Computer Networks 210 (2022) 108860

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

B2H: Enabling delay-tolerant blockchain network in healthcare for Society 5.0

Timam Ghosh [a], Arijit Roy [b,*], Sudip Misra [b]

[a] Advanced Technology Development Centre, Kharagpur, 721302, India
[b] Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, 721302, India

ARTICLE INFO

Keywords:
Blockchain
Secure healthcare
Society 5.0
Delay-tolerant
Long Short-Term Memory (LSTM)

ABSTRACT

This paper introduces an architecture – B2H – to enable a delay-tolerant public blockchain network (PBCN) in healthcare systems for Society 5.0. Healthcare systems in Society 5.0 envision an abstract paradigm that provides beyond health monitoring services to all the citizens of the society. These services include healthcare medical supply chain, clinical trial, and hospital management. To provide these services, the existing healthcare systems upload their important information, such as users' health parameters, medicinal details, and clinical trial information into the cloud using PBCN (Ioppolo et al., 2020). Additionally, PBCN provides end-to-end security in uploading of such healthcare information in healthcare systems by decentralizing and distributing the information validation among multiple end-user devices. The existing PBCN-based healthcare systems enable its users to validate information before the transaction of healthcare information. Enabling such a facility in the healthcare systems of Society 5.0 increases the validation latency of PBCN in healthcare systems, considering the presence of a huge number of citizens in Society 5.0. On the other hand, the existing PBCN-based healthcare systems are unable to detect malicious end-users, which may degrade the efficiency of the healthcare systems of Society 5.0. We introduce B2H to address the issues of increasing validation latency and detecting malicious end-users in the healthcare systems of Society 5.0. The architecture of B2H utilizes the features of PBCN. B2H introduce a layer of validation service providers (VSPs) in a PBCN that collects information from the end-user, distributes it among multiple validation devices. VSP in B2H reduces the validation time by distributing the information among a specific set of validation devices (VDs). B2H also allows the end-user to optimally select a VSP and a VSP to select a set of validation devices optimally. Through extensive experiments, we observe that B2H performs better than the existing schemes by reducing 94%–95% average network delay, 88%–94% average energy consumption, and 94%–96% average cost.

1. Introduction

Society 5.0 [1–3] conceives an abstract system that unifies different smart environments, amalgamates the physical–cyber–social world, and provides seamless services to the citizens of society. In Society 5.0, the existing healthcare systems [4,5] facilitate healthcare services beyond remote users' monitoring. By these healthcare systems, Society 5.0 aims to aid facilities in different healthcare services such as medicinal supply chain, clinical trial, and hospital managements that are evident during the pandemic situations of COVID-19 outbreak [4]. These services are depicted in Fig. 1. Typically, the healthcare systems upload remotely-sensed healthcare information to the cloud, apply analytics, and extract insights from the information. However, enabling end-to-end security of this information is essential during their transmission from the uses to the cloud. In the existing healthcare systems, the blockchain network (BCN) [6,7] promises to secure such end-to-end information transmission using a decentralized and distributed ledger system. To secure the same transmission in the context of Society 5.0, these healthcare systems give rise to the demands of incorporating a public BCN (PBCN) [8] where any citizen can enter or exit the network as per the requirement. In this work, we incorporate a PBCN-based healthcare system in Society 5.0 to enable security and proposed a scheme, B2H, that is capable of managing the increasing number of end-users and reducing data transmission delay during the validation process. The validation process is a feature of PBCNs which is discussed in the following.

1.1. Motivation

The traditional healthcare systems [9–13] use PBCN-based networks to address the security issues escalated during the transmission of

* Corresponding author.
E-mail addresses: timam.ghosh@iitkgp.ac.in (T. Ghosh), arijitroy@iitkgp.ac.in (A. Roy), smisra@cse.iitkgp.ac.in (S. Misra).

https://doi.org/10.1016/j.comnet.2022.108860
Received 17 February 2021; Received in revised form 5 February 2022; Accepted 14 February 2022
Available online 25 February 2022
1389-1286/

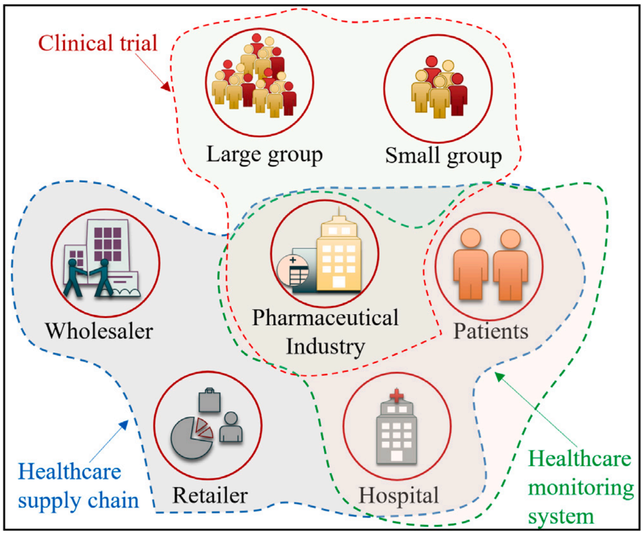

Fig. 1. Healthcare services in Society 5.0.

healthcare information. The PBCN used in these systems allows the end-user to distribute healthcare information among multiple validating devices (VDs) to validate. After validating the information, some of these VDs may approve the information, whereas others may disprove the information. The VDs send the validation decision to the end-user. If the majority of the VDs decide to approve the information, the end-user applies a proper security scheme to encrypt the information and upload it to the cloud, otherwise, the end-user discards it. Moreover, the end-user pays an incentive to these VDs for validating their information. However, being a public network, PBCN allows any end-user to be part of the network and validate it. On the other hand, the existing literature on Society 5.0 [14–16] does not include such a distributed architecture to provide the end-to-end security for information exchange in healthcare systems of Society 5.0. Thus, in this paper, we integrate the feature of the existing PBCN to provide the same in Society 5.0. However, for integrating PBCN with healthcare systems of Society 5.0, the following challenges need to be addressed:

(a) As we discussed, in a typical PBCN for healthcare, the VDs are selected to validate the users' data before it is transmitted. Additionally, these VDs are in-network devices that belong to the other users of the system. Thus, with the increase in the number of users in PBCN-based healthcare system for Society 5.0, the possibility of a huge number of VDs being selected to validate a users' data also increases. On the other hand, each of these selected VDs charges the users for validating their data. The existing PBCN for a healthcare system discusses the need for selecting the VDs for the data validation but lacks the perspective to restrict the number of VDs selected for a specific user. In this context, if the number of VDs selected for a user increases, the total expenditure charged to validate data also increases for a user. Thus, the increasing number of VDs selected to validate a user's data raises the issue of increasing user's expenditure in a PBCN-based healthcare system for Society 5.0.

(b) Some of the citizens in Society 5.0 may have the malicious intention of wrongly validating the information to reduces the efficiency of healthcare systems in society 5.0. The wrong validation of data increases the possibility of inefficient healthcare service provisioning [17] in PBCN-based healthcare system for Society 5.0. The end-user needs to pay incentives to VDs belonging to these citizens as well, in spite, they are not providing the expected services. To address the issue of wrong data validation due to malicious intentions of the users, the existing PBCN-based healthcare system extracts the majority decision from the decision collected from multiple VDs. However, if these systems can detect future malicious intentions and use this information to select more reliable, the system's efficiency can be further improved.

The increasing number of VDs, including malicious ones, increases the validation latency in the PBCN-based healthcare systems. On the other hand, for validating data, the total expense of the end-users in such PBCN-based healthcare system increases. Therefore, we motivate to design a delay-tolerant PBCN-based healthcare architecture for Society 5.0, and propose a scheme that is capable of:

- managing the high number of VDs for validating the data,
- detecting and penalizing the malicious VDs, and
- selecting an optimal set of VDs for a end-user while reducing the latency and the expenditure for information validation.

1.2. Contribution

This paper designs a PBCN-based healthcare system for Society 5.0 and introduces a scheme — B2H to address the issues of validation latency and manage validating devices in the designed architecture. The specific *contributions* of this work are as follows:

(a) The existing PBCNs-based healthcare systems raises the load of managing huge number of VDs by a UD in the presence of increasing number of users in Society 5.0. To address this issue, we design a PBCN based architecture that includes a layer of validation service providers (VSPs). This paper presume that the VSPs exhibit no malicious behavior during deployment of the designed architecture. Each VD in B2H is required to be registered under a VSP. The role of a VSP is to collect information from a UD, select an optimal set of VDs, and distribute the information among these VDs for validation. VSP also manages the cost in-flow and out-flow among the UDs and the VDs.

