIs can lead to misuse or even worse, infringement of information. Exposed, broken, and hacked APIs have serious concerns about data breaches.

Healthcare really needs to understand the safety requirements for designing and introducing visible connectors online.

5. Classification of Security Solutions in E-Health Systems

5.1. Cryptographic Security

The continued advancement of information technology and data communications strengthens the exchange of highly sensitive medical information. electronic health systems are widely used, and many medical facilities rely on the transmission and receipt of medical information online and on local networks. Over the years, many security systems have been introduced to monitor patient privacy and ensure the safety of interchangeable medical data. Cryptography is one of the techniques that often provides security for eHealth systems.

The Cryptographic method allows us to various computations to take place directly from encrypted data, without the need to define them. As such, encryption schemes with homo-morphic structures can be useful in building confidentiality agreements, where confidential information remains protected not only during exchange and storage, but also processing.

Cryptography is a method of compiling, validating data, and exchanging them using conferences with the goal of keeping track of those data set up for them to investigate. Countless methods have been suggested to protect patient health care data. However, Cryptographic methods can be seen in two forms, symmetric-key cryptography, and Asymmetric-key cryptography, where the former uses the same encryption and coding key while the latter uses different keys

It relies heavily on methods such as PKE, SKE, and a few native cryptographic devices used to protect the e-Health cloud. In PKE, two different key configurations are used, an open key and a pair of encryption and spelling keys although SKE-based methods use an equally shared private key as clearly defined in the PKE & SKE cryptography methods in other articles [34].

5.1.1. PKE & SKE (Public Key Encryption and Symmetric Key Encryption)

In PKE schemes, two different key sets are considered: public key and secret key. Pairs of private and public data encryption and encryption keys, Sache-based apache approaches use the same shared private key. Other cryptographic schemes include several encryption schemes such as Attribute-Based Encryption (ABE), Searchable Encryption (SE), proxy encryption, homomorphic encryption, and Identity-Based Encryption (IBE).

As already noted [35], cryptography has a profound effect on the security of e-health systems. However, there are some non-cryptographic methods that can also provide security, but these are not widely used as they provide partial security for the e-health cloud under the security provided by crypto methods. Therefore, these systems are used with crypto methods in the hybrid system, some of which are shown below.

Encryption is key to data security. Encryption shuts down electronic information so that no one other than the key can access the information. It does not matter if the organizer breaks the organization's security control of the information; it will be a small thing. Data encryption is the process of encrypting data in one place, then transferring data over the network, and then deciphering data in the cloud. It is an important process nowadays because unauthorized people (hackers) have access to information, which creates a data problem. That data can be stolen during transfer.

A range of encryption methods is used in the E-health system such as Broad-cast Encryption Schemes, Attribute-based Encryption, blockchain based encryption, and Searchable Symmetric Encryption.

5.1.2. Broadcast Encryption Programs

Stream encryption allows a mid-stream broadcast website to secure shipments to associate a complete set of recipients while minimizing the high-speed communications mentioned in the article [36].

5.1.3. Qualified Encryption

Privacy-based encryption can also be a form of public key cryptography in which the user's private key and the security area-based security unit deletion of text definitions is only possible if the set of user key symbols matches the text symbols discussed explicitly in the articles [37,38]

5.1.4. Blockchain-Based Encryption

In the E-health system, the verification, preservation, and synchronization of electronic medical records have always been a serious problem, and the random distribution of patient records will present various risks to the patient's privacy. Hash counts in electronic medical data and keeping the corresponding value in the blockchain ensure its consistency and integrity. Details listed in clinical records were removed from the Ethereum blockchain, and a good agreement was submitted to the Ethereum block-fasten to accept the viewing of word searches instead of the third-party person mentioned in the article [39]

5.1.5. Searchable Symmetric Encryption

Searchable Symmetric Access (SSE) when transferring to the cloud allows a person to query the data entered without the risk of data loss. Although interest is widespread, current research does not examine how buildings under SSE are constructed and how they end up in various areas of the SSE system. Most applications use a file table, where the appropriate file size and sublinear search can be done using the inverted file list. Direct referrals can only be obtained using the direct reference shown in the articles [40,41].

