




Article

STHM: A Secured and Trusted Healthcare Monitoring Architecture Using SDN and Blockchain

Ezedin Barka ^{1,*}, Sofiane Dahmane ^{2,3} , Chaker Abdelaziz Kerrache ^{2,*} , Mohamad Khayat ¹ and Farag Sallabi ¹ 

- ¹ College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 17551, United Arab Emirates; 201670294@uaeu.ac.ae (M.K.); f.sallabi@uaeu.ac.ae (F.S.)
- ² Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat 03000, Algeria; s.dahmane@lagh-univ.dz
- ³ Department of Mathematics, Ecole Normale Supérieure Abderrahmane Taleb, Laghouat 03000, Algeria
- * Correspondence: ebarka@uaeu.ac.ae (E.B.); ch.kerrache@lagh-univ.dz (C.A.K.)

Abstract: Healthcare professionals and scholars have emphasized the need for IoT-based remote health monitoring services to track the health of the elderly. Such systems produce a large amount of data, necessitating the security and privacy of that data. On the other hand, Software Defined Networking (SDN) integration could be seen as a good solution to guarantee both flexibility and efficiency of the network which is even more important in the case of healthcare monitoring. Furthermore, Blockchain has recently been proposed as a game-changing tool that can be integrated into the Internet of Things (IoT) to have the optimal level of security and privacy. However, incorporating Blockchain into IoT networks, which rely heavily on patients' health sensors, is extremely difficult. In this paper, a secure Healthcare Monitoring System (HMS) is proposed with a focus on trust management issues. The architecture seeks to protect multiple healthcare monitoring system components and preserves patient privacy by developing a security interface where separate security modules can be integrated to run side by side to ensure reliable HMS. The security framework architecture we propose takes advantage of the blockchain technology as a secure and timely information back-end. STHM is a proposal that uses Software-Defined Networking (SDN) as the communication medium that allows users to access SDN's different functional and security technologies and services. Simulation results show that the use of Blockchain for the SDN-based healthcare monitoring can ensure the desired flexibility and security for a very lightweight additional overhead.

Keywords: healthcare monitoring; software-defined networks; blockchain technology; internet of things; security and privacy



Citation: Barka, E.; Dahmane, S.; Kerrache, C.A.; Khayat, M.; Sallabi, F. STHM: A Secured and Trusted Healthcare Monitoring Architecture Using SDN and Blockchain. *Electronics* **2021**, *10*, 1787. <https://doi.org/10.3390/electronics10151787>

Academic Editor: Khaled Elleithy

Received: 9 June 2021

Accepted: 24 July 2021

Published: 26 July 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Today, healthcare encompasses a wide range of issues, including clinical care, laboratory analysis, and public health consciousness [1]. In contrast, healthcare monitoring enables not only in-hospital service control, but it also helps service providers to serve people outside the hospital, to properly track patient health outcomes, continue to provide high-quality services and to detect at-risk individuals. It also enables patients to maintain contact with their healthcare providers, be compliant with treatment schedules, and improve their wellness process. Instead of that, and due to the lack of technology and doctors, people living in remote areas are without access to modern healthcare services. Real-time surveillance of the patient's well being, environment, and treatment is critical in this case. IoT-based healthcare management is a keystone mobile health (mHealth) technology that provides constructive and preventive remote health interventions [2]. This innovative application comes to fulfill the demands of growing individuals and the high medical costs. It interconnects accessible medical resources and deliver smart, secure, and affordable healthcare services.

The internet of things (IoT) is a kind of physical technology system, such as devices, buildings, and even more medical centers and hospitals, in which full access to patient information is guaranteed through the internet. Such emergent technologies are introduced to assist advancement in the healthcare modernization process, thanks to the arising developments in the internet and computing devices. The Healthcare framework is a patient resources-based system. It includes informational, audiovisual coordination, and the retrieval of medical records. The integration of IoT in healthcare monitoring systems is complicated because of the large amounts of data and the need for encryption protocols to protect people's personal information from being leaked [3]. Any malicious person's intervention, on the other hand, that will expose and manipulate patient's vital data in any way may have serious implications, even death [4].

To face the above mentioned issues and taking advantage of the emerging security and communication technologies, developing a secure and real-time healthcare monitoring system is a must. SDN's unique control/data plane separation allows a very efficient and distant monitoring of the healthcare devices. On the other side, the blockchain technology preserves the full history of patient records as well as healthcare sensors sensed information securely and privately without any possibility of alteration. For this reason, combining different technologies such as SDN [5] and Blockchain [6] can be a solution with direct positive effect. In this paper, an efficient and reliable Healthcare Monitoring System (HMS) is proposed to prevent any insider/outsider intruder from injecting data, falsifying data, violating patients' privacy, or even launching a denial of service attack against the HMS. A first version that includes only the overall architecture was initially presented in [5]. Yet, besides validating the proposed architecture through simulations, in this work called STHM, we also implemented a modular trust management solution based on the Blockchain technology and evaluated how the benefit is relying on this technology in the HMS context. Our proposal boosts the considered priorities of trust management concerns. The approach we propose aims at protecting various healthcare monitoring system components while still protecting patient privacy by constructing a secure environment in which separate security modules will coexist to ensure a consistent HMS.

On the other hand, several patient-centered solutions focus on the Electronic Health Record (EHR) management which involves all patient-related information including the security and trust aspects of both data and body sensors [7,8]. Moreover, the network and monitoring side is known to require less improvements compared to the patients side which can be a source of undesired situations, especially during pandemics such as COVID-19 where most of the work should be done remotely to minimize the physical contact with the patients. That is why the main aim of this work is to provide a secure and trusted distant monitoring process of patients healthcare.

The contribution of this paper is threefold:

- A remote, real-time, and secure patients healthcare monitoring architecture using Blockchain and SDN;
- A flexible and scalable modular system that can activate/deactivate any module while maintaining the other modules functionality;
- An efficient lightweight trust management solution for healthcare monitoring applications.

The paper is organized as follows: In Section 2, we present the most relevant existing works. Our proposed STHM architecture and design goals are presented in Section 3. In Section 4, we describe in detail our trust management scheme. Blockchain incorporation in STHM is then discussed in Section 5 followed by experimental results and performance evaluation in Section 6. Finally, Section 7 concludes this paper.

