Article

Not peer-reviewed version

Secure Monitoring System for IoT Healthcare Data in the Cloud

Christos L. Stergiou *, Andreas P. Plageras, Maria P. Koidou, Konstantinos E. Psannis *

Posted Date: 5 July 2023

doi: 10.20944/preprints202307.0266.v1

Keywords: Internet of Things; Machine Learning; Cloud Computing; Artificial Intelligence; Security; Healthcare; Monitoring; Detection

Article

Secure Monitoring System for IoT Healthcare Data in the Cloud

Christos L. Stergiou *, Andreas P. Plageras, Maria P. Koidou and Konstantinos E. Psannis *

Department of Applied Informatics; University of Macedonia; Thessaloniki 54636; Greece
* Correspondence: kpsannis@uom.edu.gr; Tel.: +30-2310-891-737

Abstract: Even if the field of medicine has made great strides in recent years, infectious diseases caused by novel viruses that damage the respiratory system continue to plague people all over the world. This type of virus is very dangerous, especially for people who deal with serious long-term breathing problems, like triggering asthma, pneumonia, or bronchitis infections. Thus, this paper demonstrates a new Secure Machine Learning Monitoring System for a model for virus detection. Our proposed model makes use of 4 basic emerging technologies, Internet of Things (IoT), Wireless Sensor Networks (WSN), Cloud Computing (CC), and Machine Learning (ML), to detect dangerous types of viruses that infect people or animals causing panic worldwide and deregulating human daily life. The proposed system is a robust system that could be established in various buildings, like hospitals, entertainment halls, universities, etc., and will provide accuracy, speed, and privacy for data collected in the detection of viruses.

Keywords: Internet of Things; machine learning; cloud computing; Artificial Intelligence; security; healthcare; monitoring; detection

1. Introduction

It appears that there is a pressing need to incorporate new technologies into medical care for the best possible detection of such viruses. Five cutting-edge technologies—Internet of Things (IoT), Wireless Sensor Networks (WSN), Cloud Computing (CC), Machine Learning (ML), and Wireless Networks—can be utilized in conjunction to combat viruses and the threat of infectious illnesses. All these technologies can be worked under the broad term of Internet of Medical Things (IoMT), which is IoT that has reconstructed hospital settings and invented a new paradigm. Additionally, it offers numerous opportunities, due to the wearable devices used by plenty of people, to enhance health and well-being, associated with the terms of eHealth and mHealth [1]. WSN takes advantage of features such as low cost, availability, and accessibility and as a result the increase in the adoption of these mobile sensors. Additionally, these personalized healthcare systems gather pertinent biophysical data to aid in medical diagnoses and decisions, and they could be stored, maintained, and processed on the Cloud [2].

Moreover, IoT-based Big Data (BD) and ML can offer a handful of opportunities for healthcare systems relying on IoT, and therefore the new term of Artificial Intelligence of Things (AIoT). WSN systems' real-time health data can be utilized to assist patients with self-administered treatments. Furthermore, mobile devices with mobile applications are frequently used and integrated with the terms of telemedicine and mHealth through the IoMT. The results of medical data analytics from data analysis platforms established on the Cloud and increase the applicability of data interpretations and reduce the time of analyzing data outputs and thus the detection and prediction of viruses and diseases.

A Secure Monitoring System for IoT Healthcare Data in the Cloud needs to be designed to ensure the confidentiality, integrity, and availability of sensitive healthcare data generated by Internet of Things (IoT) devices [1,2]. It must aims to protect patient privacy, prevent unauthorized access, and maintain the integrity of healthcare data stored and processed in the cloud. Below, there are an overview of implementation aspects and goals of such a system: 1) *Data Encryption:* Implement strong encryption techniques to secure healthcare data both in transit and at rest. Encryption ensures that

