sensors

MDPI

Article

Blockchain Socket Factories with RMI-Enabled Framework for Fine-Grained Healthcare Applications

Saleem Ahmed [1], Abdullah Lakhan [2], Orawit Thinnukool [3] and Pattaraporn Khuwuthyakorn [3,*]

[1] Department of Computer System Engineering, Dawood University of Engineering and Technology, Karachi 74800, Sindh, Pakistan; saleem.ahmed@duet.edu.pk
[2] Department of Computer Science, Dawood University of Engineering and Technology, Karachi 74800, Sindh, Pakistan; abdullah.lakhan@duet.edu.pk
[3] College of Arts Media and Technology, Chiang Mai University, Chiang Mai 50200, Thailand; orawit.t@cmu.ac.th
* Correspondence: pattaraporn.khuwuth@cmu.ac.th

Abstract: The usage of digital and intelligent healthcare applications on mobile devices has grown progressively. These applications are generally distributed and access remote healthcare services on the user's applications from different hospital sources. These applications are designed based on client–server architecture and different paradigms such as socket, remote procedure call, and remote method invocation (RMI). However, these existing paradigms do not offer a security mechanism for healthcare applications in distributed mobile-fog-cloud networks. This paper devises a blockchain-socket-RMI-based framework for fine-grained healthcare applications in the mobile-fog-cloud network. This study introduces a new open healthcare framework for applied research purposes and has blockchain-socket-RMI abstraction level classes for healthcare applications. The goal is to meet the security and deadline requirements of fine-grained healthcare tasks and minimize execution and data validation costs during processing applications in the system. This study introduces a partial proof of validation (PPoV) scheme that converts the workload into the hash and validates it among mobile, fog, and cloud nodes during offloading, execution, and storing data in the secure form. Simulation discussions illustrate that the proposed blockchain-socket-RMI minimizes the processing and blockchain costs and meets the security and deadline requirements of fine-grained healthcare tasks of applications as compared to existing frameworks in work.

Keywords: client–server; RMI; blockchain; socket; storage

Citation: Ahmed, S.; Lakhan, A.; Thinnukool, O.; Khuwuthyakorn, P. Blockchain Socket Factories with RMI-Enabled Framework for Fine-Grained Healthcare Applications. *Sensors* **2022**, *22*, 5833. https://doi.org/10.3390/s22155833

Academic Editor: Naveen Chilamkurti

Received: 3 July 2022
Accepted: 28 July 2022
Published: 4 August 2022

1. Introduction

Innumerable emerging technologies will improve our health, including 6G wireless connection, blockchain technology, and programming interfaces of enterprise applications (such as sockets and remote method invocation) [1]. These technologies have been combined and designated as the new digital healthcare paradigm, composed of all the technologies mentioned earlier. The digital healthcare paradigm offers many remote healthcare services to mobile users to predict and analyze their healthcare issues 24/7. In practice, the users can diagnose many diseases at home by interacting with the hospital via different remote services. The latest mobile devices support many bio-healthcare sensors and enhance healthcare services for their users. Mobile devices exploit the Android operating system (X86) to run these applications. However, mobile devices suffer from resource-constrained issues and can not locally support these data-intensive and compute-intensive applications. One solution to this problem is that users can enhance the resources such as the battery, storage, and CPU inside mobile devices. However, this solution suffered from high processing and storage costs for mobile users [2]. Many solutions are suggested in the state-of-the-art to solve the resource-constraint issues of mobile devices. For instance, the remote procedure call (RPC) technique, remote method invocation (RMI), common object

request broker (CORBA), and others. The goal is to offload the heavyweight workload from mobile devices to rich resource servers of mobile devices for execution. The RMI, CORBA, and RPC exploit the socket-based architecture where users and servers are separated, as in the client and server architecture. The client and server architectures are widely designed based on socket programming, where socket client and socket server classes are designed into the application programming interface [3–5]. Recently, the socket integrated cloud computing services to enhance the performance of the client–server model to support healthcare applications. The fog node is an extended version of cloud computing that allows services at the edges of the user network. The socket programming model enables mobile devices to offload their workloads to the fog and cloud computing for execution [6]. The remote procedure call (RPC) is widely exploited with the socket to run these healthcare applications in the mobile-fog-cloud network. Cloud computing offers different resources based on on-demand, on-reserve, and spot-instantaneous models. The socket implemented these resource models with RPC and executed the distributed healthcare applications on mobile-fog-cloud networks. Distributed healthcare applications are those in which workloads run on different nodes and store their data on other storage [7–9].

Challenges: In practice, the existing blockchain technologies such as Ethereum, Corda, Fabric, and IBM are widely exploited for healthcare applications. However, many research challenges exist in the current blockchain technologies and their approaches to RPC socket architectures [1–8] for healthcare applications. (i) The existing client–server architecture based on socket RPC suffers from high processing costs for cloud computing. (ii) The two-tier mobile and fog socket RPC frameworks suffer from resource balancing, processing costs, and storage costs for healthcare applications. (iii) Security is the key issue between socket layers in the existing RPC architecture for healthcare applications.

Contribution: This study devises the blockchain-RMI socket-enabled framework for fine-grained medical applications in mobile-fog-cloud paradigms. The goal is to minimize processing and storage costs and meet the security, privacy, deadline, and resource balancing constraints of work. This study considers one healthcare application consisting of different fine-grained tasks with deadlines and operations. This study finds the decentralized nodes (mobile, fog, and cloud) where each node can connect to another node based on blockchain rules to exchange the data based on security and privacy rules. In practice, the thin client mobile device only installs lightweight RMI interfaces, has a connection with the fog and is cloud-based on socket clients and socket servers. The data validation in terms of security will be evaluated based on blockchain technology, which converts the workload into a cipher based on AES-256 during processing in the system. The fog and cloud nodes offer processing and storage resources based on a serverless model where users pay for their usage instead of long-term provisioning of the cloud.

1. This paper designs the socket programming integrated remote method invocation (RMI) runtime interface based on Android X86 for healthcare applications in a blockchain-enabled mobile cloud network. The applications are distributed and run on different nodes with the same environment (X86) based on blockchain data validation. Generally, it is a blockchain-enabled RMI-socket enabled framework for healthcare applications in mobile-fog-cloud networks to minimize the processing cost and storage and meet all the given constraints.
2. This study drives the serverless processing cost model, which will charge based on execution time and is different from the existing hourly, weekly, and monthly on-demand services model. The goal is to minimize the processing cost for the healthcare application components and execute them within their deadlines.
3. This study invents the three-layer resource-balancing storage on mobile cloud computing, in which applications can be executed without the issue of scalability, reliability, and storage cost during processing. The mobile devices offload their workload to the fog nodes, and their results are offloaded to cloud computing with the minimum storage cost.

4. The data sharing and exchange from mobile devices and fog to cloud nodes for computing and storage has high security and privacy issues in mobile cloud computing paradigms. Anonymous external attacks and threats exist on the network, and healthcare-sensitive data could be compromised. This study devises the three-layer blockchain mining manager to create and add new blocks to the mobile-cloud network. Each block has its data hashing and nonces and validates each data transaction of the previous node in work.
5. This study presents the new simulator for healthcare applications based on an RMI-socket with a blockchain-enabled mobile-fog-cloud network to run distributed applications. For the data validation and hashing matching, this study devised the distributed hybrid offloading method to enable proof of work, ensuring security and privacy inside the framework for healthcare applications.

2. Related Work

This section discusses the related healthcare applications implemented based on client–server mechanisms in the fog cloud networks. In [1], a remote method invocation (RMI)-based healthcare framework was suggested for resource-constrained mobile devices to offload their data to cloud computing for further analysis. In practice, the work obtained optimal results and improved the quality of experience on the mobile device applications. The remote procedure call (RPC)-based framework was suggested for healthcare applications in [2]. The study triggers remote services when the mobile workload offloads data to remote servers for execution. It is an Android-X86 level service and runs at the operating system level when RPC is implemented at the kernel level inside the system. The study obtained the optimal objectives in terms of resource balancing and offloading in the considered problem.

