Cyber Security and Applications 1 (2023) 100020

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Design of blockchain-enabled secure smart health monitoring system and its testbed implementation

Siddhant Thapliyal[a], Shubham Singh[a], Mohammad Wazid[a,*], D.P. Singh[a], Ashok Kumar Das[b]

[a] Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India
[b] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India

ARTICLE INFO

Keywords:
Cyber security
Internet of Medical Things (IoMT)
Healthcare
Authentication
Blockchain

ABSTRACT

Smart healthcare technology is transforming from the traditional healthcare system in every manner conceivably. Smart healthcare provides several advantages over the existing approaches. However, it suffers from healthcare data security and privacy issues. As the Internet attackers may get access to sensitive healthcare data through the use of various types of cyber attacks. In this paper, an architecture of a blockchain-enabled secure smart health monitoring system has been presented (in short, it is called as BSSHM). BSSHM consists of various health data monitoring sensors, i.e., temperature, heartbeat, etc., which monitor the real time health data of the different patients. The healthcare data of the patients can be transmitted to the connected health servers in a secure way, where this data can be stored securely for its various uses. The formal security verification of the proposed BSSHM is also done through the widely-accepted Scyther tool. It has been proved that BSSHM is able to defend various potential attacks.

1. Introduction

The Internet of Things (IoT) is a network of numerous interconnected devices and gadgets that collect data in real time. We are completely surrounded by IoT gadgets, for example smart home devices. A basic watch that tracks your activities and routines in real time, as well as a temperature sensor that detects your body temperature. One of the next evolutionary steps in internet-based computing is the Internet of Things (IoT). The Internet of Things (IoT) has progressed from a futuristic concept to a market reality in recent years. IoT has a favourable influence on a wide range of application fields, including healthcare, sustainable living, smart cities, the industrial sector and many more. The analysis of data from many IoT data sources, including as sensors, actuators, smart devices, and other internet-connected things, is referred to as IoT analytics. IoT solutions enable users to gain more automation, analysis and system integration [1]. It is possible to increase these areas and precision by making it more flawless. IoT makes use of technologies such as sensing, networking and robotics. IoT has the potential to transform the way we live and work, making our lives more efficient, convenient and connected. However, due IoT devices generate data in the enormous amount, which may be sensitive in nature. It poses critical problems regarding data privacy, security and ethical implications [2,3]. For example, in smart homes, IoT devices can be used to control and monitor everything from the temperature and lighting to the security system and home appliances. Smart cities can use IoT to manage traffic flow, monitor air quality, and even track waste management [4]. In industrial settings, IoT can be used to monitor machines and equipment, optimize production processes and prevent downtime. In healthcare, IoT devices can be used to track patient health data and monitor vital signs, enabling more personalized and remote care [5]. One of the key advantages of IoT is the ability to collect and analyze vast amounts of data in real time. This can help businesses and organizations make more informed decisions, optimize processes and improve efficiency. However, it also raises concerns around data privacy and security, as the sheer volume of data generated by IoT devices can be a challenge to manage and protect. Overall, the potential applications of IoT are vast and varied. It is an area of technology that is constantly evolving and expanding. As we continue to integrate more devices and sensors into our daily lives, the possibilities for what IoT can achieve are almost limitless.

The sensor is also known as a transducer. A transducer, often known as a sensor is any device that converts one type of energy into another. A physical occurrence is converted into an electrical impulse that can be interpreted by the sensor or transducer. Also, there are several methods for measuring the same object. The actuator is the second type of transducer. An actuator works in the opposite direction of a sensor. It uses an electrical impulse to execute a physical activity. For example, the temperature sensor can detect the heat. There may be different kinds of

* Corresponding author.
E-mail addresses: sthapliyal37@gmail.com (S. Thapliyal), shubhamsingh40643@gmail.com (S. Singh), wazidkec2005@gmail.com (M. Wazid), devesh.geu@gmail.com (D.P. Singh), iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das).

https://doi.org/10.1016/j.csa.2023.100020
Received 9 March 2023; Received in revised form 25 April 2023; Accepted 10 June 2023
Available online 16 June 2023

sensors, i.e., temperature sensor, distance sensor, optical sensors, light sensor and environmental sensor [6–8].

The practical implementation of IoT has been made possible by recent advancements in several different technologies.

- They include the availability of low-cost, dependable sensors that require little power, making them more accessible to manufacturers.
- Low-cost and low-power sensors that can easily link to the cloud and other devices through various network protocols make this possible.
- Cloud systems also make it simple to scale up infrastructure without having to manage it all.
- Companies may use advanced machine learning and analytics to acquire insights quicker by leveraging massive volumes of data stored in the cloud.
- Moreover, neural network improvements have enabled natural-language processing in IoT devices, making them more desirable and cheap for home usage.

All these allied technologies are pushing the boundaries of IoT and driving its growth. IoT has the potential to revolutionize the healthcare industry by providing efficient and timely medical attention to patients. Many patients do not receive timely medical attention due to various reasons, such as the inability to identify diseases, high medical fees, living in remote areas, etc. This delay in treatment can have adverse effects on patients' health, and many people may not even be aware of a severe illness until a critical event occurs. IoT can address this issue by monitoring patients' health and alerting them about any potential health threats. For instance, patients suffering from cardiovascular diseases can have their heart rate and blood pressure monitored by IoT devices, while diabetic patients can track their sugar levels regularly for effective medication. This way, patients can receive the necessary medical attention before a critical event occurs [9,10].

