Chapter 10
An Architecture to Improve the Security of Cloud Computing in the Healthcare Sector

Saleh M. Altowaijri

10.1 Introduction

Cloud technology is a widely adopted technology in the present era. This technology has given new life to all business organizations. It is also used in the healthcare sector and is increasing business flexibility in medical organizations. Flexibility, pay-as-you-go, cost effectiveness, greater efficiency, and agility are some of the benefits of this technology. While there are many advantages, there are also some risks, particularly with regard to the security of data in the cloud, which is the most challenging issue at all times. In cloud computing this has became more problematic because the actual data are stored in another location. So, provision of security for the data in the cloud is a tedious task for cloud computing organizations. We are talking here only about the healthcare cloud.

At present the healthcare sector requires creation of an environment that reduces time-consuming efforts and other costly operations to obtain a patient's complete medical records and uniformly integrate this heterogeneous collection of medical data to deliver them to the healthcare system. Electronic health records (EHRs) have been widely adopted to enable healthcare providers and patients to create, manage, and access healthcare information from any place and at any time. Cloud services provide the necessary infrastructure at lower cost and better quality. Cloud computing, when used in the healthcare sector, reduces the cost of storing, processing, and updating, with improved efficiency and quality. But the security of data in the cloud is not satisfactory today. The EHR consists of images of the patient's records, which are highly confidential. EHRs in healthcare include scan

S. M. Altowaijri (✉)
Faculty of Computing and Information Technology, Northern Border University, Rafha, Kingdom of Saudi Arabia
e-mail: Saltowaijri@nbu.edu.sa

R. Mehmood et al. (eds.), *Smart Infrastructure and Applications*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-13705-2_10

images, DNA reports, x-rays, etc., which are considered the patient's private data. Provision of security for a large volume of data with high efficiency is required. Data in the healthcare cloud are in an encrypted form. These data are very important and an attractive target for cybercriminals. Many researchers have proposed architecture to secure the healthcare cloud, and many techniques for securing the data in the cloud have been investigated. These researchers are both industry experts and academicians. Here, we present some of the researchers' previous work.

Kim et al. have presented a trusted model for efficient reconfiguration and allocation of computing resources, depending upon the user's request [1]. Trust calculations are made to achieve reliability. A collaborative trust model of firewall-through based on cloud computing has been proposed by Yang et al. [2]. A protocol to establish trust and confidentiality while accessing data has been proposed by Ahmed et al. [3]. Brodkin [4] has recognized seven security risks that are essential to consider before enterprises make decisions regarding transformation into a cloud computing model. Cloud computing as an approach introduces new risks, influences others, and magnifies some, according to Chen and Zhao [5]. These risks and their effect on security risks and vulnerabilities have been explained by Grobauer [6].

In earlier work, Mehmood and colleagues looked at the use of grid and cloud computing in healthcare [7, 8], transport [9–11], and distance learning [12]. In this chapter, we discuss security issues in the healthcare cloud and propose architecture to secure data in the healthcare cloud.

Section 10.2 of the chapter gives an overview of cloud computing, cloud architecture, and the advantages of cloud computing. Section 10.3 discusses the great benefits that the use of cloud computing can bring to healthcare organizations. Sections 10.4, 10.5, and 10.6 discuss cloud computing security, methods of cloud security, and security threats in the healthcare cloud, respectively. Section 10.7 describes the background to secure healthcare cloud architecture and reviews the relevant literature. Section 10.8 introduces the proposed secured architecture for the healthcare cloud and the results of using it. Section 10.9 concludes the chapter.

10.2 Cloud Computing: An Overview

Cloud computing is the spread of computing services such as servers, storage, databases, networking, software, machines and more devices over the internet, which is known as "the cloud." Those organizations who offer these services are called cloud providers and normally request money for cloud computing services on the basis of their usage, similarly to how electricity or water are paid for at home. Figure 10.1 illustrates a typical cloud, which is accessed through various devices and infrastructure.

Fig. 10.1 Cloud architecture

10.2.1 Types of Cloud Services: IaaS, PaaS, and SaaS

Cloud computing services are divided into three categories: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). These are like a computing stack, because they are created on top of one another and look like a stack. The following is a brief introduction to each type. Figure 10.2 depicts these three service categories.

(a) *Infrastructure-as-a-service* (IaaS): This is the most basic category of cloud computing. By IaaS, we mean the information technology (IT) infrastructure such as servers, virtual machines (VMs), storage, networks, operating systems, etc., from a cloud service provider on a pay-as-you-go basis [13].
(b) *Platform-as-a-service* (PaaS): This refers to cloud computing services that provide an on-demand environment for developing, testing, delivering, and managing software built applications. PaaS is considered to make it easier for developers to rapidly develop web or mobile apps, without thinking about managing the original infrastructure of servers, storage, networks, and VMs needed for development.
(c) *Software-as-a-service* (SaaS): This is a technique for providing software applications over the internet, on demand and typically on a pay-as-you-go basis. In using SaaS, cloud providers host the infrastructure and platform by using the internet, which can be connected to by using web browsers.