2. Related Work

Today, modernization of healthcare systems becomes unavoidable due to the rising demand for healthcare facilities and treatment units. In the literature, there exist several proposals that studied the main advantages and disadvantages of using or combining

new technologies such as *Software Defined Network (SDN)* and *Blockchain* to improve the healthcare sector. In this section, the related works are divided into three main categories (i) SDN-based solutions, (ii) Blockchain-based solutions, and (iii) Hybrid solutions.

2.1. SDN-Based Solutions

Today, it sounds obvious that two of the main concerns in healthcare systems are connectivity between their constituent devices and timely data delivery [9]. In such a situation, the SDN integration could be seen as a good solution to guarantee both flexibility and efficiency of the network. It enables the establishment of connections between various devices and provides a variety of network services, including network and traffic management, system discovery, authentication, policy, and access control. In [10], the scalability and network control of connected devices for Ambient Assisted Living (AAL) and Wireless Body Area Network (WBAN) is discussed by the authors (WBAN). They proposed that the SDN controller tracks traffic flows and ensures a successful exchange of traffic rules among network constituent devices for improved routing and mobility management. K. Hasan in [9] discussed the number of controllers, the key influencing factor in every amalgamation of SDN and WBAN in the healthcare context. To determine the optimal number of controllers for an SDWBAN framework, the authors proposed a mathematical model adopting the convex optimization method and taking into account the number of controllers, the latency, and the number of SDN-enabled switches (SDESW). Their mathematical proposal was also validated by the mean of simulation results. In our previous work [5], we studied the main concerns of the Healthcare Monitoring System (HMS) security and privacy. For that, they proposed a security integrated monitoring system to ensure reliable service delivery for patients and to reduce to the lowest the health-related risks. The authors of [11] presented a road map for the SDN-based QoS-improved telemedicine. They suggested SDN deployment to provide an appropriate bandwidth and to facilitate medical data real time transmissions.

2.2. Blockchain-Based Solutions

Several blockchain versions have been introduced since the release of bitcoin over a decade ago. In this subsection, we highlight how the healthcare sector could leverage emerging technology to collect, process, and interpret patients' information.

In order to maintain a broad perspective of the system's security policies, the authors of [12] propose a novel technique for distributed identity and authorization policies control by the deployment of blockchain. They integrate their proposal to the FIWARE platform. It shows better performance compared with pair solutions. In [13,14], a prospective application of blockchain in healthcare has been extensively examined and explored to highlight problems and future studies. Both literature reviews did not address all technical areas; particularly, the cost effects of the blockchain deployment in the healthcare sector. Instead of covering the performance, architectures, and standards, they discussed only security and privacy compliance.

Similarly, in [15,16], trendy blockchain applications in healthcare were systematically reviewed. They also covered the considerations of security and privacy, and analyzed healthcare data sharing using blockchain. They reviewed essential concepts including but not limited to identity management, data storage and encryption, access control, and smart contract. In [17], the authors addressed data privacy and network security for the e-health system and all their attention was focused on preventing unauthorized access. They suggested an Electronic Healthcare Records (EHR) distribution network on a mobile cloud platform that combines blockchain and the open Interplanetary File System (IPFS). Their trial deployment results are good, and they provide a viable method for securing data transfers on mobile clouds. The proposal's security review revealed performance enhancements in lightweight access management, network latency, and data protection with high security and privacy thresholds.

2.3. Hybrid Solutions

In healthcare, where security and patient safety enhance the depth of privacy and scalability of transferred data, most healthcare institutions are working on an amalgamation of SDN with blockchain solutions. In the literature, such applications are somewhat modest, and their results are not yet applied in the field of healthcare. In this work, we try to fill this gap. In [18], for security and privacy purposes, the authors shed light on the feasibility of incorporating the Blockchain technology into an SDN architecture. They focus on analyzing the current implementation of the Blockchain technology in SDN. Such an emergence provides confidentiality, integrity, and availability to network infrastructure.

To reduce the cost of network failure recovery, C. Xue in [19] introduced a blockchain-based SDN data chain, provided a distributed reliable record of SDN data, and broke the separation of multi-vendor devices for fault recovery. Their proposal was tested for validation by simulation using Ethereum services and OpendayLight. In [20], the authors presented a generic framework of blockchain-based SDN to face the centralized control plane issue, in which the control plane and the application layer are merged together to form one main component, where protection is provided by implementing additional security mechanisms. At that stage, the Blockchain technology was useful in improving distributed controller security. In [21], the authors proposed a blockchain-based collaborative DDoS attack prevention system centered on using smart contracts to enable SDN-based domain collaboration and to transfer DDoS attack information in a reliable, effective and decentralized manner.

3. STHM: An Overview

The architecture of our proposal is depicted in Figure 1. In contrast to other proposed designs, STHM considers both local and distant Wi-Fi-free patients within the hospital areas. Using their smartphones, patients can access the back-end device. Patients’ body sensors are called nodes in the body area network (BAN), which are communicated through the same smartphone-based portal. The SDN network, which distributes non-selective security policies from different SDN controllers, is in charge of these gateways.