Following are the applications and uses of IoT in healthcare. Sometimes it is also called as Internet of Medical Things (IoMT) [10].

- IoMT devices can monitor patients' health continuously and transmit the data in real-time to healthcare providers for remote monitoring, diagnosis, and treatment.
- Patients can use wearable IoT devices to track their health metrics, such as heart rate, blood pressure, blood sugar levels, and activity levels, to manage chronic conditions and receive timely interventions.
- IoMT-enabled medical equipment, such as smart beds and infusion pumps can improve patient safety and reduce errors.
- IoMT devices can help with medication adherence by reminding patients to take their medications on time and in the correct dosage.
- Healthcare providers can use IoMT-enabled inventory management systems to monitor medical supplies and reduce waste.
- IoT devices can enable telehealth services, providing patients with access to remote medical consultations and follow-ups.
- By analyzing large amounts of patient data, IoT devices can help identify patterns and insights to improve healthcare delivery and outcomes.
- There are many IoT devices which have infrared temperature sensor which can detect human body temperature.
- People with diabetes can benefit greatly from using IoT medical devices that can monitor their glucose levels continuously and provide real-time data to their healthcare providers. These devices can be worn on the body or attached to the skin, allowing patients to monitor their glucose levels frequently and accurately without the need for invasive blood tests.
- The introduction of modern hearing aids has revolutionized the way people with hearing problems can improve their hearing. These new hearing aids incorporate advanced technology, such as bluetooth connectivity, digital signal processing, and noise-cancellation features, to provide a more natural and personalized hearing experience.

1.1. Motivation

The BSSHM is helpful to observe the physiological condition of a patient. It then sends the monitored healthcare data to the connected health server. At the health server can be used for various purposes, i.e., getting the knowledge about the health of the patient remotely or make some predictions about the health of the patient. Whatever data the smart healthcare devices and health servers exchange that happens in the secure way through the steps of the used authentication and key establishment mechanism of the BSSHM. Therefore, it can protect the system against various possible cyber attacks.

1.2. Research contributions

Following are the research contributions of the paper.

- In this paper, an architecture of the blockchain-enabled secure smart health monitoring system is proposed (in short BSSHM).
- The threat model related to the BSSHM is then provided.
- The formal security verification of the BSSHM is done through the widely-accepted Scyther tool. It has proved that BSSHM is able to defend various potential attacks.
- Then in the end, a testbed of the BSSHM is provided to check its usability in the real-time.

1.3. Paper outline

The outline of the paper is as follows. The relevant related work has been discussed in Section 2. We present an architecture associated to the blockchain-enabled secure smart health monitoring system including the network and threat models in Section 3. We then discuss various phases in details related to the proposed framework in Section 4. We perform the formal security verification using broadly-used automated software validation tool, namely Scyther in Section 5. Additionally, a practical implementation of the proposed framework in Section 6 along with the blockchain implementation in Section 7. At the end, in Section 8, some concluding remarks and future research have been discussed.

2. Literature review

In recent years, access control, authentication and key management become primary security services in several networking environments [11–16].

Access control in smart devices is a very pressing and important topic, and it is also a trending technology to safeguard access and secure data. As a result, different studies and surveys in the field of access control have been offered. Rana *et.al* [17] exhibited an access control approach. They also provided a model in which they indicated that the astute health clinical framework was expected to have a significant influence on the nature of medical care administrations.

Pal *et al* [18] They proposed a method for "user authentication that used symmetric key cryptography. They discovered a safe method that was both simple and inexpensive." Roy *et.al* [19] "developed the notion of multi-cloud server access control, claiming to be the first fine-grained data access control system".

The lightweight authentication approaches for IoT-based healthcare applications were presented at Merabet [20] *et al.* They formally validated the security of "their approaches using the AVISPA and ProVerif programmes. They have also released the security analysis for their plan. The performance of the aforementioned schemes was also compared to that of other comparable schemes. These systems were eventually shown to be vulnerable to session key computation attacks utilising the CK-adversary model and sophisticated replay attacks. They also did not meet other crucial security and functionality standards."

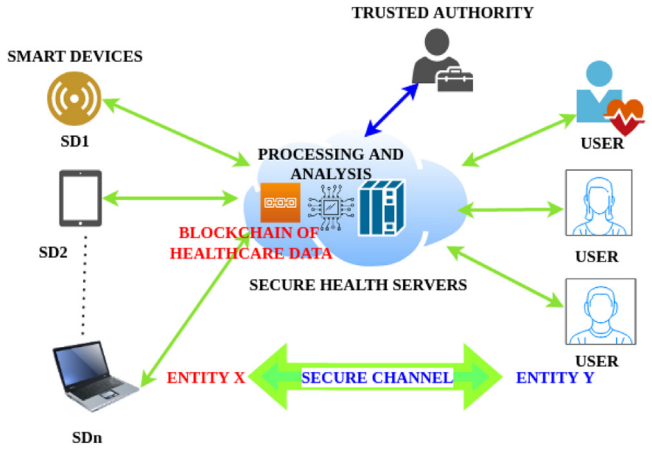

Fig. 1. Architecture of the proposed BSSHM.

Thapliyal *et al.* [4] discussed sustainable smart healthcare system in which health services may be delivered to patients in remote locations via Internet. They suggested to use biodegradable, recyclable, and environmentally friendly healthcare equipment and goods, which operate with minimal power use. They provided significant benefits over the traditional healthcare system.