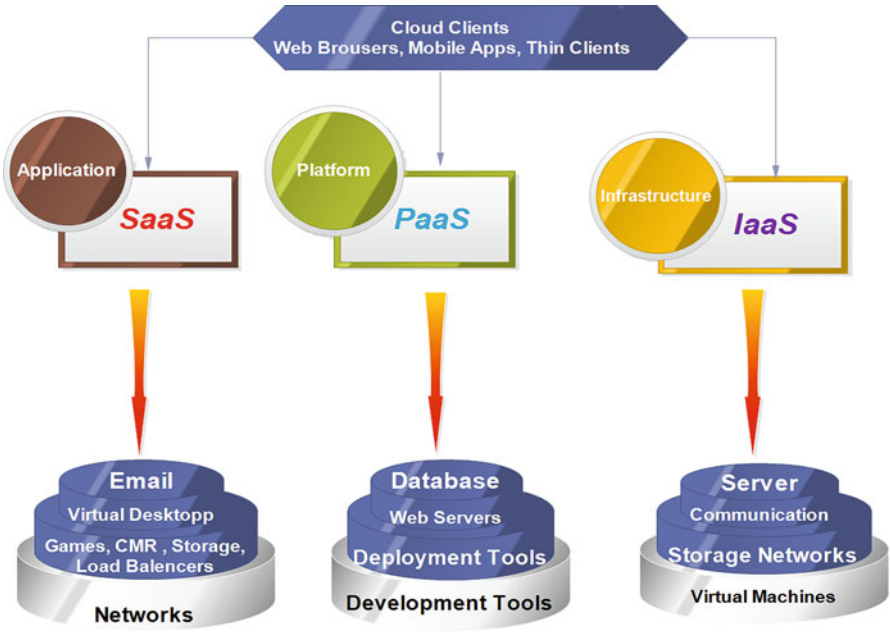

Fig. 10.2 Cloud computing overview

10.2.2 Advantages of Cloud Computing

The healthcare sector is switching to cloud computing instead of traditional IT solutions. Its main reasons are to manage dynamic needs for computational resources, scalability of human resources, high infrastructure management costs, and increases in demands for collaboration, multitenancy, and ubiquitous access. To overcome all of these issues, cloud computing offers the simplest and best solutions with cost effectiveness. These solutions are on-demand services, broad network access, resource pooling, measured service, and elasticity. These services are favorable, and their costs and maintenance requirements are easy for both clients and organizations to bear [14, 15].

Hence, cloud computing is a big move to uplift anyone's business. Let us think about IT resources when there was no cloud computing, so we can easily understand benefits of cloud computing. Why is cloud computing so popular?

Here, we give some common answers to these questions, by which we can easily understand why organizations are turning to cloud computing services. The reasons are:

1. *Cost effectiveness*: Cloud computing reduces the principal costs of buying hardware and software, and the costs of managing and running an on-site data center, i.e., a clusters of servers, round-the-clock electricity for light and cooling, IT personnel for setting up the infrastructure, and many more costs.

2. *Velocity*: Most cloud computing services provide personal service on demand, so that even large volumes of data can be provisioned in seconds, generally in just a few clicks, giving businesses a lot of ease and taking the stress off capability planning [13].
3. *Global scaling* (*regions*): The advantages of cloud computing services include the ability to scale elastically. In the cloud, that means providing the required IT resources such as servers, computing control database, storage and networking when they are needed and from the right regional location.
4. *Enhanced productivity*: On-site data centers typically require a lot of "racking and stack" hardware setup, software patching, and other sustained IT management tasks. Cloud computing removes the requirement for many of these odd jobs so that IT teams can use their time to achieve more significant business objectives [13].
5. *Better performance*: The biggest cloud computing services run on a universal network of protected data centers, which are frequently upgraded to the latest generation of fast and well-organized computing hardware. This offer several advantages over a single business data center, including compact network latency for application and greater economy of scale.

10.3 Cloud Computing and Healthcare

Trends in healthcare organizations have major impacts on health IT systems. There is a huge escalation in demand for healthcare services because of population increases and the increasing prevalence rates of chronic diseases. Moreover, there are capital pressures stemming from the requirement to do extra work and good-quality work with lesser and more costly resources and also reduced income. Expectations for improved results, good-quality treatment, and more value from the healthcare services that are provided raise the requirements for point-of-care access to medical data, and parallel evolution and adoption of mobile devices, by both medical staff and patients, are increasing the need for IT systems to become customized. Also, the major increase in digitization of health records—including greater acceptance of electronic medical records (EMRs), electronic health records (EHRs), and personal health records (PHRs), and the growing frequency of digital outputs from scanning and monitoring machines, such as magnetic resonance imaging (MRI) scanners and bedside monitors and infusers—provide more capacious and mixed digital data to take advantage of the possible advantages of cloud solutions. Healthcare provider systems deploying cloud-based computing and cloud services reap various benefits in contrast to those using domestic client–server systems, including financial, and functional advantages. The financial profit of cloud computing can be major, since cloud computing offers cost flexibility and the possibility of cost savings. Heavy asset expenses can be avoided because IT assets are acquired on demand as needed and paid for as operating expenditure. Also, the cost of the workforce required to organize and