(b) In our designed architecture, multiple VDs participate, and some of them may have malicious intentions such as wrong validation of the information and information reviling with others. Therefore, the detection of such malicious VDs is very crucial. In this work, we propose B2H that is capable of predicting a malicious VD and penalizing them as per requirement.

(c) The designed architecture helps the end-users to connect a limited number of VDs, for healthcare information validation instead of connecting all the available VDs in the network. In this system, an end-user has multiple options to select a VSP through which the information validation is performed using VDs. On the other hand, a VSP has multiple options to select the VDs. Therefore, in this work, we propose B2H that helps an end-user to select an optimal VSP. B2H also helps a VSP to select an optimal set of VDs, which are responsible to validate the information. By selecting optimal VSP for an end-user and an optimal set of VDs for a VSP, B2H reduces the validation latency of PBCN-based healthcare system designed for Society 5.0.

2. Related work

This section elaborately discusses the state-of-the-art research related to our work. We categorize the related work into three parts — Healthcare systems in Society 5.0, PBCN in healthcare system, and Synthesis.

2.1. Healthcare systems in society 5.0

Fukuyama et al. [1] documented that the concept of Society 5.0 was initially conceived by the council for science, technology and innovation, Japan in 2016. Society 5.0 gains popularity by collaborating between information sharing and related knowledge, and assuring

Table 1
Service provided by B2H in comparison with the lacuna in the existing PBCN-based healthcare systems.

Healthcare systems	Architecture for Society 5.0	Validation time reduction	Malicious VDs detection	Penalty for malicious VDs
Rahulamathavan et al. [17]	✗	✗	✗	✗
Mamoshina et al. [18]	✗	✗	✗	✗
Dwivedi et al. [19]	✗	✗	✗	✗
Kim et al. [20]	✗	✗	✗	✗
Singh et al. [21]	✗	✗	✗	✗
B2H (**proposed**)	✓	✓	✓	✓

sustainable global development. Additionally, Both Salgues et al. [14] and Ferreira et al. [15] envisaged an abstract system for Society 5.0, unifying the physical–cyber–social world using Internet of Things (IoT), artificial intelligence (AI), and smart automation, to provide real-time and seamless services to all the citizen of the society. In Society 5.0, healthcare systems envision providing healthcare-based services to all the citizens in the society. Ioppolo et al. [4] reported that healthcare systems in Society 5.0 aim to facilitate services such as remote users' monitoring, clinical trial, hospital management, and managing vaccination services. These services raise the need to store healthcare information in the remote server or cloud for analytical purposes. To secure this healthcare information, these services need to apply end-to-end security schemes during such transmission. The existing researches, e.g. Hathaliya et al. [9], Singh et al. [10], Soltanisehat et al. [11], Khezr et al. [12], and Sgantzos et al. [13], emphasized on employing BCN in the healthcare system to provide end-to-end transmission security.

2.2. PBCN in healthcare systems

Currently, BCN is a very common mechanism in healthcare systems. Misra et al. [6] and Roy et al. [7], designed the decentralized transaction monitoring systems that provide end-to-end transaction security and prevents single point security failures. With the help of PBCN [8] — a variant of BCN, a healthcare system can allow any end-user with sufficient processing capability to join the system and acquire necessary services. Moreover, PBCN-based healthcare systems enable any end-user to validate healthcare information before archiving it in the cloud. Thus, PBCN is suitable for providing end-to-end transmission security in the healthcare systems of Society 5.0. However, the existing healthcare platform in Society 5.0 does not involve a PBCN-based architecture. Contrarily, there are existing healthcare systems [17–21] that utilizes the functionality of PBCN to provide end-to-end transmission security. Among these systems, Rahulamathavan et al. [17] introduced a PBCN-based IoT ecosystem and discussed the detailed workflow of the ecosystem in the context of healthcare. Additionally, this system validates the healthcare information with the help of VDs before storing the information in the cloud. In a similar context, Mamoshina et al. [18] discussed applications of AI in healthcare systems and introduces the open-source PBCN framework. They also proposed a PBCN-based platform for enabling users to control their personal information and manage access privileges, to protect information privacy. The platform proposed by the authors allows users to benefit by receiving a crypto-currency as a reward for their data. On the other hand, Dwivedi et al. [19] proposed architecture to integrated PBCN with IoT devices to prevent the privacy and security issues of medical data in a smart city scenario. Among the recently proposed PBCN-based healthcare systems, Kim et al. [20] utilized the artificial intelligence PBCN algorithm in the healthcare system to provide safe verification of users' healthcare information. Similarly, Singh et al. [21] proposed a PBCN-enabled Intelligent IoT Architecture to provide an efficient mechanism to unify PBCN and AI in IoT-based healthcare systems.

2.3. Synthesis

We investigated the existing healthcare systems thoroughly in Society 5.0, followed by the use of PBCN in healthcare systems. We observe that the existing works [17–21] do not provide any architecture for PBCN-based healthcare systems for Society 5.0. On the other hand, integrating PBCN-based healthcare systems in Society 5.0 allows any end-user to become part of PBCN. Due to the participation of a huge number of end-users in the system, it increases the information validation time, which is undesirable for time-critical applications. Inherently, the existing systems are unable to detect malicious VDs that are prone to validate healthcare information incorrectly. Moreover, the existing systems are incapable of penalizing the malicious VDs due to the incorrect validation of the information. In Table 1, we enlist the services provided by B2H in contrast to the lacuna in the existing PBCN-based healthcare systems.

3. System model

This paper design PBCN-based architecture for healthcare systems in Society 5.0 following the architecture of traditional PBCN-based healthcare system [17]. This architecture includes four types of components — UDs, VDs, VSPs, and a cloud-server. These components communicate among themselves using a wifi-based multi-hop access point (AP) network. The different devices present in the system and the workflow among these devices are depicted in Figs. 2a and 2b. In this architecture, a UD is directly associated with an end-user. It is either procured by the individual end-user or provided by the healthcare systems. A UD collects the health parameter from the associated end-user and archives it in a remote cloud server for future analysis. Before transmitting it to the cloud, the UD need to select a VSP and transmit the healthcare information to it. On receiving the information, the selected VSP selects a set of VDs and send the information to them. A VD is responsible for validating the healthcare information. According to Rahulamathavan et al. [17], the validation of healthcare information checks whether the information belongs to a pre-defined range. For example, blood pressure value for any end-user must be between 0 mmHg and 300 mmHg. Thus, such a validation process prevents out-of-range healthcare information. The selected VSP collects all the validation decisions from the selected VDs and extracts the majority decision from it. Further, the VSP send the majority decision to the UD. Thereafter, based on the validation decision received from the VSP, the UD encrypts the information and transmits them to the remote cloud server. To implement the above information flow among UDs, VDs, and VSPs, each VD needs to register itself to a specific VSP. The different aspects of the designed architecture are as follows:

3.1. Preliminaries

This section designs the network model, validation and reward models, and delay and energy models for the proposed scheme, B2H.

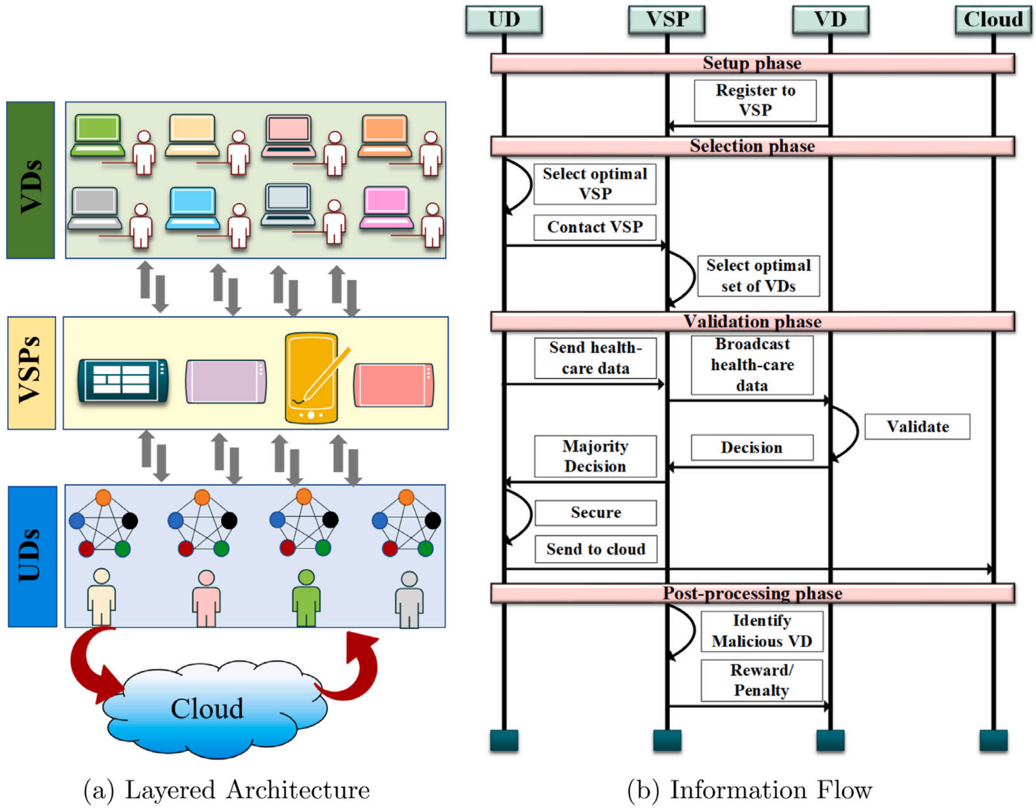

Fig. 2. System model of B2H.