even if the data is intercepted or accessed without authorization, it remains unreadable and useless. 2) *Access Control and Authentication:* Enforce strict access control mechanisms to allow only authorized personnel or systems to access healthcare data. This includes implementing strong authentication methods like two-factor authentication and role-based access control (RBAC) to limit data access based on user roles and responsibilities. 3) *Secure Communication:* Establish secure channels for communication between IoT devices, cloud infrastructure, and healthcare applications. This involves using secure protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt data in transit and prevent eavesdropping or tampering. 4) *Data Integrity and Validation:* Implement mechanisms to ensure the integrity of healthcare data. This can be achieved through digital signatures or message authentication codes (MACs), which verify that the data has not been tampered with during transit or storage. 5) *Security Monitoring and Logging:* Set up monitoring systems to detect any suspicious activities or unauthorized access attempts. Log and analyze system events, network traffic, and user activities to identify potential security breaches or anomalies. 6) *Secure Storage:* Utilize secure storage solutions to protect healthcare data within the cloud infrastructure. This may involve using encryption at rest, access controls, and redundancy to ensure data availability and resilience against hardware failures or cyber attacks. 7) *Compliance with Regulations:* Ensure compliance with relevant healthcare regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR). Adhere to the necessary security and privacy requirements specified by these regulations. 8) *Regular Security Audits and Updates:* Perform regular security audits and assessments to identify vulnerabilities and implement necessary updates and patches. Stay up to date with the latest security practices, emerging threats, and industry standards.

Therefore, the main contributions of this work are:

- A proposed system that integrates the benefits of IoT with the computation power of Cloud Computing, through a wireless network.
- The major goal of the proposed model is to immediately detect, predict, and notify the responsible surveillance personnel.
- The proposed model could be established in public service buildings, such as hospitals.
- The system operates through a wireless network, due to the high transmission data rate that could offer, aiming to have more direct notifications, and due to the IoT data produced by mobile devices.

The rest of the paper is organized as follows: Section 2 presents some related researches which have been conducted in the field of virus detection. Section 3 analyzes the limitations and barriers of conventional medical methods. Section 4 describes the technological challenges generated in Microbiology. Section 5 describes our proposed model and the involved technologies. Section 6 presents the application fields of our proposed scheme and the benefits that it can provide to the population worldwide. Finally, Section 7 concludes the paper and provides some potential future directions.

2. Related Work

The field of medicine has offered numerous studies that use various technologies to effectively detect harmful viruses and contagious diseases. The development of an autonomous robust model, though, is still being investigated. This model will utilize all of the most well-known immersive technologies.

The objective of the research by L. Bai et al. [3] is to timely diagnose patients and provide the best possible care using medical technology, namely the "COVID-19 Intelligent Diagnosis and Treatment Assistant Program (nCapp)". Real-time communication is facilitated by computer cloud technology, which is a feature of nCapp. This study shows that when a suspicious sample is found, the diagnosis is automated, and nCapp then categorizes the suspects based on how serious the problem is. The system is updated in real-time by nCapp, who also makes it a reliable resource for illnesses in the future.

 doi:10.20944/preprints202307.0266.v1

H. S. Maghdid [4] has developed a framework for COVID-19 detection using information from a smartphone's onboard sensors, including as cameras, microphones, temperature, and inertial sensors. Based on the gathered data, ML techniques are used to learn about and gain information about the disease symptoms. This is perhaps understandable given that the data generated by the smartphone sensors has already been successfully used in a number of distinct applications, and the suggested solution combines all of these applications into a single framework.

S. Muthukumar [5] suggests a smart humidity monitoring system that takes into account the strong connection between humidity and infectious disease and suggests a method that may maintain a room's relative humidity while preventing the spread of infectious diseases. It has developed a sensor-based IoT module that monitors a room's relative humidity and provides the status to the inhabitants after taking the benefits of preserving humidity into account. Specifically, the sensor-based hardware module that measures the air's relative humidity and provides the data to the user through the internet, whether they are in the same room as the user or not. The aforementioned module can also be set to maintain relative humidity levels in a room depending on the user's requirements. In order to maintain ideal humidity levels, the system also manages the room's air conditioning and humidifying equipment. Due to the significant danger of infectious disease outbreaks in hospitals, the designed module is an affordable option that can be very helpful. It can be used in homes, offices, and schools due to its inexpensive cost.