5.2. Access Control Manager (AAM)

One of the ways to authenticate and access control managers where users use tokens to access their sensitive records stored in the cloud where the server identifies users and determines their access rights is via the AAM server found in articles [42,43].

Full Private Blockchain (FPB) and Consortium Blockchain (CB)

An integrated blockchain model of a fully independent blockchain (FPB) and consortium blockchain (CB) was proposed to improve the time taken for data validation. Here, FPB is used as an old database of health care facilities and CB is used to store medical data from all participating medical professionals discussed and referred to in article [44] authors are offered multiple options on the E-health cloud-computing platform.

While the confidentiality of data converted to the cloud between institutions is not processed, medical data are sensitive. Electronic Health Applications include a shared distribution of digital information between providers and patients.

Security Transfer is an end-to-end process that must be managed regularly. As hackers continue to seek new vulnerability to take advantage of it, any cloud-driven app should be updated frequently to stay ahead of threats. It should be a complete balance protection for user access. A mobile app, EMR, or e-health is about secure access. User access should be controlled with a simple yet effective authentication.

Security can be budget-friendly, which is why EMRs and e-health programs were initially unaffordable at minimal follow-up. Today, applications that were only available to those with the same budget as hospitals have been made available by a very small ambulance site.

The non-cryptographic approach is mainly associated with policy-based approvals in the basis of labeling infrastructure such as access control methods such as RBAC, ABAC, Mandatory Access Control (MAC), IBAC, etc.

Table 1 describes multiple solutions for data security in ehealth systems.

Table 1. Custom-based solutions for security in E-Health Systems.

Reference	Security & Privacy	E-Health	Cloud	Contribution
[9] 2016	√	√	√	Proposed secure personal e-Healthcare system based on certificate CA to authorized users only.
[10] 2016	√	√	√	Proposed a prototype-based Personalised Health monitoring application
[11] 2020	√	√	x	Proposed a wearable IoT-enabled heart disease prediction system using the MDCNN classifier.
[12] 2020	√	√	x	This work addressed the development of IoT-based eHealth systems on both the hardware and software levels
[17] 2019	√	√	√	Efficient comprehensive security mechanisms for EHR also explored the techniques to maintain the integrity and confidentiality of patients' information.
[19] 2019	√	√	x	Proposed a novel collaborative eHealth system, which supports multilevel privacy-preserving data sharing (MPPDS).
[45] 2018	√	√	√	Proposed a Benchmark lossless method which is suitable for remoting health monitoring systems.
[46] 2018	√	√	√	Proposed the first secure and efficient encrypted EMR deduplication scheme for cloud-assisted eHealth systems, namely HealthDep.
[47] 2017	√	√	√	Reviewed the applications developed in the health industry which are focused on patient care from home and implemented a service-oriented (SOA) design in architecture.
[48] 2014	√	√	√	Provided an answer for privacy-preserving knowledge storage by group action of PRF-based key management for unlikability, a research and access pattern concealment theme supported redundancy, and a secure assortment technique for privacy conserving keyword search.
[49] 2017	√	√	√	Automatic IoHT building blocks to exchange the information between devices and integrated cloud computing.

6. Proposed Solutions for Security in Cloud-Based Ehealth Systems

The conventional approach to healthcare practices in the world has been changed by the growth of information and communication technologies. In the partial abandonment of paper-based medical prescription to the electronic version, this development is well noticed, particularly in most developed countries of the world. The need to federate and integrate electronic health information from different fields, such as laboratories for medical research, hospitals, and health insurance companies, has led to the development of a concept called electronic health (e-Health) [50]. Simply put, e-Health can simply be defined as the use of the infrastructure of information technology (IT) and e-commerce practices for health information processing, sharing, and manipulation. However, it is noted that the application has made it very difficult to manage the need for a cloud-based environment that enables the collaborative sharing of information across multiple administrative domains by different domains involved in the sharing of medical data [51]. Cloud computing has so many benefits, including the timely transfer and sharing of medical information seamlessly. It has also relieved the rigor involved in managing the infrastructure for healthcare providers and has provided them with ample opportunity to familiarize themselves with IT service providers. Cloud computing has been established in various academic papers to offer numerous advantages including scalability, cost-effectiveness, agility enhancement, and collaborative resource sharing [52].