3.1.1. Network model

We adopt the network model proposed in Misra et al. [22] to frame the network model for B2H. Misra et al. [22] propose a Wi-Fi access point (AP) based multi-hop network to establish communication among different IoT devices, such as edge and fog devices and cloud servers. Based on this configuration, B2H proposes to include a graph $\mathcal{G} = \{\mathcal{V}, \mathcal{L}\}$ where V represents the set of devices present in the system. Further, we categorize $\mathcal{V}$ into the following subsets: 1. UDs (U), 2. VDs (V), 3. VSPs (VS), 4. APs (A), and 5. cloud (C). The maximum numbers of UDs, VDs, VSPs, and APs present in the systems are m, n, o, and p. Additionally, a cloud platform is present in the system. A UD and a VD associate with a VSP during the information validation.

Definition 1. We define association and inverse association between two devices, v_i and v_j as $f(\cdot)$, and $f^{-1}(\cdot)$, such that $f(\cdot)$ denotes $f : v_i \to v_j$ and $f^{-1}(\cdot)$ denotes $f^{-1} : v_i \leftarrow v_j$.

Property 1. *The association properties between the different devices in B2H are as follows:*

1. *Both VD and UD are associated with a VSP. Thus,* $f : U \to VS$ *and* $f : V \to VS$ *produces one-to-one mapping.*
2. *A VSP is associated with multiple UDs and multiple VDs. Therefore,* $f^{-1} : U \leftarrow VS$ *and* $f : V \leftarrow VS$ *produces many-to-one mapping.*

Definition 2. We define a binary variable x_{ij} as the association between the ith UDs and the jth VSPs. x_{ij} is denoted as,

$$x_{ij} = \begin{cases} 1, & \text{if } f(u_i) = vs_j \text{ exists } \forall u_i \in U \text{ and } vs_j \in V \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

Definition 3. A binary variable y_{ij} is denoted as the association between the kth VDs and the jth VSPs. Therefore, y_{ij} is denoted as,

$$y_{ij} = \begin{cases} 1, & \text{if } f(v_k) = vs_j \text{ exists } \forall v_i \in V \text{ and } vs_j \in VS \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

In $\mathcal{G}$, $\mathcal{L}$ represents the set links between the devices. $P_{ij} \subset \mathcal{L}$ is a set of links denoting the shortest path between the ith and the jth devices. We consider $D(P_{ij})$ and $PD(P_{ij})$ as the distance of the shortest path P_{ij} between ith and the jth devices and the propagation delay to transmit 1 bit data for the shortest path P_{ij}, respectively. This shortest path is evaluated using the *Dijkstra* algorithm. We used Dijkstra algorithm for evaluating the shortest path for two reasons:

1. As we presumed that the network layout of the designed architecture does contain any negative edge, Dijkstra algorithm would be more suitable for evaluating the shortest path
2. The time complexity of Dijkstra Algorithm is $\mathcal{O}(\mathcal{V} + \mathcal{L}\log\mathcal{V})$, which is comparatively less than that of other shortest path algorithm such as Prims or Bellman Ford.

3.1.2. Validation and reward model

Each UD needs to upload their healthcare information, with size H, in the cloud. Before uploading to the cloud, the UD needs to validate the information. This validation is executed by a set of VDs. We consider that each VD requires $VL(D)$ time to perform validation on information D. After validating the information, the VDs share their validation decision with the UD. Based on the majority decision, the UD decides whether to drop the information or to encrypt it and send it to the cloud. The validation decision of some VDs may go against the majority decision due to having a malicious intention. These VDs are going to be penalized. On the other hand, the VDs, whose validation decision supports the majority decision, will be rewarded. We consider RW_k^t as reward value of kth at time t and rw denotes the reward fraction. If a VD is penalized, then RW_k^t is evaluated as $RW_k^{t-1}(1 - rw)$. On the other hand, if a VD is rewarded, then RW_k^t is evaluated as $RW_k^{t-1}(1 + rw)$.

The minimum and maximum of reward value for any VD is 0 and 1, respectively. Finally, we assume that each VD charges P_k amount for validating information.

3.1.3. Delay model

In this section, we discussed the delay model for B2H. We consider a log-distance pathloss model [22] with log-normal shadowing as:

$$PL_{[dB]} = 140.7 + 36.7 \log_{10} d_{[km]} + \mathcal{N}(8) \tag{3}$$

where $d_{[km]}$ is the distance between the two devices in $\mathcal{G}$, and $\mathcal{N}(8)$ is the zero-mean Gaussian distribution with standard deviation of 8. Between the ith and the jth devices in B2H, the log-shadowing is denoted as:

$$PL^{ij}_{[dB]} = a + 36.7 \log_{10} D(P_{ij}) \tag{4}$$

where $a = 140.7 + \mathcal{N}(8)$. Thereafter, we need to calculate the data rate between the ith and the jth devices. Using Shannon's Equation [22], we evaluate the data rate between the ith and the nth devices as:

$$r_{ij} = B \ln(1 + \frac{p_i^{tx} - PL^{ij}_{[dB]}}{\sigma^2}) \tag{5}$$

where B, p_i^{tx}, and σ^2 denote the link bandwidth, transmission power, and noise power, respectively. The total transmission delay is represented as,

$$\Delta^{Tx}_{ij} = \frac{Z_i}{r_{ij}} \tag{6}$$

3.1.4. Energy model

In B2H, the energy consumption for task execution in the edge devices depends on different factors such as the task type and the required clock cycle. We adopt the solution proposed by Misra et al. [22] to evaluate the energy consumption for the validation in the kth VD as $\mathcal{P}^{VL}_k = \rho\frac{\Omega_i}{\omega_k}$, where ρ is the power dissipation rate, depending on the processor architecture. Ω_i denotes the clock cycle required to validate the information Z_i, and ω_k denotes the CPU frequency. On the other hand, the energy consumption during transmission from the ith UD depends on the transmission of the information volume required by the tasks. If the transmission power of the ith UD is p_i^{tx}, the total transmission power ($\mathcal{P}^{tx}_i$) of the same device is $p_i^{tx}(\Delta^{Tx}_{in} + \Delta^{P}_{nj})$.

3.2. B2H: The proposed scheme

This paper proposes B2H that reduces the validating latency by reducing the number of VDs for a UD, detects, and penalizes the malicious VDs. The work flow of B2H is depicted in Fig. 2b. The workflow of B2H is divided into four phases, which are as follows,

3.2.1. Setup phase

In the setup phase, a new UD joins the proposed PBCN-Based healthcare systems using a software interface. It can joins the system before or during the deployment of the systems. Thus, this setup phase of B2H can occur at any time during the deployment of the systems. Additionally, while joining the system, the UD need to specify in the software interface whether it will participate in the healthcare information validation or not. Based on this information, B2H separates all the VDs in the systems form the UDs, an d allow them to register under a specific VSP. In this paper, we consider that a VD randomly selects a VSP and register to it.

Algorithm 1: Optimal VSP selection

```
Input: Set of VSPs (VS), a UD (u_i)
Output: Optimal VSP (vs*)
Randomly select vs_o ∈ VS;
vs* ← vs_o;
T_vsp ← vs_o;
while T_VSP ≢ VS do
    Randomly select vs_j ∈ VS;
    T_vsp ← vs_j;
    Calculate U_{u_i∈U,vs_j} and U_{u_i∈U,vs*};
    iif U_{u_i∈U,vs_j} ≿_{u_i∈U} U_{u_i∈U,vs*} then
        vs* ← vs_j;
    end
end
return vs*;
```

3.2.2. Selection phase

The selection phase of B2H occurs when a UD completes buffering the healthcare information and initiate validating the information. In this phase, B2H allows a UD to selects an optimal VSP before validating the information. This selection depends on the parameters such as transmission delay ($\Delta^{Tx}_{u_i,vs_j}$) and transmission energy consumed ($\mathcal{P}^{tx}_{u_i,vs_j}$) during the information transmission from u_i UD to vs_j VSP. We also consider the price (P_{vs_j}) charged by the vs_j VSP for processing the information validation. These parameters need to be normalized for making them unit less.