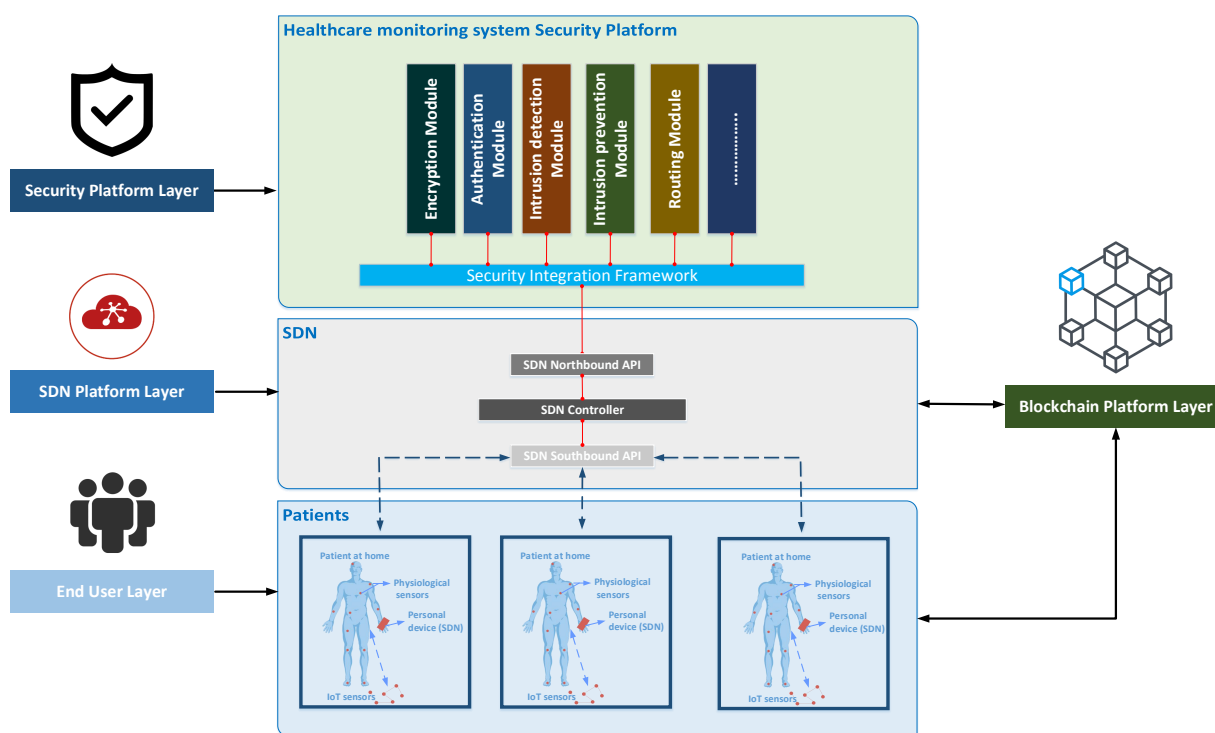


Figure 1. STHM different layers.

The rules and regulations that enable data to be directed to the proper destination will be stored on the Smartphone. The back-end structure consists of the HMS controller, database, and client application that monitors the mobile application and sensors. Figure 2 illustrates the architecture required to implement our proposal design.

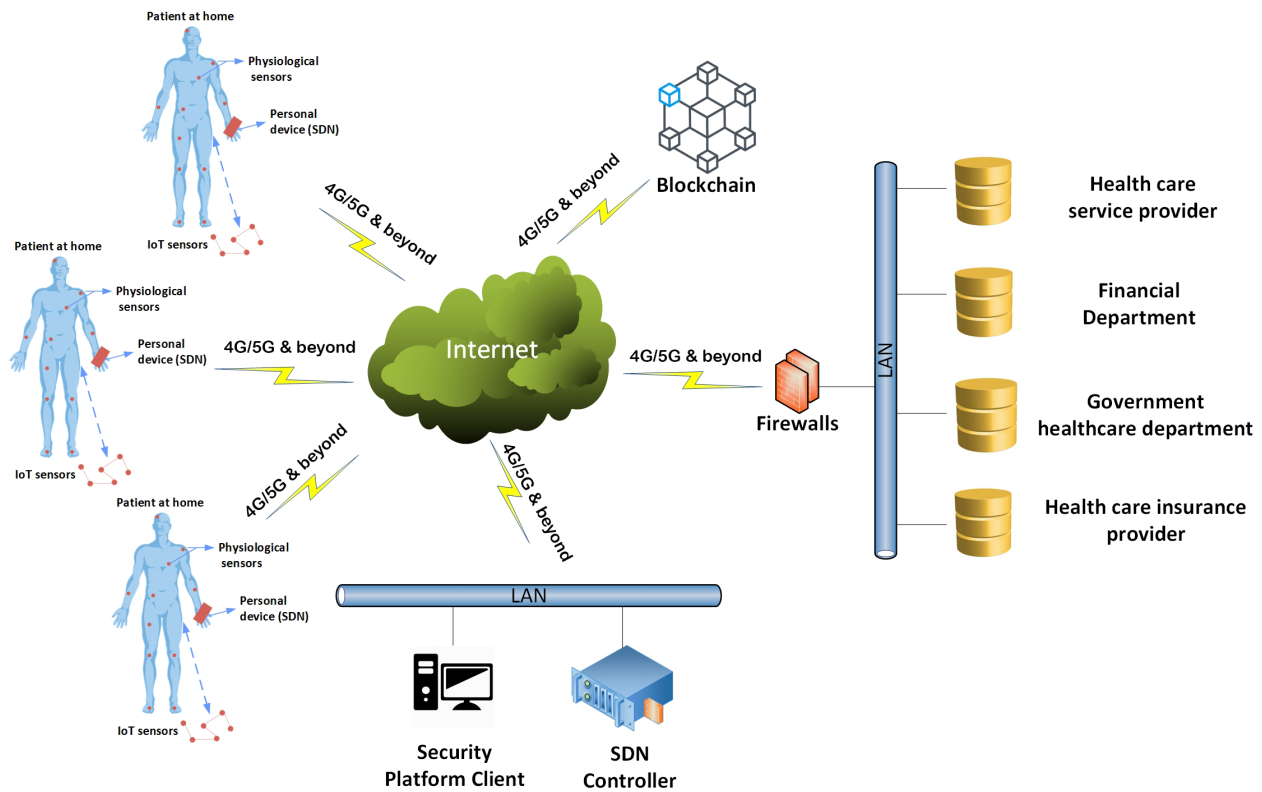


Figure 2. STHM actors and communication technologies [5].

This architecture is composed of the following four layers:

1. User Layer;
 2. SDN Layer;
 3. Security Layer;
 4. Blockchain Layer.
- **User Layer:** This layer is made up of sensors and a mobile application. As a gateway (an edge or fog node), the mobile application manages the traffic between the sensors and the target databases. Hosted and controlled by the trusted authority, rules and policies are sent to the mobile application by the HMS controller. The sensors collect crucial data from patients (e.g., heart rate, blood sugar level, blood pressure, etc.) and send them to the mobile application, which routes them to their intended destination based on the smartphone application rules and regulations. In the security layer, dedicated modules are deployed to authenticate and authorize mobile applications and sensors.
 - **SDN Layer:** The SDN layer is the core layer of our proposed architecture. According to the literature, the three primary components of the SDN network are northbound APIs, controllers, and southbound APIs. Using the Southbound APIs in our design, the mobile application will be integrated with the SDN controller. The protective layer is implemented on top of the SDN controller using Northbound APIs. As a result of this connection, the security platform's modules can access all nodes (mobile applications and sensors) linked to the SDN controller through Southbound APIs. The controller is in charge of coordinating the communication between the security layer modules and mobile apps. In addition, the controller comes with its own set

of apps and services. One of the applications in this suggested architecture is the routing application, which identifies the data acquired by the sensors and sent to the proper destination.

