AVICENNA
Healthcare development and innovation in the Arabian Gulf

Research article

Personal Healthcare Data Records Analysis and Monitoring using The Internet of Things and Cloud Computing

Atef Zaguia

Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

* Email: Zaguia.atef@tu.edu.sa

ABSTRACT

This paper presents a proposed system for cloud-based and Internet o Things (IoT)-based electronic health records (EHRs) that utilize wearable body biosensors to collect biometric data in real time and analyze it to provide personalized therapy recommendations. The study aims to ensure the confidentiality and integrity of patient data through security authorizations, device authentication, and encrypted communication channels. The research method involves describing the proposed system's communication environment and trust boundary and illustrating the communication mechanisms, including the "starting" and "authentication" procedures. The proposed communication protocols are also explained in detail, and a complete illustration of the symbols and abbreviations used throughout the work is provided. The initialization process involves contacting a body sensor network (BSN) server to register, generating a secret key, and assigning a track sequence number. The proposed systematic verification involves a dependable authentication solution to maintain secure communication between the biosensors, local processing unit (LPU), and BSN server. The verification process involves figuring out the values and generating a random integer, establishing communication with the receiver, and validating the data by searching for a corresponding tuple in the required database. The study emphasizes the importance of a robust IoT communication architecture to ensure secure data transfer between devices, networks, and individuals.

Keywords: *Internet of Things, Body Sensor Networks, Electronic health records, Cloud Computing, Healthcare*

1. INTRODUCTION

The extensive use of intelligent object technologies has hastened the creation of wireless-sensor-based software applications. Because of the widespread availability of these applications, real-time and on-demand services based on the IoT may be incorporated into people's daily lives. Data processing security is one of the most important considerations to make while developing new Internet of Things-based apps. Any devices connected to the internet. Online fraudsters can obtain personal identifying information through IoT devices connected to the internet. Nowadays, we are witnessing the exponential growth of the use of IoT through the internet or communication protocols.

http://doi.org/10.5339/avi.2023.4

Submitted: 04 April 2023
Accepted: 13 April 2023

Cite this article as: Zaguia A. Personal Healthcare Data Records Analysis and Monitoring using The Internet of Things and Cloud Computing. Avicenna 2023(1):4.
http://doi.org/10.5339/avi.2023.4

كيوساينس
QSCIENCE
دار جامعة حمد بن خليفة للنشر
HAMAD BIN KHALIFA UNIVERSITY PRESS

However, more security can be a significant problem slowing down IoT deployments. Two types of security need to be considered in the context of IoT devices: (a) physical protection for the devices themselves and (b) the preservation of data availability, confidentiality, integrity, and privacy during day-to-day operations [1]. IoT technology's increasing complexity and rapid growth has created a pressing need for advanced security solutions to safeguard IoT-based products and their associated applications. These solutions are anticipated to provide robust protection against potential IoT attacks and to protect both the software that interacts with the Internet of Things devices and the devices themselves. Since the development of the Internet of Things devices didn't consider security, there is an obvious need to improve core security measures. Standard security procedures must be modified to tackle the difficulties presented by IoT devices to safeguard IoT-based applications and infrastructure [2] with accessibility, data privacy, and data integrity. Usually, any IoT device receives stores, or processes data, making it vulnerable to attack.

IoT innovative healthcare technology raises several challenges with data security and patient privacy. Man-in-the-middle assaults, jamming, eavesdropping, spoofing, and other tactics comparable to these are included in this category. An effective technique to secure any information should be developed to prevent these exploits from making the system more vulnerable. To protect patients' data, security measures are usually required for the desired system to function correctly. It is highly advantageous to communicate encrypted data and identify devices to protect critical aspects of the MIoT. Many researchers have spent a significant amount of time and effort investigating how to integrate cloud computing that may alleviate concerns about the utility and scalability of the MIoT. The flexibility and scalability of cloud computing are obtained from the virtualized resource management system that serves as its foundation. Contributions to the invention of a Cloud-Based, Internet-of-Things-Based Electronic Healthcare System are:

- The proposed communication settings for IoT and cloud-based healthcare systems provide a secure and efficient way of collecting and analyzing patient biodata, enabling prompt and precise diagnosis and treatment.
- The system's initialization process ensures patient privacy by assigning unique identities that cannot be linked to the actual patient and developing encrypted communication channels to safeguard sensitive information.
- The systematic verification process ensures that only authorized personnel can access the system through reliable IoT authentication solutions, thereby preserving the security of communications between biosensors, the local processing unit (LPU), and the BSN server.
- The integration of cloud computing and electronic health record systems, along with hardware devices and software components, enables rapid and precise data analysis, leading to better patient outcomes.
- The proposed system allows for handling a wide variety of data, including the patient's heart rate, temperature, diagnosis, and outcomes, thereby providing healthcare providers with more comprehensive information about the nature and severity of any prevalent diseases.
- The visual representations and warnings of the patient's health state generated by the processed data provide healthcare providers with a quick and personalized therapy recommendation, further enhancing patient outcomes.
- Overall, the invention of a Cloud-Based, Internet-of-Things-Based Electronic Healthcare System contributes to the advancement of healthcare technology, providing a secure and efficient means of collecting and analyzing biodata from patients, thereby improving the quality of care provided to patients.