Jang *et al.* [21] explored the wireless body area network security requirements (WBAN). They also suggested a hybrid security method for WBANs. Their approach, however, did not support the anonymity attribute. Moreover, it lacked support for other critical security and functionality requirements. He and Zeadally [22] presented a system architecture of the ambient assisted living system (AAL) system. Its associated security requirements were explored. After that, they suggested an effective authentication strategy for the AAL system. Finally, they compared the performance of their plan to that of two other comparable schemes in order to highlight its benefits and limitations.

3. Architecture of blockchain-enabled secure smart health monitoring system

In this section, we provide the details of the architecture of the proposed BSSHM along with the information of potential threats/ attacks.

3.1. Network model of BSSHM

Fig. 1 shows the architecture of the proposed BSSHM. In the given scenario, there are smart healthcare devices which are connected to users like patient, doctors, nurses or some other related entities through health server. Smart healthcare devices collect data and then send it to the health server for further processing, storage and analysis [23]. Entire exchange of the data happens in the secure way through the deployed authentication and session key establishment. The function of the health server is critical here since it processes and saves healthcare data. This healthcare data may then be used to generate valuable outputs (for example, prediction of a disease) through some machine learning models that can be deployed over the health servers [24–26].

3.2. Threat model of BSSHM

In proposed BSSHM, we follow guidelines of widely accepted "Dolev-Yao (DY) model [27]." The communicating entities communicate over an insecure (open) or public channel, according to this model. As a result, network attacker (adversary) $\mathcal{A}$ has the ability to intercept the exchanged messages. Afterwards, $\mathcal{A}$ may leak, update, or delete the messages exchanged. In addition, different malware attacks are conceivable in such an environment. The registration authority/trusted authority has full access to control the smart devices SD_i and users of the architecture for the registering them on it. Only the authorised devices/users get access to the different resources of the system.

Table 1
Notations used in the proposed BSSHM.

Notation	Meaning
HD_i	i^{th} smart healthcare device
HS_j	j^{th} health server
U_k	k^{th} registered user
UNM_{U_k}, PWD_{U_k} and OTP_{U_k}	Username, password and one-time password (OTP) of U_k
TA	Trusted registration authority
$\mathcal{A}$	An adversary (attacker)
SK_{U_k,HS_j}	Session key established between U_k and HS_j
SK_{SD_i,HS_j}	Session key established between SD_i and HS_j
BSSHM	Proposed blockchain-enabled secure smart health monitoring system
BC_{SMS}	Blockchain of the smart health monitoring
H_{data}	Healthcare data
BLK_j	A block of BC_{SMS}
BID_j	Identity information of a block used in BLK_j
TS_j	Timestamp value used in BLK_j
RN_j	Random nonce value used in BLK_j
$CHASH_{BLK_j}$	Hash of current block used in BLK_j
$PHASH_{BLK_{j1}}$	Hash of previous block used in BLK_j
OW_{ID_j}	Owner of the block used in BLK_j
PU_{OW_j}	Public key of owner used in BLK_j
$E_{PU_{OW_j}}(T_x)$	Encrypted transactions used in BLK_j
SIG_{BLK_j}	Signature of the block used in BLK_j
TS_1 and TS_2	Used timestamp values in BSSHM

4. BSSHM: Proposed framework

The proposed BSSHM is designed in several phases, i.e., "registration phase," where we conduct the registration of devices and servers. The registration has been done the trusted authority of the system. Another important phase is "multi-factor authentication procedure", where the mutual authentication and key establishments are performed between the legitimate smart healthcare device HD_i, and health server HS_j, and HS_j and the registered genuine user U_k. This task can be performed through the steps mentioned in [6]. After the completion of this phase, there is session key establishment SK_{U_k,HS_j} between U_k and HS_j and also another session key establishment SK_{SD_i,HS_j} between SD_i and HS_j. Further, there is another important phase that is blockchain implementation process, in which we get the blockchain of the smart health monitoring system as BC_{SMS}. The BC_{SMS} stores the data of the proposed system in the form of some blocks. This data can be further utilized to make various health predictions. The details of the notations used in the proposed BSSHM are provided in Table 1. The details of the proposed BSSHM are give below.

4.1. Registration of devices and servers

There is a trusted registration authority TA, which does the registration of the other entities of the network. It mandatory to use trusted registration authority TA for the registration of the users, devices and servers. Because if we use TA for that task then the secret credentials of the entities become safe and secure and can not be revealed to $\mathcal{A}$ in any case. The registration of devices and servers is conducted as follows.

- The trusted registration authority TA registers the smart healthcare device SD_i and stores the registration information in its memory through some secure mean. Then SD_i is deployed as per the needs.
- TA registers the health server HS_j and stores the registration information in its database.

The details of registration process are provided in Algorithm 1.

Algorithm 1 Registration of devices and servers.

Output: Devices and servers with stored credentials

for All devices and servers **do**
  TA registers SD_i.
  TA stores the registration information in SD_i's memory.
  SD_i is deployed.
  TA registers HS_j.
  TA stores the registration information in the database of HS_j.
  if All devices and servers are registered **then**
    Abort the process.
  else
    Continue the registration process.
  end if
end for

4.2. Multi-factor authentication procedure

We need multi-factor authentication procedure to make the proposed BSSHM more secure. As it uses three factors to check the authenticity of a user. On the basis of three used factors, the system allows or stops the users to enter into the system. The required multi-factor authentication procedure in BSSHM is conducted as follows.