- **Security Layer:** The security integration layer serves as a connector and orchestrator for the various security modules. The security and privacy components for HMS are summarized in Figure 3.
- **Blockchain Layer:** Permissioned blockchain is used in our architecture to provide a secure and timely connection between all system actors. It is divided into two stages:
 - First, system actors log in to the system and use dedicated interfaces to document the various approved actions (APIs). This information can contain sensitive information.
 - Second, the miners in the Blockchain-enabled Infrastructure domain will insert the information into the Blockchain after solving the Proof-of-Work (PoW) algorithm. Miners are the only nodes responsible for putting data into the Blockchain. If a miner is unable to solve the PoW consensus algorithm, the data are not added to the Blockchain.

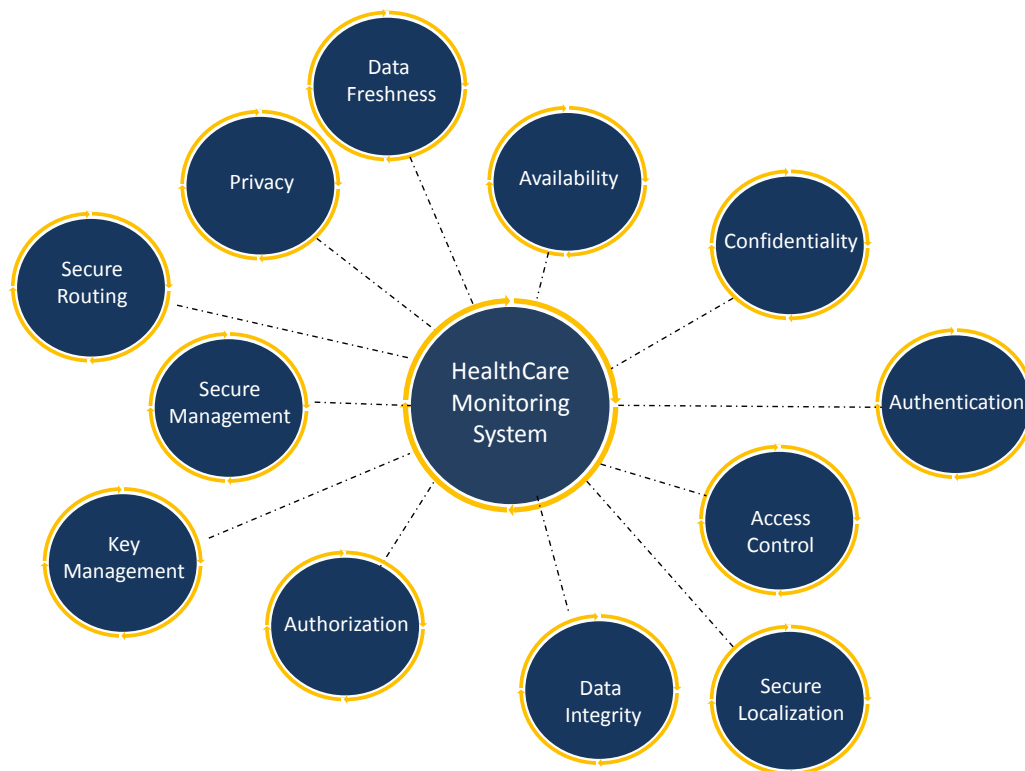


Figure 3. Components of the desired secure healthcare monitoring system.

3.1. SDN-Based Network Model

The baseline for SDN, the enabling technology for IoT, is presented in this segment. We also present an overview of the problem formulation.

3.1.1. SDN Overview

As shown in Figure 4, SDN divides the network into three planes: the data plane, the control plane, and the application plane. The data plane is in charge of sending and receiving network traffic. Decisions about traffic transfer are made in the control plane. The SDN programs are stored in the device plane.

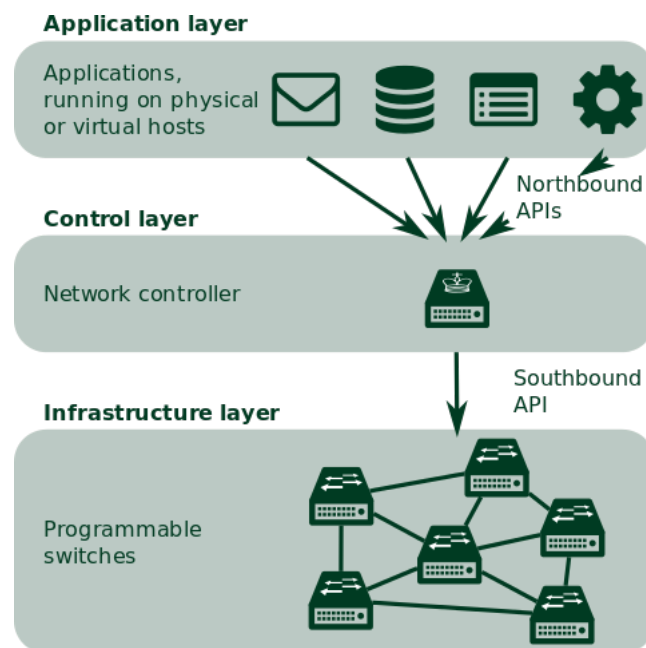


Figure 4. Software Defined Networking Architecture.

SDN applications are connected to the controller via the northbound interface. The controller may provide information such as statistics and incoming connections to applications. Applications may also submit commands to the controller for network management, such as adding or removing flow rules. It is worth noting that applications are created to accomplish particular goals. They integrate data from the controller with information from other sources to determine whether or not the network should be adjusted.

The controller maintains an access control system that grants applications only the permissions they need to safely operate the control plane. Read, write, notification, and device permissions are the four types of permissions available.

3.1.2. Problem Statement

The ability to work with different applications written to alter and control the state of the network is one of the key benefits of SDN. Supporting third-party growth, on the other hand, creates serious confidence issues. The danger posed by third-party applications is linked to the fundamental challenge of determining a software module's trustworthiness. The SDN technology is built with policies that enable network applications to modify SDN-based networks directly [22]. Existing SDN controllers, on the other hand, have not taken into account the required security measures for North-Bound Interfaces (NBI), and the majority of them lack authentication, authorization, and logging capabilities. Furthermore, administrators presume the same degree of confidence as the controller on network applications when third-party applications contact NBI. Malicious applications can abuse policies in a variety of ways, causing harm on a large scale ranging from data leakage to dedicated network harm.

