# HealthyBroker: A Trustworthy Blockchain-Based Multi-Cloud Broker for Patient-Centered eHealth Services

*electronics*

MDPI

*Article*

# HealthyBroker: A Trustworthy Blockchain-Based Multi-Cloud Broker for Patient-Centered eHealth Services

**Heba Kurdi [1,2,*], Shada Alsalamah [3,4], Asma Alatawi [1], Sara Alfaraj [1], Lina Altoaimy [5] and Syed Hassan Ahmed [6]**

1 Computer Science Department, King Saud University, Riyadh 12371, Saudi Arabia; asmasuliaman@outlook.com (A.A.); s.alfaraj@psau.edu.sa (S.A.)
2 Mechanical Engineering Department, Massachusetts Institute of Technology (MIT), Cambridge, MA 02139, USA
3 Information Systems Department, King Saud University, Riyadh 12371, Saudi Arabia; shada@mit.edu
4 Media Lab, MIT, Cambridge, MA 02142-1308, USA
5 Information Technology Department, King Saud University, Riyadh 12371, Saudi Arabia; laltoaimy@ksu.edu.sa
6 Computer Science Department, Georgia Southern University, Statesboro, GA 30460, USA; sh.ahmed@ieee.org
* Correspondence: hkurdi@ksu.edu.sa; Tel.: +966-11-805-9637

Received: 22 March 2019; Accepted: 23 May 2019; Published: 29 May 2019


**Abstract:** Delivering electronic health care (eHealth) services across multi-cloud providers to implement patient-centric care demands a trustworthy brokering architecture. Specifically, such an architecture should aggregate relevant medical information to allow informed decision-making. It should also ensure that this information is complete and authentic and that no one has tampered with it. Brokers deployed in eHealth services may fall short of meeting such criteria due to two key behaviors. The first involves violating international health-data protection laws by allowing user anonymity and limiting user access rights. Second, brokers claiming to provide trustworthy transactions between interested parties usually rely on user feedback, an approach vulnerable to manipulation by malicious users. This paper addresses these data security and trust challenges by proposing HealthyBroker, a novel, trust-building brokering architecture for multiple cloud environments. This architecture is designed specifically for patient-centric cloud eHealth services. It enables care-team members to complete eHealth transactions securely and access relevant patient data on a "need-to-know" basis in compliance with data-protection laws. HealthyBroker also protects against potential malicious behavior by assessing the trust relationship and tracking it using a neutral, tamper-proof, distributed blockchain ledger. Trust is assessed based on two strategies. First, all transactions and user feedback are tracked and audited in a distributed ledger for transparency. Second, only feedback coming from trustworthy parties is taken into consideration. HealthyBroker was tested in a simulated eHealth multi-cloud environment. The test produced better results than a benchmark algorithm in terms of data accuracy, service time, and the reliability of feedback received as measured by three malicious behavior models (naïve, feedback isolated, and feedback collective). These results demonstrate that HealthyBroker can provide care teams with a trustworthy, transparent ecosystem that can facilitate information sharing and well-informed decisions for patient-centric care.

**Keywords:** eHealth services; patient-centered care; trust management; cloud computing; broker; blockchain technology

## 1. Introduction

Modern health care employs emerging technologies such as cloud computing and blockchains to improve patient safety, health outcomes, service efficiency, and delivery models. Such efforts are dedicated to ensuring continuity of care in all services, including diagnostic, primary, and emergency care. Electronic health care (eHealth) is a modern health care delivery model defined by WHO (World Health Organization) [1] as "the use of information and communication technologies (ICT) for health." The model is deployed to help implement the holistic patient-centered care (also called "shared care") that comprises the core of modern health care services [2,3]. Patient-centered care puts patients at the heart of health care services provided based on shared, informed decision-making [3]. Services may include diagnostic, primary, preventative, rehabilitative, emergency, long-term, hospital, palliative, and home care. Patient-centered care enables clinicians to work with care teams to best tailor the services needed for a patient's anticipated integrated-care pathway. This care requires, however, relevant medical information and data to flow seamlessly among and across health care settings. One obstacle to this is that discrete legacy heterogeneous information systems are not designed to share information across hospitals [3].

Today, however, advances in cloud-computing capabilities have been widely incorporated in health care services to facilitate collaborative patient-centered care. According to [4], cloud-computing is a key solution for addressing eHealth interoperability problems due to its ability to increase information accessibility, availability, and reliability across organizations. Cloud computing also enables easy information sharing and collaboration among care teams from multiple service providers [4,5]. Although the benefits have motivated health care providers to use multi-cloud eHealth services to allow for informed decisions [4,5], this raises information security, privacy, and trust concerns [4,5] related to complying with health-data-protection regulations [3]. In this environment, delivering eHealth services across multiple cloud providers demands a reliable, trust-aware, cloud-based brokering architecture that complies with applicable data-protection laws and ensures that patient information is complete, authentic, and unsullied. Not having an architecture with this level of security can deprive health providers of consortium and, more importantly, create life-threatening situations for patients should treatment decisions be based on invalid information [1,3].

Cloud-based brokering systems, which manage and ensure the delivery of cloud services, empower users by enabling them to deploy virtual infrastructures across cloud systems through intermediation and aggregation capabilities. In addition, such systems allow users to negotiate resource allocation among multiple sites [6]. Accessing health care information is crucial and challenging. It requires integrating the information collected by various independent health-service providers in a large eHealth cloud. Such a cloud can facilitate the medical information exchange between care services at geographically distributed settings. It should achieve this at reasonable prices while maintaining a high quality of service to all end users. Unfortunately, integrating various health care cloud services can be complex and difficult to manage. One solution for this is using a multi-cloud broker that can fulfill information requests from end users without them having to interact directly with single cloud providers [7]. Multi-cloud brokers can also facilitate integration among several clouds, ensure cloud portability between different cloud vendors, improve continuity of services, and increase service level agreement (SLAs) by diversifying and leveraging multi-cloud providers.

The existing literature is limited in terms of discussing cloud brokering solutions that can enhance patient-centered eHealth services. Many of the cloud service-brokers [8–10] reported on were designed as general solutions for domain-neutral applications and thus do not suit modern health care scenarios. These brokering systems would violate international "need-to-know" [3] health-data-protection laws because they allow anonymous users to engage in random service and information exchanges. This puts patient information at great risk for improper disclosure [3,11]. It also does not allow care-team members to identify the information source or the treatment point associated with the information. In order for a care team to follow a patient's care plan, they require access to information collected at each care point along the care pathway. In these instances, care-team members can be service providers at

one treatment point and service consumers at another point. The brokering systems described here do not enable this role exchange.

Furthermore, while some researchers have proposed solutions to assess and manage service trustworthiness [6,12–14], their approach is vulnerable to users who lie when rating the quality of service (QoS) they received against the SLA. These users can work individually or collectively to harm specific users or an entire system. Therefore, brokering systems need an additional layer of transparency that promotes consensus among care teams and guarantees their mutual trust. This layer should track health care service transactions, monitor QoS, and audit user feedback for credibility. This approach will detect malicious user feedback and help decrease malicious attacks.

One technology that can help brokering systems achieve these goals is the blockchain technology used to build trust-worthy ecosystems for distributed environments [15]. More specifically, blockchain is "a peer-to-peer distributed ledger technology for a new generation of transactional applications that establishes transparency and trust" [16] in which the ledger contains the digitally tracked asset transactions of a group of networked peers [15]. Compared to other cryptography-based solutions, blockchain uniquely provides a transparent tamper-proof trail of time-stamped block sequences that are algorithmically self-policed to support secure, private, and indelible transactions. This technology can prevent malicious user feedback in health care services by tracking user credibility and sharing that information with all care-team members in the ecosystem. This would fill the security and transparency gap in traditional multi-brokering systems and meet the security requirements of modern eHealth services.