- With the help of username UNM_{U_k}, password PWD_{U_k} and one-time password (OTP) OTP_{U_k} the registered user U_k can login into the system.
- U_k performs the steps of authentication and session key establishment (i.e., session key SK_{U_k,HS_j}). For the computation and establishment of SK_{U_k,HS_j} the Steps mentioned in [6] can used. Then U_k accesses the data of HS_j in the secure way.
- SD_i and HS_j perform the steps of mutual authentication and establish the session key SK_{SD_i,HS_j}. For the computation and establishment of SK_{SD_i,HS_j} the Steps mentioned in [6] can used.
- SD_i sends the healthcare data H_{data} to HS_j through the established session key SK_{SD_i,HS_j}.
- HS_j receives the healthcare data from the connected SD_i and performs decryption over it. For example, decryption with SK_{SD_i,HS_j}.
- HS_j performs data aggregation on and H_{data} stores it through the same secure mean.

The details of multi-factor authentication procedure along with the data aggregation process are provided in Algorithm 2. Additionally, the details of blockchain implementation process are provided in Algorithm 3.

5. Formal security verification using Scyther tool

The details of formal security verification using the Scyther tool is provided in this section. The formal security verification of the BSSHM is performed through scyther tool [28–30]. It is better than the other tools, like, ProVerif and AVISPA. Scyther provides prediction on the basis of various cryptographic assumptions. It implies that an attacker would be unable to decipher the encrypted data without the secret key. Via the usage of Security Protocol Descriptive Language (SPDL), Scyther simulates user-defined security protocols. The Scyther tool follows the Dolev-Yao (DY) model plus nine more adversarial models, including the eCK model and the CK model.

The tests offered by Scyther are said to validate security aspects like "secrecy, authentication, synchronisation, aliveness, weak agreement, and agreement." In BSSHM, there are some basic roles for the "authentication and key agreement phase," i.e., SD (for smart healthcare device) and HS (for health server). The steps of BSSHM are coded via SPDL. Scyther takes the SPDL file as input and executes various analyses on the BSSHM. The SPDL snippet of the BSSHM is given in Fig. 2. Fig. 3 depicts

Algorithm 2 Multi-factor authentication procedure.

Output: Mutual authentication and session key establishment

for All devices, servers and users **do**
  U_k does login with UNM_{U_k}, PWD_{U_k} and OTP_{U_k}.
  U_k performs authentication and session key establishment.
  U_k establishes SK_{U_k,HS_j} with HS_j. For the computation and establishment of SK_{U_k,HS_j} the Steps mentioned in [6] can used.
  U_k accesses the data of HS_j through SK_{U_k,HS_j}.
  SD_i and HS_j perform mutual authentication and establish the session key SK_{SD_i,HS_j}. For the computation and establishment of SK_{SD_i,HS_j} the Steps mentioned in [6] can used.
  SD_i sends H_{data} to HS_j via SK_{SD_i,HS_j}.
  HS_j receives H_{data} via SK_{SD_i,HS_j}.
  HS_j performs decryption over H_{data} through SK_{SD_i,HS_j}.
  HS_j performs data aggregation on and H_{data} stores it.
  if Data aggregation over **then**
    Abort the process.
  else
    Continue data aggregation.
  end if
end for

Algorithm 3 Blockchain implementation process.

Output: Blockchain of smart health monitoring system BC_{SMS}

for All devices, servers and users **do**
  HS_j receives data H_{data} from connected SD_i in a secure way (i.e., via SK_{SD_i,HS_j}).
  HS_j creates a block BLK_j with the help of H_{data}. BLK_j contains values like, block' ID BID_j, timestamp value TS_j, random nonce value RN_j, hash of current block $CHASH_{BLK_j}$, hash of previous block $PHASH_{BLK_{j_1}}$, owner of the block OW_{ID_j}, public key of owner PU_{OW_j}, encrypted transactions $E_{PU_{OW_j}}(T_x)$, signature of the block SIG_{BLK_j}.
  HS_j broadcasts BLK_j to its peer-to-peer cloud server (P2PCS) network.
  A consensus for the addition of BLK_j is called using a consensus algorithm, i.e., Practical Byzantine Fault Tolerance.
  if A fraction of minor nodes commit for the addition of BLK_j **then**
    BLK_j is added in blockchain BC_{SMS}.
  else
    Start the consensus process again.
  end if
end for

the outcome of the Scyther tool. Upon examination, it was determined that the BSSHM is protected by the aforementioned claims.

6. Practical implementation of BSSHM

In this section, we provide the details practical implementation of the proposed BSSHM. In BSSHM, we have worked on the smart temperature monitoring device. The non-contact infrared temperature sensors can measure body temperature without physical contact, making them a useful tool for identifying those who may have a fever and potentially be infected with the virus. However, it's important to note that fever is not always a reliable indicator of some viral infection, i.e., COVID-19. As some infected individuals may not have a fever, and some non-infected individuals may have a fever for other reasons. Therefore, it's important to use a combination of different screening measures to identify potentially infected individuals. IoT has brought about a significant change in