This paper proposes a confidence management system for the NBI of SDN controller for healthcare monitoring in this context. The approach should take into account the following trust management characteristics [23].

- **DynamiCity:** The level of confidence should not remain constant over the duration of a user's interaction with a given application;
- **Content dependency:** The application's ability to gain confidence may be contingent on the task for which it was created;
- **Subjectivity:** The features (equipment and information assets) of the SDN network with which it interacts should be considered by the trust management system.

Furthermore, any SDN trust management solution must meet the following criteria and adhere to the underlying principles.

- **Proof of identity:** Where authentication is needed, communicating nodes must authenticate each other;
- **Least privilege:** The privileges granted must be consistent with the request;
- **Inspect and log:** The incidents must be inspected and reported to an appropriate level for security purposes.

Since the range of approaches to network trust management is so broad, the proposed solution combines multiple frameworks, which are described below [24].

- **A certificate-based** framework should provide authentication;
- **Policy-based:** To differentiate between permissible acts for applications, a framework is used;
- **Behavior-based:** The framework tracks and analyzes application activity and assigns a confidence rating based on it.

4. Proposed Trust Management Scheme

The proposed trust management framework for an SDN-based healthcare platform is described in this section. It is worth remembering that we concentrate on the SDN architecture, which is the communication part of the overall healthcare system. The goal of our proposed architecture is to establish and maintain trust between the control layer and network applications.

Figure 5 shows the framework that can be used to link applications to the control layer in an SDN architecture. The structure is made up of the following five elements:

1. Authentication and Authorization modules;
2. Trust module;
3. Trust database;
4. Access control decision module;
5. Monitoring and Evaluating module.

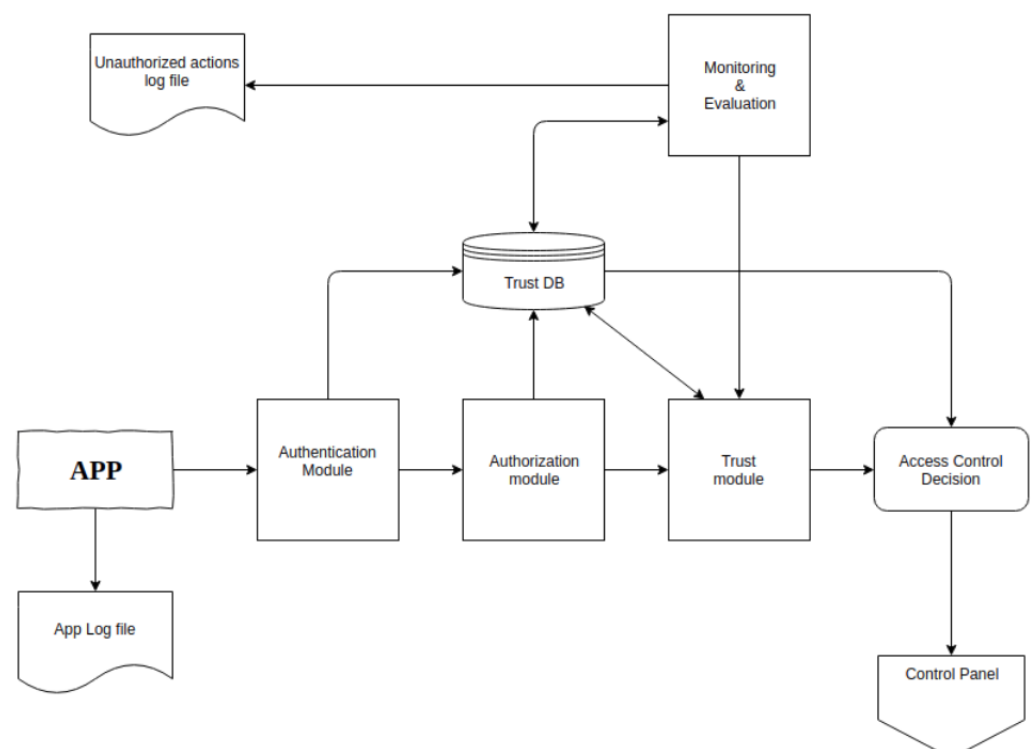


Figure 5. Trust management different modules and interactions.

The following subsections go through each element in detail.

4.1. Authentication Module

When an application requests network modifications to be applied through the control plane, the framework's authentication is enabled. The control plane sends a challenge request for the application credentials after it receives the submission. After successful verification and validation of the application credentials, the controller either allows or denies the application access to network services. The authentication procedure is depicted in full in Figure 6.

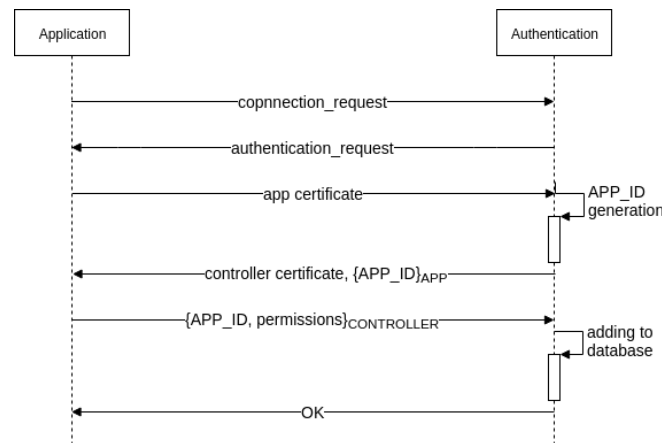


Figure 6. STHM Authentication process.

4.2. Authorization Module

The authorization module is responsible for the application's permissions. All permits are divided into two groups. The first category comprises important rights that, if exploited, might result in serious consequences, whereas the second group comprises non-critical rights. All permissions are tracked in the Trust Database.

Furthermore, based on the functions they execute, applications are split into two categories. Security programs provide the first and most crucial role. Applications that are not related to security are assigned to second place, which has the lowest priority.

In response to new run-time threats, such as malicious traffic, infected internal assets, blacklist-worthy external entity, and the appearance of malicious aggregate traffic patterns, the security applications can restrict a static administrator's network security policy.