maintain IT assets is built into the cost of cloud computing, so the need for further healthcare supplier–trained IT staff and the associated costs may be decreased when cloud services are used for IaaS and PaaS platforms, and even more so for SaaS solutions, where the cloud service provider takes on the major share of the work. From an operational viewpoint, cloud services offer elasticity and the ability to adjust to demand quickly. Cloud services can propose better security and privacy for health data and health systems. Cloud service provider data centers are normally very safe and well secured against stranger and insider threats by use of administrative, physical, and technical methods implemented and maintained by expert professional staff. Cloud services can offer sophisticated security controls, including data encryption and fine-grained access controls and access logging. Medical systems created by using cloud services can give web access to information, avoiding the necessity to save information on consumer devices. The requirement for limited IT security skills within the healthcare sector is also minimized. Cloud service providers normally function on such a level that they have all of the required IT skills, with the range of those skills being spread across many customers. Healthcare functionality can be improved by cloud-based healthcare IT systems that propose the possibility of broad interoperability and integration. Healthcare cloud services are internet based and usually use normal protocols; thus, connecting them to other systems and applications is typically simple, although EHR/EMR vendor contractual and scientific impediments continue to present a challenge. The key to sharing information simply and securely is complex potential, and cloud services are good enablers for this. Cloud services also maintain fast progress and improvements, particularly for mobile and internet of things (IoT) devices, thus meeting the demands imposed on healthcare IT systems by these new and rapidly advancing technologies. Cloud services can enable remote ways into applications and data via the internet through use of wired and wireless systems to enable access at any time from anywhere that internet connectivity can be established. Also, cloud services present the right to use to a much enhanced ecosystem of healthcare suppliers, financiers, life science entities, and IT solution buddies, all of which raise the potential for a wide variety of services to healthcare provider industries. The main difference between traditional IT and cloud services is the way of sharing responsibilities. In traditional IT, the IT organization is responsible for almost everything. With cloud services, responsibility is shared between the cloud service provider and the healthcare organization as the cloud service customer [16]. Perhaps the greatest functional advantage of healthcare cloud services is the wide range of new capabilities that they are able to propose. These services offer the chance to extend the capability on hand to health organization employees, in order to apply better ways of working and to offer new services to patients. Complicated analytical capability can be brought to bear to achieve better patient-specific and population-based appraisal and organization [17].

10.4 Cloud Computing Security

Nowadays, people are very conscious about their health; this is also the biggest business in the world. People can pay a lot of money to doctors and hospitals to save their lives. From the business point of view, this is a business whose demise will never occur. Before the availability of technology, the hospital was the only medium for provision of healthcare, but nowadays the scene has changed. Most people have adopted these services as a business, and healthcare is now provided online. This has become possible only because of cloud computing. With the help of cloud computing, companies are changing their ways of providing services, e.g., by offering online consultations with doctors or online clinics and pharmacies, with impacts on the quality of service delivery and the cost of these services. To manage these changes, two forces are applied: the first is to fulfill the business imperative to cut costs, and the second is to improve the quality of healthcare services. In the past 10 years, a large number of hospital IT departments have started to use good backup and disaster recovery (DR) tools to keep their systems and data safe and recoverable in the event of a system failure. Hospital users have always been assured that their IT staff can promise a system uptime of 99.9%. However, with the increasing use of cloud services for data protection purposes, IT must adjust to the new reality of cloud-based DR options. For this, they use DRaaS (disaster-recovery-as-a-service) [13].

The appearance of cloud computing technology with major advantages is one of the present key challenges. This is a new prototyping technology based on "pay-on-demand" for the use of information and communications technology (ICT) [18]. The National Institute of Standards and Technology (NIST) in the USA has focused on three models of cloud computing: SaaS, PaaS, and IaaS [19]. In healthcare cloud computing for internal communications, an extensive number of computers and servers are dedicated to meeting the requirements of the medical care business. Healthcare services can be delivered to users (patients or physicians) through an internet connection [20].

First, there is SaaS, where the cloud service provider provides access to particular software functions, such as table processing or email. The cloud service provider also manages any software upgrades and fixes protection problems. In PaaS, clients may have remotely accessible computing control and can run their personal applications. However, maintenance is the responsibility of the cloud providers. Finally, IaaS is a latent option. In this scenario, customers may have remotely accessible computing control, are able to run some of their own applications, and are charged for resolution of any maintenance problems. There are many advantages to using the healthcare cloud, such as allowing enclosed entities to store information off-site. Moreover, if employees need to work remotely or move from one location to another, healthcare cloud options provide them with the liberty to do so while still being able to access important and critical information [21, 22].

Additionally, this can assist organizations to reduce their operating or storage costs, update services, and devote more resources to maintenance of software, platforms, or infrastructure.

Also, it is important to note that the [US] Health Insurance Portability and Accountability Act (HIPAA) compilation rule requires patient data to be well protected, regardless of where it is stored. Organizations that are working as contractor firm and do not necessarily analyze the data on a normal basis must adhere to HIPAA rules. This particular system records every access attempt by the username and include the date, time, relationship to the patient, etc. Still, more research work is required in this field to increase the security of patient data and users' trust levels [16, 23].

Cloud computing has some major security issues. Because they have only limited cybersecurity resources, many healthcare service providers have become vulnerable to various attacks and have attracted cybercriminals [24]. Cloud computing has a similar name to internet computing. How safe are our data? Data security is the biggest concern in cloud computing. Reliability, authentication, availability, and integrity are different aspects of data security. Reliability is related to trust in computing. How we can trust cloud computing when we are not there? A person should not share his or her data over the cloud if he or she is not comfortable with the internet. Besides reliability there are many other security concerns in cloud computing, such as authenticity, data locality, licensing security, and physical damage. In the next section we discuss some of these security issues with their previously proposed solutions. Here, we define the major security concerns for any type of computing [25].