3. Limitations & Barriers of Conventional Medical Methods

Although conventional medical methods and techniques play an important role in fighting against viruses and infectious diseases caused by them, there are several limitations and barriers which are related to the identification, and hence the treatment of fatal diseases, which are very dangerous for human population.

The branch of Medicine and especially this of Microbiology is evolving continuously, using novel techniques for enhanced healthcare results. However, the integration of technological methods in Microbiology is still in the early stage. The human population still suffers from fatal diseases caused by dangerous viruses which insult the respiratory system. Such viruses, like the new Coronavirus COVID-19, are very hazardous both generally for all people and especially for those who face serious long-term breathing problems, like triggering asthma, pneumonia, or bronchitis infections.

The medical sector has to deal with infectious diseases and several limitations and barriers, such as the lack of health personnel and health infrastructure (medical centers, hospitals, etc.), in combination with the difficult organizational healthcare of emergency cases [6], like nowadays with the COVID-19 spread. These problems make the fight against the sudden epidemic, such as this of recent days, very difficult, causing many delays in virus identification and treatment of infectious diseases, and in many cases deaths. In addition, this weakness of the medical sector also has an impact on the economy, as most businesses have been forced to close, and thus, a lot of employees were left without work and salary.

4. Technological Challenges in Microbiology

Previous works [7–10] has demonstrated that the rapid development of wired and mobile networks has resulted in a rapid growth in data. Therefore, managing, analyzing, and transferring these kinds of data present us with significant hurdles. These challenges regarding the vast amount of data are related to their representation, their expendability, their existing redundancy, their quality and variety, their storage, the knowledge exported from them, the management of their life cycle, the energy management, the heterogeneity, the speed and accuracy, the security and privacy, the confidentiality, the generation or development of tools, methods, and algorithms for analysis, and the overall performance of them [11]. The most recent research shows that there are "gaps" in the way that such data are managed, analyzed, and transported at various levels, as well as issues that arise from their use. As a result, it is necessary to optimize them by applying new techniques and

 doi:10.20944/preprints202307.0266.v1

algorithms [9]. Moreover, state mechanisms of many countries, mainly the ones of third countries, are not ready to apply cutting-edge technologies to their population.

5. Proposed System

In this Section, the major emerged technologies used for the proposed system are presented, in addition to the architecture of our proposed system.

5.1. Involved Technologies

The following cutting-edge technologies, when combined to form our suggested system, can provide a strong system with enhanced virus detection capabilities.

5.1.1. Internet of Things (IoT)

IoT is a cutting-edge new technology that makes it possible to connect any commonly used physical devices to the Internet. This fact creates a vast global network of distinctive items that can communicate with one another to fulfill predetermined tasks, resulting in a variety of positive effects in various scientific fields, including medicine [4]. Surprisingly, wearable IoT-based gadgets can be used in healthcare and have applications, offering a wide spectrum of new possibilities because of pervasive connectivity [5].

5.1.2. Wireless Sensor Networks (WSN)

Wireless Sensor Networks (WSNs) are networks of small, inexpensive sensor nodes, which use wireless communication to gather and send data from their surroundings. These sensor nodes can monitor physical or environmental variables because they are furnished with a variety of sensors, including temperature, humidity, light, motion, and gas sensors. The primary goal of WSN is to connect IoT-based devices (such as those belonging to a patient) in order to offer helpful information whenever and wherever it is required, such as in a hospital [4].