Definition 4. We define $\mathcal{U}^{\Delta}_{u_i,vs_j}$ as the normalized transmission delay between u_i and vs_j, which is formulated as,

$$\mathcal{U}^{\Delta}_{u_i,vs_j} = \frac{\Delta^{Tx}_{u_i,vs_j}}{\Delta^{max}} \tag{7}$$

Definition 5. $\mathcal{U}^{\mathcal{P}}_{u_i,vs_j}$ is defined as the normalized energy consumption during the information transmission between u_i and vs_j. $\mathcal{U}^{\mathcal{P}}_{u_i,vs_j}$ is calculated as,

$$\mathcal{U}^{\mathcal{P}}_{u_i,vs_j} = \frac{\mathcal{P}^{tx}_{u_i,vs_j}}{\mathcal{P}^{max}} \tag{8}$$

Definition 6. We define $\mathcal{U}^{P}_{vs_j}$ as the normalized price charged by vs_j, which is formulated as,

$$\mathcal{U}^{P}_{vs_j} = \frac{P_{vs_j}}{P^{max}} \tag{9}$$

In Eq. (7), (8), and (9), Δ^{max} and $\mathcal{P}^{max}$ denotes maximum allowable delay and energy consumption for any transmission between two devices, and P^{max} denotes maximum allowable price charged by any VSP or VD. Based on this normalized parameters, we evaluated the utility $\mathcal{U}_{u_i\in U,vs_j}$ for each UD in Eq. (10).

$$\mathcal{U}_{u_i\in U,vs_j} = \sum_{vs_j\in VS} x_{u_i,vs_j}(\frac{\alpha\mathcal{U}^{\Delta}_{u_i,vs_j} + \beta\mathcal{U}^{\mathcal{P}}_{u_i,vs_j}}{\mathcal{U}^{P}_{vs_j}}) \tag{10}$$

In Eq. (10), x_{u_i,vs_j} denotes the association between u_i UD and vs_j VSP. This association is defined in Section 3.1.1. For this selection, we need to find an optimal VSP ($vs^* \in VSP$) for which x_{u_i,vs^*} is 1 and $\mathcal{U}_{u_i\in U,vs^*}$ is minimized. This minimization problem is formulated in Eq. (11).

$$\min_{x_{u_i,vs^*}} \quad \mathcal{U}_{u_i\in U,vs^*} \tag{11a}$$

$$\text{s.t.} \quad \text{C1: } x_{u_i,vs^*} = 1 \tag{11b}$$

$$\text{C2: } P_{vs_*} \leq P_{u_i} \tag{11c}$$

$$\text{C3: } \Delta^{Tx}_{u_i,vs^*} \leq \Delta^{max} \tag{11d}$$

$$\text{C4: } \mathcal{P}^{Tx}_{u_i,vs^*} \leq \mathcal{P}^{max} \tag{11e}$$

$$\text{C5: } P_{vs^*} \leq P^{max} \tag{11f}$$

The minimization problem formulated in Eq. (11) includes 5 constraints. Among them, constraint C1 suggests that only one VSP is selected through this minimization problem. Constraint C2 and C5 states that the price (P_{vs^*}) charged by the selected VSP vs^* is need to be less than the maximum allowable charged price (P^{max}) and the price (P_{u_i}) desired by u_i. On the other hand, constraint C3 and C4 upper-bound the transmission delay and transmission energy consumption between u_i and vs_j by maximum allowable transmission delay and energy consumption. However, for selection optimal VSP (vs^*), we need to define the preference relation ($\succsim_{u_i \in U}$) of u_i.

Definition 7. We define $\mathcal{U}_{u_i \in U, vs_1} \succsim_{u_i \in U} \mathcal{U}_{u_i \in U, vs_2}$ as the preference relation of $u_i \in U$ for choosing vs_1 over vs_2. For the optimal VSP selection in B2H, we state that $\mathcal{U}_{u_i \in U, vs_1} \succsim_{u_i \in U} \mathcal{U}_{u_i \in U, vs_2}$ iff $\mathcal{U}_{u_i \in U, vs_1} \leq \mathcal{U}_{u_i \in U, vs_2}$.

The process for selecting optimal VSP is discussed in Algorithm 1. During the selection process, we define T_{VSP} as the set of VSP which are traversed once. Initially, we select a VSP $vs_o \in VS$, consider it as vs^*, and assign it to T_{vsp}. Further, we select another VSP $vs_j (\in VS, \notin T_{VSP})$ and calculate $\mathcal{U}_{u_i \in U, vs^*}$ and $\mathcal{U}_{u_i \in U, vs_j}$. We assign the newly selected VSP in T_{VSP}. If $\mathcal{U}_{u_i \in U, vs_j} \succsim_{u_i \in U} \mathcal{U}_{u_i \in U, vs^*}$, then we assign vs_j to vs^*, otherwise we select another VSP randomly. We continue this selection until no VSP is left to be traversed ($T_{VSP} \equiv VS$). At the end of the selection process, we assign vs^* to u_i for information validation.

3.2.3. Validation phase

In the selection phase, a UD selects an optimal VSP ($vs_j \in VS$) to which the UD uploads its healthcare information for validation. In this phase, the selected VSP further selects a set of VDS from its registered VDs ($v_k \in V$). This selection of set of VDs includes decision parameters such as the delay ($\Delta^{Tx}_{vs_j,v_k}$) and energy consumption ($\mathcal{P}^{Tx}_{vs_j,v_k}$) during the information transmission between the VSP and the its registered VDs, the price (P_{v_k}) charged by each of the registered VDs for information validation, and the current reward ($RW^t_{v_k}$) of each of the registered VDs. The current reward ($RW^t_{v_k}$) for each of the registered VDs (v_k) is predicted from the previous reward values ($RW^{t-1}_{v_k}$) of these VDs using the learning model $M(\cdot)$. The evaluation of previous reward values ($RW^{t-1}_{v_k}$) for these VDs is discussed in Section 3.1.2.

In B2H, a pre-trained Long–Short Term Model (LSTM) [23] is used to predict the future reward of the VDs. A LSTM model has three gates: (a) forget gate, (b) storing gate, and (c) update gate. The forget gate decides the volume of information to be removed from the current knowledge-base. In contrast, the storing gate determines the volume of information in the current event to be stored in the knowledge-base. Based on the outcome of the previous gates, the update gate periodically refreshes the knowledge-base before providing the predicted output. For predicting the next reward of a VD, it may be sufficient to use the knowledge obtained from the pattern of a few historical rewards. Moreover, the number of historical rewards needed to be observed may change over time due to the randomness in the VDs' behaviors. The possible number of rewards for a VD is uncountable. Prediction models, such as the Markov predictor [24], transforms the set of rewards into a set of states, where a state represents a set of rewards under a constraint. Such prediction models predict the future rewards in terms of the state based on fixed historical rewards. On the other hand, LSTM maintains the knowledge-based of the prediction model to a certain degree using the gates. It provides flexibility for observing the historical events while accumulating the knowledge in the model. Further, it does not require a state-based historical data-set to train a model and predict the future location.

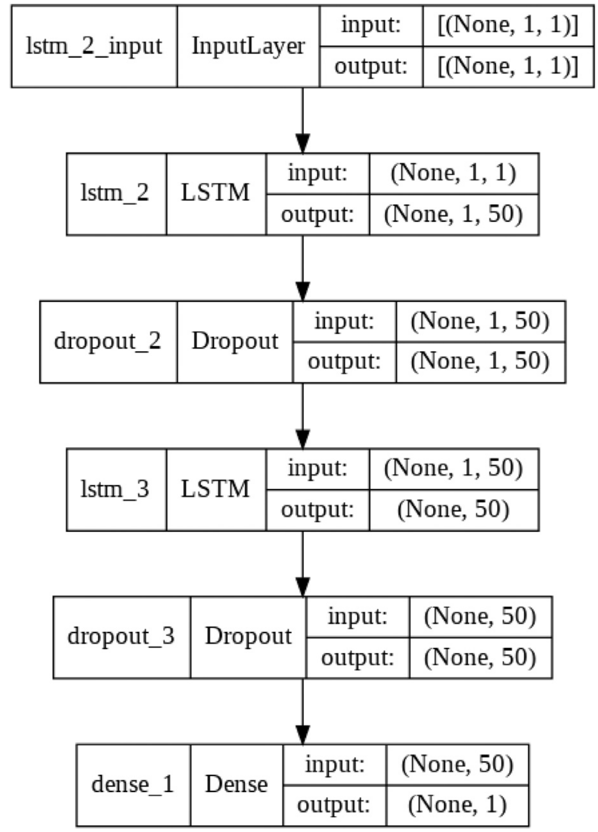

Fig. 3. Layered architecture of the pre-trained LSTM-based future reward prediction model.