To summarize, modern eHealth collaborative environments require multi-cloud brokering architectures that can identify care-team members and allow them to act as providers and consumers as needed based on a patient's treatment plan. eHealth brokering systems also need to establish trust and transparency among the care-team members by auditing service transactions and feedback. With that need in mind, this paper proposes HealthyBroker, a novel, trust-building multi-cloud broker specifically tailored to improve patient safety, health outcomes, service efficiency, and care delivery models. As designed, HealthyBroker provides care teams with an ecosystem that facilitates timely, transparent, and trustworthy sharing of critical medical information.

The remainder of this paper is organized as follows. Section 2 gives an overview of related work. Section 3 provides a general overview of the proposed model. The system architecture is outlined in Section 4. Section 5 describes the methodology used in the study. Experimental results are presented in Section 6 and, finally, conclusions are drawn in Section 7 along with suggestions for future work in this area.

## 2. Related Work

Considerable literature exists that investigates cloud brokering services and trust management in cloud environments. We summarize some relevant approaches here. For instance, the EigenTrust algorithm [12] uses individual user upload histories to generate a trust value for that user in peer-to-peer file-sharing networks. Following this approach, the system can identify malicious users and isolate them to minimize harm. In [17], a hardware security module is presented to prevent cloud administrators from tampering with the security of guest virtual machines. The private cloud monitoring system (PCMONS) [14] was developed as a modular monitoring system for private clouds. Basically, it gathers and prepares information relevant for data visualization and can be integrated with other cloud management toolkits such as Nagios [9]. The optimized infrastructure services (OPTIMIS) scheme, introduced in [8] for private clouds, allows interaction with a rich ecosystem of public clouds and many cloud providers. OPTIMIS can identify, capture, and codify a "picture" of an optimized cloud ecosystem driven by trust, risk, eco-efficiency, and cost. Its framework supports deployment and runtime decisions based on prior evaluation of providers. As another example, the architecture in [18] can build a cloud infrastructure from volunteer resources shared by their owners. On top of the infrastructure, an extra layer is added to provide QoS and SLA and eliminate unreliable,

intermittent cloud providers. In [19], a reputation-based, trust-supporting framework is introduced. It includes a coherent, adaptive trust model for quantifying and comparing the trustworthiness of peers based on transactions from a feedback system. It introduces three trust parameters (user feedback, total transactions, and credibility of feedback sources), along with two adaptive factors (transaction context factor and community context factor). It combines these factors to compute a general trust metric. T-Broker [6] is a trust-aware service-brokering scheme proposed for multi-cloud environments. T-Broker implements a hybrid and adaptive trust model that calculates the overall degree of trust using the maximum deviation method to compute the direct trust (first-hand trust) of service resources. This can overcome some traditional trust model limitations in which the trusted attributes are judged subjectively. T-Broker uses the lightweight trust feedback algorithm [6] for trust computation. Lightweight collects locally generated user feedback and aggregates it to yield global evaluation scores for future transactions based on Equation (1):

$$Lightweight = \frac{P+1}{P+N+2} \tag{1}$$

where $P$ is the number of positive ratings and $N$ is the number of negative ratings. The lightweight trust algorithm [6] involves simple arithmetic operations and a counting operation. Therefore, it was used as a benchmark for our system.

The blockchain technology described earlier is gaining increasing attention as a way to track reputation in a distributed environment [20]. For example, it was used in [20] to build a reputation-aware solution that can track cache content in a vehicular environment. This solution uses blockchain to ensure reputation and enhance trust between provider and consumer (in this case, cache stores and consumer vehicles). However, it has not been applied to multi-cloud brokers or eHealth applications.

The authors in [21] introduced a deep-learning-based methodology for monitoring critical infrastructures using restricted boltzmann machine-based clustered intrusion detection system (RBC-IDS). The RBC-IDS technique classifies intruders from sensory data collected from wireless sensor networks (WSNs). However, the overhead computation cost is high.

An IoT-based health care monitoring system has been proposed in [22]. Its aim is to provide home-based health care monitoring. Based on the results, the system efficiently monitored patient symptoms remotely and in real time. However, the authors did not consider the security and trust issues regarding the exchanged patient data.

In [23], the authors introduced a framework that provides a secure cloud service for smart connected vehicles in a smart city. The authors proposed the use of a deep-belief network and decision tree for intrusion classification. The results showed the system's accuracy to be 99.92%, which is very high.

The authors in [24] proposed using the clustered hierarchal hybrid-intrusion detection system (CHH-IDS) to ensure that WSNs used in smart grid applications operate in secure environments. The simulation was run on real datasets, and the accuracy improved when using random forest.

Although most of the above solutions are general and do not apply to health care, the authors in [25–28] propose solutions that are tailored specifically for modern health care services by managing resources or controlling access to shared data. In [25], the authors designed and deployed a sensor medium access control-based model to control access to epilepsy patients' monitoring systems. Resources were managed in [26] by developing a smart health care framework, while authors in [28] built a smart health care reward model for resource allocation in a smart city. The authors in [27] helped with the early detection and prediction of cancer patients by designing a secure health care data-system architecture. However, although such solutions were tailored for health care services, some were limited to resources relevant to specific health services (like epilepsy care services for example). Moreover, they are vulnerable to malicious users as no mechanisms were deployed to achieve trustworthiness and transparency.

The main drawback of all the previously reviewed systems is that they do not check the credibility of incoming feedback to identify malicious users. In contrast, [13] introduces CloudArmor as a decentralized reputation-based trust management framework designed to deliver "trust as a service" (TaaS). This goal is achieved by spanning various distributed nodes so that users can provide their feedback or inquire about the trust results. CloudArmor measures the credibility of trust feedback to protect cloud services from malicious users.

Based on the above literature survey, it appears that existing brokering models for cloud computing have two main limitations. First, all except CloudArmor [13] rely on directly monitoring information or feedback from users without evaluating feedback credibility. Second, they fail to consider the particular needs of patient-centered care in modern eHealth services. Modern eHealth services require architectural models that can bridge this gap by offering a service broker for multi-cloud environments that can identify care-team members, grant them access to anticipated treatment points and patient data on a "need-to-know" basis, prevent malicious user behavior, and ensure the service's trustworthiness.

## 3. System Overview

Sharing patient information is fundamental to successfully operating a health care system. The right information must be seamlessly accessible to the right care team member at the right time across discrete heterogeneous parties in various health care settings [29,30]. HealthyBroker achieves this by proposing a multi-cloud eHealth service broker architecture that allows care-team members to provide and consume cloud services on a "need-to-know" basis. Such services are related to the integrated care pathways in generic health care settings and include, among others, diagnostic, primary, preventative, rehabilitative, emergency, long-term, hospital, palliative, and home care. At the core of this system is a virtual cloud-based electronic patient record, as illustrated in Figure 1. The storing, accessing, and processing of these records should only be done by trustworthy care team members. For example, when a patient follows an anticipated care pathway that implements a treatment plan, a care team member collects information during a treatment point using HealthyBroker. To ensure care continuity, once the patient moves to the next treatment point, another care team member caring for this patient uses HealthyBroker to request access to relevant information previously recorded. Additionally, HealthyBroker maintains care provider's ownership to information collected locally and even after sharing using blockchain technology. However, this information still needs to be shared among trusted care team members, and therefore, HealthyBroker ensures trust by assessing and tracking it using a neutral tamper-proof distributed blockchain ledger. Trust is assessed among team members based on two factors: meeting the QoS in the SLA, and the care team's feedback on exchanged services. The service transactions and user feedback are tracked and audited in the immutable distributed ledger that provides a tamper-proof trail of block sequences across service providers and users. To accomplish this, HealthyBroker mandates that each user provide positive or negative feedback on his/her last service transaction based on the SLA. However, only feedback coming from trusted parties (with QoS matching SLA) is taken into consideration. The total of all trusted feedback values (positives and negatives) of a specific user is used to calculate the user's reputation, as shown in Equation (2):

$$Rep(y) = \frac{\sum_{x=1}^{|Tf(y)|} Tf(x,y)}{|Tf(y)|} \quad (2)$$

where:

$|Tf(y)|$ number of trusted feedback received on provider $y$.
$Tf(x,y)$ trusted feedback of user $x$ on provider $y$.