Accordingly, this study aims to showcase a secure approach to facilitate communication between IoT devices and cloud-based healthcare networks. However, IoT-cloud-based e-health systems will always rely on various other technologies for data gathering, processing, transmission, actual research, data management, and software activities. Sensors, actuators, and transceivers are all examples of such technology. Therefore, it is critical to develop robust protocols that can operate under the conditions typical of IoT medical devices while still providing the necessary security.

The rest of this paper is organized as follows; related works were reviewed in section 2, while section 3 provided a detailed exploration of cloud computing and Internet of Things-based electronic healthcare systems. Section 4 focused on critical security issues and presented an overview of existing security procedures. The implementation was discussed in Section 5, and the paper is concluded in section 6.

2. BACKGROUND

This section covers the basic security features required for e-health systems.

2.1 The current highest level of performance

EHRs kept in the cloud must be kept private and secure. Privacy standards and different levels of protection have led to the creation of multiple systems that are much better at managing patient data [5]. These systems may be found in hospitals and other medical facilities [6], proving that effectively integrating cloud computing. The authors provided examples to demonstrate their argument and show that successful solutions for integrating cloud computing and the Internet of Things are viable to create and implement. This technique could enhance the diagnostic procedure, therapy duration, therapeutic outcome quality, and cost. “Internet of Things” refers to a hardware, software, and computer system network that may communicate, exchange data, and share information [7]. By facilitating the adoption of appropriate security solutions, the proposed architecture reduces the risk of an attack being initiated. A thorough study of every security-related component must be done to discover any potential risks.

With SHNIE, NDN-medical data may be successfully provided from edge devices to many users. These edge devices are physically closest to the users and contain essential data. All NDN- interactions are safe and private since the verification token is a hashed ciphertext comprising [8, 9] a unique technique to overcome interoperability, heterogeneity, and Internet-aware resistances when developing their solution. The proposed devices would include built-in electronics and a direct Internet connection. As a result, data collection, processing, and analysis may all happen very quickly. The ability of the suggested gadgets to connect to the internet allows their owners to keep an eye on them and even control them from a distance. To maintain track of each patient’s medical records, acquire the necessary data, and transfer it all to a central server, a system was built employing wireless Wi-Fi modules. A thorough evaluation of privacy and security concerns for cloud-based electronic health record systems resulted in the compilation of an exhaustive list [10, 11]. To better man, A more comprehensive security and privacy framework was developed to manage sensitive personal data better to enhance data management and facilitate efficient handling of patients’ electronic health data. The VICINITY security architecture [9] is potentially applicable for geriatric e-health apps that utilize an array of online-connected devices. The concept illustrated how AAL and mHealth (using the VICINITY IoT platform) could collaborate to provide the requisite privacy and safety levels. These electronic health solutions are likely to secure and safe approaches to managing and storing patients’ confidential medical information remotely. The authors suggest that the “Internet of Medical Things” (IoMT) is designed to provide greater levels of access to patient data and additional services such as data processing, therapeutic support, and data storage to both patients and clinicians [12]. They have designed a cryptosystem that allows LPUs, intelligent sensors, and network hubs to authenticate each other and communicate more securely. The system employs a wireless sensor network-based EHRs system with three different levels of access, which are determined by the system’s programming.

2.2. Needed to keep electronic health records safe in the cloud and on the Internet of Things

This section will address the essential security components that are imperative for e-health management frameworks utilizing IoT-cloud technologies. The following security requirements are crucial: Dynamic identity-based authentication techniques have been extensively researched by scientists for more than 20 years, revealing significant benefits such as user-friendliness and efficiency. Additionally, vital session keys must be generated in advance to guarantee secure communication between objects, necessitating anonymous and unpredictable identities for the objects. Furthermore, login and authentication procedures that are session-key-free are highly susceptible to a variety of security concerns. After authentication, adding more security layers, such as SSL and TLS, is possible, but their high computational cost renders them ineffective [14].

2.2.1. Protection from Impersonation or Phishing

BSNs are an offshoot of conventional wireless sensor networks that monitor a person’s health and wellness using a variety of biosensors implanted throughout the body. First and foremost, these personal biosensors pose a security risk due to the sensitive nature of the data they gather. This is due to the critical relevance of taking these needs into account. Here are a few examples: the capacity to confirm a user’s identity, the preservation of data confidentiality and untraced ability, and protection against spoofing attacks at both the device and network levels. These are only a handful of the numerous advantages of utilizing encryption [17, 18]. Coping with these critical safety factors requires various techniques, including anonymous authentication. The ideal functionality of Internet of Things devices is the ability to receive and store accurate data. Under ad hoc network settings, IoT-based systems must be able to keep out intruders while still permitting interoperability amongst linked devices. Furthermore, IoT devices must be built with encryption and decryption functions to protect data security on the device end. This prevents unauthorized parties from accessing the raw data stored on the IoT device. Theft of sensitive information, for instance, might have severe consequences for users and patients. In one scenario, insider/outsider attacks are employed by malicious actors to steal biometric data and patient registration details. The integration of user authentication into cloud computing is discussed in this work as a means of preventing spoofing attacks.