1. *Authentication*: Authentication is the process of confirming the truth about an entity or a piece of data. Authenticity is a phenomenon that allows users to use particular services.
2. *Confidentiality*: Confidentiality means a set of rules that restrict access to some information to certain individuals.
3. *Integrity*: Integrity in terms of cloud security is the assurance that only authorized or authenticated users can access or modify the data.
4. *Availability*: Availability, in the context of a computer system, means the ability to access data, information, or resources in an appropriate format. It must be ensured by the storage, which may be local or at an off-site facility.
5. *Nonrepudiation*: This means that neither the sender nor the receiver can deny the validity of the data or information.

The above are the major security concerns in any type of computing. All issues related to cloud computing refer to one of the above security concerns. In cloud computing there are three components: SaaS, PaaS, and IaaS.

10.5 Methods of Cloud Security

On one side, the job of cybercriminals is to steal confidential data. On the other side, researchers and security experts propose the architecture needed to make data secure in the cloud.

Multitenant Platform This healthcare cloud platform has been published in a paper by Oh et al. [13]. This healthcare SaaS platform (HSP) provides an easy-to-use, cloud-based, modular EHR system. In this architecture, the functional and software analysis of an HSP has been designed in a layered architecture. Exterior systems can interface with the HSP by using the Simple Object Access Protocol (SOAP) and Representational State Transfer/JavaScript Object Notation (REST/JSON). The multitenancy model of the HSP is designed as a shared database, with a different schema for each tenant through a single application, although healthcare data can be physically located in the cloud or at a hospital, depending on regulations. The Consumer Directed Services (CDS) services are categorized into rule-based services for medications, alert registration services, and knowledge services. The above process of multitenant architecture is depicted in Fig. 10.3.

How to protect the data Protection of critical patient information and medical records is one of the most basic duties of the healthcare industry and one of the most firmly regulated. To defend data as they move in and out of the cloud requires data

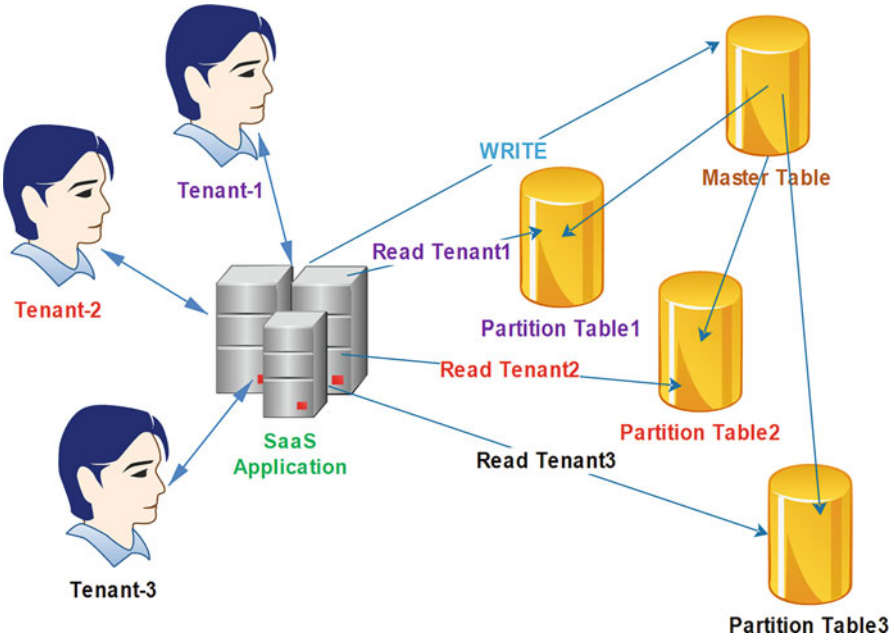

Fig. 10.3 Multitenant storage model

encryption, which makes the data unusable if they are compromised. It also demands safe communication connections, which limit browser access and encrypt content as it is moved over the network and throughout the cloud. However, data encryption based on the Advanced Encryption Standard (AES) algorithm is very compute intensive. This type of software-based encryption relies on compute-intensive algorithms that can impact the performance of the computing network, particularly when used pervasively to protect the massive volumes of information that pass to and from the cloud. Traditional encryption solutions can create computing logjams due to high performance overheads, making them less than optimal for protecting cloud data traffic. Intel has worked to mitigate these performance penalties [26].

How to provide security against unauthorized access Realizing cloud computing advantages while meeting stringent requirements for data security and compliance requires hardening of the underlying platform, including the hardware, software, and process methodologies. Better securing of both server and client platforms helps safeguard cloud infrastructures, and better management of identities and access control points at the network edges helps ensure that only authorized users can enter the cloud. With malware attacks now moving beyond software to target the platform, organizations face new risks from rootkit and other low-level exploits that can infect system components such as hypervisors and the BIOS to quickly spread throughout the cloud environment.