There are security and privacy challenges, despite the various advantages, that urgently deserve the utmost attention for the realization of its efficient and full-scale use [53]. On several occasions, cryptographic and non-cryptographic approaches have been used to ensure the preservation of cloud-computing security and privacy of health information. In addition, fine-grained as well as patient-centric access control systems are frequently used to achieve electronic health privacy. In this paper, different security measures are reviewed that are used to protect data. Their strengths and weaknesses are exposed as well. Efforts have been made to provide better options for securing e-health information.

Simplicio et al. (2015) demonstrated how a lightweight framework was used to introduce a Transport Layer Security/Secure Sockets Layer (TLS/SSL)-based Secure Health architecture to protect server data exchange that requires no additional security layer. Secure Health, which includes many security features, such as authorization, provides transmitted and stored data security services. It has a good advantage in preventing from accessing the system containing health information without authorization. In addition to this, it provides the manager with the ability to identify errors from the information provided. The primary challenge is that it is platform-dependent and not scalable, despite the advantages of this framework. The security policy and framework must provide room for scalability and future expansion in a cloud-based environment. To ensure that e-Health care service providers reduce the cost of maintaining data and allowing them to be securely accessible online, Barua et. al., proposed a security mechanism with different levels of hierarchy. Provision of access control was carried out at a central level. In such a way that privileges were mapped and juxtaposed to different roles with ABE access structures, they adopted Attribute-Based Encryption (ABE). The main challenge with this approach is the complexity of responding to various requests from different users due to storage of health information located in a centralized server. In addition, when there is a concurrent request by users, priority needs to be set. The distributed and collaborative nature of the e-Health system was considered by Guo et al. (2012) to solve the challenge of having data storage of health information in a centralized server. They did not allow a centralized server to handle authentication and authorization procedures; instead, they allowed both the patients and doctors to carry out the authorization process. In reality, without disclosing their attributes and identities, users are given access based on their privileges.

7. Discussion

Specialists have developed a system for IoT-based shrewd well-being systems used in their proposal as an e-Health platform, zeroing in on interoperability, different criteria for creativity, correspondence protocols, and framework prerequisites. Web developments, correspondence conventions, and equipment schedules were used in the relevant conventions and guidelines. Their structure was shown to be safe through trust tests that showed that it was possible to achieve interoperability between various IoT gadgets, concepts, and conventions in an e-Health system all the time in the Internet world. In order to upgrade the transmitted delegate layer of information between sensor hubs and the Cloud, specialists suggested the concept of Fog registering in a medical services IoT environment as a savvy e-Health framework. They took advantage of the omnipresence of current patient care systems to reduce the weight of sensors, organizations, and remote populations of medical facilities, solving challenges of portability, energy consumption, flexibility, and reliability in this manner. The efficient implementation of their e-Health platform is an entryway known as UT-Gate that offers more high-level highlights, such as an IoT-based Early Warning Score (EWS) well-being assessment framework with commonly updated framework awareness, efficiency, execution, interoperability, security, and usability. To facilitate access to patient's data by way of the network using distributed computing, specialists planned a platform integrating IoT gadgets. Doctors were best trained to take care of their patient conditions in an effective design by facilitating the acquisition and aggregation of the knowledge needed to screen well-being comprehension. Using distributed computing, gadgets, knowledge conglomeration, and handling, information stockpiling and information investigation were designed for a four-venture engineering for e-health frameworks. They portrayed applications where the system will be useful, essential associated developments to make it work, and benefits and limitations of chaperons. Specialists suggested the invention of the IoT-based body sensor network using lightweight remote sensor hubs with IoT to transmit and receive information via distributed computing. In order to obtain the patient care system and to ensure that information stays confidential, they recognize privacy and security conventions. In e-Health frameworks, specialists investigated the production of the mixture of IoT gadgets and distributed computing and delineated applicable challenges, opportunities, and limitations. They offered confirmation that the security of the IoT-cloud-based e-Health platform is urgent and suggested a validation strategy to receive IoT-cloud-based e-Heath frameworks with standard deployment and accommodation conventions. Seniors outlined the cloud-facilitating administrative benefits and assumed that IoT-cloud-based systems improve new industries by increasing accessibility and expandability and by reducing costs through the temperance of an as-you-use pay structure. By combining three different security models, they achieved their design: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) to come up with a new architecture that allows access privileges to be dictated and set by health care providers and patients. The main disadvantage of this framework lies in its ability to be useful only as a standalone safety model in order to achieve the requirements for health electronic records. Barua et al. proposed a secure patient-centered electronic health information scheme to provide reliable access privileges in a cloud-based environment using a protocol called Proxy Encryption. In order to allow patient-centered access control, the schema with five main stages uses Attribute Based Encryption. The performance analysis shows that the performance of the schema is excellent. The shortcoming is that it is not sufficiently flexible for other types of distributed systems. Furthermore, there is no room for scalability and flexibility in the schema. Only a limited number of users was considered during evaluation.