2.2.2. Defense against Attacks Carried Out by a Man in the Middle

Among the most severe security shortcomings that must be addressed is the inability to survive a denial-of-service attack during authentication. To deceive communication equipment into believing they are talking to genuine users, unethical actors may intercept authentication signals. By interacting with the server in this way, the attacker may steal or modify data by pretending to be a trusted user. Spoofing may be used to impersonate legitimate users and cause them problems. For example, the threat actor may pose as a trusted server, initiate communication with the authorized user, and ultimately get the latter's credentials. All device IDs used in contact should be included in the protocol messages for authentication mechanisms. This is an excellent technique to prevent man-in-the-middle attacks. They came up with a registration and verification procedure that uses a fuzzy-verifier approach, and they also devised additional verification carried out inside cloud servers.

2.2.3. The Need for Concurrent Management of a Wide Range of Security and Privacy Attributes

BSNs use insecure wireless connection protocols. Due to this lack of protection, the system is open to potentially catastrophic assaults from the outside world. To begin with, an authentication protocol is used between communication devices to protect the system against spoofing and unauthorized access to data. To prevent the disclosure of biosensor data, sensitive personal information, or patient diagnostic data, the system must first and foremost achieve and preserve anonymity and untraced ability. As a third step, anti-forgery and anti-replay protections must be built into the system. Additionally, a solution for completing the requirements for several healthcare applications was described in research [19], which provided a comprehensive protection foundation for Healthcare 4.0. The proposed framework protects the confidentiality of patients' medical records and makes for more accurate diagnoses.

3. PROPOSED SYSTEM

In this section, the communication environment is described, the trust boundary is defined, and the solutions for cloud-based, Internet of Things-based electronic health records are explained. The precise communication mechanisms involved in the proposed system are then illustrated, including two distinct procedures: "starting" and "authentication." Relevant literature analysis shows that IoT-cloud-based e-health systems could handle a broad range of data, such as patient heart rate, temperature, diagnosis, and outcomes [20-22]. Patient privacy is protected, while the processed data is utilized to create visual representations and warnings of the patient's health state.

3.1. The Circumstances of the Communication

The e-health communication system comprises a BSN server, an LPU, and wearable body biosensors. Edge devices are considered as body biosensors since they are permanently attached to people. They collect biodata from a single patient and transfer it to the LPU and the BSN server for evaluation. This interaction is highly effective, allowing prompt and accurate diagnosis and treatment. Biometric data such as ECG, EEG, EMG, and BP readings can be collected in real-time. BSN servers analyze the collected data to provide patients with quick and personalized therapy recommendations, leading to better patient outcomes.

After the first registration, the stated security authorizations will be sent to the biosensors, the chosen LPU, and the authorized BSN server, where they will be securely maintained. The approved security permissions are also applied to devise authentication and develop encrypted communication channels to safeguard sensitive information. The confidentiality and integrity of the data are guaranteed once this step is completed. The initial step of applying the technology is known as the setup phase, followed by the authentication phase. An authentication procedure will protect all subsequent data and information sent between connected devices.

3.2. System Initialization

The biosensor implanted in a person's body initiates contact with a BSN server for registration. The sensor's unique identification (cloud-based server) must be included to complete this request. As a further step, the server generates a random number (based on its identifier) to derive the secret key. Upon receiving the request, the designated entity begins to assign new identities to the individual that cannot be traced back to the real one. The next stage is to assign a track sequence number, which facilitates quick identification and discourages further attacks. Before every authentication session, it is essential to ensure that both entities are up to date. During the authentication session, the server can verify whether it already has the necessary information about the requesting party in a backend database. These identity checks can be performed during the operation. The system verifies whether the relevant security certificate is stored in the system. The designated entity then performs the calculation using the newly created public key. Once completed, a shared security key is passed around. Finally, creating a database backup containing the security certificate and all related information is essential. Upon verifying the token, the compiler allows sensor access or adds it to an allowlist.

3.3 Systematic Verification

Access to mobile devices is essential for healthcare staff, such as doctors and nurses. The suggested cloud-based electronic healthcare solutions utilize IoT technology. Since the communication network is publicly accessible, it is critical to establish a reliable authentication solution to ensure secure communication between the biosensors, LPU, and BSN servers. A robust IoT communication architecture is necessary to guarantee secure data transfer between devices, networks, and individuals. **Figure 1** presents a comprehensive overview of the channels utilized in the authentication process.