Protection of identity in the cloud Protection of identity on a cloud platform begins with managing who has access to it. Identity protection devices (such as Intel® IPT) provide a simple way for healthcare organizations to validate that legitimate employees or approved users are allowed in from a trusted device. IPT offers token generation incorporated into the hardware, which gets rid of the need for (and cost of) a different physical token. It also confirm transactions and protects against malware [27]. Figure 10.4 explains the extra security layer in the healthcare cloud. Any user who wants to access a cloud application first needs to enter his or her credentials (username and password) on the identity protection system and then receives a one-time password (OTP) on his or her registered cell phone or email address. Only if both are correct will the identity protection system allow that user to access the cloud.

Protection of API keys Application programming interfaces (APIs) are the fundamental method used for exposing cloud applications to third parties and mobile services. A hacker tries to break these API keys for unauthorized access. Many researchers and scientists have suggested algorithms to protect API keys [28].

10.6 Security Threats in the Healthcare Cloud

Healthcare organizations have always struggled with information security. Because the healthcare industry stores massive volumes of critical data and is subject to strict compliance rules, it must make security its primary concern. Therefore, the

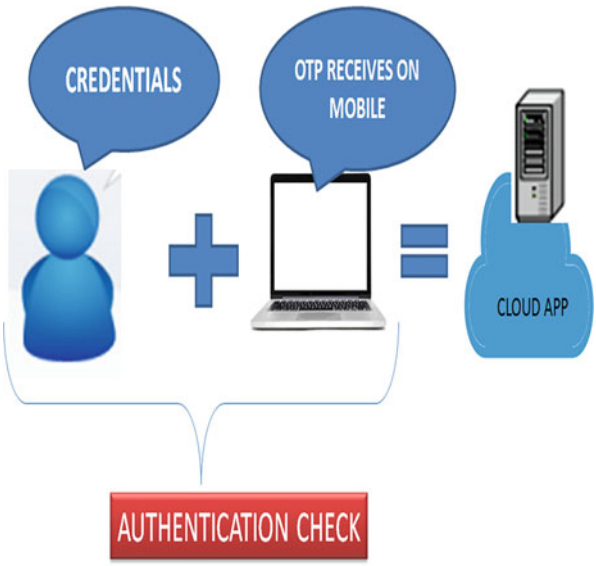

Fig. 10.4 Identify protection in the cloud

industry has long been doubtful about new technologies that could put data at risk, including cloud technologies. Cloud computing poses many risks to data security, data confidentiality, and overheads because of the huge volumes of data involved. Data processed in the cloud are highly confidential, such as business records, patient records, military records, etc. Therefore, proper encryption standards and architecture must be applied to secure sensitive data against tampering [29].

However, everything changes, and the healthcare industry is changing as well. In January 2018, an important decision was made: the National Health Service (NHS)—the largest healthcare provider in the UK—officially approved the use of US-based cloud providers to store patient data. According to the *2018 Netwrix Cloud Security In-Depth Report*, 84% of healthcare organizations already store data in the cloud, but the NHS is the first state healthcare organization to give the go ahead [4, 22, 29].

Here, we discuss some of the major security risks in the healthcare cloud.

Malware and viruses Malware and viruses are being developed continuously, and ransomware (a type of malware that, once it has taken over the computer, threatens harm) is one of the most frequent sources of attack. According to one report, a company is targeted by ransomware every 40 seconds. Malware—such as NotPetya, WannaCry, and Locky, in particular—has spread among healthcare providers. Even the NHS itself has been targeted by WannaCry: the attack resulted in disruptions at 37% of NHS organizations and cancellation of many appointments and surgeries. Although the NHS did not pay the ransom, it did incur extra costs to cover cancelled appointments, hire IT consultants, and restore data and systems after the attack, besides incurring damage to its reputation. Unsurprisingly, nearly 61% of healthcare organizations are reportedly worried about malware and the threat of unauthorized access [30].

Identity protection and access management Unauthorized access is the biggest challenge in all types of cloud computing. This is a major security issue throughout the world and a huge challenge in healthcare cloud computing. Many researchers and IT industry developers are working to resolve this issue. According to a Netwrix survey in January 2018, 68% of unauthorized access security concerns are related to the healthcare cloud. This is the biggest security issue. Existing organizational identification and authentication frameworks may not expand into the cloud, and if these are based on unique username–password combinations for individual applications, they can be a weak link in the security chain. In the cloud, identity management helps to preserve security, visibility, and management, and centralization of IT control of identities and access is useful.

Data encryption Data saved in the cloud usually reside in a multitenant environment—a distribution virtualized server space—with data from other clients of the cloud provider. Healthcare entities that move critical and synchronized data into the cloud must make sure the data are encrypted at rest and in transit. One of the main risks of multitenancy and shared computing resources within cloud infrastructures is possible failure of the separation instrument that provides separation of memory, storage, and routing between tenants.

Data compliance regulations Security laws and regulations vary at national, regional, and local levels, making fulfillment a potentially complex issue for cloud computing. For example, some countries in the European Union (EU) stipulate that some health data must never cross those countries' own borders. Other authorities have detailed data compliance regulations that stipulate special handling of certain kinds of health information (medical treatment of minors, disease history, etc.), controlling transmission across local or state borders. To comply with these strict data privacy laws, cloud infrastructures must be auditable for such features as encryption, security controls, and geometric location.