Algorithm 2: Optimal set of VDs selection

Input: Set of VDs (V), a VSP (vs_j)
Output: Optimal set of VDs ($v^*_{vs_j}$)

```
Produce v^{vs_j} = {v_k | v_k ∈ V, x_{vs_j,v_k} = 1};
Randomly select v_o ∈ v^{vs_j};
v*_{vs_j} ← v_o;
T_vsp ← v_o;
Randomly select v*1_{vs_j};
while v*1_{vs_j} ∉ T_VD do
    T_vsp ← v*1_{vs_j};
    Calculate U_{vs_j, v*_{vs_j}} and U_{vs_j, v*1_{vs_j}};
    iif U_{vs_j, v*1_{vs_j}} ≿_{vs_j} U_{vs_j, v*_{vs_j}} then
        v*_{vs_j} ← v*1_{vs_j};
    end
    Randomly select v*1_{vs_j};
end
return v*_{vs_j};
```

We illustrate the architecture of the pre-trained LSTM-based future reward prediction model in Fig. 3. This model is divided into three layers. The first layer consists of two sub-layers: (a) LSTM layer and (b) dropout layer. The LSTM layer consists of 50 LSTM models with 1 time

Table 2
Simulation parameters.

Parameters	Values
Area	1000×1000 m^2
Number of UDs	100, 200, 300, 400, 500
Number of VDs	500, 600, 700, 800, 900, 1000
Number of VSP	50
Information size	10, 20, 30, 40, 50 MB
Transmission power	2.2 W
Noise	−100 dB
Bandwidth	1 Gbps
Confidence interval	95%
Price charged by VDs and VAPs	[100, 500] unit

step and 1 feature. Additionally, the dropout layer includes 50 dropout models with 1 time step and 1 feature. On the other hand, the second layer of the pre-trained model repeats the layered architecture of the first layer. Finally, the third layer of the pre-trained model includes a dense sub-layer with 50 dense models.

Definition 8. We define $\mathcal{U}^{\Delta}_{vs_j,v_k}$ as the normalized transmission delay between vs_j and v_k, which is formulated as,

$$\mathcal{U}^{\Delta}_{vs_j,v_k} = \frac{\Delta^{Tx}_{vs_j,v_k}}{\Delta^{max}} \tag{12}$$

Definition 9. $\mathcal{U}^{\mathcal{P}}_{vs_j,v_k}$ is defined as the normalized energy consumption during the information transmission between vs_j and v_k. $\mathcal{U}^{\mathcal{P}}_{vs_j,v_k}$ is calculated as,

$$\mathcal{U}^{\mathcal{P}}_{vs_j,v_k} = \frac{\mathcal{P}^{tx}_{vs_j,v_k}}{\mathcal{P}^{max}} \tag{13}$$

Definition 10. We define $\mathcal{U}^{P}_{v_k}$ as the normalized price charged by v_k, which is formulated as,

$$\mathcal{U}^{P}_{v_k} = \frac{P_{v_k}}{P^{max}} \tag{14}$$

Definition 11. $\mathcal{U}^{RW^t}_{v_k}$ is defined as the normalized reward of v_k for validating information at time t, which is formulated as,

$$\mathcal{U}^{RW^t}_{v_k} = \frac{RW^t_{v_k}}{RW^{max}} \tag{15}$$

For selecting the optimal set of VDs, we need to normalize the decision parameters for making them unit less. In Eqs. (12), (13), and (14), we use Δ^{max}, $\mathcal{P}^{max}$, and P^{max} for the production of normalized transmission delay and energy consumption and normalized price to validate information with respect to v_k. These constant values are discussed in Section 3.2.2. On the other hand, in Eq. (15), we used RW^{max} as maximum allowable reward to normalize the reward for any VDs. Based on this normalized parameters, we evaluated the utility $\mathcal{U}_{vs_j,v_k}$ for each UD in Eq. (10).

$$\mathcal{U}_{vs_j \in VS, v_k} = \sum_{v_k \in V} w_{vs_j,v_k} y_{vs_j,v_k} \left(\frac{\alpha \mathcal{U}^{\Delta}_{vs_j,v_k} + \beta \mathcal{U}^{\mathcal{P}}_{vs_j,v_k}}{\delta \mathcal{U}^{P}_{v_k} + \gamma \mathcal{U}^{RW^t}_{v_k}}\right) \tag{16}$$

In Eq. (10), y_{vs_j,v_k} reports the association between vs_j VSP and its registered v_k VSP. This association is defined in Section 3.1.1. However, we need to select a set of optimal VDs among these registered VDs. Thus, we define a binary variable w_{vs_j,v_k} whose value is assigned 1 if v_k VD is selected for VSP (vs_j); otherwise 0. We also define $v^*_{vs_j} \in VSP$) as the optimal set of VDs which is selected for vs_j and produce minimized utility value. This minimization problem is formulated as,

$$\begin{aligned}
&\min_{w_{vs_j,v^*_{vs_j}}} \mathcal{U}_{vs_j,v^*_{vs_j}} = \frac{1}{|v^*_{vs_j}|} \sum_{v_k \in v^*_{vs_j}} \mathcal{U}_{vs_j,v_k} \\
\text{s.t. } &\text{C1: } \sum_{v_k \in v^*_{vs_j}} w_{vs_j,v_k} \le \sum_{v_k \in V} x_{vs_j,v_k} \\
&\text{C2: } \sum_{v_k \in v^*_{vs_j}} w_{vs_j,v_k} P_{v_k} \le P^{max}_{vs_j} \\
&\text{C3: } \Delta^{Tx}_{vs_j,v_k \in v^*_{vs_j}} \le \Delta^{max} \\
&\text{C4: } \mathcal{P}^{Tx}_{vs_j,v_k \in v^*_{vs_j}} \le \mathcal{P}^{max} \\
&\text{C5: } \sum_{v_k \in v^*_{vs_j}} w_{vs_j,v_k} P_{v_k} \le P^{max}
\end{aligned} \tag{17}$$

The minimization problem formulated in Eq. (17) includes 5 constraints. Constraint C1 suggests on selecting multiple VDs through this minimization problem. However, the number of selected VDs should be less than the number of registered VDs under vs_j. On the other hand, the constraint C2 and C5 states that the total price charged by the selected VDs is less than the maximum allowable charged price (P^{max}) and the price (P_{vs_j}) desired by vs_j. Similar to Eq. (11), constraint C3 and C4 upper-bound the transmission delay and transmission energy consumption between vs_j and the selected VDs $v^*_{vs_j}$ by maximum allowable transmission delay and energy consummation. However, for selection optimal VSP ($v^*_{vs_j}$), we need to define the preference relation ($\succsim_{vs_j}$) of vs_j.

Definition 12. We define $\mathcal{U}_{vs_j,v^{*1}_{vs_j}} \succsim_{vs_j} \mathcal{U}_{vs_j,v^{*2}_{vs_j}}$ as the preference relation of vs_j for choosing $v^{*1}_{vs_j}$ over $v^{*2}_{vs_j}$. For the selection of optimal set of VDs in B2H, we state that $\mathcal{U}_{vs_j,v^{*1}_{vs_j}} \succsim_{vs_j} \mathcal{U}_{vs_j,v^{*2}_{vs_j}}$ iff $\mathcal{U}_{vs_j,v^{*1}_{vs_j}} \le \mathcal{U}_{vs_j,v^{*2}_{vs_j}}$.