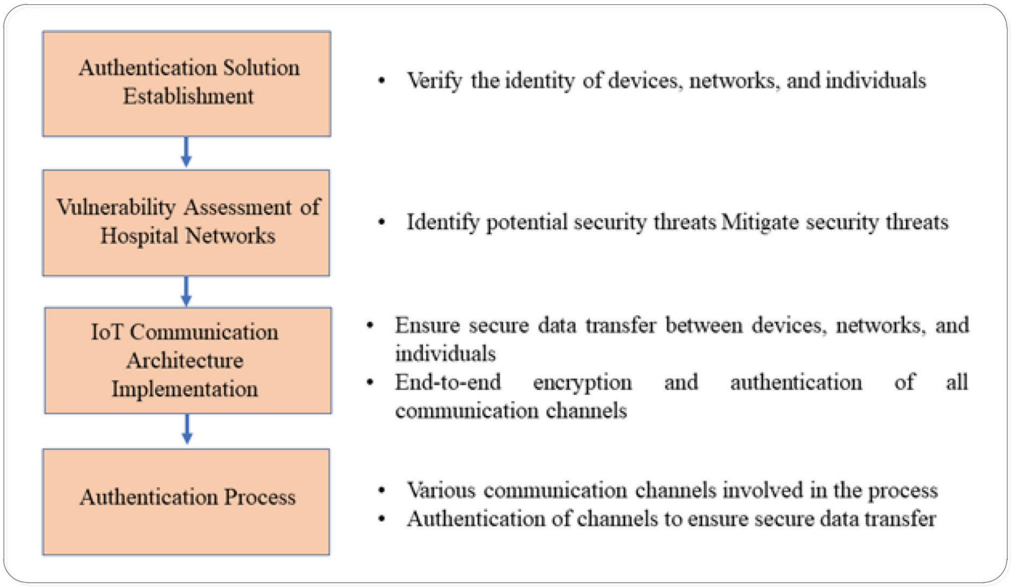
Authentication Solution Establishment
• Verify the identity of devices, networks, and individuals
Vulnerability Assessment of Hospital Networks
• Identify potential security threats Mitigate security threats
IoT Communication Architecture Implementation
• Ensure secure data transfer between devices, networks, and individuals
• End-to-end encryption and authentication of all communication channels
Authentication Process
• Various communication channels involved in the process
• Authentication of channels to ensure secure data transfer

Figure 1. Verification Process Works, (source: author).

The verification process is as follows:

Step 1: Authentication solution establishment

A reliable authentication method must be created so that the biosensors, the LPU, and the BSN servers can safely talk to each other. An authentication system must be able to check the identities of the people, devices, and networks that are part of the communication process.

Step 2: A vulnerability assessment of hospital networks

Because hospital networks are open to the public, these institutions are vulnerable to various security threats. You need to do a vulnerability assessment to determine possible risks and then take the proper steps to reduce them.

Step 3: IoT communication architecture implementation

A robust Internet of Things communication architecture ensures that users, networks, and devices can safely share data. From the beginning to the end, all communication channels used in the healthcare ecosystem must be authenticated and encrypted. This architecture must make that possible.

Step 4: Overview of the authentication process

Figure 1 shows the different ways that people interact with each other during the process, as well as the authentication methods used to ensure the safety of data.

4. SECURITY ANALYSIS

Security evaluation will be provided in this section of the research paper based on the previously discussed system criteria. A logical model is employed to investigate authentication.

4.1. Hypothesis 1: Mutual Authentication Between BSN Communication Entities Allows for Strict Access Control

This section describes some fundamental limitations and assumptions in logic, including the range of principles, claims, and long-term secret keys. Hypothesis 1 asserts that B believes and P perceives, whereas Hypothesis 0 asserts that B believes precisely as stated. Consider the following scenario: suppose someone observes, then observes again. Given that one feels and does the latter, one must also follow. All freshness in a recipe is assumed if even one of its ingredients is fresh. This is because newness is linked to timeliness. If one believes that new beliefs are held, one must conclude that one has new ideas. Before beginning an investigation of the BSN authentication process, the following constraints must be considered: As a primary limitation, I trust that both the client and the server must hold it. The second constraint states that the client and the server must have faith. Lastly, it must be seen as novel to meet the third requirement. As a fourth criterion, you must believe that the food is freshly prepared. It must oversee how one's mind works. Having faith in the safeguards is the seventh rule. Methods and techniques for physically authenticating a BSN are defined below.

4.2. The Second Hypothesis: Complete Privacy and Anonymity

Authentication utilizes random numbers to ensure each message is unique and cannot be reused. Specific numerals, such as the symbol "," have particular meanings in this context. It is important to note that each unique token can only be used once and does not store critical system information in its memory. Additionally, it is refreshed dynamically after every authenticated session. The process involves exchanging information using an anonymous identity, whether a one-time or a disposable identity, and evaluating the outcome. This approach provides only leads for the missing person to identify their whereabouts.

4.3. The Third Hypothesis: Protected Data and Immunity to Spoofing Attacks

Most importantly, security can only be ensured once two session keys have been generated. Both must approve the first session key and nominate the second. Two unique session keys are proposed to be developed within the BSN to safeguard the data transfers between IoT devices.