Table 1 shows the related work of existing client–server architecture and their security mechanism based on existing security and blockchain in the distributed mobile edge cloud network. The main limitations with the RPC and RMI are live client and server connection stability, where intermittent service changes make the connection unreliable for the applications. The connection-enabled framework based on sockets is presented in [3,5]. The study achieved a strong connection and stored the running data on the cache without disruption of the request of applications during their executions.

Regardless, these sockets, RMI, and RPC did not support the security mechanism for healthcare applications in an open network. Security is a critical issue in an available network where many types of nodes are connected, and centralized security on one node cannot give feasible solutions to the applications. Decentralized and autonomous security mechanisms based on blockchain technology have been suggested in [4,6–10]. These blockchain-based frameworks improve the application-level abstractions of the Ethereum blockchain for healthcare applications. The applications offload their data into valid data transactions among all connected nodes.

These security mechanisms are based on extended versions of the existing security algorithms. For instance, AES-256, RSA, CRC-32, and others encrypt and decrypt data with asymmetric and symmetric paradigms for healthcare applications in the network. These algorithms are resource and time-hungry and are implemented in the blockchain technology to achieve hashing for security purposes only. The blockchain-enabled AES-256, SHA-256 and RSA-based solutions presented in [11–17] make valid and immutable transactions between connected autonomous nodes for healthcare applications. The RMI interfaces implemented for the blockchain classes, however, still consume much more of the server's resources and lead to high processing costs for the applications.

The RPC-based blockchain presented in [18–24] to modify the blockchain technologies from bitcoin applications into healthcare applications. The RPC offers embedded level abstraction and allows modification inside the operating system to support healthcare applications based on blockchain technologies. These applications successfully obtained the security objectives and ran the healthcare applications on different nodes. However, ap-

plications' delay, cost, and deadline are widely compared in these frameworks. The energy and delay level blockchain frameworks suggested in [25–30] improve the constraints on the above frameworks; however, resource consumption, costs, and deadlines of applications are still compared to the state-of-the-art blockchain in the system. The blockchain consensus has been widely implemented for different applications such as proof of work [31], proof of stake [32], delegated proof of stake (DPoS) [33], and leased proof of stake (LPoS) [34] to enable transaction validation in the blockchain nodes during processing in the network.

Table 1. Existing Healthcare Client Server Frameworks Based on RMI, RPC, and Socket.

Study	Hashing Techniques	Application	Architecture	Layers	Language	Node
[1]	MD5	Heartbeat	CORBA	Client–Server	JAVA	Mobile-Cloud
[2]	SHA-256	Blood-P	RPC	Client–Server	JAVA	Mobile-Cloud
[3]	AES	Healthcare	RPC	Client–Server	JAVA	Mobile-Cloud
[4,5]	RSA	Medical Care	RMI	Client–Server	C/C++	Mobile-Cloud
[6]	AES	Medical Care	SOA	Client–Server	C/C++	Mobile-Edge
[7–10]	Blockchain	Medical Care	Ethereum	Client–Server	PYTHON	Mobile-Edge
[11–20]	Blockchain	Medical Care	Open-Source	Client–Server	PYTHON	Mobile-Edge
[21,22]	Privacy	Healthcare	fixed	Client-client	PYTHON	Mobile-Edge
[23–25]	Privacy	Healthcare	fixed	Server-Server	PYTHON	Mobile-Edge
[26,27]	Privacy	Healthcare	fixed	Server-Server	PYTHON	Mobile-Edge
[28,29]	Privacy	Healthcare	fixed	Nodes	PYTHON	Mobile-Edge
[30]	Privacy	Healthcare	fixed	Hybrid-Client–Server	PYTHON	Mobile-Edge
Proposed	AES-256	Fine-Grained Tasks	RMI-Socket-Blockchain	Many Clients-Servers	JAVA	Mobile-Fog-Cloud

In the proposed work, we introduce novel blockchain socket factories with an RMI-enabled framework for fine-grained healthcare applications. The main objective of this study is to minimize processing and blockchain validation costs while meeting the application deadlines and security constraints in distributed mobile, fog, and cloud networks. The costs are determined by the processing scheduling cost, security encryption and decryption and validation cost, and storage cost for healthcare applications.

Table 2 determines the mathematical symbols of the problem and their descriptions.

Table 2. Problem Constraints and Notations.

Notations	Description
I	Number of fine-grained healthcare functions
i	Fine-grained function I
W	Amount of function data
w_i	Particular data of function i
d_i	Deadline of fine-grained function i
M	Number of client nodes
m	Particular node such as mobile
ϵ_m	Resources of particular node
ζ_m	Speed of node m
K	Number of homogeneous fog nodes
k	Particular node such as fog node k
ϵ_k	Resources of particular node
ζ_c	Cloud storage processing node
ζ_k	Speed of node k
BC	Number of blockchain blocks
$Hash$	Hash of the block
$Pre\text{-}hash$	Pre-Hash of the block
$Private\text{-}Key$	Private key of the block
$Public\text{-}Key$	Public key of the block
S	Number of cloud storage available
s	Particular storage of cloud
$logn(\frac{N}{noise})$	Logarithm of inference N and network noise
$Bandwidth$	Available bandwidth network

3. Proposed Blockchain Enabled RMI-Socket Framework

This study devises the three-layer blockchain-enabled RMI-Socket framework, as shown in Figure 1. The client layer is the application, which consists of different fine-grained functions. Each function can be executed and offloaded with detailed data at the client layer. The procedures are only overridden methods from RMI-Socket, which offload data to the fog layer for execution. For instance, three functions, ECG, EEG, and numeric heart function, have their own data and deadline constraints. The client node can accept data as the request for the particular function and apply a hash on the request based on the blockchain and offload it to the fog layer for data analysis and execution. The offloaded hash data of all functions are to be validated and verified with the private key as the signature and the public key as the validation. All the fog nodes are homogeneous and can exchange their data for execution.

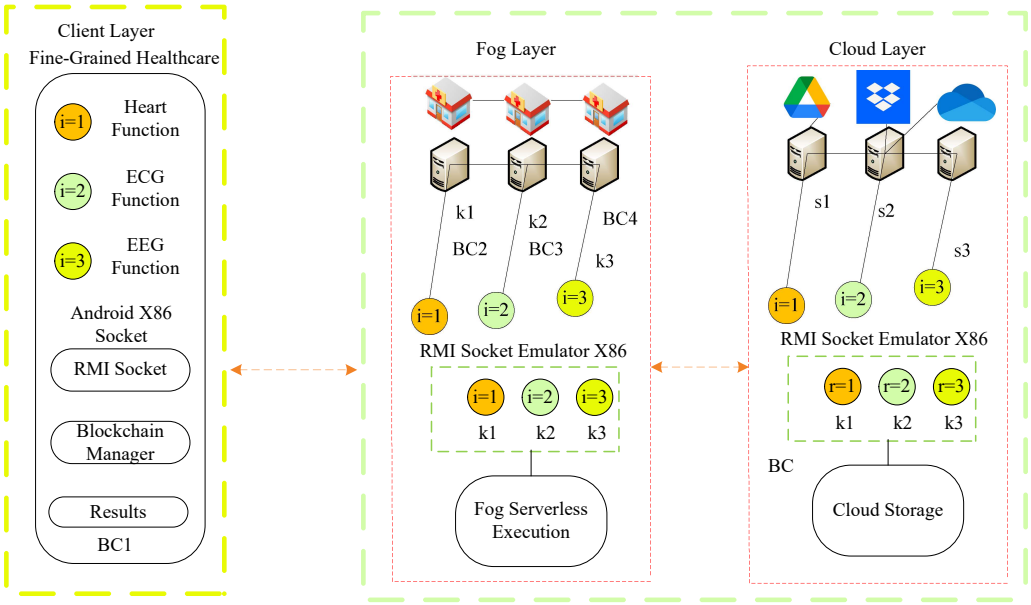

Figure 1. Blockchain RMI Socket-Enabled Framework.