Reputation of provider $y$ ($Rep(y)$) is used by user $x$ to calculate trust on provider $y$ ($T_r(x,y)$) based on Equation (3):

$$T_r(x,y) = \begin{cases} \text{High trust} & if Rep(y) \geq \rho \\ \text{Medium trust} & if Rep(y) \geq \mu \\ \text{Low trust} & if Rep(y) \geq \varepsilon \\ \text{New provider} & if Rep(y) = \varphi \end{cases} \quad (3)$$

where:

$\rho$ denoted as threshold for high-trust providers.
$\mu$ denoted as threshold value of medium-trust providers.
$\varepsilon$ denoted as threshold value of low-trust providers.
$\varphi$ defined a threshold value to represent new providers.

These values are experimental variables and can be tuned based on the trust level required by the system. In addition, in HealthyBroker we have imposed three levels of trustworthiness to allow users to choose different levels of trust that are inversely correlated with time consumed to calculate trust values. For instance, if the user wants only good providers he can choose a high trust level. However, this will result in long delays due to the time required for calculating such high trust values.

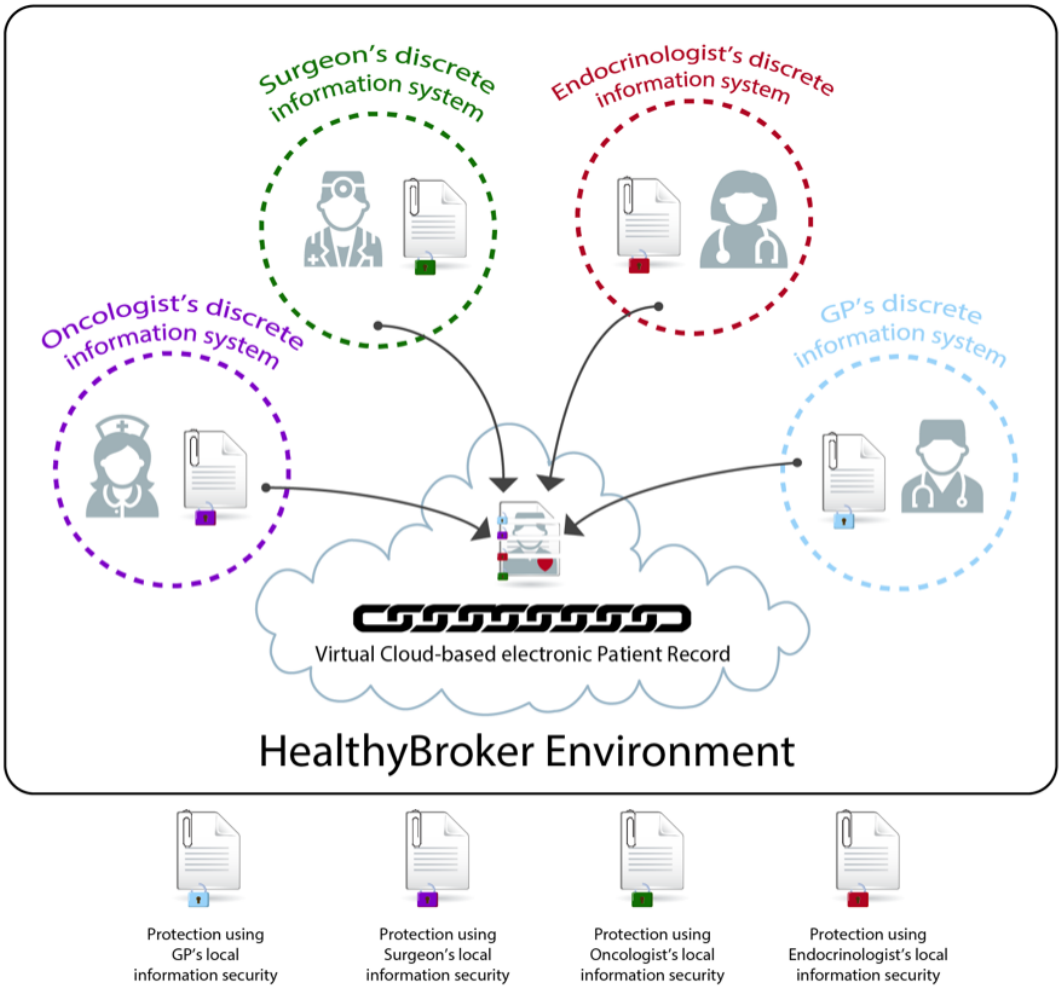


**Figure 1.** HealthyBroker environment.

## 4. Layered Architecture

The HealthyBroker model collects user feedback and aggregates it to evaluate cloud service providers based on their reputations. Additionally, the system architecture is designed to evolve trustworthiness capabilities in brokering systems. Figure 2 illustrates the system architecture, which comprises the following three layers:

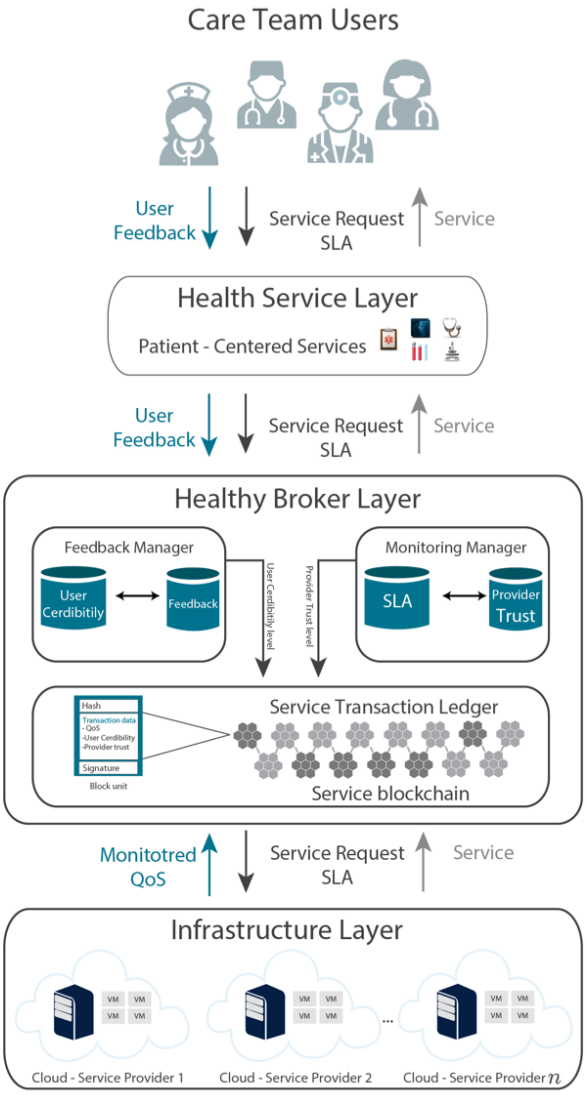


**Figure 2.** HealthyBroker architecture. Service level agreement (SLAs), quality of service (QoS).

1. Health service layer: Care-team users request a service through this layer along with the SLA that meets their needs. Once they receive the service, they provide their feedback, which is checked by the system to ensure user credibility. A credible user will provide positive feedback for service that matches the SLA and negative feedback otherwise. On the other hand, a non-credible user will do the opposite.
2. HealthyBroker layer: This layer tracks each provided service in a distributed ledger and the user's credibility level for this service along with the provider's trust level, and QoS. This layer includes three modules:

    - Monitoring manager: This module calculates the provider's trust level by checking the QoS he/she provides against the SLA.