4.4 Common Electronic Attacks Can Be Protected

IoT in healthcare necessitates fast and accurate identification of fake signals and eliminating or mitigating possible risks. Malicious actors employ many artistic methods to create fake messages, and since IoT devices have diverse network topologies, the origin of these adversarial approaches may lie inside the IoT itself. Thus, a comprehensive inspection system that can detect fraudulent communications and shield users from harmful attacks is crucial. The proposed method uses a unique key only used once throughout the session, making it very difficult to launch assaults based on fake documents. During the authentication process, random numbers are chosen to ensure each message is unique; some of these numerals have specific meanings. Additionally, the proposed method can provide secure communication paths using two easily broken secrets to safeguard any communication that occurs during the authentication process. Every message sent across the protocol suggests unique identifiers for communication objects. The authentication procedures are irreversible, rendering forged or scavenged messages containing unauthorized identities useless. The robust authentication mechanism uses two enormous random numbers with an encoded auxiliary value, so sent messages cannot be modified or reused. The proposed strategy is inherently resistant to attacks that rely on location spoofing.

5. IMPLEMENTATION

This section presents the detailed implementation of the electronic health system. For the communication to be effective, the prototype's software and hardware must actively engage and exchange information in both directions. Following creating an estimate of the cost to maintain the entire system operational, the method proceeds to develop safety measures (Raspberry PI, biosensors). A connection between an intelligent device and a wireless access point or router can be formed using a unique identification (body sensor). After being designed in the Arduino Integrated Development Environment (C and JavaScript), the Raspberry PI's onboard CPU will then apply the needed security procedures. A client app was created that can be installed on any device owned by a user, whether a smartphone, laptop, desktop or any other machine that can connect with cloud APIs. This was the final act, but it was critical. This software client may be used by exploiting cloud application programming interfaces. Data is saved in a MySQL database using this cloud-based API, where authorized users can access it whenever they want. The following step assesses the system's practicality, efficacy, and potential applications. A user cannot interact with IoT devices that are not in their possession. A mechanism that transfers data to the cloud computing system is used by integrating various widely available hardware components. This category contains physical parts such as microcontrollers and networking devices. It has been proven that a cryptosystem based on a programmable microcontroller has a substantially lower computational cost than more traditional approaches. Cryptography is a mathematical approach for masking the content of a message before it is conveyed. The sender and receiver must employ an encrypted communication channel to secure the material while it is being sent. Threat actors will need help listening in on or changing these discussions. The recipient needs the corresponding decryption key to decipher the ciphertext. This essential activity must take place initially. The rest of the arrangement was created using this first set of numbers as a starting point. When some time has passed after initiating a primality-testing unit, the last phases of the encrypting and decrypting operations may begin. They are the "last stages," in a sense. **Figure 2** depicts the communication technique of the proposed electronic healthcare system. For optimal performance, this system will use both IoT and cloud computing.

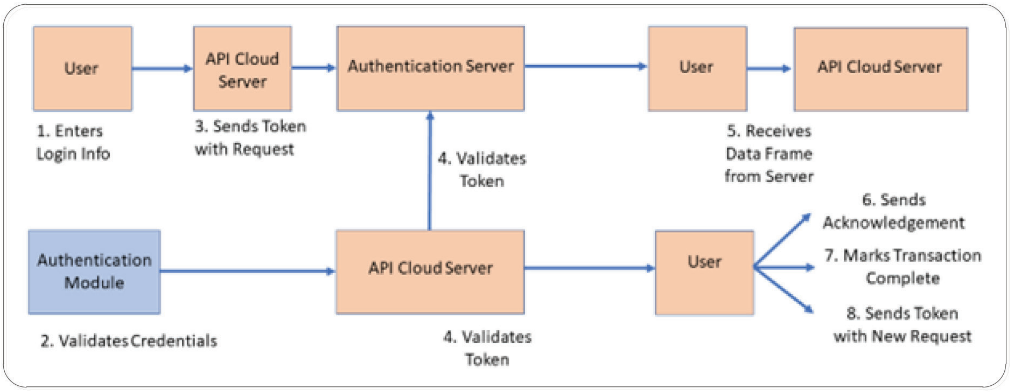

Figure 2. A visual representation of the diverse nature of communication, (source: author).

1. The user initiates a login process by entering their username and password.
2. The authentication module receives the login information and validates it against the user database.
3. If the credentials are valid, the authentication module generates a token and sends it back to the user.
4. The user then sends the token to the API cloud server along with their request for data.
5. The API cloud server receives the request and validates the token by checking it against the authentication server.
6. The API cloud server sends the requested data frames to the user if the token is valid.
7. The user receives the data frames and sends an acknowledgment (ACK) back to the API cloud server.
8. The API cloud server receives the ACK and marks the transaction as complete.
9. If the user wants to perform another action, they must send the token with the following request to ensure authentication.
10. The process continues until the user logs out or the session expires.

The system’s security has not been jeopardized, as shown in **Figure 3**.