WSNs have a number of benefits over conventional wired sensor networks, including quick deployment, adaptability, scalability, and affordability. Numerous industries, such as environmental monitoring, industrial automation, healthcare, agriculture, transportation, and smart cities, all find use for them. WSNs can have their capabilities and potential applications increased by merging them with other internet technologies [8].

A wide range of opportunities for improving data gathering, analysis, and decision-making capabilities are made possible by the integration of WSNs with other internet technologies. WSNs can aid in the creation of intelligent and interconnected systems in a variety of sectors by utilizing the power of connection and cutting-edge computation [4].

5.1.3. Cloud Computing (CC)

The transmission of on-demand computing resources, such as storage, processing power, and software programs, through the internet is referred to as cloud computing. Cloud computing enables users to access and utilise these resources remotely from any location with an internet connection, as opposed to relying on local servers or personal devices. The adoption of cloud computing in the healthcare industry has improved the effectiveness, usability, and security of healthcare services. Also, in the field of medicine, CC can give medical professionals like doctors and nurses access to patient records anytime and wherever they are [9].

The healthcare industry now has access to scalable infrastructure, data sharing capabilities, cutting-edge analytics, and remote healthcare delivery thanks to the integration of cloud computing with other internet technologies [9]. Collaboration between healthcare providers is facilitated, data-driven decision-making is made possible, and ultimately patient care and outcomes are improved.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 July 2023 doi:10.20944/preprints202307.0266.v1

5.1.4. Machine Learning (ML)

Machine learning (ML) algorithms can help identify various virus kinds more accurately so that they can be dealt with and prevented as soon as feasible. Additionally, this will stop susceptible populations from spreading. Based on the properties of the air in the environment, ML can be helpful in the prognosis, diagnosis, and control of patients infected with certain type of flu throughout the period of preventing and controlling the pandemic [12]. The respiratory pattern differs from the typical cold and other infections, according to the most recent clinical studies [13]. However, with the improved efficiency of these algorithms and the capacity to utilize huge volumes of data with various properties, the advantages of adopting ML techniques in risk management will be highly beneficial [14]. Artificial Intelligence (AI) technology and machine learning can be treated as subversive technologies that come to change established procedures for monitoring effective virus recognition, and in particular, because of the current situation, it could contribute to the prevention and control of fatal viruses, like COVID-19.

5.2. System's Primary Goals

The primary goals of the proposed Secure Monitoring System for IoT Healthcare Data in the Cloud are listed below:

1. ***Confidentiality:*** Protect the privacy and confidentiality of sensitive healthcare data, preventing unauthorized access or disclosure.
2. ***Integrity:*** Ensure the accuracy, consistency, and reliability of healthcare data by preventing unauthorized modification or tampering.
3. Availability: Maintain high availability of healthcare data and systems, minimizing downtime and ensuring that authorized users can access the data when needed.
4. ***Compliance:*** Meet the legal and regulatory requirements for protecting healthcare data, such as HIPAA, GDPR, or any other applicable regulations.
5. ***Detection and Response:*** Detect and respond to security incidents, anomalies, or breaches in a timely manner to minimize the impact on patient safety and data security.
6. ***Auditability:*** Enable comprehensive logging and auditing capabilities to track and monitor user activities, system events, and data access for forensic analysis and compliance purposes.

By focusing on these implementation aspects and goals, the proposed Secure Monitoring System for IoT Healthcare Data in the Cloud can help safeguard sensitive healthcare information, maintain the trust of patients and healthcare providers, and ensure the delivery of quality healthcare services.

5.3. System's Architecture

The main goal of this work is to introduce a Secure Machine Learning Monitoring System for IoT Healthcare data in the Cloud which integrates the benefits delivered by a Machine Learning scenario, and the immediacy of the data produced by IoMT, with the computation power offered from a Cloud Computing server, operated through a wireless network. This system could produce, manage and control IoMT data produced by air condition-quality sensors and thermal-IR cameras, in addition to various mobile devices.