The process for selecting optimal VSP is discussed in Algorithm 2. During the selection process, we define T_{VD} as the set of VDs which are traversed once. In the algorithm, we initially select a VSP $v_o \subset V$, assign it to $v^*_{vs_j}$ and T_{VD}. Thereafter, we randomly select another set of VDs $v^{*1}_{vs_j} (\subset V, \notin T_{VD})$ and calculate $\mathcal{U}_{vs_j,v^*_{vs_j}}$ and $\mathcal{U}_{vs_j,v^{*1}_{vs_j}}$. We also assign the newly selected VSP to T_{VSP}. If $\mathcal{U}_{vs_j,v^{*1}_{vs_j}} \succsim_{vs_j} \mathcal{U}_{vs_j,v^*_{vs_j}}$, we nullify $v^*_{vs_j}$ and assign $v^{*1}_{vs_j}$ to $v^*_{vs_j}$; otherwise we select another set of VDs randomly. We continue this selection until no all the permuted selection of VDs are considered. At the end of the selection process, we assign $v^*_{vs_j}$ to vs_j for information validation.

After selecting the optimal set of VDs, the VSP collects information from a UD, distributes it to the selected VDs. These VDs perform validation operations and share their validation decision with the associated VSP. Based on the decisions collected from the VDs, the VSP selects the majority decision and reply back to the UD.

3.2.4. Post-processing phase

B2H initiate this phase when a VSP completes the information validation with the help of selected VDs and reply back the majority decision regarding the validation. In this phase, B2H allows a VSP to evaluate the performance of each registered VDs based on their validation decision and detect the malicious VDs. During the validation phase, the VSP collects the validation decision from the set of optimally selected VDs and selects the majority decision. It may happen that the validation decision of some selected VDs reports against the majority decision. On the other hand, the remaining selected VDs may support the majority decision. Thus, the VSP rewards the selected VDs, who supports the majority decision, by incriminating the reward value. However, the same VSP penalizes the selected VDs, who reject the majority decision, by reducing the reward value. This rewarding mechanism is discussed in Section 3.1.2. Using this rewarding mechanism, a VSP is able to observe the change in the reward value of its

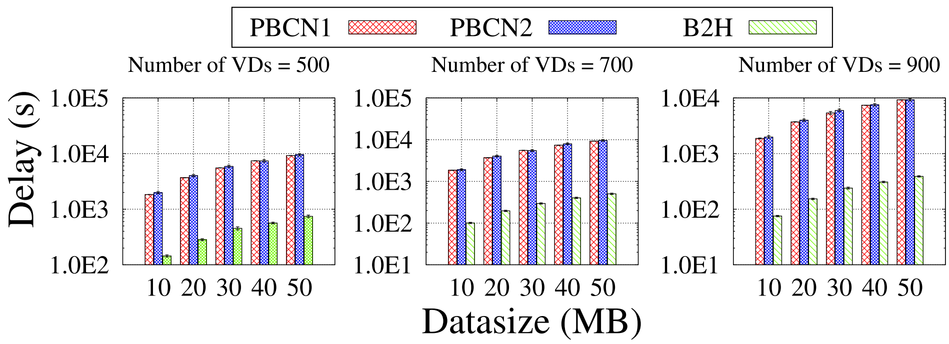

Fig. 4. Average delay for 500 UDs.

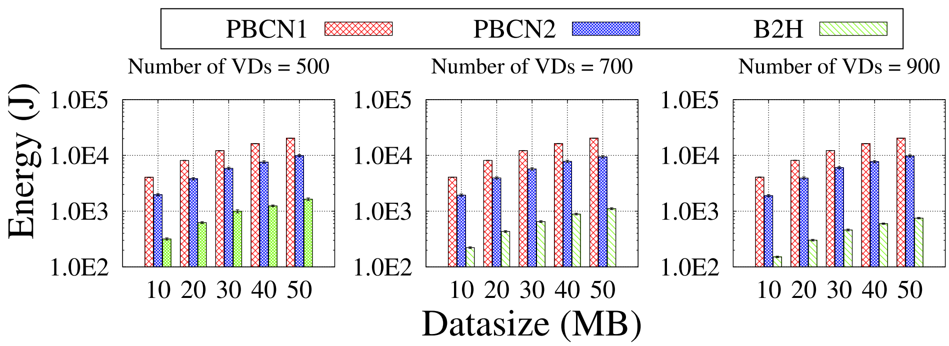

Fig. 5. Average energy consumption.

registered VDs over multiple rounds of information validation . In this observation, a VD with decreasing reward value is highly possible to be a malicious node. Thus, based on this observation, the VSP is able to detect the malicious VDs and exclude them from the future information validation rounds. Additionally, this reward value is a different entity than the price charged by the VDs.

4. Performance evaluation

4.1. Experimental design

We conduct the experiment considering 100–500 UDs, 500–1000 VDs, 50 VSP, and a cloud platform to evaluate the performance of the proposed scheme, B2H. These devices are randomly deployed over 1000×1000 m^2 simulation area. The UDs validate the healthcare information with a size of 10–50 MB before uploading it to the cloud. Furthermore, they transmit the information with 2.2 W transmission power over the channel having -100 dB noise and 5 Mbps Gbps bandwidth. The VDs in the system charge a random price in the range of $[100, 500]$ unit to validate a piece of information. Furthermore, we design the simulation using the network model mentioned in Section 3.1.1 and compare with the traditional PBCN e.g. [19,20]. For better representation, we denote these benchmark scheme as PBCN1 and PBCN2. In the simulation, we initialize the aforementioned devices with random positions. We trained the last-based reward prediction model using a reward data set with 10,000, 30,000, and 50,000 records. We generate this reward data set using $rand()$ function in MatlaB R2020a. The evaluation parameters and their values are listed in Table 2.

4.2. Performance matrices

We evaluate the performance of the proposed scheme, B2H, against the existing benchmark schemes [19,20] considering the following parameters:

(1) *Network metrics:* We evaluate the performance of B2H using the network metrics — average delay, average energy consumption, and the average cost charged by the VDs as depicted in Figs. 4, 5, and 6. Considering the average delay and average energy consumption, we determine the reduction in validation latency and network lifetime in B2H compared to the benchmark schemes.

(2) *Scalability metrics*: Similarly, we evaluate the impact of scalability on B2H using the metrics — average delay, average energy consumption, and the average cost charged by the VDs. While evaluating the scalability, we varied the number of VDs and UDs and information size as depicted in Figs. 7 and 8.

(3) *Prediction performance metrics*: B2H uses an LSTM-based model to predict the future behavior of VDs in terms of reward. Thus, we evaluate the prediction performance in terms of average prediction accuracy and average prediction latency. Using average prediction accuracy, we infer the suitability of the model in B2H. On the other hand, using the average prediction latency, we observe the feasibility of implementing such a model in resource constraint VSPs.

4.3. Results and discussion

In this section, we elaborately discuss the analysis of the results obtained from our experiments. We also discuss the performance of B2H in contrast to the existing approaches — PBCN1 [20] and PBCN2 [19].

(1) *Analysis on Network Metrics:* As discussed, we consider average network delay, average energy consumption, and average packet loss as network metrics for evaluating the performance of B2H. In Figs. 4, 5, and 6, we depict the obtained results of these metrics over a varying number of VDs and the data size. These results report that B2H reduces the average network delay, the average energy consumption, and the average cost in contrast to the existing approaches — PBCN1 [20] and PBCN2 [19]. B2H allows a UD to transmits its healthcare information to a VSP. Thereafter, the VSP distributes the information among its registered VDs for validation. Unlike the benchmark schemes, a VSP does not distribute the information among all the VDs present in the system. Thus, B2H reduces the average validation latency, average energy consumption, and average cost by reducing the number of VDs

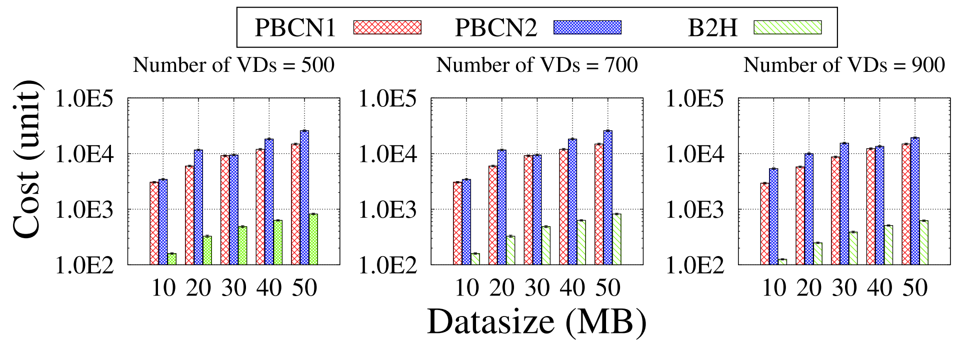

Fig. 6. Average cost for 500 UDs.