Scyther: sidd.spdl

File Verify Help

Protocol description Settings

```
1 const SKSDHS:Function;
2 const SKHSSD:Function;
3 protocol Demo(SD,HS)
4 {
5  role SD
6  {
7  const TS1,TS2,DT1,DT2;
8  send_1(SD,HS,{DT1}SKSDHS,TS1);
9  recv_2(HS,SD,{DT2}SKHSSD,TS2);
10  claim_SD1(SD,Niagree);
11  claim_SD2(SD,Nisynch);
12  claim_SD3(SD,Secret,(SKSDHS));
13  claim_SD4(SD,Weakagree);
14  claim_SD5(SD,Alive);
15  }
16  role HS
17  {
18  const TS1,TS2,DT1,DT2;
19  recv_1(SD,HS,{DT1}SKSDHS,TS1);
20  send_2(HS,SD,{DT2}SKHSSD,TS2);
21  claim_HS1(HS,Niagree);
22  claim_HS2(HS,Nisynch);
23  claim_HS3(HS,Secret,(SKHSSD));
24  claim_HS4(HS,Weakagree);
25  claim_HS5(HS,Alive);
26  }
27 }
```

Fig. 2. SPDL snippet of BSSHM.

the way we live our lives. It has enabled the development of various systems that can be monitored and controlled from remote locations. The proposed scheme utilizes the power of IoT to create a temperature monitoring device that is based on Raspberry Pi and MLX90614 [5]. Through which the temperature of a subject (i.e., a human user-patient) can be monitored in a smart way without making the physical contact. The readings of the temperature are available 24×7 hours in a web-based software tool or in the form of a smartphone application. Therefore, the physiological symptoms of a patient can be monitored easily with the help of the implemented system.

The details of system specifications are given in Table 2. We have used Windows 10 as the platform along with processor AMD Ryzen 5 5600H with Radeon Graphics 3.30 GHz. The programming environment was Python 3. The online storage was Google firebase real-time database. The random-access memory (RAM) size was 8.00 GB along with Pyrebase for firebase libraries.

The hardware requirements are given in Table 3. We have used MicroSD Card for booting up the Raspberry Pi. There was a Raspberry Pi case to protect and hold the Raspberry Pi. Moreover, there was a HDMI cable to connect the Raspberry Pi to a monitor or TV. Again a keyboard and mouse was used to control the RasSpberry Pi. A Wi-Fi dongle has been used to connect the Raspberry Pi to the Internet in case of any needs. The light-emitting diodes (LEDs) display were used for indicating the status of the device. The breadboard was deployed for prototyping and testing purposes. We also used jumper wires for connecting the components together. There was a power supply (5V,2A/3A) to provide the power supply to the Raspberry Pi and other associated components.

It is important to ensure that all components are compatible with the Raspberry Pi and that they are of good quality to ensure the smooth execution of the experiments. A view of implemented testbed of the BSSHM is given in Fig. 4.

Table 2
System specifications.

Parameter	Description
Platform	Windows 10
Processor	AMD Ryzen 5 5600H with Radeon Graphics 3.30 GHz
Programming environment	Python 3
Online storage	Google firebase real-time database
Dataset used	Patient data fetched through MLX60614
Random-access memory (RAM) size	8.00 GB
Libraries used	Pyrebase for firebase

Table 3
Hardware requirements.

Hardware	Use
MicroSD Card	For booting up the Raspberry Pi
Raspberry Pi Case	To protect and hold the Raspberry Pi
HDMI Cable	To connect the Raspberry Pi to a monitor or TV
Keyboard and Mouse	To control the RasSpberry Pi
Wi-Fi Dongle	To connect the Raspberry Pi to the Internet (optional)
Resistors	For voltage regulation and protection
LEDs	For indicating the status of the device
Breadboard	For prototyping and testing
Jumper Wires	For connecting the components together
Power Supply (5V,2A/3A)	To power up the Raspberry Pi and other components

6.1. Raspberry Pi

The Raspberry Pi is a small, credit card-sized computer designed for educational/experimentation purposes, which has gained popularity among developers and hobbyists for its affordable price and impressive specifications. It features onboard Wi-Fi, Bluetooth, and a programmable GPIO header, making it ideal for learning programming skills, building hardware projects, and even industrial use. Raspberry Pi boards can run a variety of operating systems, including various versions of Linux, Windows 10 IoT Core, and others. They are popular for a wide range of projects, including media centers, game consoles and home automation systems.

6.2. Various models of Raspberry pi

There are several types of Raspberry Pi boards available, each with their own set of features and capabilities. Here are some of the most popular Raspberry Pi models.

- **Raspberry Pi 1 Model A+:** This was the first model released in 2012. It has 256 MB of RAM, one USB port, and no Ethernet port.
- **Raspberry Pi 1 Model B+:** This model was released in 2014, with a more powerful processor, 512 MB of RAM, and additional USB and Ethernet ports.
- **Raspberry Pi 2 Model B:** This model was released in 2015 and has a quad-core processor, 1 GB of RAM, and four USB ports. It also has improved GPIO capabilities.

Scyther results : verify

Claim				Status	Comments
Demo	SD	Demo,SD1	Niagree	Ok	No attacks within bounds.
		Demo,SD2	Nisynch	Ok	No attacks within bounds.
		Demo,SD3	Secret SKSDHS	Ok	No attacks within bounds.
		Demo,SD4	Weakagree	Ok	No attacks within bounds.
		Demo,SD5	Alive	Ok	No attacks within bounds.
	HS	Demo,HS1	Niagree	Ok	No attacks within bounds.
		Demo,HS2	Nisynch	Ok	No attacks within bounds.
		Demo,HS3	Secret SKHSSD	Ok	No attacks within bounds.
		Demo,HS4	Weakagree	Ok	No attacks within bounds.
		Demo,HS5	Alive	Ok	No attacks within bounds.

Done.

Fig. 3. Outcome of formal security verification via SPDL implementation in Scyther tool.