The XMPP (Extensible Messaging and Presence Protocol) has been used to communicate the various amounts of data generated by various devices, such as sensors and cameras. This protocol has undergone extensive use and testing and is an open standard. It is based on an efficient model, the publish/subscribe model presented in Figure 1 [15].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 July 2023 doi:10.20944/preprints202307.0266.v1

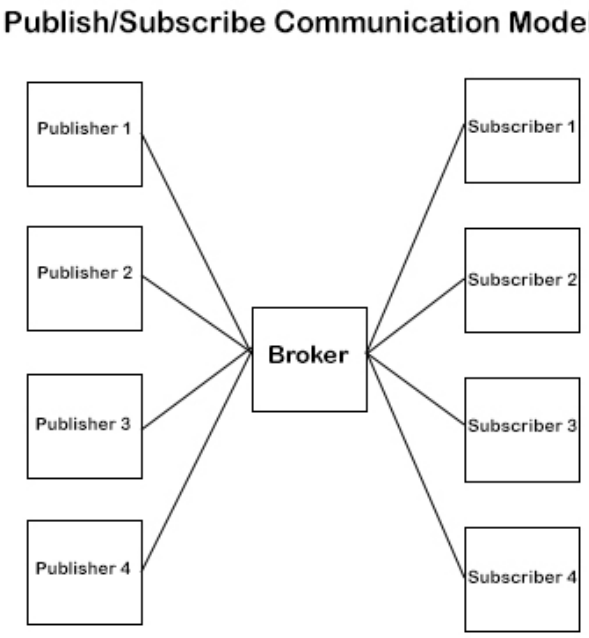

Figure 1. Publish/Subscribe Communication model.

In this paradigm, data is sent from a publisher (an IoT device) to a broker device in a safe and effective manner. Any subscriber device that requests a certain "topic" is then forwarded the updated data by the broker device. As an illustration, the temperature sensor will publish temperature information to the broker under the "temperature" subject. Those that request the temperature topic will have access to these data. The requirements of storage and cloud systems are met by the XMPP protocol. Additionally, a framework that provided an abstraction of the network devices was employed to create the system and facilitate communication across all devices, servers, and databases. The interface between the IoT devices [XMPP] and the API (Application Programming Interface), which is hosted in the user's device, is made simpler by this framework.

The system architecture for our suggested model implementation is depicted in Figure 2. Each surveillance infrastructure is under the direction of the cloud server. An installed infrastructure that is not directly connected to a Cloud server may also provide data to it. To export the appropriate conclusions for each monitoring region, the Cloud server managed and organized all the data that the system had acquired. Additionally, the cloud offers a safe environment for gathering, managing, and processing the data generated by IoMT.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 July 2023 doi:10.20944/preprints202307.0266.v1