- Feedback manager: This module calculates the user credibility level by comparing user feedback against the QoS provided. If they match, then the user is considered honest. This increases the credibility level. Otherwise, the level decreases.
- Service transaction ledger: This module links the feedback and monitoring components by updating the service transaction ledger once a service is provided. The update includes the QoS provided, the user's credibility level, and the provider's trust level. This information is stored in a distributed immutable ledger that is shared among all care-team members.

3. Infrastructure layer: In this layer, cloud service providers offer a virtual machine (VM) with different configurations of hardware, CPU, memory space, and hard-disk capacity. This layer manages all resources offered by service providers.

Figures 3–5 show the main algorithm of HealthyBroker in pseudo code, flowchart, and interaction diagram representations. The system works as follows. Once a service request arrives from a user, the system calculates the credibility of each provider of this service and sends a list of these providers along with their reputation levels. The user selects a provider based on the level of trust desired. The system mandates that the user rate his last transaction by giving negative or positive feedback. Once the feedback is received, it is checked against the real-time monitored QoS provided to the user. If the feedback is correct, the user credibility level in increased by one and vice versa.

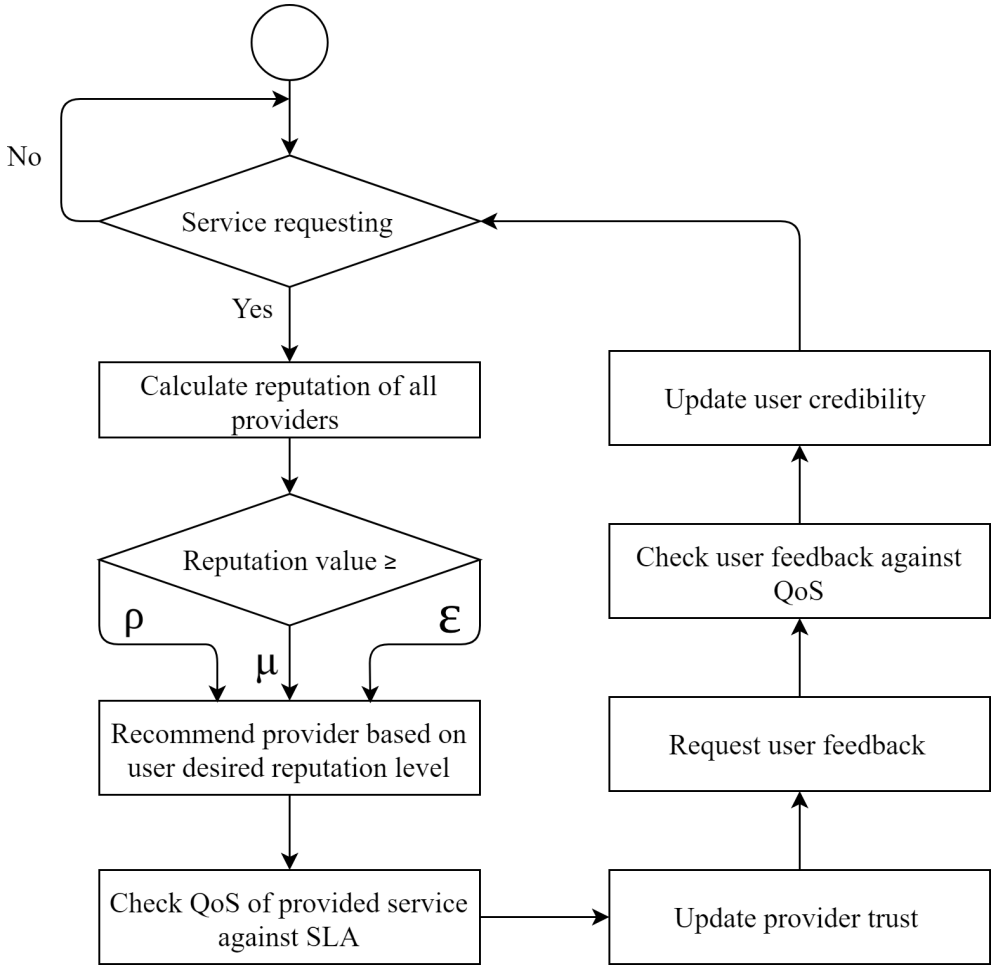


**Figure 3.** HealthyBroker flowchart.

**Trust Model Algorithm**

```
Input: user ID, level of trust, service request
Output: service(Sx)
for each cloud_providers do
   T(y) = ∑_{x=1}^{|Tf(y)|} Trusted feedback(Service X, Provider Y)
   Rep(y) = T(y) /| T(y) |
end
if user registered in cloud then
   for each service_request do
      threshold = Level of Trust
      if threshold >= ρ then
         Providers_Lis t= List of high trust provider (Rep(y))
      else if threshold >= μ then
         Providers_List = List of medium trust provider(Rep(y))
      else if threshold >= ε then
         Providers_List = List of Low trust provider (Rep(y))
      else
         Providers_List = List of new trust provider
      end
      if user_selected_a_service then
         Feedback(Service X) = feedback of selected service (Sx)
         Feedback_database = store (Feedback(Service X))
      else
         continue user_selected_a_service
      end
   continue service_request
   end
else
   do user registration
end
```

**Figure 4.** HealthyBroker algorithm pseudo code.

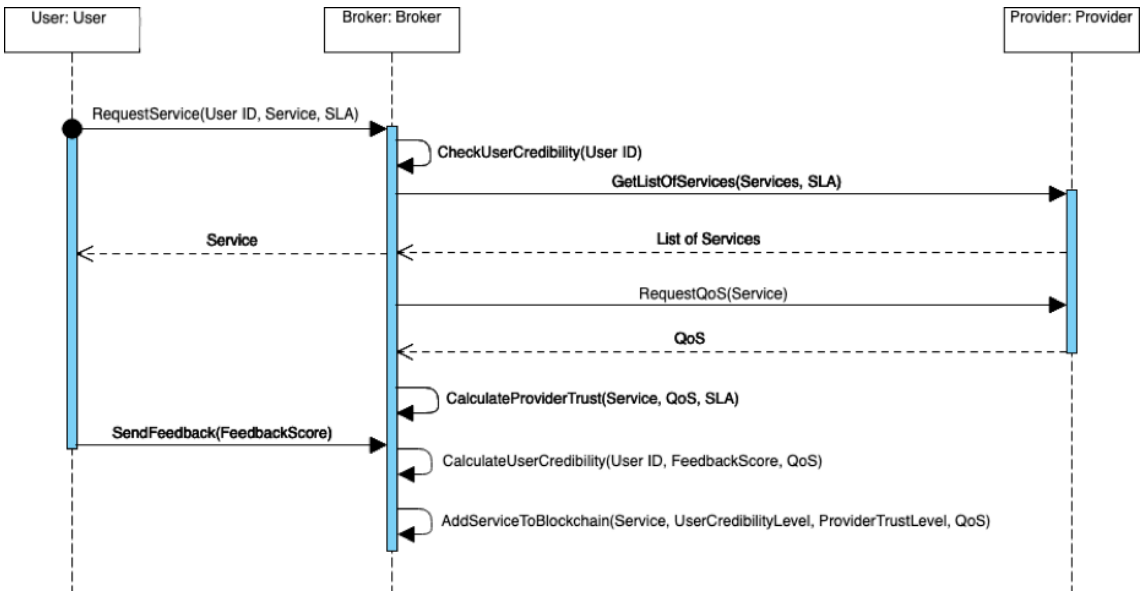


**Figure 5.** Interactions between the users and HealthyBroker model.

## 5. Evaluation Methodology

To evaluate HealthyBroker, a multi-cloud model was built on NetBeans integrated development environment (IDE) 8 using the peer to peer (P2P) simulator in [31]. The experimental setting considered 50,000 transactions related to patient treatment, 25,000 medical files, 50 care-team members as users, and the following three types of malicious behaviors with different percentages of presence in the cloud environment (from 10% to 70%):

1. Naïve malicious: This malicious model provides negative feedback to care-team members who sent them valid services. Additionally, they provide inauthentic files.
2. Feedback malicious isolated: This malicious model provides positive feedback to an anonymous user from outside the patient-trusted care team who sent them an invalid file.
3. Feedback malicious collectives: This malicious model represents sets of cooperative users who know one another. Each user from these sets gives all users in these sets high trust values and gives low trust values to all other users.