The cloud layer only offers storage services to avoid the storage costs of the fog nodes, which are not cost-efficient and are expensive in terms of saving data for a long time. All three layers were designed based on the RMI-Socket client, where the Java virtual machine (JVM) supports all Android X86 and Emulator X86 fog and cloud layers. All the nodes connect via socket-RMI registries in the framework.

3.1. System Model

This study presents the designs for a blockchain-socket-RMI-enabled open-source framework for healthcare applications that consists of mobile, fog, and cloud nodes, as shown in Figure 2.

The proposed framework has an abstraction level where socket, RMI, and blockchain-customized libraries can be easily modified and updated for new healthcare applications in the network. The main goal is to develop such an application with only interfaces at the user level, implementation on the fog node, and storage of workload on the cloud-based blockchain technology. The blockchain is an open application programming interface (API) based on hashing, validation, and immutable transactions in the proposed integrated socket-RMI (client and servers) based on the interface level of RMI in the system. Therefore, it is a distributed and customized open-source framework that can be easily modified for new healthcare applications. Therefore, this study's main goal is to suggest an open-source distributed socket-based client–server framework in which libraries can be updated for new applications in the network. The patients have mobile application access for uploading and downloading as well as doctor communication services in the system. The healthcare professionals have different hospital servers, which are implemented in different hospitals as the healthcare fog and cloud servers. Patients can update, upload, and download data from the mobile application's patient access, and the healthcare professional can update, analyze, and classify the data on the server at different hospitals.

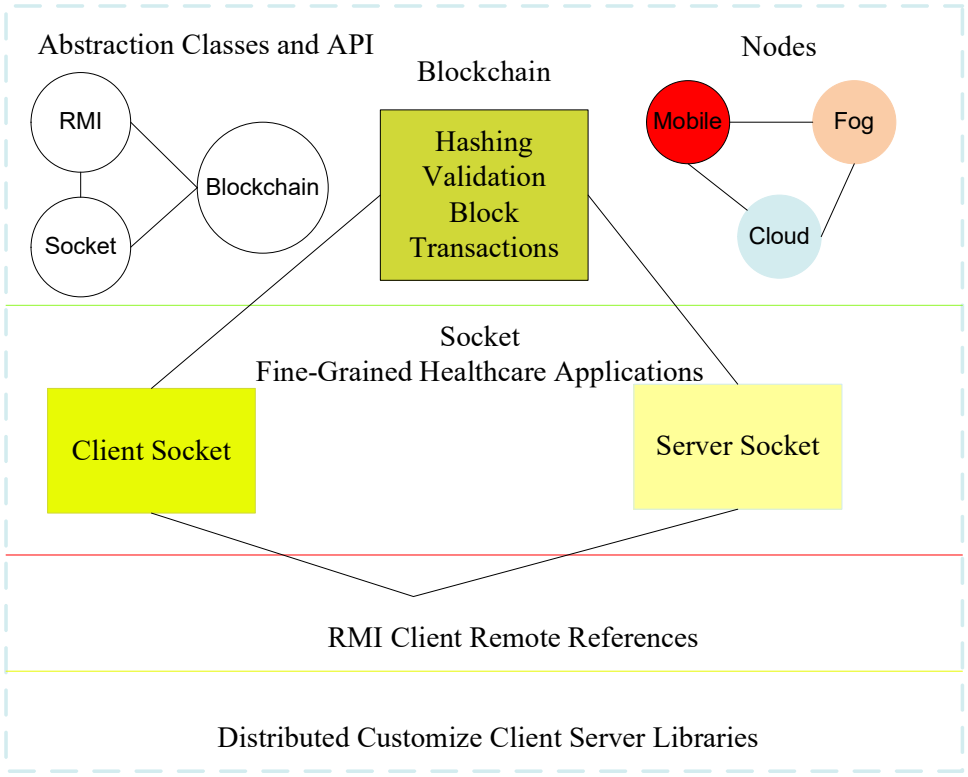

Figure 2. Abstraction of Socket RMI Blockchain for Healthcare Applications.

3.2. Node Scheduling

There are three nodes in the system, i.e., mobile node, fog node and cloud node, for healthcare application processing. The mobile node can only execute the lightweight tasks and offload them to the fog nodes for further processing with the minimum end-to-end latency, whereas fog nodes have minimum lateness due to the proximity of the site to the execution of the application. However, fog nodes have a higher storage cost for saving the data in the system. Therefore, we implement a public cloud node with fewer storage costs in the system. In general terms, the cloud has a longer communication delay but smaller processing and storage costs in the system. Therefore, to keep the balance between resource constraints, processing delay, and storage costs, this study implemented different nodes and ran the application on the mobile, fog, and cloud nodes in the system.

3.3. Security and Privacy Mechanism

In the system, we consider both the security and privacy mechanisms for the healthcare application. Privacy is the authenticated login and access of the controls in the client–server-based application, and security is the data validation, encryption and decryption and attacks in the system. We devised a blockchain-based security mechanism in which both security and privacy are maintained for the healthcare application in the system.

3.4. Problem Formulation

This study considers the healthcare application I with different fine-grained functions, e.g., $\{i = 1, \ldots, I\}$. Each fine-grained function i has workload w_i, deadline d_i and storage address s_i in the framework. All the fine-grained functions operate in real-time and are independent of each other in the framework. This study considers K number of serverless homogeneous fog nodes, e.g., $\{k = 1, \ldots, K\}$ where each fog k has uniform speed ζ_k and resource ϵ_k. This study considers the S number of heterogeneous cloud storage services, $\{s = 1, \ldots, S\}$, with the storage capacity, ϵ_s. This study considers the m number of mobile devices, e.g., $\{m = 1, \ldots, M\}$, with the storage capacity ϵ_m and

processing speed ζ_m. Each mobile, fog and cloud has different blockchain blocks with the following attributes. For instance, a number of blocks, e.g., $\{BC = 1 \ldots, BC\}$ has $BC =< hashing, private - key, public - key, pre - hash, timestamp >$ attributes.

$$x_{i \in I} = \begin{cases} \frac{w_i}{\zeta_m}, & x_i = 1, \, mobile - assignment, \\ \frac{w_i}{\zeta_k}, & x_i = 2, \, fog - assignment, \\ \frac{w_i}{\zeta_s}, & x_i = 3, \, cloud - assignment. \end{cases} \tag{1}$$

Equation (1) determines the assignment of the fine-grained function on different mobile-fog-cloud networks. The fine-grained workload offload and blockchain validation time are determined in the following way. This is the binary assignment variable in the formulation.

$$local_i^e = \sum_{i=1}^{I} \sum_{m=1}^{M} \frac{w_i}{\zeta_m} + BC_1 + \tau_i. \tag{2}$$

Equation (2) determines the local execution and blockchain process at the local device during offloading in the framework. All blockchain attributes and validation on mobile devices are determined based on Equation (2)

$$\begin{aligned} BC_i = i \leftarrow < hashing, private - key, \\ public - key, pre - hash, timestamp > . \end{aligned} \tag{3}$$

Equation (3) determines blockchain offloading by requesting hashing and exchanging data to the fog cloud based on hashing, public key, private key, and timestamp.

$$mobile_i^{cost} = \sum_{i=1}^{I} \sum_{m=1}^{M} local_i^e \times \phi_i. \tag{4}$$

Equation (4) determines local execution and offloading costs for the mobile devices.

$$\tau_i^{m,k} = \frac{w_i}{Bandwidth} + logn(\frac{N}{noise}). \tag{5}$$

Equation (5) determines local execution time from mobile device to fog node based on exchanging data. The execution time on serverless fog nodes is determined in the following way.

$$fog_i^e = \sum_{i=1}^{I} \sum_{k=1}^{K} \frac{w_i}{\zeta_k} + BC_1 + \tau_c'. \tag{6}$$

Equation (6) determines the execution on the fog nodes. The execution cost on serverless fog nodes is determined in the following way.

$$fog_i^{cost} = \sum_{i=1}^{I} \sum_{k=1}^{K} \frac{w_i}{\zeta_k} + BC_1 + \tau_c'. \tag{7}$$

Equation (7) determines the execution cost of the fog nodes.

$$\tau'^{k,c}_i = \frac{w_i}{Bandwidth} + logn(\frac{N}{noise}). \tag{8}$$

Equation (8) determines the exchange and offload of data between the fog and cloud.

$$cloud_i^{cost} = \sum_{i=1}^{I} \sum_{s=1}^{S} \frac{w_i}{\zeta_c} + BC_1 \tag{9}$$

Equation (9) determines the cloud storage cost in the framework.