8. Research Issues and Future Directions

The main concern at this stage is to discuss future indicators related to privacy and security in Electronic Health Records (EHRs). EHR data are extremely sensitive, confidential, and in particular, are stored on third-party servers, leading to significant risks in terms of data privacy and security. Some of the major research problems include:

- Procedures and procedures on how to protect and secure the data stored in the cloud.
- The use of confidential health care data.
- What will be the best encryption system that can be used to maintain data security?

The above points highlight various research issues related to the privacy and security of e-health information. Therefore, we have analyzed and identified the need to use security infrastructure in e-health systems that will ensure the privacy and security of data and thus protect patient privacy and trust.

Privacy is one of the most important aspects of the healthcare industry. Maintaining breach of confidentiality and keeping track of confidentiality through medical records are essential to detecting and preventing fraud. Keeping track of data sources and programs is advisable.

This research can be further enhanced by using user authenticity and privacy in Cloud Big secure data. A secure authentication method that incorporates tree-based hashing in the authorization structure, used for user authentication during multi-level configuration, resists fraudulent attacks and protects privacy. The authoritative structure of hierarchical attributes leads to a lot of confusion and final problems. Artificial Intelligence (AI) or Big Data Analytics (BDA) incorporates system design controls for each process. More recently, commands have been compared to replica nodes. Leaked privacy of users and their data are displayed with random action keys in secure data connections. By using analytics, it is easier to make a normal life for one or more patients with one view instead of one at a time.

9. Conclusions

Healthcare has already adopted cloud-based solutions to solve multiple problems cost effectively. While considering the future and growth of cloud-based healthcare services, we focused on the security of critical electronic health records (EHRs) and proposed an identity-based secure and encrypted data-sharing technique. We have studied the existing PKE, IBE, IBBE, & ABE and then proposed multiple solutions to safeguard cloud-based data in ehealth systems. Appropriate security solutions should be developed and maintained to protect data security. The future of cloud-based eHealth services will be the integration of file-based and cloud-based applications that integrate a computer-based hybrid IT solution that measures the flexibility and scalability associated with cloud management and healthcare data security. This review highlights a comprehensive study of existing cloud-based eHealth solutions that are cryptographic and non-cryptographic methods for protecting the privacy and security of digital data.

Author Contributions: R.S. and Z.A.Z.; methodology: R.S.; data curation: R.S.; resources: R.S.; writing—original draft preparation: R.S.; writing—review and editing: R.S. and Z.A.Z.; supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank the anonymous reviewers for their valuable comments and suggestions, which helped us to improve the content of our paper.