The threshold values used to compute the trust, defined in Equation (3), are experimental variables and can be tuned based on the level of trust. In this paper, we defined these values as follows:

1. $\rho$ denoted as threshold for high trust providers where the reputation $Rep(y) > 0.8$.
2. $\mu$ denoted as threshold value of medium trust providers where reputation $Rep(y) > 0.4$.
3. $\varepsilon$ denoted as threshold value of low trust providers where reputation $Rep(y) > 0.01$.
4. $\varphi$ defined a threshold value to represent new providers, the reputation $Rep(y) = zero$.

Furthermore, the lightweight trust algorithm [6] was used as a benchmark, and the following three performance indicators were considered:

1. Accuracy: This measure checks whether the proposed brokering algorithm can accurately provide a trust measurement by calculating the mean absolute deviation (MAD) as follows:

$$MAD = \frac{\sum Rep(y) - \overline{Rep(y)}}{n} \quad (4)$$

   where $Rep(y)$ is the reputation of provider $y$ (Equation (2)), $\overline{Rep(y)}$ is the mean of provider $y$'s reputations, and $n$ is the number of feedback received on provider $y$.
2. Service time: This measure specifies the time from when the system receives a user request to when the service is delivered.
3. Feedback reliability: This measure represents the amount of user feedback received from non-malicious users.

## 6. Results and Discussion

To assess the HealthyBroker system, we compared it to a benchmark, the lightweight trust algorithm. Tables 1–3 and Figures 6–8 present the results obtained from the MAD measure considering the naïve, isolated, and collective malicious user models, respectively. From the tables, it is clear that decreasing the percentage of malicious user models leads to the MAD increasing. Also, the accuracy increases in HealthyBroker in contrast to lightweight trust. The figures illustrate the differences between the HealthyBroker and lightweight trust algorithms more clearly in the instances when malicious collective, isolated, and naïve users are introduced to the system, respectively. A small percentage of malicious users (10%) was used initially, and this percentage was increased gradually to 70%. The results across all figures clearly show that HealthyBroker performs considerably better than the benchmark. This occurs because HealthyBroker considers direct and indirect trust parameters, while the lightweight trust algorithm considers only the indirect parameters.

In addition, the service time was measured with the different provider reputation levels. Tables 4–7 and Figures 9–12 list the findings. However, we note that high-trust providers consumed more service

time than low and medium-trust providers. Moreover, the feedback malicious collective consumed more time than isolated and naïve because of its cooperative strategies. From the figures, the observed correlation between the service time and level of trust is explained with different percentages of malicious users. Nevertheless, in some cases, the difference was not significant when decreasing the number of malicious users.

**Table 1.** Mean absolute deviation (MAD) results with naïve malicious.

| | **Percentage of Malicious** | | | |
|---|---|---|---|---|
| | **10%** | **30%** | **50%** | **70%** |
| HealthyBroker | 0.199827 | 0.091433 | 0.061557 | 0.05144 |
| Lightweight trust | 0.468135 | 0.417374 | 0.398155 | 0.317507 |

**Table 2.** MAD results with feedback malicious isolated.

| | **Percentage of Malicious** | | | |
|---|---|---|---|---|
| | **10%** | **30%** | **50%** | **70%** |
| HealthyBroker | 0.079445 | 0.053207 | 0.043396 | 0.040154 |
| Lightweight trust | 0.816009 | 0.802237 | 0.707643 | 0.606073 |

**Table 3.** MAD results with feedback malicious collective.

| | **Percentage of Malicious** | | | |
|---|---|---|---|---|
| | **10%** | **30%** | **50%** | **70%** |
| HealthyBroker | 0.099427 | 0.073312 | 0.053462 | 0.043296 |
| Lightweight trust | 0.820141 | 0.742743 | 0.637262 | 0.600131 |

**Table 4.** Service time with 70% malicious.

| | **Naïve** | **Isolated** | **Collective** |
|---|---|---|---|
| High | 3.064 | 3.696 | 9.817 |
| Medium | 2.98 | 3.329 | 9.786 |
| Low | 2.243 | 2.441 | 6.837 |
| No trust | 3.85 | 3.098 | 7.229 |

**Table 5.** Service time with 50% malicious.

| | **Naïve** | **Isolated** | **Collective** |
|---|---|---|---|
| High | 5.512 | 7.732 | 5.614 |
| Medium | 4.504 | 6.682 | 5.113 |
| Low | 2.804 | 6.529 | 65.192 |
| No trust | 3.477 | 3.117 | 5.499 |

**Table 6.** Service time with 30% malicious.

| | **Naïve** | **Isolated** | **Collective** |
|---|---|---|---|
| High | 5.163 | 5.847 | 6.213 |
| Medium | 4.454 | 4.326 | 4.821 |
| Low | 4.026 | 4.028 | 4.511 |
| No trust | 4.924 | 6.863 | 5.514 |

**Table 7.** Service time with 10% malicious.

| | Naïve | Isolated | Collective |
|---|---|---|---|
| High | 3.211 | 4.138 | 5.375 |
| Medium | 2.939 | 4.004 | 4.91 |
| Low | 2.099 | 4.017 | 1.266 |
| No trust | 3.734 | 3.334 | 6.819 |