The objective function of this study is to minimize the local cost, processing cost and storage cost of all fine-grained functions, and these can be determined in the following way.

$$T_{total-Cost} = mobile_i^{cost} + fog_i^{cost} + cloud_i^{cost}. \quad (10)$$

Equation (10) determines the total cost of all fine-grained functions and their workloads.

4. Blockchain-Socket-RPC Algorithm Framework

This study devises the blockchain-socket-RMI for fine-grained healthcare applications in mobile-fog-cloud networks. The main objective is to design a flexible and reliable healthcare framework in which the total costs of fine-grained applications could be minimized. This study devises blockchain-socket-RMI schemes in which different phases are analyzed to meet the requirements of the fine-grained application, as shown in Algorithm 1.

Algorithm 1 Blockchain Socket RPC Algorithm Framework.

Input : $\{m = 1, \ldots, M, i = 1, \ldots, I, k = 1, \ldots, K, s = 1, \ldots, S, BC1, \ldots, BC\}$
Output: $\{\min T_{total-cost}\}$

begin
- Call Blockchain-RMI-Socket Scheme;
- $x_{i,m,k,BC,s} = 1$;
- Call Client-Socket Scheme;
- $x_{m,i} = 1$;
- Optimize $mobile_i^{cost}$;
- Call Blockchain Consensus Scheme;
- $x_{m,i,BC} = 1$;
- Call Initial Offloading Scheme;
- $\tau_i^{m,k}$;
- Call Fog-Socket Scheme;
- $x_{k,i,BC} = 1$;
- Optimize fog_i^{cost};
- Call Migration Offloading Scheme;
- $\tau_c' = 1$;
- Call Cloud-Socket Storage Scheme;
- $x_{s,i,BC} = 1$;
- Optimize $cloud_i^{cost}$;
- The overall objective is to be optimized;
- Optimize $T_{total-cost}$;

End Main

The proposed blockchain-socket-RMI consists of different schemes, as shown in Algorithm 1. The proposed algorithm determines the optimal allocation of all mobile, fog, and cloud costs for the healthcare function to work. All the schemes of Algorithm 1 solve the problem with the help of different methods explained in the following way.

- Client-Socket Scheme: In this scheme, we start the application process of the mobile devices, such as installed applications, and display the healthcare interfaces as fine-grained tasks. These tasks are fine-grained and have autonomous data for processing. Each workload encrypts and decrypts and is validated based on Equation (3) before offloading to the fog node for processing.
- Call Blockchain Consensus Scheme: In order to validate the fine-grained workload of healthcare data, we devise the partial proof of validation (PPoV) scheme at the mobile, fog and cloud nodes for validation during data migration.
- Initial Offloading Scheme: This scheme will allow the data to be encrypted and validated based on PPoV, and the data can be offloaded to the fog node for further processing.

- Fog-Socket Scheme: This is a scheduler where all requested fine-grained workloads are scheduled based on their given deadlines and cost constraints.
- Call Migration Offloading Scheme: This scheme offloads executed data to cloud computing to further analysis and storage in the framework.

Algorithm 2 validated each transaction between the mobile device and the fog node for each workload based on hashing values in the system. The data validation will be performed based on PPoV between the fog node and cloud node during data offloading in the system.

Algorithm 2 Partial proof of validation (PPoV).

```
Input  : m, k, i, s
begin
    foreach (i = 1 to I) do
        i ← m ← k = 1;
        Valid all transactions based on hashing for processing;
        i ← k ← s = 1;
        Valid all transactions based on hashing for storage;
End Main
```

4.1. RMI-Socket-Registry

This study uses remote method invocation (RMI) to construct bespoke socket factories. Custom socket factories can be used to regulate how network-level remote method invocations are conveyed. They can be used to regulate socket settings, address binding, and data migration-based blockchain hashing and consensus methods. The framework creates the RMI registry at different nodes to ensure the network communication at different nodes and allow a serverless model to work with the mobile and cloud layers from the centralized fog layer. This study merged the factory pattern stub and skeleton with the client socket, server socket-based unicast binding, and acceptance rules in the three-layer socket. The data are exchanged in the network in the form of hashing instead of serialization. The RMI is the method in which three layers can exchange their data, and the socket offers the application programming interface and allows the method to declare and execute in different client–server nodes.

4.2. Blockchain Consensus of Mobile-Fog-Cloud-Socket-RMI Mechanism

This study devises the proof of work with the signature matching and hashing validation features on the mobile, fog and cloud layers to ensure the security of the exchange of data between nodes, as shown in Figure 3.

The goal is to ensure security and privacy and restrict unauthorized access to the data in the distributed mobile-fog-cloud network. The fine-grained function data are to be converted into hash based on the designed public key and signature understanding based on the private key. The partial proof of validation (PPoV) method is distributed, ensuring both signature and validation on all interconnected nodes in the system. Figure 3 shows that all the exchange data are replicated on all nodes. However, the cloud only stores the processed data on different storage services.

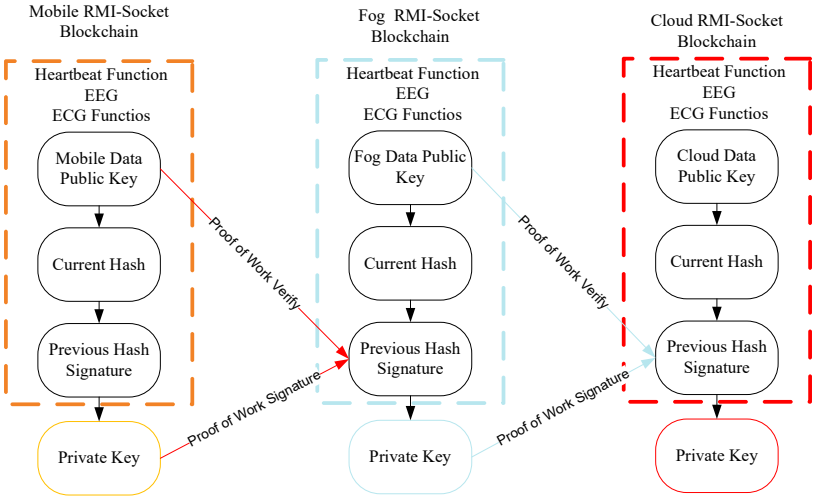

Figure 3. Blockchain RMI-Socket.

4.3. Hybrid Offloading in Blockchain RMI-Socket

This study considers the hybrid offloading mechanism, which aims to minimize the processing cost and storage cost in the work. Initially, the fine-grained functions offload their data to the fog nodes for execution to minimize the processing cost of healthcare applications, where, after the execution, the fog nodes offload their application-related data to the cloud node for storage. In the system, there are two types of offloading performed between mobile and fog nodes and fog nodes and cloud computing.