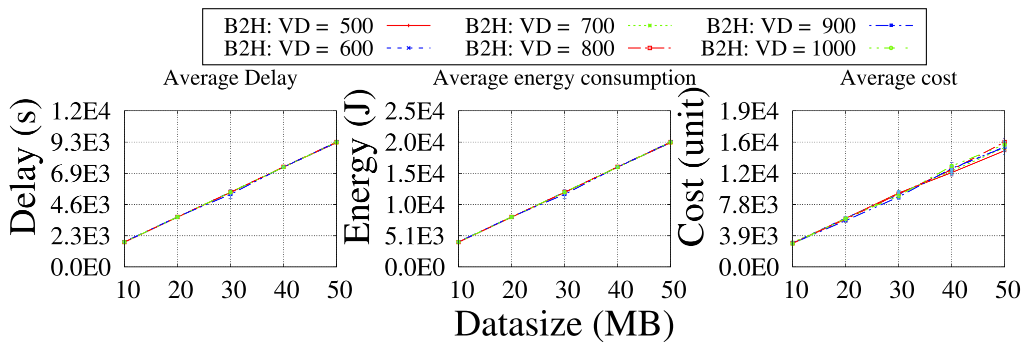

Fig. 7. Impact of varying VDs on B2H over 500 UDs.

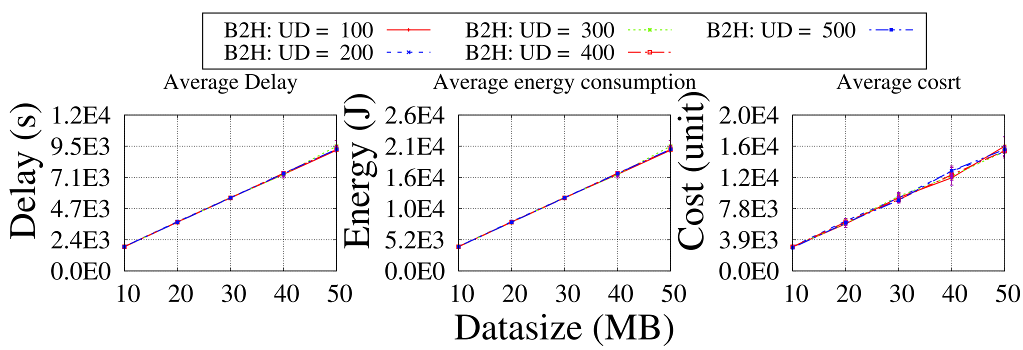

Fig. 8. Impact of varying UDs on B2H over 1000 VDs.

per UD. Furthermore, it seems that the results depicted in Figs. 4, 5, and 6 justify this theoretical analysis. Furthermore, we observe that B2H reduces the average delay and average cost by $94-95\%$ and $94-96\%$ in comparison with the benchmark schemes.

Typically, the network lifetime of a system depends on the average energy consumption. Moreover, the network lifetime measures the operating time of a network. On the other hand, the increase in average energy consumption reports that the network devices consume their energy resources at an increased rate. Due to such a consumption rate, the network may not provide services to the end-users for an expected duration, and thus, the network lifetime reduces. Contrarily, we observe in Fig. 5 that B2H reduces the energy consumption by $88-94\%$ as compared to the benchmark schemes. As discussed previously, a UD in B2H share its healthcare information with A VSP, and the VSP again share this information with its registered VDs during the validation phase. Using such information distribution, B2H reduces the number VDs required in contrast to the existing schemes during the validation phase. Thus, B2H reduces the energy consummation for information transmission and validation during the same phase. Such reduction is supported by the evaluated results depicted in Fig. 5. Therefore, B2H increases the network lifetime.

(2) *Analysis of learning parameters:* B2H allows the VSPs to predict the future reward of its registered VDs using a pre-trained LSTM-based model. The pre-trained model is initially trained on a computationally-rich machine. This training phase of the model is not included in the B2H. Thus, we only analyze the learning parameters for reward prediction in B2H. We consider average prediction latency and average accuracy as the learning parameters depict the evaluated results in Fig. 9. In these figures, we observe that the LSTM-based prediction model requires less time for predicting future rewards. On the other hand, based on these results, we infer that the pre-trained LSTM-based model is able to provide a significant accuracy in predicting the future rewards of the VDs.

(3) *Analysis on scalability of B2H:* We analyze the scalability of B2H by observing the impact of a varying number of VDs, UDs, and data size on its network metrics. Figs. 7 and 8 depicts evaluated results on network metrics such as the average network delay, average energy consumption, and average cost over varying VDs, UDs, and data size. In these results, we observe that B2H reports a linear increase in these network metrics over varying VDs, UDs, and data size. While simulating B2H, we fix the number of VSPs and vary the number of UDs and VDs

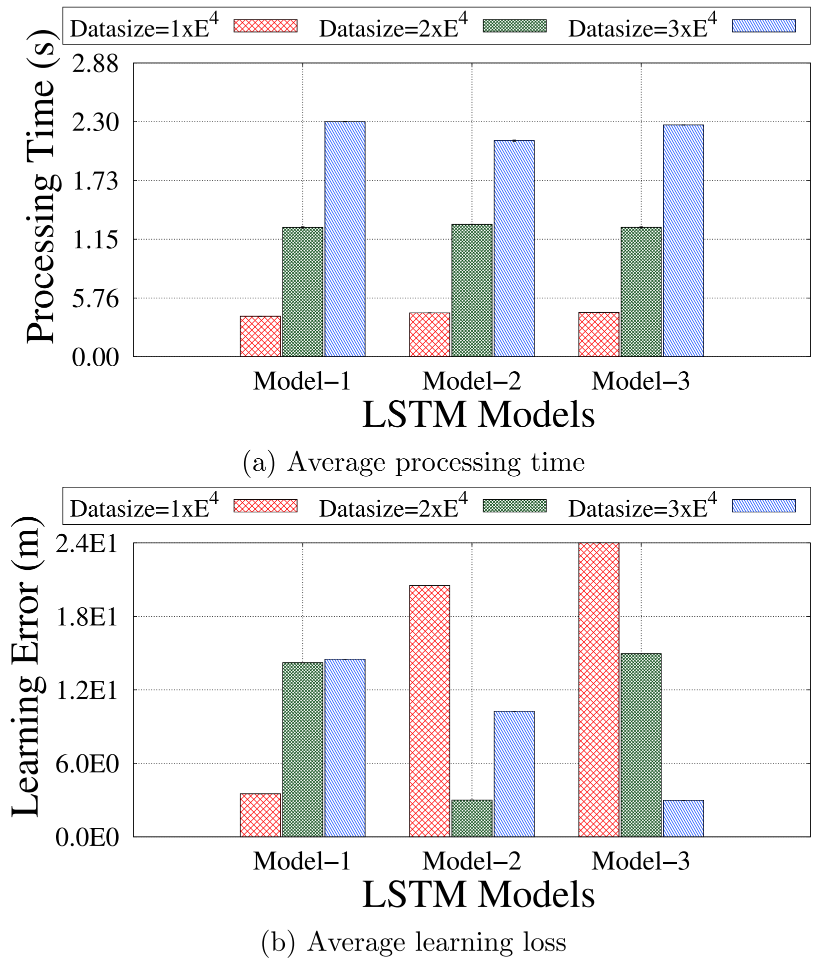

Fig. 9. Performance of reward learning using LSTM.

and the data size. As the number of VSP is fixed, a VSP in B2H reports negligible increase in the number of UDs and VDs associate with itself in comparison with the increase in the number of UDs and VDs. We also observe a minute variation in the network metrics for different number of UDs and VDs which is caused due to the randomness in simulating the deployment of the network devices. Based on this analysis, we state that B2H is scalable.

4.4. Overall observation

Based on the obtained results, we observe that B2H reduces the average network delay by 94 – 95%, the average energy consumption by 88 – 94%, and the average cost by 94 – 96% in comparison with the benchmark schemes. Moreover, B2H is scalable and improves the network lifetime.

5. Conclusion

This paper introduced an architecture – B2H – to enable a delay-tolerant public blockchain network (PBCN) in healthcare systems for Society 5.0. B2H used a VSP that collects healthcare information from UDs, distributes it among multiple registered VDs. B2H also allows the end-user to optimally select a VSP and allows a VSP to select a set of VDs optimally. On the other hand, B2H predicts the future reward of a registered VDs using a LSTM-based model. Using this prediction, B2H detects the malicious behavior of the VDs, and isd able to exclude it from the validation process. Through the extensive experiment, we observe that B2H performs better than the existing schemes. Moreover, we observe that B2H is scalable and improves the network lifetime.