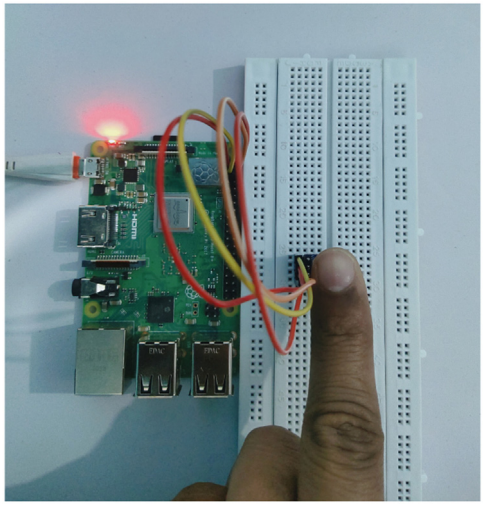

Fig. 4. Implemented testbed of the BSSHM.

- **Raspberry Pi 3 Model B:** This model was released in 2016 and is similar to the Raspberry Pi 2, but with a faster processor, built-in Wi-Fi and Bluetooth, and improved Ethernet capabilities.
- **Raspberry Pi 4 Model B:** This model was released in 2019 and is the most powerful Raspberry Pi board to date, with up to 8 GB of RAM, dual-band Wi-Fi, gigabit Ethernet, and support for up to two 4K displays.
- **Raspberry Pi Zero:** This is a smaller and more affordable model, released in 2015. It has a single-core processor and 512 MB of RAM, and is popular for projects where space and cost are important factors.

There are also several other models and variations of Raspberry Pi boards available, including the Raspberry Pi Compute Module, which is designed for use in industrial and commercial applications.

6.3. Sensor

There are several temperature sensors available in the market that can be used with Raspberry Pi. Some of the popular options are given below.

- **DS18B20:** This is a popular digital temperature sensor that can be connected to the Raspberry Pi using a 1-Wire interface. It has a temperature range of -55°C to 125°C.
- **DHT22:** This is a digital temperature and humidity sensor that can be connected to the Raspberry Pi using a 1-Wire interface. It has a temperature range of -40°C to 80°C and a humidity range of 0% to 100%.
- **BMP280:** This is a digital pressure and temperature sensor that can be connected to the Raspberry Pi using I2C or SPI interfaces. It has a temperature range of -40°C to 85°C.
- **LM35:** This is an analog temperature sensor that can be connected to the Raspberry Pi using an analog-to-digital converter (ADC). It has a temperature range of -55°C to 150°C.
- **Mlx90614:** The MLX90614 is a non-contact infrared temperature sensor made by Melexis N.V. It has a high accuracy and a wide temperature measurement range from -70°C to 380°C.

6.4. MLX90614 IR temperature sensor

The MLX90614 is an infrared thermometer module made by Melexis. It is a non-contact temperature sensor that can measure the temperature of an object without physical contact, using infrared radiation. The sensor can measure the temperature of an object between -70° C and

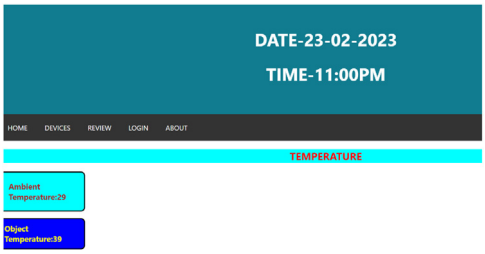

Fig. 5. Real time sensed healthcare data on the web page.

380° C, with an accuracy of ±0.5° C. The MLX90614 is a popular sensor for a wide range of applications, including temperature measurement in industrial, automotive, and medical equipment. It is also commonly used in hobbyist projects, such as building a contactless thermometer or integrating temperature sensing into a home automation system. One of the key advantages of the MLX90614 is its non-contact nature, which makes it useful in situations where physical contact with a temperature sensor is not possible or desirable.

The view of real time sensed healthcare data on the web page is given in Fig. 5. It shows ambient temperature as 29°C and object (i.e., patient) temperature as 39°C.

7. Implementation of blockchain phase

Here, the details of the implementation of blockchain phase of the BSSHM are given [31,32]. Since the proposed BSSHM processes and stores the sensitive healthcare data. Therefore, under these circumstances, it is mandatory to maintain the secrecy of the sensitive healthcare data. Otherwise, the sensitive healthcare data may be leaked, or updated in an authorised way. Blockchain is a distributed ledger technology, which maintains the data in the form of blocks and each block contains some information inside them. Due to such mechanism of storing the data in the blockchain, we can store the healthcare data in the form of certain number of encrypted transactions. Due to the encrypted transactions, the revealing and updating of healthcare is not possible for $\mathcal{A}$. Hence the sensitive healthcare data is protected due to the deployment of blockchain technology in the proposed BSSHM. Various scenarios are considered during the simulation study. It is implemented on a "Windows 10 64-bit system with an Intel (R) core i5-8250U processor running at 1.60 GHz-1.80 GHz." This system contains random-access memory (RAM) of 8 GB. "Eclipse IDE 2019-12" has been utilized for the platform part and the Java langauge is used for coding. The number of "smart healthcare devices" taken in each scenario as 15 (in case-1), 30 (in case-2), and 45 (in case-3). Number of blocks consider as 5 in case-1, 10 in case-2, and 15 in case-3. The number of users are taken as 10 in case-1, 20 in case-2, and 40 in case-3. Moreover, 4 miner nodes in each case are taken. The details of the estimated results are given below.