Due to lightweight and constraint issues, the mobile devices offload their workloads to the available fog nodes, while after the execution of workloads at the fog nodes, the executed workload results are offloaded to the cloud computing for storage in the system.

4.4. Socket Offloading and Scheduling Scheme

In the proposed framework, three different computing nodes are implemented to facilitate users at their devices, create a robust and efficient execution with minimum processing time and cost, and provide low-cost storage for the healthcare application. This study presents a hybrid offloading and scheduling-enabled cost-efficient scheme that executes all fine-grained tasks with deadlines and validates the data transactions in a secure form with minimum system costs. The algorithm has two ways of offloading: offloading data between mobile devices to the fog node and fog node to cloud computing for a single application in the network. The scheduler allocates applications on the three different nodes during execution. Therefore, executing the applications among resource constraint devices and rich resource servers with optimal results is more reasonable. This study devises the cost-optimal mobile-fog-cloud offloading and scheduling scheme to ensure the execution of fine-grained tasks is based on their requirements.

Algorithm 3 determines the cost-efficient scheduling and offloading in the mobile-fog-cloud network for the fine-grained healthcare functions of the application. From steps 1 to 7, This study performs mobile computing on the blockchain with function requests at the minimum execution cost time and offloads them based on a proof of work method to ensure the signature and validation of the next fog socket. The initial offloading happened between the mobile-socket and fog-socket-based blockchain proof of work. From steps 10 to 15, the fog nodes schedule all fine-grained functions on the serverless fog nodes and send their results to cloud computing for storage. All the function executions must be less than the capacity of the system's mobile devices and fog nodes. Further offloading to be completed between the fog nodes and cloud computing for data storage based on the objective function is shown in steps 16 to 21.

Algorithm 3 Optimal cost mobile-fog-cloud offloading and scheduling scheme.

Input : $\{m = 1, \ldots, M, i = 1, \ldots, I, k = 1, \ldots, K, s = 1, \ldots, S, BC1, \ldots, BC\}$
Output: $\{\min T_{total-cost}\}$

begin
  Schedule local execution;
  if $(x_{m,i} \leq \epsilon_m)$ **then**
    Determined local based on Equation (4);
    $x_{m,k,BC}$;
    Call PPoV scheme;
    $\tau_i^{m,i,BC}$;
    send to fog socket;
  if $(x_{k,i} \leq \epsilon_k)$ **then**
    Determined optimal scheduling based on Equation (7);
    $x_{i,k,BC}$;
    Call Proof of work scheme;
    $\tau'^{m,k,BC}_i$;
    send to cloud socket;
  if $(x_{s,i} \leq \epsilon_s)$ **then**
    Determined optimal storage based on Equation (9);
    $x_{i,s,BC}$;
    Call Proof of work scheme;
    $\tau'^{k,s,BC}_i$;
    send to cloud socket;
  $\min T_{total-cost}$;
  Optimize total cost based on Equation (10);
  End offloading and scheduling;

5. Performance Evaluation

In this part, we analyze the results, show the implementation, and evaluate the performances of schemes for the healthcare application. In the performance evaluation, we conducted experiments on different parameters, as defined in Table 3. The parameters are fine-grained tasks with their data, e.g., $\{i = 1, \ldots, I\}$, computing nodes $\{k = 1, \ldots, K\}$ and users devices, $m \sim M$. All the parameters are configured in the simulation file during the experiments for healthcare applications. The simulation was conducted on an open-source solidity framework along with the Android X86 Flutter emulator to ensure practical use of the applied engineering application. The main difference is that we only created the different interfaces at the client socket based on RMI, called and executed them on the fog nodes, and stored the application data on the cloud. We defined the implementation of the simulator in the respective subsection with the different abstractions of classes and methods.

Table 4 shows the different node costs in the simulation.

5.1. Implementation of Socket-RMI-Blockchain

This study defines the different classes from higher abstraction levels to integrated enumerated interfaces in the system, as shown in Figure 4.

Table 3. Simulation Parameters of Blockchain Socket RMI for Fine-Grained Healthcare Application.

Config Parameters	Parameters Values
Socket-Programming API	JAVA
$i = 1$	200 MB heartbeat workload
$i = 2$	900 MB Blood pressure
$i = 3$	2 GB EEG Values
$i = 4$	4 GB MB ECG pictures
$i = 5$	600 MB heartbeat workload
$i = 6$	900 MB Blood pressure
$i = 7$	2 GB EEG Values
$i = 8$	4 GB MB ECG pictures
$i = 9$	1200 MB heartbeat workload
$i = 10 \sim 15$	1900 MB Blood pressure
$i = 16$	5 GB EEG Values
$i = 17 \sim 20$	7 GB MB ECG pictures
$m = 1$	Android 64 GB ROM, 8 GB RAM
$m = 2$	Android 128 GB ROM, 16 GB RAM
$k = 1$	Core I5 30 GB ROM
$k = 2$	Core I7 100 GB ROM
$k = 3$	Core I9 500 GB ROM

Table 4. Cost of Nodes.

Node	Cost
$s = 1$	2 dollar per Hourly use for applications
$s = 2$	3 dollar per Hourly use for applications
$s = 3$	0.5 dollar per Hourly use for applications
$k = 1$	1 dollar per Hourly use for applications Core I5 30 GB ROM
$k = 2$	2 dollar per Hourly use for applicationsCore I7 100 GB ROM
$k = 3$	3 dollar per Hourly use for applications Core I9 500 GB ROM

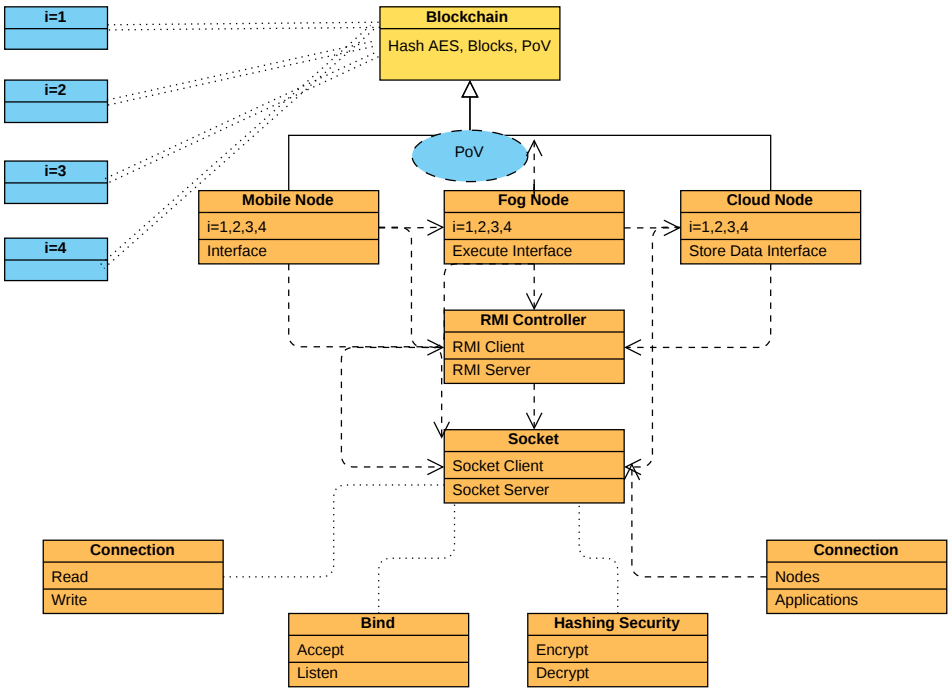

Figure 4. Abstraction of Socket-RMI-Blockchain for Healthcare Application.