We plan to extend this work in the future, by selecting an optimal VSP and an optimal set of VDs with cost-effectiveness. Using such a selection process, we need select the VDs and VSPs while maximizing the profit of VSP and VDs, and minimizing the expenditure of UDs.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Fukuyama, Society 5.0: Aiming for a new human-centered society, Jpn. Spotlight 27 (2018) 47–50.
[2] T. Ghosh, A. Roy, S. Misra, N.S. Raghuwanshi, CASE: A context-aware security scheme for preserving data privacy in iot-enabled society 5.0, IEEE Internet Things J. (2021) 1, http://dx.doi.org/10.1109/JIOT.2021.3101115.
[3] T. Ghosh, R. Saha, A. Roy, S. Misra, N.S. Raghuwanshi, AI-based communication-as-a-service for network management in society 5.0, IEEE Trans. Netw. Serv. Manage. 18 (4) (2021) 4030–4041.
[4] G. Ioppolo, F. Vazquez, M. Hennerici, E. Andrès, Medicine 4.0: New technologies as tools for a society 5.0, J. Clin. Med. 9 (7) (2020).
[5] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, J. Inform. Secur. Appl. 50 (2020) 102407.
[6] S. Misra, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, M. Rajarajan, Blockchain at the edge: Performance of resource-constrained IoT networks, IEEE Trans. Parallel Distrib. Syst. 32 (1) (2020) 174–183.
[7] C. Roy, S. Misra, S. Pal, Blockchain-enabled safety-as-a-service for industrial IoT applications, IEEE Internet Things Mag. 3 (2) (2020) 19–23.
[8] T.A. Syed, A. Alzahrani, S. Jan, M.S. Siddiqui, A. Nadeem, T. Alghamdi, A comparative analysis of blockchain architecture and its applications: Problems and recommendations, IEEE Access 7 (2019) 176838–176869.

[9] J. Hathaliya, P. Sharma, S. Tanwar, R. Gupta, Blockchain-based remote patient monitoring in healthcare 4.0, in: 9^{th} International Conference on Advanced Computing (IACC), IEEE, 2019, pp. 87–91.
[10] P. Singh, N. Singh, Blockchain with IoT and AI: A review of agriculture and healthcare, Int. J. Appl. Evol. Comput. 11 (4) (2020) 13–27.
[11] L. Soltanisehat, R. Alizadeh, H. Hao, K.-K.R. Choo, Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review, IEEE Trans. Eng. Manage. (2020).
[12] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: A comprehensive review and directions for future research, Appl. Sci. 9 (9) (2019) 1736.
[13] K. Sgantzos, I. Grigg, Artificial intelligence implementations on the blockchain. Use cases and future applications, Future Internet 11 (8) (2019) 170.
[14] B. Salgues, Society 5.0: Industry of the Future, Technologies, Methods and Tools, John Wiley & Sons, 2018.
[15] C.M. Ferreira, S. Serpa, Society 5.0 and social development, Manage. Organ. St. (5) (2018) 26–31.
[16] Y.A. Prasetyo, A.A. Arman, Group management system design for supporting society 5.0 in smart society platform, in: International Conference on Information Technology Systems and Innovation (ICITSI), IEEE, 2017, pp. 398–404.
[17] Y. Rahulamathavan, R.C.-W. Phan, M. Rajarajan, S. Misra, A. Kondoz, Privacy-preserving blockchain-based IoT ecosystem using attribute-based encryption, in: International Conference on Advanced Networks and Telecommunications Systems (ANTS), IEEE, 2017, pp. 1–6.
[18] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, et al., Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare, Oncotarget 9 (5) (2018) 5665.
[19] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.
[20] S.-K. Kim, J.-H. Huh, Artificial neural network blockchain techniques for healthcare system: Focusing on the personal health records, Electronics 9 (5) (2020) 763.
[21] S.K. Singh, S. Rathore, J.H. Park, Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence, Future Gener. Comput. Syst. 110 (2020) 721–743.
[22] S. Misra, N. Saha, Detour: Dynamic task offloading in software-defined fog for IoT applications, IEEE J. Sel. Area Commun. 37 (5) (2019) 1159–1166, http://dx.doi.org/10.1109/JSAC.2019.2906793.
[23] S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily, J.B. Othman, QoS enhancement with deep learning-based interference prediction in mobile IoT, Comput. Commun. 148 (2019) 86–97.
[24] F. Piccialli, S. Cuomo, F. Giampaolo, G. Casolla, V.S. di Cola, Path prediction in IoT systems through Markov chain algorithm, Future Gener. Comput. Syst. 109 (2020) 210–217.

Timam Ghosh is a Senior Research Fellow and Ph.D. Scholar in the Advanced Technology Development Center, Indian Institute of Technology Kharagpur, India. Prior to that, he completed a Master of Technology (M.Tech.) degree from the West Bengal University of Technology (in-house), India. His current research interests include Internet of Things, cloud and fog computing, THz communications, Society 5.0, and Wireless Body Area Networks.

Dr. Arijit Roy is the Co-founder and Director of an IoT start-up, ''SensorDrops Networks Pvt. Ltd.''. He did his Ph.D. studies from the Indian Institute of Technology Kharagpur (IIT Kharagpur), India. Dr. Roy was a Senior Research Fellow of the Council of Scientific & Industrial Research, Govt. of India. Prior to that, he completed an M.S. (by research) degree and B.Tech. degree in Information Technology from the Indian Institute of Technology Kharagpur and the West Bengal University of Technology, respectively. After completion of B.Tech., he worked as a Network Engineer in IntecInfonet Pvt. Ltd., India. He has 9 years of teaching experience at IIT Kharagpur. Dr. Roy has experience in handling several government-funded national and international research projects. His research works are published in different reputed SCI journals (including IEEE/ACM Transactions) and reputed conferences (IEEE WCNC, IEEE ICC, IEEE GLOBECOM, ACM ICDCN). He won the IEEE Systems Journal Best Paper Award 2020. Arijit delivered several talks in India and abroad. Additionally, he filed 6 Indian patents, which are along the same line of his research work. He received the Council of Scientific & Industrial Research Senior Research Fellowship (CSIR-SRF) in 2017. He has been recognized with several awards such as Samsung Innovation Award 2014 and IBM Day Award 2017. One of his research projects was selected (among the top 9 worldwide) in the IEEE ComSoc Student competition in 2014. He received the prestigious Gandhian Young Technological Innovation (GYTI) Award-2018, for society relevant innovation (the award was received from the honorable President of India). He was awarded the prestigious India–France Raman-Charpak Fellowship-2018 (only 4 students were selected in Engineering Sciences from India), for visiting a French university and pursuing short-term collaborative research. Dr. Roy received different travel grants from IIT Kharagpur and Microsoft Research (MSR) for attending international conferences and research events. He was selected as a young researcher to participate in the 6th Heidelberg Laureate Forum 2018, organized in Heidelberg, Germany, in which only the 200 most qualified Young Researchers (worldwide) are given the opportunity to enrich and share the unique atmosphere of the Heidelberg Laureate Forum. His research interests include Internet of Things (IoT), Sensor-cloud Architecture, Wireless Sensor Networks, Cloud Computing, Society 5.0, and Wireless Body Area Networks. Dr. Roy, along with his team, developed different societal impactful products and prototypes in the domain of healthcare and agriculture.

Dr. Sudip Misra received the bachelor's degree from the Indian Institute of Technology, Kharagpur, India; the master's degree from the University of New Brunswick, Fredericton, NB, Canada; and the Ph.D. degree in computer science from Carleton University, Ottawa, ON, Canada. He is an Associate Professor with the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur. Prior to this, he was with Cornell University, Ithaca, NY, USA; Yale University, New Haven, CT, USA; Nortel Networks, Canada; and the Government of Ontario, Canada. He has several years of experience working in academia, government, and the private sectors in research, teaching, consulting project management, architecture, software design, and product engineering roles. Currently, Dr. Misra is the Associate Editor of the IEEE Transactions Mobile Computing. He served as a TPC member in several IEEE conferences. He is the author of over 290 scholarly research papers (including 160 journal papers). His current research interests include algorithm design for emerging communication networks and Internet of Things. Dr. Misra has been a recipient of nine research paper awards in different conferences. He was awarded the IEEE ComSoc Asia Pacific Outstanding Young Researcher Award at IEEE GLOBECOM 2012. He was also awarded the Canadian Government's prestigious NSERC Post Doctoral Fellowship and the Humboldt Research Fellowship in Germany. He has edited eight books in the areas of wireless ad hoc networks, wireless sensor networks, wireless mesh networks, communication networks and distributed systems, network reliability and fault tolerance, and information and coding theory, which were published by reputed publishers such as Springer, Wiley, and World Scientific.