Applications with the first role have access to all permissions. Applications with the second role have access to any non-critical and fewer than five crucial permissions defined in the following Trust module.

4.3. Trust Module

This module is in charge of computing a permissions-requesting program's trust value. When determining the trust value, we take into account four elements, as in [25].

1. **Reputation:** The assessment of historical interactions between nodes.
2. **Operational risk:** The affected parts of the network due to the application might be lost. These risks are detailed below.

$$\frac{h * t * L}{N} \quad (1)$$

where h represents the number of affected hosts, t represents downtime, L represents the financial loss per unit of downtime, and N represents the total number of hosts in the network.

3. **Information risk:** Loss of knowledge disclosure is a possibility. It is calculated in the following manner.

$$L_i(t) = \sum_{i=1}^N Imp_i (L_i^{dl} + L_i^{il}) \quad (2)$$

where Imp_i is the information importance coefficient, L_i^{dl} is the total amount of direct losses, and L_i^{il} is the total amount of indirect losses.

4. **Privacy level** is the network device traffic that the SDN controller can see.

The trust module measures the Trust Value (TV) using the aforementioned variables and some predefined values. The mechanism is depicted in Figure 7 as a flowchart. The display, i.e., TV, is sent to the ACD module (Access Control Decision).

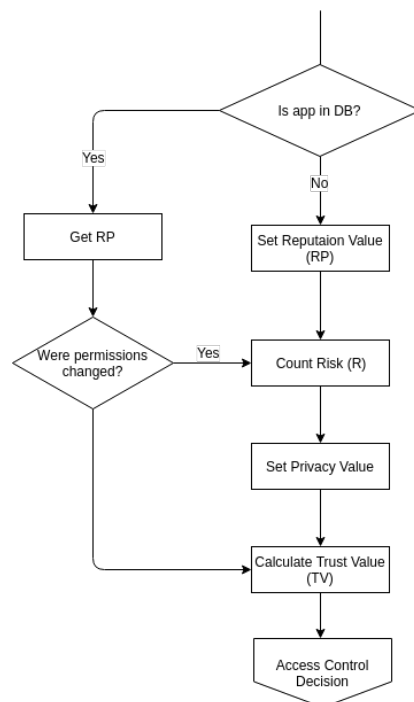


Figure 7. Trust Value (TV) computation.

Because risk factors differ per network, a user will be presented with an interface that allows him to count appropriate and significant risks as well as establish two Threshold Trust Values (TTV): acceptable and critical.

4.4. Access Decision Control (ACD) Module

This module assigns the computed TV from the trust module to one of the three zones listed below. Based on this TV, the ACD module determines how much to trust the application.

1. **Critical zone:** When an application's confidence level is exceedingly low, it should be decided to cease working on it and disconnect it;
2. **Surveillance zone:** When the application has a medium level of confidence, the decision is to focus on the Monitoring and Evaluation (ME) module;
3. **Trusted zone:** When the application has a high level of confidence, it continues working with the ME module, which will monitor it regularly.

The application's confidence level decreases as the TV's value decreases. The ME module is in charge of making the observation decision in this case.

4.5. Monitoring and Evaluation (ME) Module

The link between a controller and network applications should be examined and assessed regularly. The ME module is responsible for monitoring the observation actions that the ACD module has assigned to it. The ME module inspects for trusted region log files, which contain all requests for improper activity. The module additionally inspects the application log files for the surveillance region and delivers a report to the SDN controller administrator.

The assessment functionality of this module assists in managing and changing a Reputation Value (RP) depending on the app's observed behavior. The complete management process is depicted in Figure 8. If the program has requested any illegal rights, this module reduces the RP, and it might increase the RP if no deviant activities have been identified.

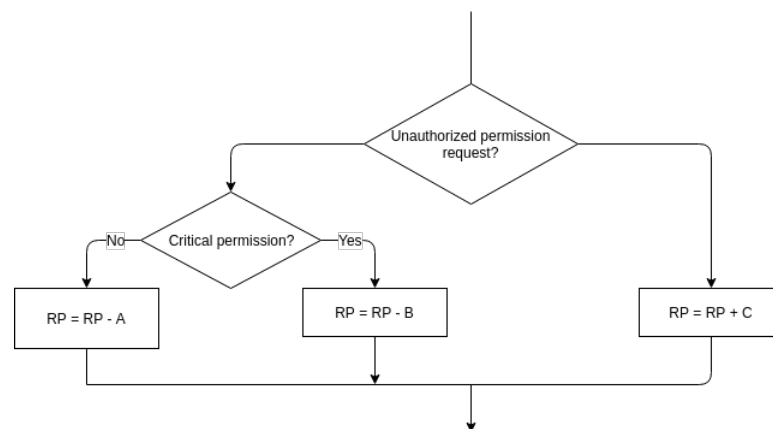


Figure 8. ME module evaluation process where A , B and C are positive constants defined by users.

4.6. Trust Database

The trust database is a data storage component that keeps track of all the values and characteristics needed for the framework assessments and determinations. Both modules consult the database for stored data. The values assigned to various network applications are arbitrary and determined by the network administrator.

5. Blockchain as a Secure HEALTH Monitoring Back-End

Blockchain-based healthcare monitoring is a promising technological development that can address data collecting security and privacy concerns during patient monitoring. All monitoring procedures in STHM are related to the previously computed trust value. They are subsequently encrypted and kept in the blockchain, ensuring the system security. Similarly to all blockchain-based structures, the construction of X_i (Miners' hash threshold) is a sequence of binary bits beginning with a number of zeros.

The relationship between X_i and Y_i (the sum of the trust compensations' absolute values) as shown in [26] is given by the equation:

$$N_z = \text{int}(e^{-(\eta \cdot Y_i + \nu)}), X_i = 2^{N_m - N_z} - 1 \quad (3)$$

$\text{int}(\cdot)$ is a function that takes as a parameter the integer part of the introduced value; N_z is the number of zeros that Y_m begins with; and N_m is the hash value that was generated using the hashing algorithm.

The blockchain domain server validates the nonce's authenticity before adding it to the blockchain when a miner's (in our example, SDN Controller) block is received. On the other side, a single server can receive a high number of blocks at once. As a result, the blockchain may tend to fork. To solve this challenge, a distributed consensus strategy should be adopted. Servers have the option of forking one block or continuing to add new blocks. Then, the branch with the most servers expands at a quicker rate than the

others. Finally, the longest one is chosen as the distributed consensus for the network, while the others are removed. Furthermore, the servers will store their produced blocks in the deleted forks and seek to add them to the blockchain at a later stage. This method ensures that every server has an identical copy of the blockchain.