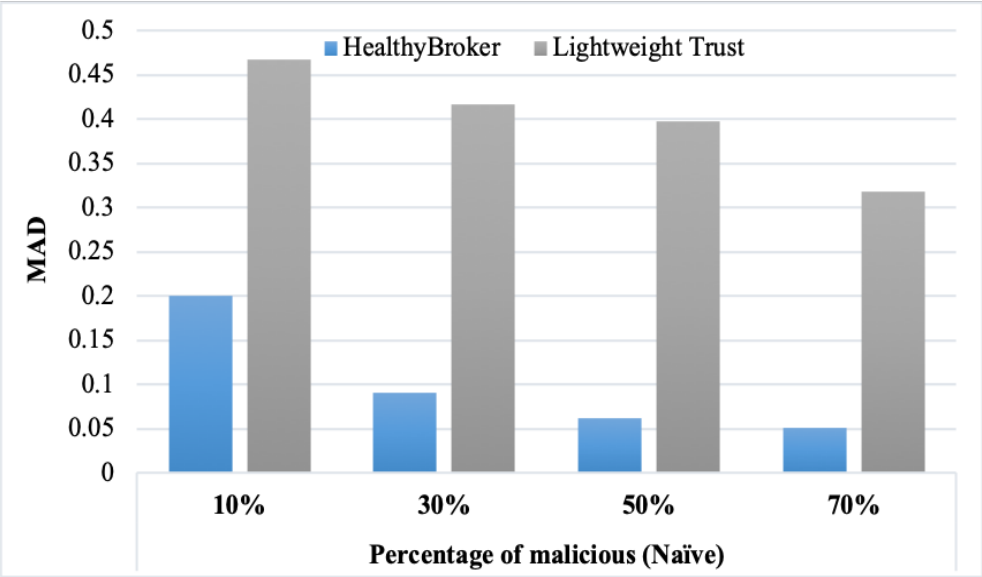


**Figure 6.** Mean absolute deviation (MAD) result with naïve malicious.

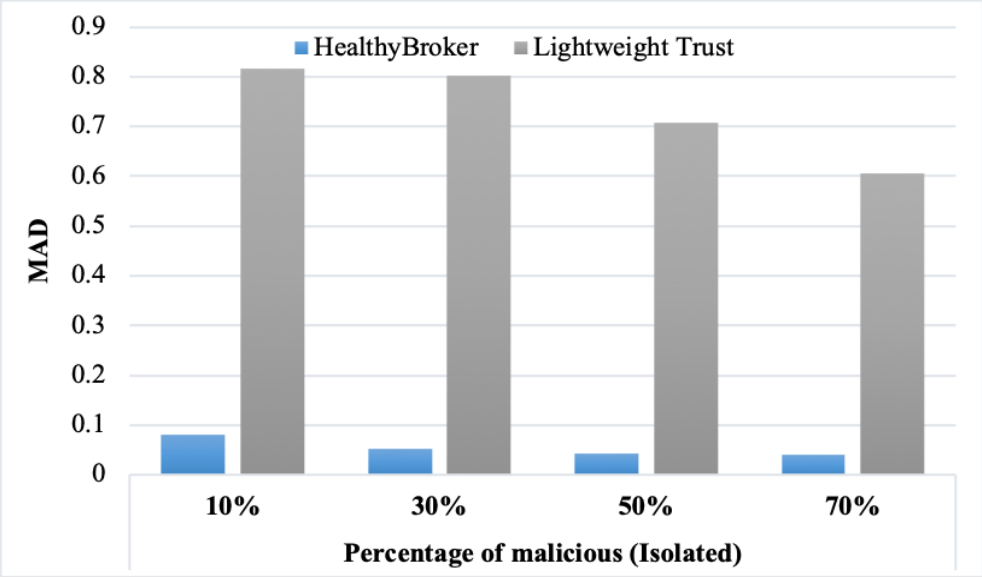


**Figure 7.** MAD result with feedback malicious isolated.

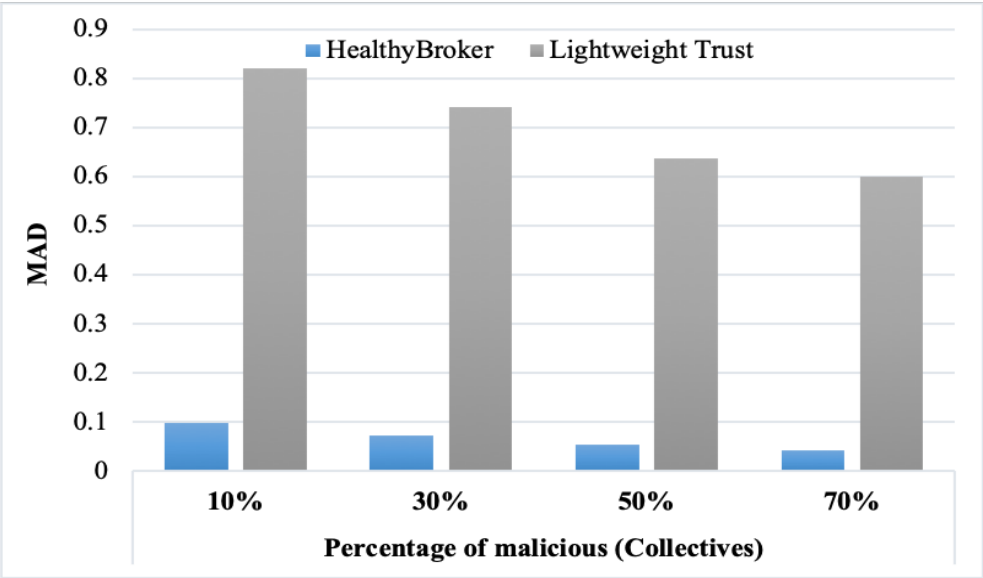


**Figure 8.** MAD result with feedback malicious collectives.

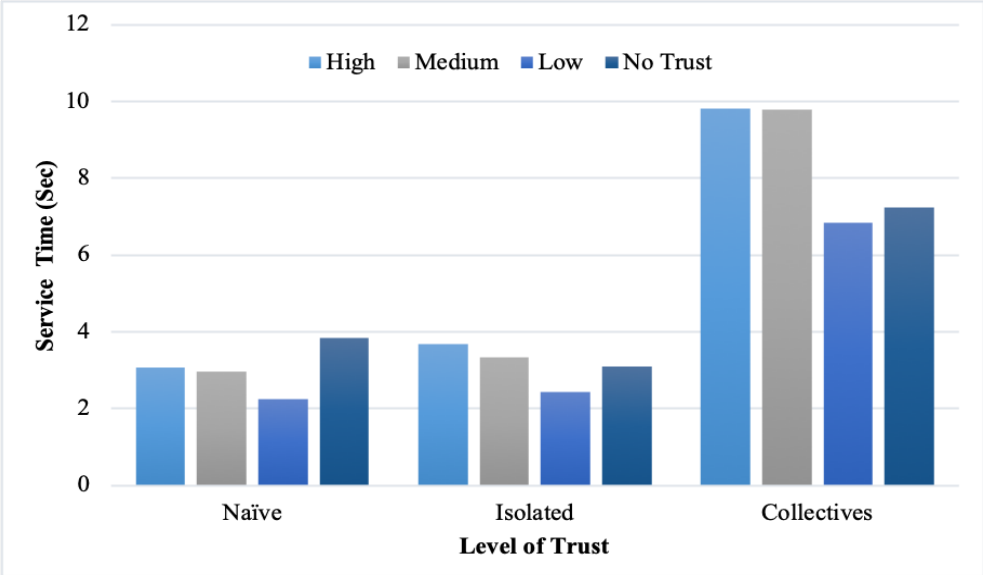


**Figure 9.** Service time with 70% of malicious.

Therefore, we measured the feedback reliability when naïve, isolated, and collective malicious users are introduced. As shown in Tables 8–10, when the level of trust increases, the percentage of malicious decreases and vice versa. In addition, we can see that "No Trust" in feedback reliability is the same in all cases. This is because "No Trust" denotes a new provider in HealthyBroker. Thus, there is no feedback reported for this new provider.

**Table 8.** Feedback reliability result with naïve malicious.

| | **Percentage of Malicious (Naïve)** | | | |
|---|---|---|---|---|
| | **10%** | **30%** | **50%** | **70%** |
| High | 81 | 68 | 41 | 20 |
| Medium | 97 | 80 | 55 | 35 |
| Low | 49,720 | 49,751 | 49,762 | 49,781 |
| No trust | 102 | 101 | 102 | 102 |

**Table 9.** Feedback reliability result with feedback malicious isolated.

| | Percentage of Malicious (Isolated) | | | |
|---|---|---|---|---|
| | **10%** | **30%** | **50%** | **70%** |
| High | 49 | 47 | 25 | 10 |
| Medium | 63 | 40 | 24 | 12 |
| Low | 49,786 | 49,786 | 49,786 | 49,786 |
| No trust | 102 | 101 | 102 | 102 |