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

References

1. Kruse, C.S.; Mileski, M.; Vijaykumar, A.G.; Viswanathan, S.V.; Suskandla, U.; Chidambaram, Y. Impact of electronic health records on long-term care facilities: Systematic review. *JMIR Med. Inform. IEEE* **2017**, *5*, e35. [CrossRef] [PubMed]
2. Butpheng, C.; Yeh, K.-H.; Xiong, H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. *Symmetry* **2020**, *12*, 1191. [CrossRef]
3. Ismail, L.; Materwala, H. Blockchain Paradigm for Healthcare: Performance Evaluation. *Symmetry* **2020**, *12*, 1200. [CrossRef]
4. Malluhi, Q.; Tran, V.D.; Trinh, V.C. Decentralized Broadcast Encryption Schemes with Constant Size Ciphertext and Fast Decryption. *Symmetry* **2020**, *12*, 969. [CrossRef]
5. Hassen, O.A.; Abdulhussein, A.A.; Darwish, S.M.; Othman, Z.A.; Tiun, S.; Lotfy, Y.A. Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IOT Blockchain Network. *Symmetry* **2020**, *12*, 1699. [CrossRef]
6. Abdulghani, H.A.; Nijdam, N.A.; Collen, A.; Konstantas, D. A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. *Symmetry* **2019**, *11*, 774. [CrossRef]
7. Huh, J.-H. Big Data Analysis for Personalized Health Activities: Machine Learning Processing for Automatic Keyword Extraction Approach. *Symmetry* **2018**, *10*, 93. [CrossRef]