Illegal activities of IT staff Although it seems strange, employees have been identified as a security threat. Only 21% of healthcare industries have a complete perception of what their IT staff members are doing in the cloud, and visibility of the actions of business users is even rarer. Actually, the overall visibility of inner actors is the lowest among all organizations surveyed. IT people are aware of this difference, but the majority of them do not get essential support from the C-level to address it. Only 50% of respondents say that they get top management support to implement cloud security projects; this is the lowest outcome across all businesses surveyed.

Human error This is also one of the biggest security threats; with just one small mistake, the industry can lose billions of dollars within a second. According to Verizon's *2016 Breach Investigations Report*, healthcare data breaches in 2015 were most likely to be caused by human error or unintentional error in the form of stolen or lost assets, insider and privilege misuse, and miscellaneous errors, such as improper device disposal or mishandling.

Detailed above are some of the common threats that are spreading in the healthcare cloud. The healthcare cloud also contains massive volumes of data. Thus, the healthcare industry is worried about protecting these data. The HIPAA and public health authorities (PHAs) have issued regulations to secure data in the healthcare cloud. In the next section we describe some methods by which the healthcare industry can save its data in the cloud.

10.7 Secure Healthcare Cloud Architecture

From past studies it has become clear that a large number of cybercriminals are targeting the healthcare cloud. The reason behind this is that it is the most crucial cloud and can generate a terabyte of data in a single day. Also, people are less vigilant about security of health information than about the security of banking or other organizations' information, so this cloud is the easiest target for hackers. However, in recent years, researchers have worked to ensure that data in the healthcare cloud are censured and have proposed some architecture. Some of these architectures are explained in this chapter.

The architecture proposed by Chondamrongkul and Chondamrongkul is very similar to our method. This supports a healthcare system that allow patients to be checked by mobile applications. A personal record application helps gather health data from secure mobile cloud architecture for linked wearable devices and cell phones, before saving them in the cloud. After that, a monitoring application retrieves these data to enable doctors and other relevant medical staff to supervise the patient's condition [31].

Zhang and Liu have presented a paper in which they discuss EHR sharing and integration in healthcare and analyze arising security and privacy issues in access to and management of EHRs [14].

In 2013, Khan and Wan proposed an architecture to make data secure in the healthcare cloud. In this work they introduced a trusted authority between the cloud and the user. When any user want to access the healthcare cloud, it must be passed by the trusted authority, which is usually linked to the private key store. They gave a review of the wireless body area network (WBAN). They provided an outlook on this promising field and discussed a cloud-enabled WBAN architecture for pervasive healthcare systems. This system can be accessed by smart phones with an enabled Wi-Fi connection or something similar [20].

10.8 Our Architecture

We have obtained help from big data to solve this issue. In our architecture to store the data, there are some slave nodes and a master node. A slave node is responsible for storing data, while a master node stores metadata. If anyone wants to store or

process the data, than he or she must submit a request to the master node. The master processes that request and sends it to the appropriate node. All customer information can be accessed by the sensors, meaning that the system is very easy to use and it is easy to generate quasistructured data. All of these data must be in an encrypted form. This design security scheme is based on public key infrastructure (PKI) and the RSA [Rivest–Shamir–Adleman] algorithm, ensuring that only authorized users can access a particular patient's data at a certain time. There are two types of data storage in the cloud: master storage and slave storage. The master storage holds metadata, and the slave storage holds electronic patient records (EPRs) and consists of medical and health data. The master storage can be accessed through the data access service (DAS) containing the REST service for the application client. The master storage holds the EPR, which is encrypted with the patient's public key so that only the personal record application on the patient's device can decrypt it with the patient's own private key. The proxy storage holds the EPR as it is requested by the monitoring application. The EPR's metadata in the master storage are encrypted with the public key of those who request and have permission to access it, then it is signed by the patient's private key for integrity and authenticity checks. Once a doctor or medical staff member retrieves the EPR using the monitoring application, he or she verifies the EPR using the patient's public key to prove its authenticity, before decrypting it with his or her own private key [2]. Figure 10.5 illustrates our proposed architecture. All requests will go on the master where the metadata will be located. After that, the master system will send the request to the slave and the slave will respond to the master again. One master can easily manage many slaves.