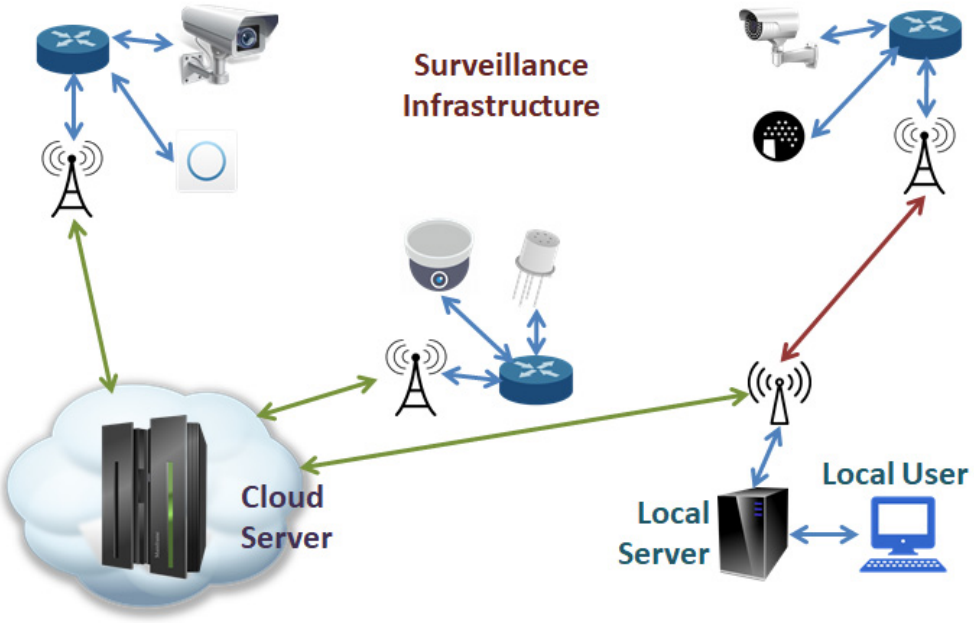

Figure 2. Proposed System's architecture.

Thermal-IR cameras measure the ambient temperature and, more precisely, the temperature of people arriving or moving through the surveillance area. Each camera sends pictures it has taken to a cloud server over a wireless network. A server in the cloud runs a data analysis algorithm that determines whether the temperature reading of each camera is greater than 37 Celsius. Then, in order to stop the spread and isolate that person in another, separated space, a notification signal appears in the monitoring system of that area if a temperature over that particular threshold is observed.

The area's environment has a high level of air pollution, according to air quality sensors. The cloud server received the detection data via the wireless network. The data analysis algorithm established on the Cloud server inspects if the rate of air pollution in the area exceeds normal. If it exceeds then a notification signal appears in the monitoring system of that area, and then the local surveillance and control personnel will be notified.

A machine learning scenario is set up in the cloud server that will be able to detect and tell about the state of the monitored area. After many calculations and iterations, the ML algorithm will be able to export automated conclusions about whether or not a location is at risk. It manages and controls the data shared from the IoT sensors, both cameras and air sensors, as well as the data produced and collected by the connected mobile devices. It will therefore alert the local surveillance and control people based on the data given via the IoT sensors. The goal of the ML algorithm is to be able to detect without the need for human supervision and then properly notify about the detection it made.

5.4. System's Algorithm Approach

The proposed system's algorithm presented below with a python source code implementation paradigm (Algorithm 1):

Algorithm 1

```
import ssl
import hashlib
import socket
import cryptography
from cryptography.fernet import Fernet
# Example IoT device data
iot_data = {
    "patient_id": "123456",
```

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 July 2023 doi:10.20944/preprints202307.0266.v1


```
    "heart_rate": 75,
    "temperature": 37.2
}
# Generate encryption key
encryption_key = Fernet.generate_key()
cipher_suite = Fernet(encryption_key)
# Encrypt IoT data
encrypted_data = cipher_suite.encrypt(str(iot_data).encode())
# Secure communication with SSL/TLS
context = ssl.create_default_context(ssl.Purpose.related-client)
context.check_hostname = False
context.verify_mode = ssl.CERT_NONE
# Connect to cloud server securely
cloud_server = "cloud server's host"
cloud_port = 443
cloud_socket = context.wrap_socket(socket.socket(socket.AF_INET),
server_hostname=cloud_server)
cloud_socket.connect((cloud_server, cloud_port))
# Send encrypted data to the cloud server
cloud_socket.sendall(encrypted_data)
# Receive response from cloud server
response = cloud_socket.recv(1024)
# Decrypt and validate the response
decrypted_response = cipher_suite.decrypt(response)
if hashlib.md5(response).hexdigest() == hashlib.md5(decrypted_response).hexdigest():
    print("Response integrity verified: ", decrypted_response)
else:
    print("Response tampering detected!")
# Close the connection
cloud_socket.close()
```

The algorithm proved above presented in python source code scenario and it is a simplified example created for illustrative purposes and tries to cover the major aspects or security considerations of a real-world implementation. In this implemented scenario, it needs to be considered additional measures such as proper error handling, authentication mechanisms, secure storage, and compliance with relevant standards and regulations.