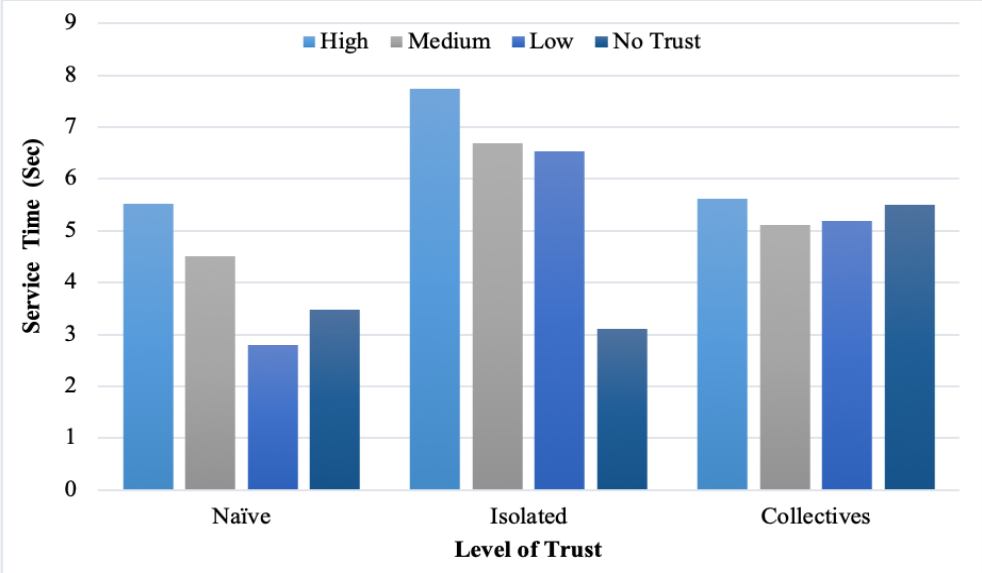


**Figure 10.** Service time with 50% of malicious.

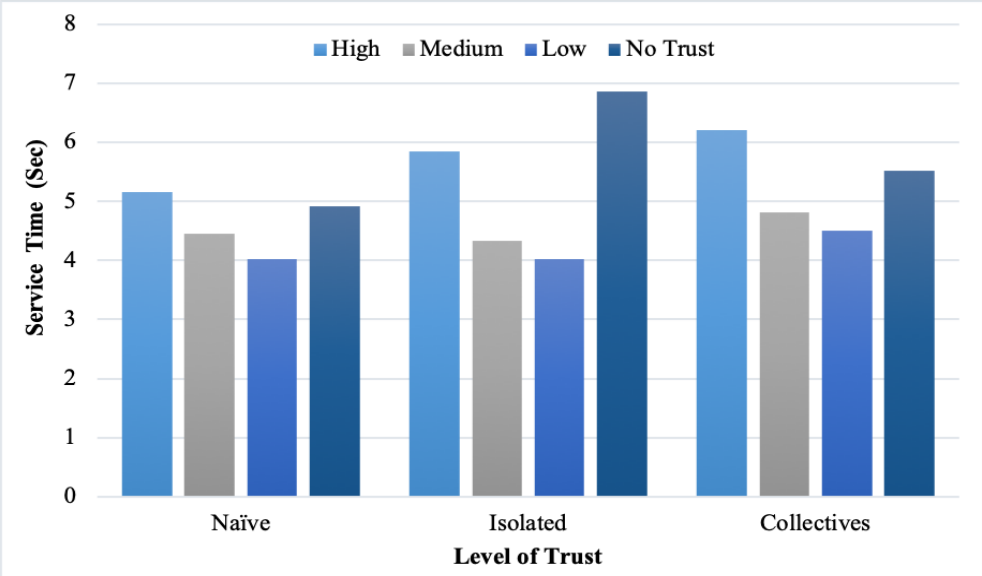


**Figure 11.** Service time with 30% of malicious.

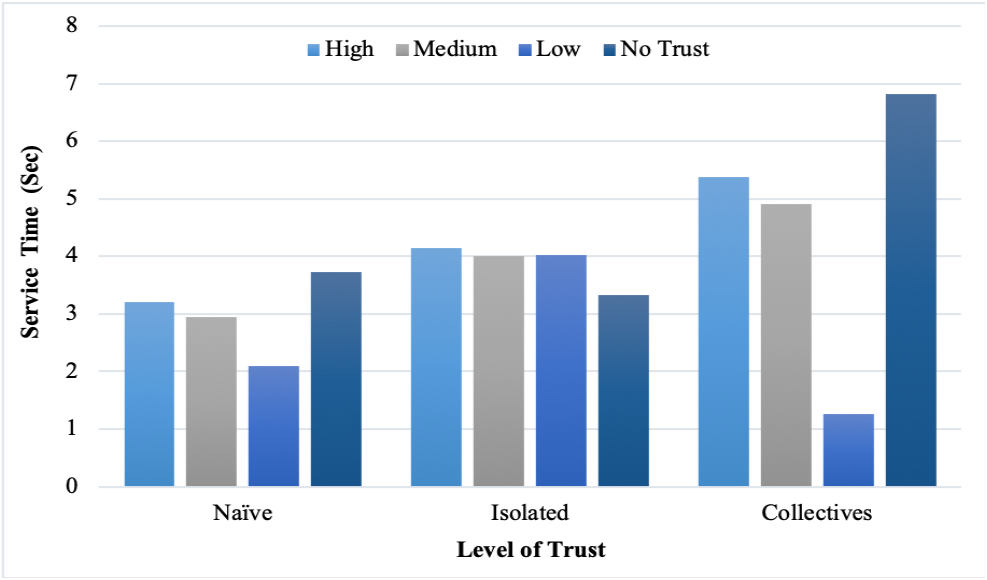


**Figure 12.** Service time with 10% of malicious.

**Table 10.** Feedback reliability result with feedback malicious collective.

| | Percentage of Malicious (Collective) | | | |
|---|---|---|---|---|
| | **10%** | **30%** | **50%** | **70%** |
| High | 53 | 47 | 23 | 12 |
| Medium | 76 | 48 | 25 | 16 |
| Low | 49,769 | 49,804 | 49,850 | 49,870 |
| No trust | 102 | 101 | 102 | 102 |

## 7. Conclusions

Cloud-brokering systems have emerged to improve cloud-computing services, especially in multi-cloud environments for collaborative environments. Delivering electronic health care (eHealth) services across multi-cloud providers to implement patient-centric care demands a trustworthy brokering architecture that can ensure that shared patient information among multi-care providers is complete and authentic and that no one has tampered with it. However, existing brokering models fall short in addressing these special requirements of patient-centered eHealth services holistically. In this work, we introduced HealthyBroker, a multi-cloud blockchain-based eHealth service model that meets such needs. Following an anticipated treatment pathway for a planned treatment, the care team member uses HealthyBroker at a treatment point to access relevant patient information needed for informed-decision making. HealthyBroker also ensures service trustworthiness against malicious behavior by managing trust among care teams. It uses blockchain technology to track each service, the user's credibility, and providers trust in a neutral ledger creating a tamper-proof trail of block sequences distributed among service providers and users for transparently.

The service time, accuracy, and reliability of received user feedback were measured to test HealthyBroker's performance in a simulated multi-cloud environment using three malicious behavior models: Naïve, feedback isolated, and feedback collective. The experimental results show that HealthyBroker outperformed the benchmark algorithm, lightweight trust, in all scenarios. The differences between the HealthyBroker and lightweight trust algorithms are most clear in the instances when malicious collective, isolated, and naïve users are introduced to the system, respectively. Furthermore, results show that HealthyBroker performs considerably better than the compared benchmark because HealthyBroker considers direct and indirect trust parameters, while the lightweight trust algorithm considers only the indirect parameters. However, high-trust providers consumed more service time than low and medium-trust providers, while the feedback malicious collective

consumed more time than isolated and naïve because of its cooperative strategies. In terms of future research, it would be valuable to explore other types of malicious behaviors such as Sybil attacks and malicious spies. Ultimately, it is hoped that this solution will lay a sound foundation for future trust management solutions that tackle loss of trust and the adoption of blockchain technology in multi-cloud environments.

**Author Contributions:** Conceptualization, H.K. and S.A. (Shada Alsalamah); Methodology, H.K. and S.A. (Shada Alsalamah); Software, A.A. and S.A. (Sara Alfaraj); Formal Analysis, H.K., and S.A. (Shada Alsalamah); Investigation, S.A. (Shada Alsalamah), A.A. and S.A. (Sara Alfaraj); Writing—Original Draft Preparation, S.A. (Shada Alsalamah), L.A. and S.H.A.; Writing—Review and Editing, S.A. (Shada Alsalamah), L.A. and S.H.A.; Visualization, S.A. (Shada Alsalamah), A.A. and S.A. (Sara Alfaraj); Validation, H.K. and S.A. (Shada Alsalamah); Supervision, H.K.; Funding Acquisition, H.K. and S.A. (Shada Alsalamah).