The proposed framework has different abstractions of classes, such as the application of fine-grained tasks (e.g., $i = 1, 2, 3, 4$). The blockchain has four functions: hashing based

on AES-256 (e.g., asymmetric mode), proof of validation, transaction of data, and block of unique numbers in the class. The partial proof of validation (PoV or PPoV) has to be used in different classes, such as mobile classes, fog classes, and cloud classes, for the validation of the data during their declaration, initialization, and calling in the framework. The mobile node only shows the interfaces for the healthcare functions, such as heart function, ECG function, EEG function, and general doctor–patient monitoring tasks. However, the data are encrypted and decrypted at the mobile devices and offloaded to the fog node for further processing. The fog node has two objectives. At first, the fog node validated the offloaded interface data based on the PPoV scheme and applied execution on the interfaces. The fog nodes offloaded the processed data to the cloud for the storage interface at work. The RMI controller is the main class, which consists of many interfaces such as client, server, connection, acceptance, and others. The RMI controller classes implement the interfaces inside the socket. At the same time, the socket is the open-source API that consists of a client stub socket and a server skeleton socket with the different sub-classes. These classes are connection (e.g., read/write properties), bind (e.g., accept and listen), hash security transport level (encryption and decryption and validation), and client connection with applications and their nodes for the healthcare execution in the network.

In this work, we implemented the blockchain technology with the socket-RMI in the solidity framework with an open API for developers. The fundamental API guideline has been taken from the tutorial in [35], where all open-source classes are defined, and source code is available for further usage. Initially, the solidity framework implemented different smart-contract methods for the other blockchain frameworks, and for this, we have also modified the classes in the network in the current work.

5.2. Results Discussion

The execution cost is a logical cost of workload execution in a socket-based RPC framework. Socket programming has different steps, such as client-socket and server socket. The study implemented remote procedure call services with the designed blockchain technology in the implementation part. This study implemented the existing baseline approaches, such as blockchain-offloading [12,17,19,23,24], blockchain-socket [9,11,14,16,20] and proposed blockchain socket-RPC, in the system.

Socket programming has a peer-to-peer network in terms of client–server architecture; in RPC, we considered the different nodes, and each workload was offloaded to the one fog node. The blockchain process was performed on the same machine as the initial execution and with the minimum hashing and proof of work validation in the blocks. All the workloads are hashed, based on SHA-256, and make transactions between the mobile device client socket and the server socket fog node for processing. The consensus algorithm validated each transaction using proof of work from execution to storage. The existing Ethereum [11] and Fabric [12] blockchains for distributed healthcare applications have a lot of validity and security. However, Ethereum and Fabric were initially designed for financial applications and, thus, need a lot of resources for execution.

Figure 5a shows the local cost execution during the initial phase of the blockchain process and then offloads it to the fog node for execution. The signature and validation process of proof of work is applied at each node; therefore, each process has a cost at each node. Figure 5a shows that the proposed RMI-socket blockchain gained optimal results compared to the existing offloading blockchain and socket-blockchain. The main reason is that all of the existing blockchain frameworks only focus on security and validation and ignore the offloading cost and processing in their model. However, this study devises the lightweight proof of work based on serverless functions and has less resource consumption than existing proof of work and validation in the mobile-fog-cloud environment. The proposed system has efficient layers in which mobile applications offload secure data to the fog node for processing, and fog nodes save their results on cloud computing with the cheaper data storage services in the system. Figure 5b,c shows that the blockchain cost and

fog and cloud cost were the optimal systems in the proposed work compared to existing blockchain-based systems for fine-grained applications.

Figure 5 shows that the proposed blockchain RMI-socket is more efficient in terms of cost compared to the existing one. Each hospital offers different storage options in the framework, as shown in Table 4. Figure 5d shows that the optimal storage from an existing third-party provider suffered from resource leakage due to the limited resource availability in their fog nodes.

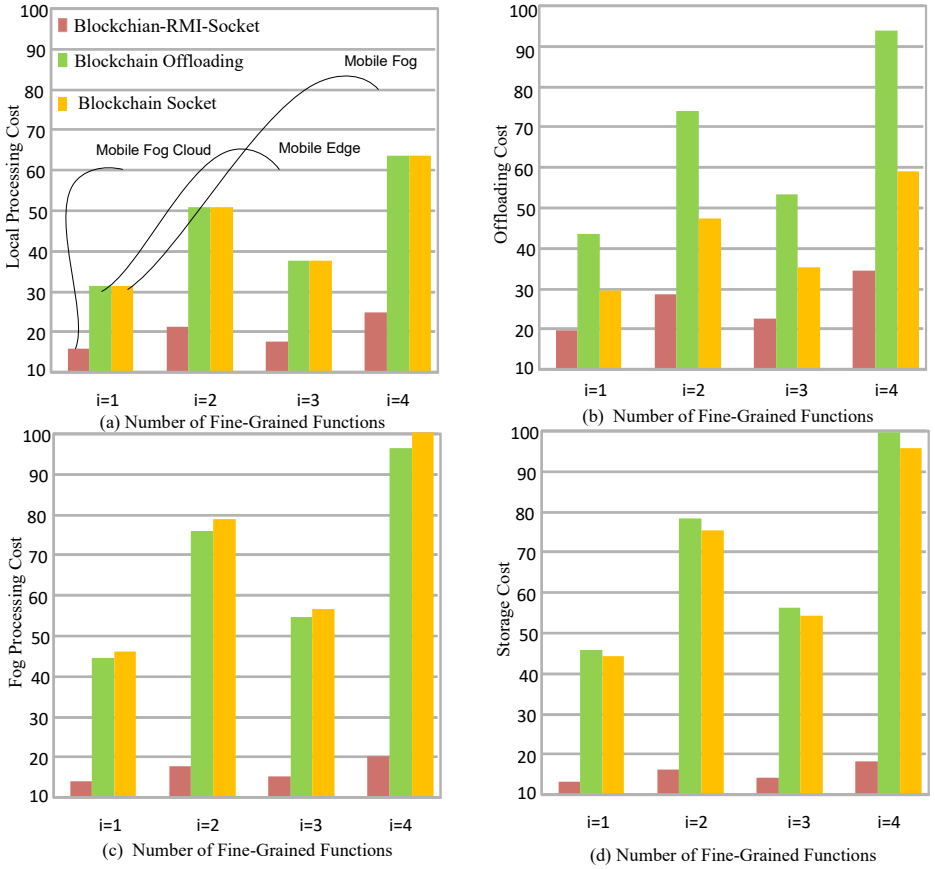

Figure 5. Cost-Efficient RMI-Socket-Blockchain System for Healthcare Functions in a Mobile-Fog-Cloud Network.

Figure 5d shows that the storage mechanism of the proposed blockchain socket RPC has fewer service costs compared to the existing storage and processing costs of socket-based methods and RPC-based methods for healthcare applications. The main goal of this study was to divide the workload between different nodes as existing workloads were executed on the same node, and the execution of this huge workload results in extra costs. Then, the workload is offloaded to a particular hospital, which has different fog nodes based on their costs. All workloads were executed on schedule.

Figure 6a,b shows the resource leakage at the mobile devices and fog nodes during the implementation of blockchain technology with the proof of work, signature matching and node and hash validation in the two-node network. Figure 6a shows that mobile devices have higher resource leakage because of their limited resource capacity and can not locally support the entire blockchain mining process for fine-grained functions. Figure 6b shows that the fog nodes cannot support the entire blockchain process during execution and storage during the random arrival of hash data to the system. The main reason is that all the blockchain cryptographic schemes are resource-hungry and require a lot of resources to meet their validation goals for healthcare applications. Therefore, there are many possibilities that it may face resource leakage during the blockchain validation for the healthcare application with the different schemes for

the specific node. Therefore, this study devised a three-layer lightweight blockchain mechanism where fine-grained functions are executed on different nodes to manage their resource leakage and minimize the processing and storage costs of the system.