The proposed source code algorithm snippet demonstrates the encryption of IoT data using the *cryptography* library and the use of SSL/TLS to establish a secure connection with the cloud server. It also includes a basic integrity check using the *hashlib* library to verify the response received from the server.

6. Application Fields

Public buildings will be the primary target of this implementation system because they are places where a lot of people congregate and have high traffic volumes. Nevertheless, in the early stages of this model, we are not so much interested in data security, as the main purpose is the immediacy and speed in forecasting and informing about possible risk detection.

The detection of deadly viruses will benefit greatly from the usage of our suggested model. The proposed method can be used to detect possible viruses that are in the air or on objects and surfaces in both indoor and outdoor settings. Moreover, the proposed system can be used to check incoming people if they are potentially infected by a virus, warning them appropriately.

As a result, it is true that our suggested model can be used in medical facilities, hospitals, universities, amusement parks, and outdoor venues, offering a practical means of fending off not

only well-known viruses but also novel spreading viruses like the recently discovered deadly Coronavirus, COVID-19.

Evidently, two industries that suffered during a pandemic are airlines and tourism. One of the first actions to minimize the impact of spreading a virus is to stay isolated as much as possible and of course not to travel abroad. So, the totals of airline companies are obligated to cancel the majority of their scheduled itineraries as a precaution against spreading the disease. Consequently, countries that are considered touristic may face a huge financial recession. Thus, the deployment of the proposed system could mitigate the losses of both industries.

7. Conclusion & Future Work

Emerging technologies should be incorporated into healthcare systems' plans since they can be beneficial in a number of ways. While fewer individuals are physically crammed into hospital facilities, patients can nevertheless receive the same level of clinical care. Additionally, the use of various AI-based triage systems could possibly decrease the clinical burden on doctors. An online medical system may instruct individuals on the value of hand cleanliness, assist patients in identifying early symptoms, and refer them for medical care should symptoms escalate. In conclusion, a wide range of technologies are now available that can be utilized to supplement and improve existing public-health methods, even if the COVID-19 pandemic is still being addressed by traditional public-health approaches around the world. The proposed system is a reliable model that, as a result of its cutting-edge and potent identification methods, might result in a restriction of virus dissemination.

To extract instantaneous data at the sensor level, an expansion of this model that adopts a federated learning scenario at the local node of each sensor is envisaged as future development. In order to improve the detecting situation, installing humidity sensors will be a helpful addition to the surveillance infrastructure.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. S. Oniani, G. Marques, S. Barnovi, I. M. Pires, A. K. Bhoi, "Artificial Intelligence for Internet of Things and Enhanced Medical Systems", Springer, Bio-inspired Neurocomputing. Studies in Computational Intelligence, vol. 903 pp 43-59, July 2020. [DOI: 10.1007/978-981-15-5495-7_3]
2. C. L. Stergiou, K. E. Psannis, B. B. Gupta, "InFeMo: Flexible Big Data Management Through a Federated Cloud System", ACM Transactions on Internet Technology, vol. 22, No. 2, Article 46, June 2022. [DOI: 10.1145/3426972]
3. L. Bai. D. Yang, X. Wang, L. Tong, X. Zhu, N. Zhong, C. Bai, C. A. Powell, R. Chen, J. Zhou, Y. Song, X. Zhou, H. Zhu, B. Han, Q. Li, G. Shi, S. Li, C. Wang, …, F. Tan, "Chinese experts' consensus on the Internet of Things-aided diagnosis and treatment of coronavirus disease 2019", Elsevier, Clinical eHealth, vol. 3, pp. 7-15, March 2020. [DOI: 10.1016/j.ceh.2020.03.001]
4. H. S. Maghdid, K. Z. Ghafoor, A. S. Sadiq, K. Curran, D. B. Rawt, K. Rabie, "A Novel AI-enabled Framework to Diagnose Coronavirus COVID 19 using Smartphone Embedded Sensors: Design Study", in Proceedings of 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), vol. 1, pp. 180-187, 11-13 August 2020, Las Vegas, NV, USA. [DOI: 10.1109/IRI49571.2020.00033]
5. S. Muthukumar, W. S. Mary, R. Rajkumar, R. Dhina, J. Gayathri, J., A. Mathivadhani, "Smart Humidity Monitoring System for Infectious Disease Control", In Proceedings of 2019 International Conference on Computer Communication and Informatics (ICCCI), pp. 127-132, 23-25 January 2019, Coimbatore, Tamil Nadu, India. [DOI: 10.1109/ICCCI.2019.8821792]
6. A. P. Plageras, C. Stergiou, K. E. Psannis, Byung-Gyu Kim, Brij Gupta, Y. Ishibashi, "Solutions for Inter-connectivity and Security in a Smart Hospital Building", in Proceedings of 15th IEEE International