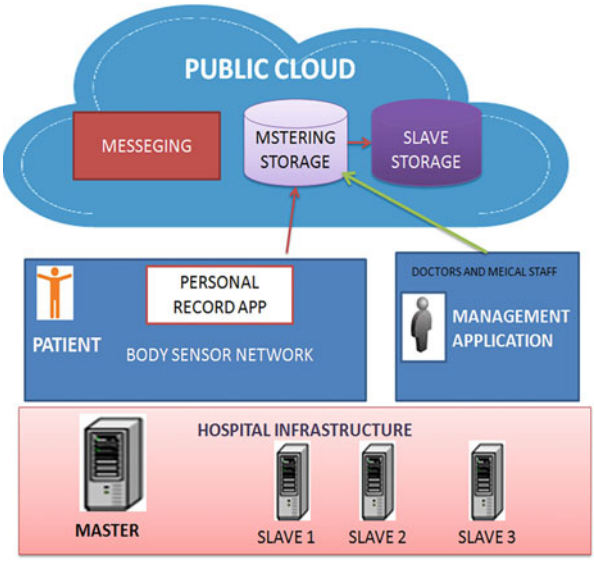

Fig. 10.5 Secured architecture for the healthcare cloud

10.8.1 Results

The messaging between users and the cloud's server occurs on the Secure Sockets Layer (SSL), which ensures the privacy and integrity of message sending and receiving between two parties. But the public server is consider nonliable as it is operated and preserved by the cloud provider company. The cloud provider has no legal right to access information belonging to the user. There is, however, a potential risk that a cloud-based server could be attacked by a malicious program, which could cause unauthorized data access. The security scheme offers fine-grained access management of encrypted data in the cloud. Furthermore, it also ensures the integrity and authenticity of messages transferred through the cloud between the patient and the doctor. Throughout this chapter we use Ω (a, b) → c to denote the operation of running an algorithm Ω with inputs a, b, ... and output c [27].

The key manager generates key pairs and keeps and provides public keys for different users involved in the application system. The access control contains policies that enable personal record applications to validate who can access which patient's data at what level (e.g., pulmonology doctor has read-write access to data on patients with lungs disease, while nurses have only read access). The patient can supervise the access policy on his or her records to take full access control of his or her own data. In a critical situation, that control policy can be overridden other medical staff for a short time. The hospital information system (HIS) is integrated into our organization to provide patients' health records. The key manager, access control, and HIS are hosted by the hospital infrastructure to minimize safety risks. The messaging service on the cloud support sends a notification when access to the EPR is requested or when the latest updated data are available in proxy storage [28].

The EPR has two parts:

1. *Health data*, which are quasistructured data and come from sensors.
2. *Medical data*, which come from the medical staff's personal information, such as their ID, name, etc. When we need to use the record application, a new patient is registered on this system. We can understand what happens in the background during registration, as follows:

   (a) The key manager executes KeyGen() → (Private[P], Public[P]) to generate a key pair for the patient, using the RSA algorithm. Here, P stands for "patient."
   (b) Private [P] is securely stored on the patient's system using the AES algorithm to protect authentication.
   (c) The EPR is loaded from the HIS and encrypted with Encrypt(KEY, Public[P], Tn) → KEYPublict[P], where T represents the data attribute of a vital sign and n is the number of attributes to be encrypted.
   (d) KEYPubP is saved in the master storage through the DAS.
   (e) Finally, the master processes these data, normalizes them, classify them, and sends them to the slave for storage.

For retrieving the data, our proposed architecture will request the credentials by using the visualizing application. The visualizing application supports direct access application (DAA) for an authorized person by which he or she can retrieve the EPR. This DAA is used to decrypt the information, using the public key. If the permission is verified, the following steps will be executed:

1. *Decrypt* (KEYPublic[P], Private[P], Tn) → KEY to decrypt the EPR retrieved from the master storage. Then the master will search for these data in the slave to get the data.
2. *Encrypt* (KEY, Public[R], Sn) → KEYPublic[R] to encrypt with the requester's public key. Here, R stands for the user who is using this application.
3. *Sign* (Private[P], T) → TPrivate[P] to sign a generated hash key denoted by T with the patient's private key to ensure the authenticity of the EPR before sending it together with KEYPublic[R] to the slave storage.

10.9 Conclusion

From the discussion in this chapter, one can easily understand healthcare security issues, healthcare responsibility, and how we can secure our information in the healthcare cloud. With time, we can modify our architecture to make data more secure in the healthcare cloud. Therefore, use of cloud computing in healthcare systems makes health services more affordable, as well as helping nations to achieve health equity. In this chapter, cloud computing and the healthcare cloud have been introduced. Furthermore, cloud computing security issues, particularly in the context of the healthcare cloud, have been presented. This chapter has also proposed and discussed some methods to improve cloud security for healthcare along with our proposed architecture.

References

1. Kim, H., Lee, H., Kim, W., Kim, Y.: A trust evaluation model for QoS guarantee in cloud systems. Int. J. Grid Distrib. Comput. **3**, 125 (2010)
2. Yang, Z., et al.: A collaborative trust model of firewall-through based on cloud computing. 14th International Conference on Computer Supported Cooperative Work in Design, 2010, China
3. Ahmed, M.: Above the trust and security in cloud computing: a notion towards innovation. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, Australia
4. Brodkin, J.: Gartner: Seven cloud-computing security risks, InfoWorld, 2008. https://www.infoworld.com/article/2652198/security/gartner%2D%2Dseven-cloud-computing-security-risks.html. Accessed 15 July 2018
5. Chen, D., Zhao, H.: Data security and privacy protection issues in cloud computing. Int. Conf. on Comput. Sci. Elect. Eng. **1**, 647–651 (2012)
6. Grobauer, B., Walloschek, T., Stocker, E.: Understanding Cloud Computing Vulnerabilities. IEEE Secur. Priv. Mag. **9**(2), 50–57 (2011)