- **Calculation of computational time:** In all considered cases, the impact of increasing number of users and healthcare devices was computed in the form of computation time (in seconds). For example, for case-1, case-2, and case-3, the appraise computational time (in seconds) are 4.25, 5.50, and 6.12, respectively. The results are depicted in Fig. 6. It's important to mention that the "computational time" has increment when "number of smart healthcare devices" and "number of users" increases when we go from case-1 to case-2 and case-2 to case-3. That happened because "creation and addition of more number of blocks in the blockchain" were required under those circumstances.
- **Calculation of transactions per second (TPS):** In all considered cases, the impact of increasing number of users and healthcare devices was also estimated in the form of transactions per second (TPS). For example, for case-1, case-2, and case-3, the appraise TPS values are 118, 182, and 245, respectively. The results are depicted in Fig. 7.

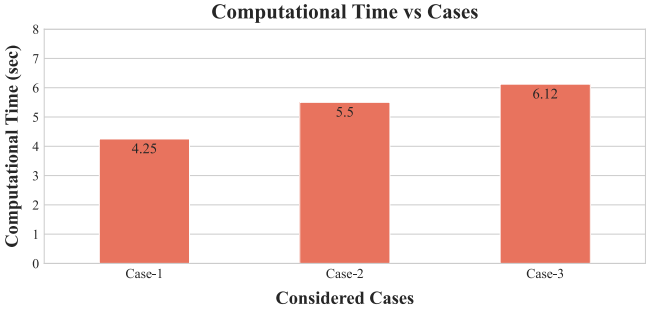

Fig. 6. Calculations of computational cost.

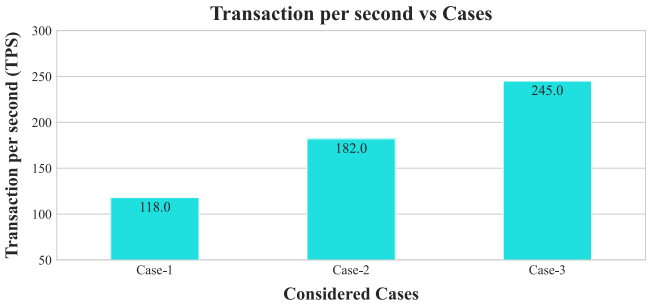

Fig. 7. Calculations of transactions per second (TPS).

It's important to note that the number of transactions per second (TPS) increases as the blockchain expands in size with more number of smart healthcare devices, and users. That happened because "creation and addition of more number of blocks in the blockchain" were required under those circumstances. Eventually, that increases the value of TPS.

8. Conclusion and future scope

The smart health monitoring system is an important aspect of healthcare as it is used to diagnose and treat various illnesses and conditions. In this paper, an architecture of the blockchain-enabled secure smart health monitoring system was presented. The threat model related to the BSSHM was given. The formal security verification of the BSSHM is done through Scyther tool. It has proved that BSSHM is able to defend various potential attacks. Finally, a testbed of the BSSHM was implemented to check its usability in the real-time.

In future, we would like to add more features in the proposed BSSHM. In addition, the Big data analytics in cloud computing environment for the discussed smart health monitoring system would be helpful as it was performed in [33].

Declaration of Competing Interest

The authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest, or non-financial interest in the subject matter or materials discussed in this manuscript.

Acknowledgements

The authors would like to thank the anonymous reviewers and the editor for their valuable suggestions and comments which helped in improving the presentation and technical quality of this article.

References

[1] N. Lath, K. Thapliyal, K. Kandpal, M. Wazid, A.K. Das, D.P. Singh, BDESF-ITS: blockchain-based secure data exchange and storage framework for intelligent transportation system, in: IEEE INFOCOM 2022 - IEEE Conference on Computer Com-