6. Experimental Results

We implemented blockchain-related actions (i.e., blockchain creation, update, and validation process) in Java using the MultiChain framework. To assess the impact of Blockchain on the HMS’s resources, we calculated the average consumed energy per hour for the SDN controller.

Figure 9 compares the average energy consumption of the SDN controller with and without Blockchain. It shows that using Blockchain increased the energy consumption of the servers by 15% over the standard situation for a number of 2000 patients’ Electronic Health Records (EHR) <https://mimic.physionet.org/> (accessed on 29 April 2021). However, when compared to the benefits of a fully distributed school system, this additional overhead is still minimal. Furthermore, if all computations will be performed at the network’s edge, the expense of implementing the whole scheme will be very reduced.

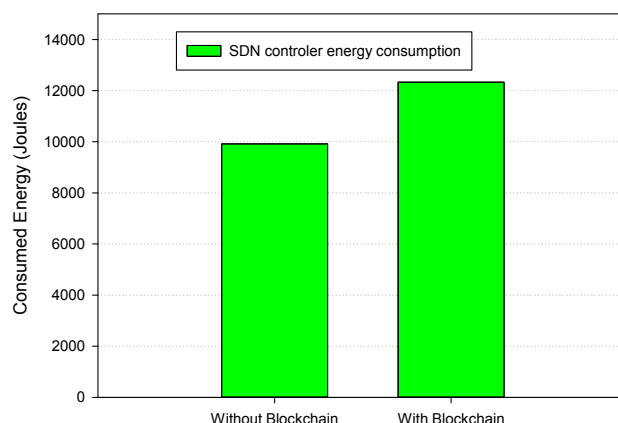


Figure 9. Blockchain additional tasks impact on the SDN controller’s energy consumption.

Figure 10 shows the communication throughput as a function of the number of SDN controllers. It reveals that, as the number of controllers (miners) increased, the number of validated transactions increase as well, until reaching a stable level of more than 15 miners, which is sufficient to validate all incoming transactions promptly. This is due to the fact that, on a global scale, more than 15 controllers are necessary to monitor a large number of patients. As a consequence, all transactions are received by controllers in a timely way.

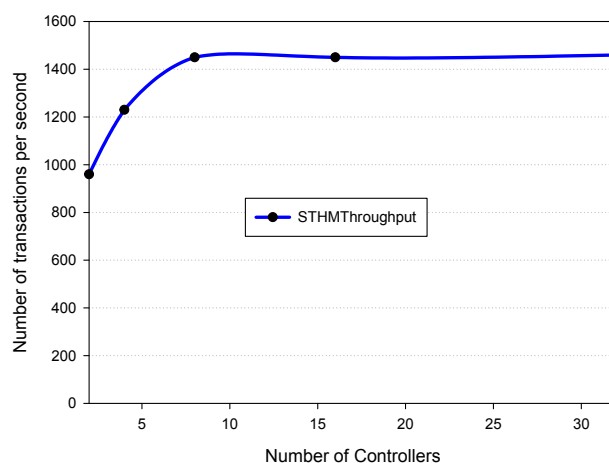


Figure 10. STHM Throughput for different number of SDN controllers.

The use of blockchain in STHM results in more messages being exchanged between domains. Figure 11 depicts the produced overhead for various numbers of monitored patients with having an average of four monitored devices. It shows the induced overhead does not exceed 5 Kb, which has no effect on network activity due to the small packets exchanged representing the updates in the patients electronic health records (detection of abnormal situation).

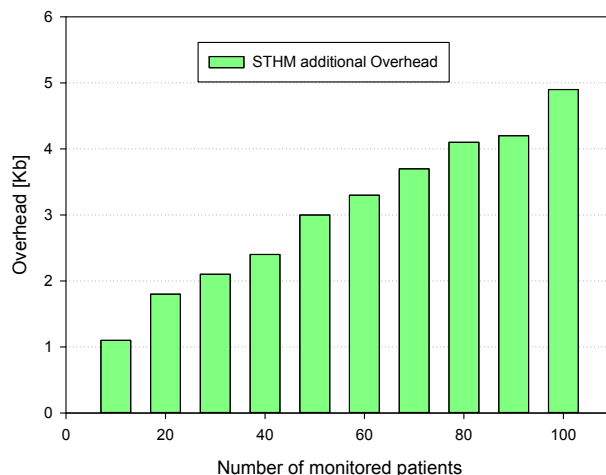


Figure 11. STHM additional network overhead.

The SDN architecture will allow them to work together to develop a complete secure HMS by providing a blockchain-based security framework on which various security modules may be added to reduce the generated negative falses (See Figure 12). Any malicious activity originating from or going to the sensors, for example, can be detected and monitored by an SDN-based Intrusion Detection System (S-IDS). Using the data collected by these sensors in a predictive and pattern analysis to enhance and provide the finest and most optimum patients services is also an option. Another example is that the S-IPS will cooperate with the S-IDS and access control modules to prevent unauthorized access to the sensors by terminating connections through the firewall. This will both reduce the immediate threat to the patient’s health and decrease the risks of death. Finally, using rules produced at the access control module and communicated to the application mobile, data acquired by the sensors may be segregated and compelled to move to a certain destination (the gateway). This will protect patient data privacy, which is critical to HMS’s success.

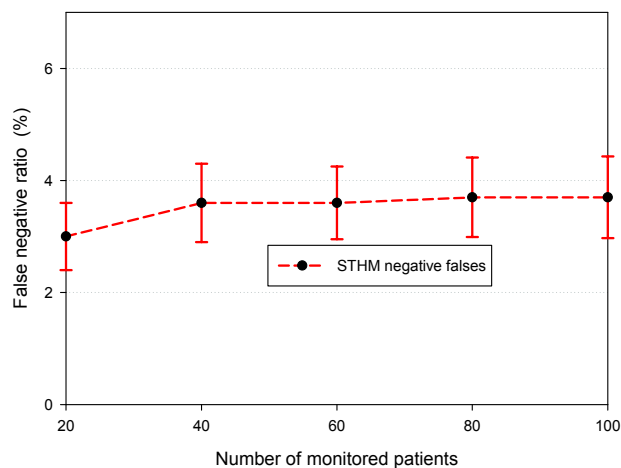


Figure 12. STHM generated negative falses.