7. Altowaijri, S., Mehmood, R., Williams, J.: A quantitative model of grid systems performance in healthcare organisations. Int. Conf. on Intellig. Syst. Model. Simulat. Liverpool, United Kingdom, pp. 431–436 (2010)
8. Mehmood, R., Faisal, M.A., Altowaijri, S.: Future networked healthcare systems: a review and case study. Handbook of research on redesigning the future of internet architectures, pp. 531–558, (2015)
9. Alazawi, Z., Alani, O., Abdljabar, M.B., Altowaijri, S., Mehmood, R.: A smart disaster management system for future cities. Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart cities - WiMobCity'14, Philadelphia, Pennsylvania, USA, 2014, pp. 1–10
10. Alazawi, Z., Abdljabar, M.B., Altowaijri, S., Vegni, A.M., Mehmood, R.: ICDMS: An Intelligent Cloud Based Disaster Management System for Vehicular Networks. In: Vinel, A., Mehmood, R., Berbineau, M., Garcia, C.R., Huang, C.-M., Chilamkurti, N. (eds.) Communication Technologies for Vehicles, vol. 7266, pp. 40–56. Springer, Berlin, Heidelberg (2012)
11. Alazawi, Z., Altowaijri, S., Mehmood, R., Abdljabar, M.B.: Intelligent disaster management system based on cloud-enabled vehicular networks. In 2011 11th International Conference on ITS Telecommunications, St. Petersburg, Russia, pp. 361–368 (2011)
12. Mehmood, R., Alam, F., Albogami, N.N., Katib, I., Albeshri, A., Altowaijri, S.M.: UTiLearn: A Personalised Ubiquitous Teaching and Learning System for Smart Societies. IEEE Access. **5**, 2615–2635 (2017)
13. Oh, S., et al.: Architecture Design of Healthcare Software-as-a-Service Platform for Cloud-Based Clinical Decision Support Service. Healthc. Inform. Res. **21**(2), 102 (2015)
14. Zhang, R., Liu, L.: Security models and requirements for healthcare application clouds. 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, pp. 268–275 (2010)
15. Wan, J., Zou, C., Ullah, S., Lai, C.-F., Zhou, M., Wang, X.: Cloud-enabled wireless body area networks for pervasive healthcare. IEEE Netw. **27**(5), 56–61 (2013)
16. Barton, J., et al.: Impact of cloud computing on healthcare V2.0| Object Management Group. https://www.omg.org/cloud/deliverables/impact-of-cloud-computing-on-healthcare.htm. Accessed 29 June 2018
17. Ahmed, M., Xiang, Y., Ali, S.: Above the trust and security in cloud computing: a notion towards innovation. In 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, pp. 723–730 (2010)
18. Bildosola, I., Río-Belver, R., Cilleruelo, E., Garechana, G.: Design and Implementation of a Cloud Computing Adoption Decision Tool: Generating a Cloud Road. PLoS One. **10**(7), e0134563 (2015)
19. Balasubramaniam, S., Kavitha, V.: Geometric Data Perturbation-Based Personal Health Record Transactions in Cloud Computing. Sci. World J. **2015**, 1–9 (2015)
20. Elizabeth, S.: HealthITSecurity, data security considerations in healthcare interoperability. HealthITSecurity. https://healthitsecurity.com/features/data-security-considerations-in-healthcare-interoperability. Accessed 24 June 2018
21. Saurabh: Security issues in cloud Computing. http://serl.iiit.ac.in/cs6600/saurabh.ppt. (2009). Accessed 17 June 2018
22. Sherry, D.: Cloud computing: security risks and compliance implications. http://media.techtarget.com/searchFinancialSecurity/downloads/FISD09_Breakout_Session5_ CloudComputing_Sherry.pdf, Brown University (2009). Accessed 14 June 2018
23. Ryoo, J., Rizvi, S., Aiken, W., Kissell, J.: Cloud Security Auditing: Challenges and Emerging Approaches. IEEE Secur. Priv. **12**(6), 68–74 (2014)
24. Kwon, J., Johnson, M.E.: Protecting patient data-the economic perspective of healthcare security. IEEE Secur. Priv. **13**(5), 90–95 (2015)
25. Schoo, P., et al.: Challenges for cloud networking security. In Mobile Networks and Management, 2011, pp. 298–313
26. Yang, Z., Qiao, L., Liu, C., Yang, C., Wan, G.: A collaborative trust model of firewall-through based on Cloud Computing. The 2010 14th International Conference on Computer Supported Cooperative Work in Design, Shanghai, China, pp. 329–334 (2010)

27. Goyal, S.: 5 reasons why you should choose multi-tenant architecture for your SaaS application. Insights—Web and Mobile Development Services and Solutions, https://www.netsolutions.com/insights/5-reasons-why-you-should-choose-multi-tenant-architecture-for-your-saas-application/. Accessed 11 July 2018
28. Shaikh, R., Sasikumar, M.: Security Issues in Cloud Computing: A survey. Int. J. Comput. Appl. **44**(19), 4–10 (2012)
29. Rathi, G., Abinaya, M., Deepika, M., Kavyasri, T.: Healthcare data security in cloud computing. IJIRCCE, 3(3), (2015). ISSN(Online): 2320-9801 ISSN (Print): 2320-9798
30. Almond, C.: A practical guide to cloud computing security, (2009). http://www.avanade.com/Documents/Research%20anad%20Insights/practicalguidetocloudcomputingsecurity574834.pdf. Accessed 11 July 2018
31. Chondamrongkul, N., Chondamrongkul, P.: Secure mobile cloud architecture for healthcare application. Int. J. Fut. Comput. Commun. **6**(3), 77–86 (2017)