munications Workshops (INFOCOM WKSHPS), 2022, pp. 1–6, doi:10.1109/INFOCOMWKSHPS54753.2022.9798114. London, UK
[2] M. Wazid, A.K. Das, N. Mohd, Y. Park, Healthcare 5.0 security framework: applications, issues and future research directions, IEEE Access 10 (2022) 129429–129442, doi:10.1109/ACCESS.2022.3228505.
[3] S. Thapliyal, M. Wazid, D.P. Singh, Blockchain-driven smart healthcare system: challenges, technologies and future research, in: J. Choudrie, P. Mahalle, T. Perumal, A. Joshi (Eds.), ICT with Intelligent Applications, Springer Nature Singapore, Singapore, 2023, pp. 97–110.
[4] S. Thapliyal, M. Wazid, D.P. Singh, A.K. Das, A. Alhomoud, A.R. Alharbi, H. Kumar, ACM-SH: an efficient access control and key establishment mechanism for sustainable smart healthcare, Sustainability 14 (8) (2022).
[5] M. Wazid, S. Thapliyal, D.P. Singh, A.K. Das, S. Shetty, Design and testbed experiments of user authentication and key establishment mechanism for smart healthcare cyber physical systems, IEEE Trans. Network Sci. Eng. (2022), doi:10.1109/TNSE.2022.3163201. 1–1
[6] M. Wazid, A.K. Das, S. Shetty, J.J.P.C. Rodrigues, M. Guizani, AISCM-FH: AI-Enabled secure communication mechanism in fog computing-Based healthcare, IEEE Trans. Inf. Forensics Secur. 18 (2023) 319–334, doi:10.1109/TIFS.2022.3220959.
[7] N. Garg, M.S. Obaidat, M. Wazid, A.K. Das, D.P. Singh, SPCS-IoTEH: secure privacy-preserving communication scheme for IoT-Enabled e-Health applications, in: IEEE International Conference on Communications (ICC), 2021, pp. 1–6, doi:10.1109/ICC42927.2021.9500388. Montreal, Canada
[8] D. He, N. Kumar, J.H. Lee, R.S. Sherratt, Enhanced three-factor security protocol for consumer USB mass storage devices, IEEE Trans. Consum. Electron. 60 (1) (2014) 30–37.
[9] Q. Feng, D. He, H. Wang, L. Zhou, K.-K.R. Choo, Lightweight collaborative authentication with key protection for smart electronic health record system, IEEE Sens J 20 (4) (2020) 2181–2196.
[10] N. Garg, M. Wazid, J. Singh, D.P. Singh, A.K. Das, Security in IoMT-driven smart healthcare: acomprehensive review and open challenges, Security and Privacy 5 (5) (2022) e235.
[11] S. Chatterjee, A.K. Das, An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks, Security and Communication Networks 8 (9) (2015) 1752–1771.
[12] A.K. Das, A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications, Networking Science 2 (1) (2013) 12–27.
[13] A.K. Das, A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks, Int. J. Inf. Secur. 11 (3) (2012) 189–211.
[14] M. Wazid, A.K. Das, A.V. Vasilakos, Authenticated key management protocol for cloud-assisted body area sensor networks, Journal of Network and Computer Applications 123 (2018) 112–126.
[15] P. Bagga, A.K. Das, M. Wazid, J.J.P.C. Rodrigues, Y. Park, Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges, IEEE Access 8 (2020) 54314–54344, doi:10.1109/ACCESS.2020.2981397.
[16] A. Vangala, A.K. Sutrala, A.K. Das, M. Jo, Smart contract-based blockchain-envisioned authentication scheme for smart farming, IEEE Internet Things J. 8 (13) (2021) 10792–10806, doi:10.1109/JIOT.2021.3050676.
[17] S. Rana, D. Mishra, Efficient and secure attribute based access control architecture for smart healthcare, J Med Syst 44 (5) (2020) 97.
[18] S. Pal, M. Hitchens, V. Varadharajan, T. Rabehaja, Policy-based access control for constrained healthcare resources in the context of the internet of things, Journal of Network and Computer Applications 139 (2019) 57–74.
[19] .R Sandip, . Das, .A Kumar, .C Santanu, .K Neeraj, .C Samiran, .R Joel J.P.C, Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications, IEEE Trans. Ind. Inf. 15 (1) (2019) 457–468.
[20] F. Merabet, A. Cherif, M. Belkadi, O. Blazy, E. Conchon, D. Sauveron, New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications, Peer-to-Peer Netw. Appl. 13 (2) (2020) 439–474.
[21] C.S. Jang, D.G. Lee, J.-w. Han, J.H. Park, Hybrid security protocol for wireless body area networks, Wireless Communications and Mobile Computing 11 (2) (2011) 277–288.
[22] D. He, S. Zeadally, Authentication protocol for an ambient assisted living system, IEEE Commun. Mag. 53 (1) (2015) 71–77.
[23] C. Li, C. Weng, C. Lee, C. Wang, A hash based remote user authentication and authenticated key agreement scheme for the integrated EPR information system, J Med Syst 39 (11) (2015) 144:1–144:11.
[24] C.-T. Li, M.-S. Hwang, Y.-P. Chu, Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments, Comput Commun 31 (18) (2008) 4255–4258.
[25] C.C. Lee, Y.M. Lai, C.T. Li, An improved secure dynamic ID based remote user authentication scheme for multi-server environment, International Journal of Security and Its Applications 6 (2) (2012) 203–209.
[26] C. Li, C. Lee, C. Weng, C. Fan, A secure dynamic identity based authentication protocol with smart cards for multi-Server architecture, Journal of Information Science and Engineering 31 (6) (2015) 1975–1992.
[27] D. Dolev, A.C. Yao, On the security of public key protocols, IEEE Trans. Inf. Theory 29 (2) (1983) 198–208.
[28] B. Khadem, A.M. Suteh, M. Ahmad, A. Alkhayyat, M.S. Farash, H.S. Khalifa, An improved WBSN key-agreement protocol based on static parameters and hash functions, IEEE Access 9 (2021) 78463–78473.
[29] C.J.F. Cremers, Scyther : semantics and verification of security protocols, 2022, (????). https://pure.tue.nl/ws/files/2425555/200612074.pdf. Accessed on November 2022.
[30] M. Tanveer, A.H. Zahid, M. Ahmad, A. Baz, H. Alhakami, Lake-iod: lightweight authenticated key exchange protocol for the internet of drone environment, IEEE Access 8 (2020) 155645–155659.
[31] M. Fan, X. Zhang, Consortium blockchain based data aggregation and regulation mechanism for smart grid, IEEE Access 7 (2019) 35929–35940.
[32] N. Garg, M. Wazid, A.K. Das, D.P. Singh, J.J.P.C. Rodrigues, Y. Park, BAKMP-IoMt: design of blockchain enabled authenticated key management protocol for internet of medical things deployment, IEEE Access 8 (2020) 95956–95977.
[33] A. Jindal, A. Dua, N. Kumar, A.K. Das, A.V. Vasilakos, J.J.P.C. Rodrigues, Providing healthcare-as-a-service using fuzzy rule based big data analytics in cloud computing, IEEE J Biomed Health Inform 22 (5) (2018) 1605–1618.