8. Kang, J.; Chung, H.; Lee, J.; Park, J.H. The Design and Analysis of a Secure Personal Healthcare System Based on Certificates. *Symmetry* **2016**, *8*, 129. [CrossRef]
9. Griebel, L.; Prokosch, H.-U.; Köpcke, F.; Toddenroth, D.; Christoph, J.; Leb, I.; Engel, I.; Sedlmayr, M. A scoping review of cloud computing in healthcare. *BMC Med. Inform. Decis. Making* **2015**, *15*, 17. [CrossRef]
10. Venčkauskas, A.; Štuikys, V.; Toldinas, J.; Jusas, N. A Model-Driven Framework to Develop Personalized Health Monitoring. *Symmetry* **2016**, *8*, 65. [CrossRef]
11. Khan, M.A. An IoT Framework for Heart Disease Prediction Based on MDCNN Classifier. *IEEE Access* **2020**, *8*, 34717–34727. [CrossRef]
12. Yang, M.; Hara-Azumi, Y. Implementation of Lightweight eHealth Applications on a Low-Power Embedded Processor. *IEEE Access* **2020**, *8*, 121724–121732. [CrossRef]
13. Guo, L.; Li, Z.; Yau, W.; Tan, S. A Decryptable Attribute-Based Keyword Search Scheme on eHealth Cloud in Internet of Things Platforms. *IEEE Access* **2020**, *8*, 26107–26118. [CrossRef]
14. Edemacu, K.; Park, H.K.; Jang, B.; Kim, J.W. Privacy Provision in Collaborative Ehealth With Attribute-Based Encryption: Survey, Challenges and Future Directions. *IEEE Access* **2019**, *7*, 89614–89636. [CrossRef]
15. Ma, H.; Xie, Y.; Wang, J.; Tian, G.; Liu, Z. Revocable Attribute-Based Encryption Scheme with Efficient Deduplication for Ehealth Systems. *IEEE Access* **2019**, *7*, 89205–89217. [CrossRef]
16. Caiza, J.C.; Martin, Y.; Guaman, D.S.; del Alamo, J.M.; Yelmo, J.C. Reusable Elements for the Systematic Design of Privacy-Friendly Information Systems: A Mapping Study. *IEEE Access* **2019**, *7*, 66512–66535. [CrossRef]
17. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F. Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access* **2019**, *7*, 74361–74382. [CrossRef]
18. Razaque, A.; Amsaad, F.; Khan, M.J.; Hariri, S.; Chen, S.; Siting, C.; Ji, X. Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. *IEEE Access* **2019**, *7*, 168774–168797. [CrossRef]
19. Kim, J.W.; Edemacu, K.; Jang, B. MPPDS: Multilevel Privacy-Preserving Data Sharing in a Collaborative eHealth System. *IEEE Access* **2019**, *7*, 109910–109923. [CrossRef]
20. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. *Sensors* **2020**, *20*, 483. [CrossRef]
21. Seol, K.; Kim, Y.; Lee, E.; Seo, Y.; Baik, D. Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System. *IEEE Access* **2018**, *6*, 9114–9128. [CrossRef]
22. Zhu, L.; Zhang, C.; Xu, C.; Liu, X.; Huang, C. An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing. *IEEE Access* **2018**, *6*, 19025–19033. [CrossRef]
23. Qadir, J.; Mujeeb-U-Rahman, M.; Rehmani, M.H.; Pathan, A.S.K.; Imran, M.A.; Hussain, A.; Rana, R.; Luo, B. IEEE Access Special Section Editorial: Health Informatics for the Developing World. *IEEE Access* **2017**, *5*, 27818–27823. [CrossRef]
24. Yeh, K.H. A Secure IoT-Based Healthcare System with Body Sensor Networks. *IEEE Access* **2016**, *4*, 10288–10299. [CrossRef]
25. Islam, S.M.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
26. Tahir, A.; Chen, F.; Khan, H.U.; Ming, Z.; Ahmad, A.; Nazir, S.; Shafiq, M. A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. *Sensors* **2020**, *20*, 5392. [CrossRef] [PubMed]
27. Vilela, P.H.; Rodrigues, J.J.P.C.; Righi, R.R.; Kozlov, S.; Rodrigues, V.F. Looking at Fog Computing for E-Health through the Lens of Deployment Challenges and Applications. *Sensors* **2020**, *20*, 2553. [CrossRef]
28. Haque, R.U.; Hasan, A.S.M.T.; Jiang, Q.; Qu, Q. Privacy-Preserving K-Nearest Neighbors Training over Blockchain-Based Encrypted Health Data. *Electronics* **2020**, *9*, 2096. [CrossRef]
29. Stamatellis, C.; Papadopoulos, P.; Pitropakis, N.; Katsikas, S.; Buchanan, W.J. A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric. *Sensors* **2020**, *20*, 6587. [CrossRef] [PubMed]
30. 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. [CrossRef]
31. Seh, A.H.; Zarour, M.; Alenezi, M.; Sarkar, A.K.; Agrawal, A.; Kumar, R.; Ahmad Khan, R. Healthcare Data Breaches: Insights and Implications. *Healthcare* **2020**, *8*, 133. [CrossRef]
32. Liu, H.; Crespo, R.G.; Martínez, O.S. Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. *Healthcare* **2020**, *8*, 243. [CrossRef]
33. Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. *Electronics* **2019**, *8*, 768. [CrossRef]
34. Huang, Q.; Yue, W.; He, Y.; Yang, Y. Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing. *IEEE Access* **2018**, *6*, 36584–36594. [CrossRef]
35. Celesti, A.; Fazio, M.; Galán Márquez, F.; Glikson, A.; Mauwa, H.; Bagula, A.; Celesti, F.; Villari, M. How to Develop IoT Cloud e-Health Systems Based on FIWARE: A Lesson Learnt. *J. Sens. Actuator Netw.* **2019**, *8*, 7. [CrossRef]
36. Schiza, E.C.; Kyprianou, T.C.; Petkov, N.; Schizas, C.N. Proposal for an eHealth Based Ecosystem Serving National Healthcare. *IEEE J. Biomed. Health Inform.* **2019**, *23*, 1346–1357. [CrossRef] [PubMed]
37. Lin, H.-Y.; Jiang, Y.-R. A Multi-User Ciphertext Policy Attribute-Based Encryption Scheme with Keyword Search for Medical Cloud System. *Appl. Sci.* **2020**, *11*, 63. [CrossRef]