Keeping sensitive patient information safe is vital to any company’s information management. This is particularly true in the medical field, where patient data is routinely kept. To prevent unauthorized access, data breaches, and data theft from occurring to the data that has been saved, a variety of steps must be carried out in precise order. The initial stage of the procedure is user profiling. Users who will have access to the stored data are identified and profiled based on the duties and responsibilities they will undertake throughout this stage. After creating the user profiles, the access control policies and regulations that regulate access to the data and who may view, change, or remove it are made. The next stage includes security and privacy safeguards, such as encryption and tokenization, to prevent unauthorized access to data and data breaches. The data is then saved at the application and service layers, where it is managed and where users may access it. In addition, a cloud security layer is put into place to provide customers with an extra line of defense against data breaches and cyberattacks. The information is presented to the end user in a user-friendly way, making it straightforward to obtain and interpret. Since healthcare information is sensitive, there is much focus on keeping patient and doctor information private.

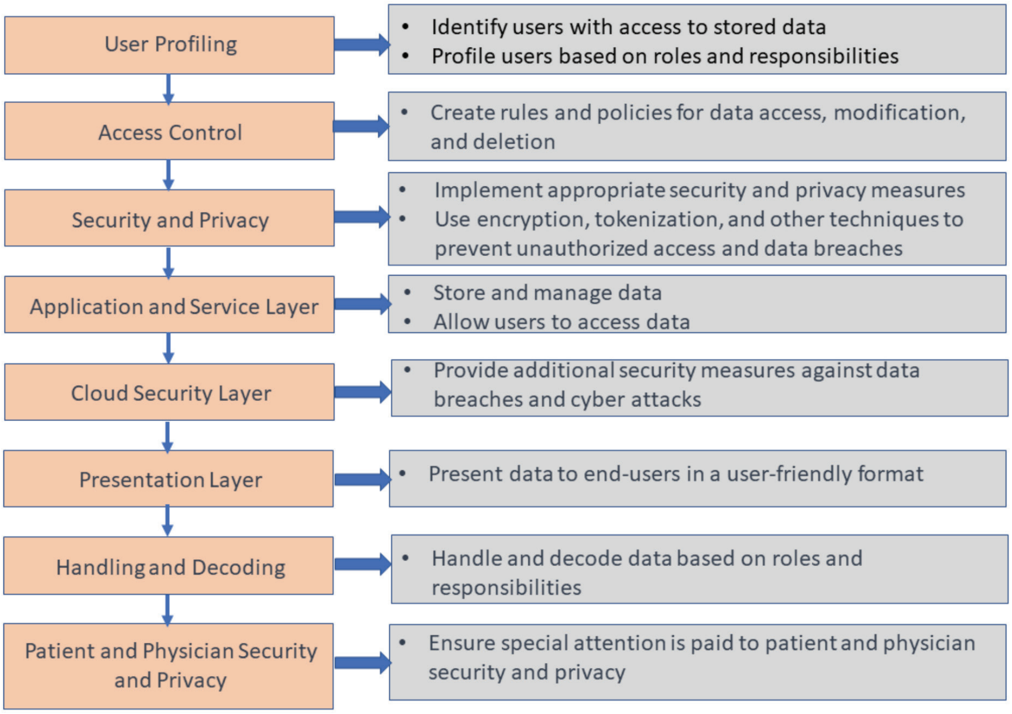
User Profiling
Identify users with access to stored data
Profile users based on roles and responsibilities
Access Control
Create rules and policies for data access, modification, and deletion
Security and Privacy
Implement appropriate security and privacy measures
Use encryption, tokenization, and other techniques to prevent unauthorized access and data breaches
Application and Service Layer
Store and manage data
Allow users to access data
Cloud Security Layer
Provide additional security measures against data breaches and cyber attacks
Presentation Layer
Present data to end-users in a user-friendly format
Handling and Decoding
Handle and decode data based on roles and responsibilities
Patient and Physician Security and Privacy
Ensure special attention is paid to patient and physician security and privacy

Figure 3. The primary forms of storage utilized by IoT devices, (source: author).

Data and information modifications performed during a user session are coordinated with the remote servers after the connection ends. E-Health systems may use the UIs to gather information about their users’ health and provide them with feedback based on that information. The interface is linked to cloud servers via middleware, allowing for global reach connections to both the database and the interface. The cloud database allows for this interconnection to take place. **Figure 4** displays the utilization of the Internet of Things and cloud-based electronic health systems in identifying and monitoring COVID-19. Middleware uses web services developed on top of cloud software programming interfaces to securely transmit confidential data between remote servers and websites.