Conference on Industrial Informatics (INDIN 2017), 24-26 July 2017, Emden, Germany. [DOI: 10.1109/INDIN.2017.8104766]
7. C. Stergiou, A. P. Plageras, K. E. Psannis, B. B. Gupta, "Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network", Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications, pp. 525-554, January 2020. [DOI: 10.1007/978-3-030-22277-2_21]
8. A. P. Plageras, C. L. Stergiou, K. E. Psannis, "Internet of Things for Healthcare: Challenges & Perspectives", in Proceedings of New Technologies in Health: Medical, Legal & Ethical Issues, 21-22 November 2019, Thessaloniki, Greece.
9. A. P. Plageras, C. Stergiou, K. E. Psannis, G. Kokkonis, Y. Ishibashi, Byung-Gyu Kim, Brij Gupta, "Efficient Large-Scale Medical Data (eHealth Big Data) Analytics in Internet of Things", in Proceedings of 19th IEEE International Conference on Business Informatics (CBI'17), International Workshop on the Internet of Things and Smart Services (ITSS2017), 24-26 July 2017, Thessaloniki, Greece. [DOI: 10.1109/CBI.2017.3]
10. C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018. [DOI:10.1016/j.future.2016.11.031]
11. S. Sahu, Y. Dhote, "A study on big data: Issues, challenges and applications", International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, issue 6, pp. 10611-10616, 2016.
12. A. S. S. Rao, J. A. Vazquez, "Identification of COVID-19 can be Quicker through Artificial Intelligence Framework using a Mobile Phone-Based Survey in the Populations when Cities/Towns are Under Quarantine", Infection Control & Hospital Epidemiology, vol. 1, pp. 1-18, May 2020. [DOI: 10.1017/ice.2020.61]
13. Y. Wang, M. Hu, Q. Li, X. Zhang, G. Zhai, and N. Yao, "Abnormal respiratory patterns classifier may contribute to large-scale screening of people infected with COVID-19 in an accurate and unobtrusive manner," Cornell University, arXivpreprint arXiv:2002.05534, 2020.
14. F. Shi, J. Wang, J. Shi, Z. Wu, Q. Wang, Z. Tang, K. He, Y. Shi, D. Shen, "Review of Artificial Intelligence Techniques in Imaging Data Acquisition, Segmentation and Diagnosis for COVID-19", EEE reviews in biomedical engineering, vol. 14, pp. 4-15, January 2021. [DOI: 10.1109/RBME.2020.2987975]
15. H. Wang, D. Xiong, P. Wang, Y. Liu, "A Lightweight XMPP Publish/Subscribe Scheme for Resource-Constrained IoT Devices", IEEE Access, vol. 5, pp. 16393–16405, August 2017. [DOI: 10.1109/ACCESS.2017.2742020]