7. Conclusions and Future Directions

Healthcare monitoring systems are particularly useful when it comes to mentoring and assessing the well-being of patients. In addition, they put patients' relative information at risk of computer hacking. In this research, we introduced a novel HMS architecture called STHM. Our proposal aims at securing all Healthcare monitoring system components. It also preserves patient privacy by constructing a security framework that allows diverse security modules to operate together and, depending on the Blockchain technology, to secure HMS. Furthermore, the SDN has been used as communication support, providing more flexibility and control over the monitored healthcare devices. It has been demonstrated how this integrated platform, along with its built-in applications, can be used to improve the functionality and security of the HMS proposed architecture. The study revealed that STHM provides efficient HMS monitoring operations with minimal energy consumption and overhead, which is important in the healthcare sector.

As part of future work, we plan to add more functionalities to this architecture, such as distance actions in emergency situations and the prediction of any unfavorable health situation. We also intend to create a user-friendly API interface to make the different tasks easier.

Author Contributions: Authors equally contributed to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Albahri, A.; Alwan, J.K.; Taha, Z.K.; Ismail, S.F.; Hamid, R.A.; Zaidan, A.; Albahri, O.; Zaidan, B.; Alamoodi, A.; Alsalem, M. IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. *J. Netw. Comput. Appl.* **2021**, *173*, 102873. [[CrossRef](#)]
2. Philip, N.Y.; Rodrigues, J.J.P.C.; Wang, H.; Fong, S.J.; Chen, J. Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges and Future Directions. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 300–310. [[CrossRef](#)]
3. Hamim, M.; Paul, S.; Hoque, S.I.; Rahman, M.N.; Baqee, I.A. IoT Based Remote Health Monitoring System for Patients and Elderly People. In Proceedings of the 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 10–12 January 2019; pp. 533–538. [[CrossRef](#)]
4. Almalki, F.A.; Soufiene, B.O. EPPDA: An Efficient and Privacy-Preserving Data Aggregation Scheme with Authentication and Authorization for IoT-Based Healthcare Applications. *Hindawi WCMC* **2021**, *2021*. [[CrossRef](#)]
5. Khayat, M.; Barka, E.; Sallabi, F. SDN-Based Secure Healthcare Monitoring System (SDN-SHMS). In Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July–1 August 2019; pp. 1–7.
6. Dhillon, V.; Metcalf, D.; Hooper, M. Blockchain in Healthcare. In *Blockchain Enabled Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 201–220.
7. Mayer, A.H.; da Costa, C.A.; Righi, R.D.R. Electronic health records in a blockchain: A systematic review. *Health Inform. J.* **2020**, *26*, 1273–1288. [[CrossRef](#)] [[PubMed](#)]
8. Fatokun, T.; Nag, A.; Sharma, S. Towards a blockchain assisted patient owned system for electronic health records. *Electronics* **2021**, *10*, 580. [[CrossRef](#)]
9. Hasan, K.; Ahmed, K.; Biswas, K.; Islam, M.S.; Kayes, A.S.M.; Islam, S.M.R. Control Plane Optimisation for an SDN-Based WBAN Framework to Support Healthcare Applications. *Sensors* **2020**, *20*, 4200. [[CrossRef](#)] [[PubMed](#)]
10. Isravel, D.P.; Silas, S.; Rajasingh, E.B. SDN-Based Traffic Management for Personalized Ambient Assisted Living Healthcare System. In *Intelligence in Big Data Technologies—Beyond the Hype*; Peter, J.D., Fernandes, S.L., Alavi, A.H., Eds.; Springer: Singapore, 2021; pp. 379–388.
11. Jnr, B.A.; Nweke, L.O.; Al-Sharafi, M.A. Applying software-defined networking to support telemedicine health consultation during and post Covid-19 era. *Health Technol.* **2020**, 2190–7196. [[CrossRef](#)] [[PubMed](#)]
12. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manag.* **2021**, *58*, 102468. [[CrossRef](#)]
13. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemeč Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [[CrossRef](#)]
14. Vazirani, A.A.; O'Donoghue, O.; Brindley, D.; Meinert, E. Implementing Blockchains for Efficient Health Care: Systematic Review. *J. Med. Internet Res.* **2019**, *21*, e12439. [[CrossRef](#)] [[PubMed](#)]

15. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [[CrossRef](#)]
16. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A Review of Secure and Privacy-Preserving Medical Data Sharing. *IEEE Access* **2019**, *7*, 61656–61669. [[CrossRef](#)]
17. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access* **2019**, *7*, 66792–66806. [[CrossRef](#)]
18. Alharbi, T. Deployment of Blockchain Technology in Software Defined Networks: A Survey. *IEEE Access* **2020**, *8*, 9146–9156. [[CrossRef](#)]
19. Xue, C.; Xu, N.; Bo, Y. Research on Key Technologies of Software-Defined Network Based on Blockchain. In Proceedings of the 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 4–9 April 2019; pp. 239–2394. [[CrossRef](#)]
20. Wenjuan, L.; Weizhi, M.; Zhiqiang, L.; Man-Ho, A. Towards Blockchain-Based Software-Defined Networking: Security Challenges and Solutions. *IEICE Trans. Inf. Syst.* **2020**, *E103.D*, 196–203. [[CrossRef](#)]
21. El Houda, Z.A.; Hafid, A.; Khoukhi, L. Co-IoT: A Collaborative DDoS Mitigation Scheme in IoT Environment Based on Blockchain Using SDN. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [[CrossRef](#)]
22. Canini, M.; Venzano, D.; Peresini, P.; Kostic, D.; Rexford, J. A “nice” way to test openflow applications. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, San Jose, CA, USA, 25–27 April 2012.
23. Yan, Z. *Trust Management in Mobile Environments: Autonomic and Usable Models*, 1st ed.; IGI Global: Hershey, PA, USA, 2013.
24. Alqallaf, M.A. Software defined secure ad hoc wireless networks. In *A Dissertation*; Wright State University: Dayton, OH, USA, 2016.
25. Burikova, S.; Lee, J.; Hussain, R.; Sharafitdinova, I.; Dzheriev, R.; Hussain, F.; Sharieh, S.; Ferworn, A. A Trust Management Framework for Software Defined Networks-based Internet of Things. In Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 0325–0331.
26. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [[CrossRef](#)]