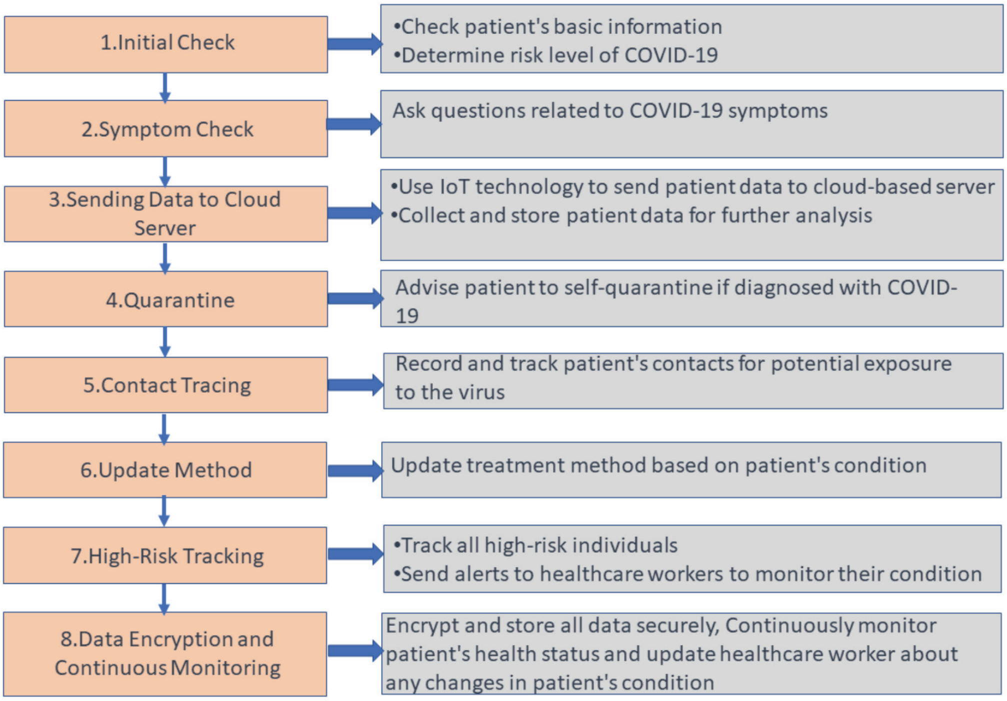
1.Initial Check
•Check patient's basic information
•Determine risk level of COVID-19
2.Symptom Check
Ask questions related to COVID-19 symptoms
3.Sending Data to Cloud Server
•Use IoT technology to send patient data to cloud-based server
•Collect and store patient data for further analysis
4.Quarantine
Advise patient to self-quarantine if diagnosed with COVID-19
5.Contact Tracing
Record and track patient's contacts for potential exposure to the virus
6.Update Method
Update treatment method based on patient's condition
7.High-Risk Tracking
•Track all high-risk individuals
•Send alerts to healthcare workers to monitor their condition
8.Data Encryption and Continuous Monitoring
Encrypt and store all data securely, Continuously monitor patient's health status and update healthcare worker about any changes in patient's condition

Figure 4. IoT and cloud-based systems now facilitate COVID-19 identification and monitoring, (source: author).

The use of the Internet of Things (IoT) and cloud-based electronic health systems for COVID-19 identification and monitoring is depicted in **Figure 4**. The middleware employs web services built on top of the cloud software programming interface to transfer private information between websites and remote servers securely. This enables medical professionals to monitor and care for patients more efficiently and accurately. Physicians and nurses can collect and analyze real-time data using mobile gateways, leading to faster and better treatment for patients. The system's modifications have improved data collection, storage, and analysis convenience while providing reliable assurance depth at a reasonable computational cost. The designated physician receives daily emails with a new app or website alerts, including each patient's most current health information. The accessibility of health records through the app benefits users and doctors. Security and privacy measures, such as user and service authentication protocols, message encryption, accountability monitoring, and data anonymization, have been implemented to safeguard the system further. A cloud- and Internet-of-Things-based electronic health system is now being used to find and track COVID-19.

A new proposed system that utilizes the Internet of Things (IoT) and cloud-based electronic health systems for identifying and monitoring COVID-19 may have significant implications. It may facilitate quicker and more accurate patient monitoring and care for medical professionals, enable real-time data gathering and analysis, and provide patients with better treatment. Additionally, it may improve the accessibility and convenience of health records for both users and doctors. On the other hand, the implementation of such a system may also raise concerns regarding data privacy and security, which would need to be addressed appropriately.

6. CONCLUSION

The development and expansion of IoT systems have been rapid, and various commercial fields have benefitted from this innovation. Additionally, there has been a global trend towards new administration and operating models across diverse medical organizations. Through the integration of smart IoT devices, a pervasive IoT-based network architecture can be established, but it may also reveal undiscovered security vulnerabilities. A dependable e-health management system was developed, utilizing IoT-based BSN topologies and operating in the cloud. An alternative authentication method was implemented to meet even the strictest security requirements. A comprehensive formal analysis was performed to confirm the system's robustness, efficiency, security, and privacy. The positive results validate the feasibility of the blockchain-based e-health management solution. However, there is potential for future enhancements through more efficient algorithms, codes, and structures. The method could be updated to enable encryption and decryption with a larger bit size, and design sets could be utilized to test a range of public and asymmetric key encryption algorithms beyond DES and AES.