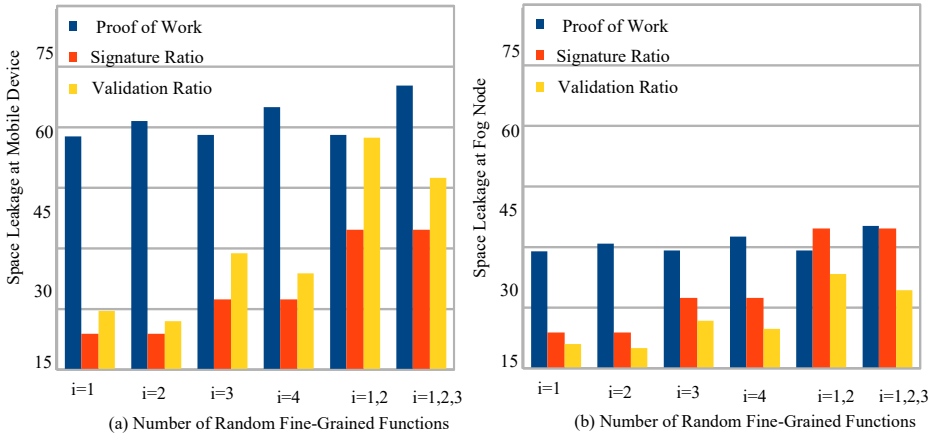

Figure 6. Resource Leakage Issue in Blockchain Technologies While Performing Cryptograhic Schemes for Healthcare Applications

5.3. Proof of Validation of Fine-Grained Tasks

This study compared the consensus methods of blockchain technologies for healthcare applications in a simulation environment. This study implemented four existing blockchain consensus schemes, i.e., PoW [31], PoS [32], DPoS [33] and LPoS [34], to compare them with the PPoV for fine-grained healthcare applications in the framework.

Figure 7 shows that the proposed PPoV has lower processing costs compared to all consensus schemes when running healthcare applications in a mobile-fog-cloud environment.

Initially, in the simulation environment, we submitted all fine-grained tasks to the system and analyzed the cost of application during execution in the system. After that, we submitted random fine-grained tasks to the system for execution. Figure 7 shows that partial validation on different nodes is lightweight and has lower processing and validation costs than existing blockchain methods during the processing of an application in the system.

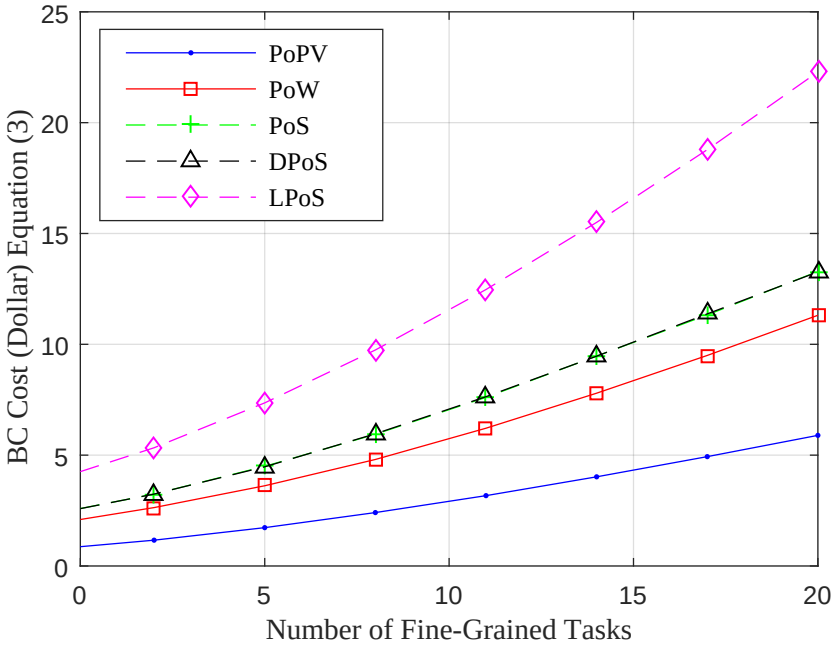

Figure 7. Proof of Validation Costs with All Healthcare Application Fine-Grained Tasks.

The blue PPoV line shows the lowest processing costs for fine-grained tasks of an application in the system.

Compared to other consensus blockchain algorithms, the PPoV outperformed in terms of cost and security validation among nodes in the system. There are many reasons for this better performance. (1) All the consensus blockchain algorithms work on homogeneous nodes in the form chain and share common protocols during their data transactions. However, these algorithms only focused on security and data validation without checking the resource availability at the nodes for the verification during data transportation in the network. In the blockchain, each node must verify the data validation to make the transaction immutable. Therefore, each node requires substantial resources to make huge transactions for different fine-grained tasks. In the experiment section, we analyzed that heterogeneous nodes have higher processing costs that the existing consensus algorithms because not all nodes have the same computing capabilities, such as mobile, fog, and cloud; therefore, they lead to increased processing costs during transactions in heterogeneous nodes of healthcare applications. In our case, we checked the resources in advance and applied partial validation to avoid resource leakages and overflow at the nodes. For example, the mobile device can encrypt, decrypt, and offload data to the fog nodes; if the mobile device has sufficient resources, it may validate the data. Otherwise, fog nodes validate the data instead of the mobile device, and the mobile device then acknowledges the valid data, resulting in the lowest processing costs in the system. (2) Another reason is that we divided data validation among different nodes; the powerful nodes can validate the hashing of data efficiently compared to resource-constraint devices in the network. Hence, it has been proved that PPoV is a reliable and cost consensus method for fine-grained applications in a heterogeneous network and obtained the optimal results, as shown in Figure 7.

6. Conclusions

This paper presented the blockchain-socket-RMI-based framework for fine-grained healthcare applications in a mobile-fog-cloud network. The proposed partial proof of validation (PPoV) scheme outperformed all existing blockchain schemes and validated the data with the minimum processing costs compared to all blockchain consensus methods. This study presented the abstraction levels of classes in a framework, which can be further improved for other healthcare applications.

In our future work, we will optimize the energy efficiency of mobile devices, fog nodes and blockchain processes in the framework for healthcare applications.

Author Contributions: Conceptualization, S.A., A.L., P.K. and O.T.; methodology, S.A., A.L., P.K. and O.T.; software, S.A. and A.L.; validation, P.K. and O.T.; formal analysis, S.A. and A.L.; investigation, S.A., A.L. and P.K.; resources, S.A. and A.L.; data correction, P.K.; writing—original draft preparation, S.A., A.L., P.K. and O.T.; writing—review and editing, S.A., A.L., P.K. and O.T.; visualization, A.L. and P.K.; supervision, A.L. and P.K.; project administration, A.L. and O.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was partially supported by Dawood University of Engineering and Technology, where this research has received funding support from the NSRF via the Program Management Unit for Human Resources and Institutional Development, Research and Innovation (Grant number B16F640189).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All the experimental data are generated at the local institution servers. Therefore, it cannot be made publicly available for other researchers.