**Funding:** Research funded by Female Center for Scientific and Medical Colleges, Deanship of Scientific Research, King Saud University.

**Acknowledgments:** This work was supported by Saudi Aramco under the "Ibn Khaldun Fellowship for Saudi Women" in partnership with the Center for Clean Water and Clean Energy at MIT and the "Research Center of the Female Scientific and Medical Colleges", Deanship of Scientific Research, King Saud University.

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

## References

1. WHO. In Proceedings of the e-Health 2019 Committee, Toronto, ON, Canada, 26–29 May 2019.
2. Fix, G.M.; VanDeusen Lukas, C.; Bolton, R.E.; Hill, J.N.; Mueller, N.; LaVela, S.L.; Bokhour, B.G. Patient-centred care is a way of doing things: How healthcare employees conceptualize patient-centred care. *Health Expect.* **2018**, *21*, 300–307, doi:10.1111/hex.12615. [CrossRef] [PubMed]
3. Alsalamah, S.; Alsalamah, H.; Gray, A.W.; Hilton, J. Information Security Threats in Patient-Centred Healthcare. In *Health Care Delivery and Clinical Science: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2018; pp. 1531–1552.
4. Hu, Y.; Bai, G. A systematic literature review of cloud computing in eHealth. *arXiv* **2014**, arXiv:1412.2494.
5. Fabian, B.; Ermakova, T.; Junghanns, P. Collaborative and secure sharing of healthcare data in multi-clouds. *Inf. Syst.* **2015**, *48*, 132–150, doi:10.1016/j.is.2014.05.004. [CrossRef]
6. Li, X.; Ma, H.; Zhou, F.; Yao, W. T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1402–1415, doi:10.1109/TIFS.2015.2413386. [CrossRef]
7. Mohan, K.; Aramudhan, M. Broker based trust architecture for federated healthcare cloud system. *Intell. Autom. Soft Comput.* **2017**, *23*, 477–483. [CrossRef]
8. Optimized Infrastructure Services (OPTIMIS). Available online: http://www.optimis-project.eu/project (accessed on 1 February 2019).
9. Chaves, S.A.D.; Uriarte, R.B.; Westphall, C.B. Toward an architecture for monitoring private clouds. *IEEE Commun. Mag.* **2011**, *49*, 130–137, doi:10.1109/MCOM.2011.6094017. [CrossRef]
10. Rochwerger, B.; Breitgand, D.; Levy, E.; Galis, A.; Nagin, K.; Llorente, I.M.; Montero, R.; Wolfsthal, Y.; Elmroth, E.; Caceres, J.; et al. The Reservoir model and architecture for open federated cloud computing. *IBM J. Res. Dev.* **2009**, *53*, 4:1–4:11, doi:10.1147/JRD.2009.5429058. [CrossRef]
11. Anderson, R.J. *Security Engineering*, 2nd ed.; Wiley Publishing: Indianapolis, India, 2008.
12. Kamvar, S.D.; Schlosser, M.T.; Garcia-Molina, H. The Eigentrust Algorithm for Reputation Management in P2P Networks. In Proceedings of the 12th International Conference on World Wide Web, Budapest, Hungary, 20–24 May 2003; ACM: New York, NY, USA, 2003; pp. 640–651, doi:10.1145/775152.775242. [CrossRef]
13. Noor, T.H.; Sheng, Q.Z.; Yao, L.; Dustdar, S.; Ngu, A.H.H. CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 367–380, doi:10.1109/TPDS.2015.2408613. [CrossRef]
14. PCMONS, Pcmons-Private Clouds MONitoring Systems. Available online: http://www.findbestopensource.com/product/pcmons (accessed on 1 February 2019).

15. Al-megren, S.; Alsalamah, S.; Altoaimy, L.; Alsalamah, H.; Soltanisehat, L. Blockchain Use Cases in Digital Sectors: A Review of the Literature. In Proceedings of the 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, Halifax, NS, Canada, 30 July–3 August 2018; IEEE: Halifax, NS, Canada, 2018; pp. 1417–1424.
16. Linn, L.A.; Koo, M.B. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*; ONC/NIST: Gaithersburg, MD, USA, 2017.
17. Seol, J.; Jin, S.; Lee, D.; Huh, J.; Maeng, S. A Trusted IaaS Environment with Hardware Security Module. *IEEE Trans. Serv. Comput.* **2016**, *9*, 343–356, doi:10.1109/TSC.2015.2392099. [CrossRef]
18. Cuomo, A.; Di Modica, G.; Distefano, S.; Puliafito, A.; Rak, M.; Tomarchio, O.; Venticinque, S.; Villano, U. An SLA-based Broker for Cloud Infrastructures. *J. Grid Comput.* **2013**, *11*, 1–25, doi:10.1007/s10723-012-9241-4. [CrossRef]
19. Filali, F.Z.; Yagoubi, B. Classifying and Filtering Users by Similarity Measures for Trust Management in Cloud Environment. *Scal. Comput. Pract. Exp.* **2015**, *16*, 289–302. [CrossRef]
20. Khelifi, H.; Luo, S.; Nour, B.; Moungla, H.; Hassan Ahmed, S. Reputation-Based Blockchain for Secure NDN Caching in Vehicular Networks. In Proceedings of the 2018 IEEE Conference on Standards for Communications and Networking (CSCN), Paris, France, 29–31 October 2018; pp. 1–6, doi:10.1109/CSCN.2018.8581849. [CrossRef]
21. Otoum, S.; Kantarci, B.; Mouftah, H.T. On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Netw. Lett.* **2019**, *1*, 68–71. [CrossRef]
22. Al-khafajiy, M.; Baker, T.; Chalmers, C.; Asim, M.; Kolivand, H.; Fahim, M.; Waraich, A. Remote health monitoring of elderly through wearable sensors. *Multimed. Tools Appl.* **2019**, 1–26. [CrossRef]
23. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **2019**, *90*, 101842. [CrossRef]
24. Otoum, S.; Kantarci, B.; Mouftah, H.T. Mitigating False Negative intruder decisions in WSN-based Smart Grid monitoring. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 153–158.
25. Otoum, S.; Ahmed, M.; Mouftah, H.T. Sensor Medium Access Control (SMAC)-based epilepsy patients monitoring system. In Proceedings of the 2015 IEEE 28th Canadian conference on electrical and computer engineering (CCECE), Halifax, NS, Canada, 3–6 May 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1109–1114.
26. Oueida, S.; Kotb, Y.; Aloqaily, M.; Jararweh, Y.; Baker, T. An Edge Computing Based Smart Healthcare Framework for Resource Management. *Sensors* **2018**, *18*, 4307. [CrossRef] [PubMed]
27. Alloghani, M.; Baker, T.; Al-Jumeily, D.; Hussain, A.; Kaky, A.; Mustafina, J. Early Detection and Prediction of Lung Cancer using Machine Learning Algorithms Applied on a Secure Healthcare Data System Architecture. In *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices*; CRC Press: Boca Raton, FL, USA, 2019; pp. 233–257.
28. Oueida, S.; Aloqaily, M.; Ionescu, S. A smart healthcare reward model for resource allocation in smart city. *Multimed. Tools Appl.* **2018**, 1–22. [CrossRef]
29. Healthcare Information and Management Systems Society (HIMSS), 2016, Patient Engagement. Available online: http://www.himss.org/ResourceLibrary/ContentReg.aspx?ItemNumber=33952 (accessed on 1 February 2019).
30. Goldwater, J. The use of a blockchain to foster the development of patient-reported outcome measures. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*; ONC/NIST: Gaithersburg, MD, USA, 2016.
31. Penn Engineering. QTM: P2P Trust Simulator. Available online: https://rtg.cis.upenn.edu/qtm/p2psim.php3 (accessed on 1 February 2019).