38. Mehmood, Z.; Ghani, A.; Chen, G.; Alghamdi, A.S. Authentication and Secure Key Management in E-Health Services: A Robust and Efficient Protocol Using Biometrics. *IEEE Access* **2019**, *7*, 113385–113397. [CrossRef]
39. Khezr, S.; Yassine, M.A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
40. Li, H.; Yang, Y.; Dai, Y.; Yu, S.; Xiang, Y. Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data. *IEEE Trans. Cloud Comput.* **2020**, *8*, 484–494. [CrossRef]
41. Zhang, R.; Xue, R.; Liu, L. Searchable Encryption for Healthcare Clouds: A Survey. *IEEE Trans. Serv. Comput.* **2018**, *11*, 978–996. [CrossRef]
42. Edemacu, K.; Jang, B.; Kim, J.W. Collaborative Ehealth Privacy and Security: An Access Control with Attribute Revocation Based on OBDD Access Structure. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2960–2972. [CrossRef] [PubMed]
43. Tong, Y.; Sun, J.; Chow, S.S.M.; Li, P. Cloud-Assisted Mobile-Access of Health Data with Privacy and Auditability. *IEEE J. Biomed. Health Inform.* **2014**, *18*, 419–429. [CrossRef] [PubMed]
44. Kurdi, H.; Alsalamah, S.; Alatawi, A.; Alfaraj, S.; Altoaimy, L.; Ahmed, S.H. HealthyBroker: A Trustworthy Blockchain-Based Multi-Cloud Broker for Patient-Centered eHealth Services. *Electronics* **2019**, *8*, 602. [CrossRef]
45. Zhang, Y.; Xu, C.; Li, H.; Yang, K.; Zhou, J.; Lin, X. HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4101–4112. [CrossRef]
46. Yeh, L.; Chiang, P.; Tsai, Y.; Huang, J. Cloud-Based Fine-Grained Health Information Access Control Framework for Lightweight-IoT Devices with Dynamic Auditing andAttribute Revocation. *IEEE Trans. Cloud Comput.* **2018**, *6*, 532–544. [CrossRef]
47. Avila, K.; Sanmartin, P.; Jabba, D.; Jimeno, M. Applications Based on Service-Oriented Architecture (SOA) in the Field of Home Healthcare. *Sensors* **2017**, *17*, 1703. [CrossRef]
48. Guo, L.; Zhang, C.; Sun, J.; Fang, Y. A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks. *IEEE Trans. Mob. Comput.* **2014**, *13*, 1927–1941. [CrossRef]
49. Liu, Y.; Zhang, Y.; Ling, J.; Liu, Z. Secure and finegrained access control on e-healthcare records in mobile cloud comp ting. *Future Gener. Comput. Syst* **2017**, *78*, 1020–1026.
50. Elgendi, M.; Al-Ali, A.; Mohamed, A.; Ward, R. Improving Remote Health Monitoring: A Low-Complexity ECG Compression Approach. *Diagnostics* **2018**, *8*, 10. [CrossRef]
51. Liagkou, V.; Kavvadas, V.; Chronopoulos, S.K.; Tafiadis, D.; Christofilakis, V.; Peppas, K.P. Attack Detection for Healthcare Monitoring Systems Using Mechanical Learning in Virtual Private Networks over Optical Transport Layer Architecture. *Computation* **2019**, *7*, 24. [CrossRef]
52. AbuKhousa, E.; Mohamed, N.; Al-Jaroodi, J. e-Health Cloud: Opportunities and Challenges. *Future Internet* **2012**, *4*, 621–645. [CrossRef]
53. Sahmin, S.; Gharsellaoui, H. Privacy and Security in Internet-based Computing—Cloud Computing, Internet of Things, Cloud of Things: A review. *Procedia Comput. Sci.* **2017**, *112*, 1516–1522. [CrossRef]