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

References

1. Mohammed, M.A.; Rashid, A.N.; Kadry, S.; Abdulkareem, K.H. Deadline aware and energy-efficient scheduling algorithm for fine-grained tasks in mobile edge computing. *Sensors* **2022**, *18*, 168–193.
2. Dootio, M.A.; Lakhan, A.; Hassan Sodhro, A.; Groenli, T.M.; Bawany, N.Z.; Kumar, S. Secure and failure hybrid delay enabled a lightweight RPC and SHDS schemes in Industry 4.0 aware IIoHT enabled fog computing. *Math. Biosci. Eng.* **2021**, *19*, 513–536. [CrossRef] [PubMed]
3. Pinnarong, R.; Siangpipop, S.; Harncharnchai, A.; Nimmolrat, A.; Thinnukool, O. Thai Pregnant Mobile Application: Review and Development Report. *Int. J. Interact. Mob. Technol.* **2021**, *15*, 57. [CrossRef]
4. Li, X.; Tao, B.; Dai, H.N.; Imran, M.; Wan, D.; Li, D. Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic? *Pervasive Mob. Comput.* **2021**, *75*, 101434. [CrossRef] [PubMed]
5. Pintavirooj, C.; Keatsamarn, T.; Treebupachatsakul, T. Multi-Parameter Vital Sign Telemedicine System Using Web Socket for COVID19 Pandemics. *Healthcare* **2021**, *9*, 285. [CrossRef]
6. Dai, H.N.; Wu, Y.; Wang, H.; Imran, M.; Haider, N. Blockchain-empowered edge intelligence for internet of medical things against COVID-19. *IEEE Internet Things Mag.* **2021**, *4*, 34–39. [CrossRef]
7. Tuli, S.; Mahmud, R.; Tuli, S.; Buyya, R. Fogbus: A blockchain-based lightweight framework for edge and fog computing. *J. Syst. Softw.* **2019**, *154*, 22–36. [CrossRef]
8. Novakovic, A.; Marshall, A.H.; McGregor, C. Introducing a Conceptual Framework for Architecting Healthcare 4.0 Systems. In *Advances in Computer Vision and Computational Biology*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 579–589.
9. Kumar, S.; Raw, R.S.; Bansal, A.; Mohammed, M.A.; Khuwuthyakorn, P.; Thinnukool, O. 3D location oriented routing in flying ad-hoc networks for information dissemination. *IEEE Access* ***2021***, 9, 137083–137098. [CrossRef]
10. Khoso, F.H.; Arain, A.A.; Soomro, M.A.; Nizamani, S.Z.; Kanwar, K. A microservice-based system for industrial internet of things in fog-cloud assisted network. *Eng. Technol. Appl. Sci. Res.* **2021**, *11*, 7029–7032. [CrossRef]
11. Khoso, F.H.; Arain, A.A.; Kanwar, K. Serverless based functions aware framework for healthcare application. *Int. J. Emerg. Trends Eng. Res.* **2021**, *9*, 446–450.
12. Lakhan, A.; Mastoi, Q.U.A.; Elhoseny, M.; Memon, M.S.; Mohammed, M.A. Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud. *Enterp. Inf. Syst.* **2021**, *16*, 1883122. [CrossRef]
13. Ni, Y.; Luo, R.; Luo, H. Fabrication and mechanical properties of 3-D Cf/C-SiC-TiC composites prepared by RMI. *J. Alloys Compd.* **2019**, *798*, 784–789. [CrossRef]
14. Lakhan, A.; Ahmad, M.; Bilal, M.; Jolfaei, A.; Mehmood, R.M. Mobility aware blockchain enabled offloading and scheduling in vehicular fog cloud computing. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4212–4223. [CrossRef]
15. Lakhan, A.; Mohammed, M.A.; Kozlov, S.; Rodrigues, J.J. Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows. *Trans. Emerg. Telecommun. Technol.* **2021**, e4363. doi: 10.1002/ett.4363. [CrossRef]
16. Lakhan, A.; Mohammed, M.A.; Rashid, A.N.; Kadry, S.; Panityakul, T.; Abdulkareem, K.H.; Thinnukool, O. Smart-contract aware ethereum and client-fog-cloud healthcare system. *Sensors* **2021**, *21*, 4093. [CrossRef] [PubMed]
17. Tang, W.; Zhao, X.; Rafique, W.; Dou, W. A blockchain-based offloading approach in fog computing environment. In Proceedings of the 2018 IEEE International Conference on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, VIC, Australia, 11–13 December 2018; pp. 308–315.
18. Ren, J.; Li, J.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2021**, *27*, 760–776. [CrossRef]
19. Lakhan, A.; Dootio, M.A.; Alqahtani, F.; R Alzahrani, I.; Baothman, F.; Shah, S.Y.; Shah, S.A.; Anjum, N.; Abbasi, Q.H.; Khokhar, M.S.; et al. Hybrid workload enabled and secure healthcare monitoring sensing framework in distributed fog-cloud network. *Electronics* **2021**, *10*, 1974. [CrossRef]
20. Alli, A.A.; Alam, M.M. The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. *Internet Things* **2020**, *9*, 100177. [CrossRef]
21. Bi, H.; Liu, J.; Kato, N. Deep learning-based privacy preservation and data analytics for IoT enabled healthcare. *IEEE Trans. Ind. Informatics* **2021**, *18*, 4798–4807. [CrossRef]
22. Xu, L.; Zhou, X.; Tao, Y.; Liu, L.; Yu, X.; Kumar, N. Intelligent Security Performance Prediction for IoT-Enabled Healthcare Networks Using an Improved CNN. *IEEE Trans. Ind. Inform.* **2021**, *18*, 2063–2074. [CrossRef]
23. Wang, K.; Chen, C.M.; Tie, Z.; Shojafar, M.; Kumar, S.; Kumari, S. Forward Privacy Preservation in IoT-Enabled Healthcare Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1991–1999. [CrossRef]
24. Alazab, M.; RM, S.P.; Parimala, M.; Reddy, P.; Gadekallu, T.R.; Pham, Q.V. Federated learning for cybersecurity: concepts, challenges and future directions. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3501–3509. [CrossRef]
25. Barati, M.; Aujla, G.S.; Llanos, J.T.; Duodu, K.A.; Rana, O.F.; Carr, M.; Rajan, R. Privacy-Aware cloud auditing for gdpr compliance verification in online healthcare. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4808–4819. [CrossRef]
26. Godla, S.R.; Fikadu, G.; Adema, A. Socket programming-based rmi application for Amazon web services in distributed cloud computing. In *Innovative Data Communication Technologies and Application*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 517–526.

27. Lakhan, A.; Morten Groenli, T.; Majumdar, A.; Khuwuthyakorn, P.; Hussain Khoso, F.; Thinnukool, O. Potent Blockchain-Enabled Socket RPC Internet of Healthcare Things (IoHT) Framework for Medical Enterprises. *Sensors* **2022**, *22*, 4346. [CrossRef] [PubMed]
28. Vaezi, A.; Azarnoush, S.; Mohammadian, P. A Hundred Attacks in Distributed Systems. 2022. Available online: https://hal.archives-ouvertes.fr/hal-03657061/document (accessed on 28 January 2020).
29. Sodhro, A.H.; Pirbhulal, S.; Muzammal, M.; Zongwei, L. Towards blockchain-enabled security technique for industrial internet of things based decentralized applications. *J. Grid Comput.* **2020**, *18*, 615–628. [CrossRef]
30. Talat, R.; Obaidat, M.S.; Muzammal, M.; Sodhro, A.H.; Luo, Z.; Pirbhulal, S. A decentralised approach to privacy preserving trajectory mining. *Future Gener. Comput. Syst.* **2020**, *102*, 382–392. [CrossRef]
31. Lasla, N.; Al-Sahan, L.; Abdallah, M.; Younis, M. Green-PoW: An energy-efficient blockchain proof-of-work consensus algorithm. *Comput. Netw.* **2022**, *214*, 109118. [CrossRef]
32. Lendák, I.; Indig, B.; Palkó, G. WARChain: Consensus-based trust in web archives via proof-of-stake blockchain technology. *J. Comput. Secur.* **2022**, *30*, 499–515. [CrossRef]
33. Geng, T.; Njilla, L.; Huang, C.T. Delegated Proof of Secret Sharing: A Privacy-Preserving Consensus Protocol Based on Secure Multiparty Computation for IoT Environment. *Network* **2022**, *2*, 66–80. [CrossRef]
34. Du, Y.; Wang, Z.; Li, J.; Shi, L.; Jayakody, D.N.K.; Chen, Q.; Chen, W.; Han, Z. Blockchain-Aided Edge Computing Market: Smart Contract and Consensus Mechanisms. *IEEE Trans. Mob. Comput.* **2022**. [CrossRef]
35. Zheng, G.; Gao, L.; Huang, L.; Guan, J. *Ethereum Smart Contract Development in Solidity*; Springer: Berlin/Heidelberg, Germany, 2021.