The limitations of this research or system can take various forms. Firstly, the scope of the research or system may be limited, and it may only be able to address some aspects or factors that contribute to the problem. Secondly, limited data can impact the accuracy and effectiveness of the research or system, particularly when the available data is insufficient or biased. Technical constraints such as computational power, memory, or processing speed can also limit the research or system's functionality. Moreover, human factors such as human error, biases, or the lack of expertise or knowledge in the field can also limit the system's effectiveness. Finally, time constraints can limit the thoroughness and completeness of the work, particularly if the research or system must be developed within a tight timeframe.

Table of abbreviations

EHRs	electronic health records
BSN	body sensor network
LPU	local processing unit
TLS	Transport Layer Security
SSL	Secure Sockets Layer
DES	data encryption standard
AES	advanced encryption system

REFERENCES

1 Kooli, C., and Al Muftah, H.: 'Artificial intelligence in healthcare: a comprehensive review of its ethical concerns', Technological Sustainability, 2022

2 Yousefnezhad, N., Malhi, A., and Främling, K.: 'Security in product lifecycle of IoT devices: A survey', Journal of Network and Computer Applications, 2020, 171, pp. 102779

3 Vehko, T., Hyppönen, H., Puttonen, S., Kujala, S., Ketola, E., Tuukkanen, J., Aalto, A.-M., and Heponiemi, T.: 'Experienced time pressure and stress: electronic health records usability and information technology competence play a role', BMC medical informatics and decision making, 2019, 19, pp. 1-9

4 Wang, X., and Cai, S.: 'Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud', Future Generation Computer Systems, 2020, 112, pp. 320-329

5 Kooli, C.: 'Chatbots in Education and Research: A Critical Examination of Ethical Implications and Solutions', Sustainability, 2023, 15, (7), pp. 5614

6 Xu, R., and Ren, Q.: 'Cryptoanalysis on a Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System', IEEE Access, 2022, 10, pp. 23618-23624

7 Thilakarathne, N.N., Kagita, M.K., and Gadekallu, T.R.: 'The role of the internet of things in health care: a systematic and comprehensive study', Available at SSRN 3690815, 2020

8 Chenthara, S., Ahmed, K., Wang, H., and Whittaker, F.: 'Security and privacy-preserving challenges of e-health solutions in cloud computing', IEEE access, 2019, 7, pp. 74361-74382

9 Koutli, M., Theologou, N., Tryferidis, A., Tzovaras, D., Kagkini, A., Zandes, D., Karkaletsis, K., Kaggelides, K., Miralles, J.A., and Oravec, V.: 'Secure IoT e-Health applications using VICINITY framework and GDPR guidelines', in Editor (Ed.)^(Eds.): 'Book Secure IoT e-Health applications using VICINITY framework and GDPR guidelines' (IEEE, 2019, ed.), pp. 263-270

10 Parashar, V., Kashyap, R., Rizwan, A., Karras, D.A., Altamirano, G.C., Dixit, E., and Ahmadi, F.: 'Aggregation-based dynamic channel bonding to maximise the performance of wireless local area networks (WLAN)', Wireless Communications and Mobile Computing, 2022, 2022

11 Chattopadhyay, A.K., Nag, A., Ghosh, D., and Chanda, K.: 'A secure framework for IoT-based healthcare system', in Editor (Ed.)^(Eds.): 'Book A secure framework for IoT-based healthcare system' (Springer, 2019, ed.), pp. 383-393

12 Quy, V.K., Hau, N.V., Anh, D.V., and Ngoc, L.A.: 'Smart healthcare IoT applications based on fog

computing: architecture, applications and challenges', Complex & Intelligent Systems, 2022, 8, (5), pp. 3805-3815

13 Hameed, S.S., Selamat, A., Abdul Latiff, L., Razak, S.A., Krejcar, O., Fujita, H., Ahmad Sharif, M.N., and Omatu, S.: 'A hybrid lightweight system for early attack detection in the IoMT fog', Sensors, 2021, 21, (24), pp. 8289

14 Yeh, K.-H.: 'A secure IoT-based healthcare system with body sensor networks, IEEE Access, 2016, 4, pp. 10288-10299

15 Kashyap, R.: 'Security, reliability, and performance assessment for healthcare biometrics': 'Design and Implementation of Healthcare Biometric Systems' (IGI Global, 2019), pp. 29-54

16 Ding, L., Wang, Z., Wang, X., and Wu, D.: 'Security information transmission algorithms for IoT based on cloud computing, Computer Communications, 2020, 155, pp. 32-39

17 Al-Haija, Q.A., Al Tarayrah, M., Al-Qadeeb, H., and Al-Lwaimi, A.: 'A tiny RSA cryptosystem based on Arduino microcontroller useful for small scale networks', Procedia Computer Science, 2014, 34, pp. 639-646

18 Stepień, K., Poniszewska-Marańda, A., and Marańda, W.: 'Securing connection and data transfer between devices and IoT cloud service', Integrating Research and Practice in Software Engineering, 2020, pp. 83-96

19 Yu, Y., Hu, L., and Chu, J.: 'A secure authentication and key agreement scheme for IoT-based cloud computing environment', Symmetry, 2020, 12, (1), pp. 150

20 Kashyap, R.: 'Machine learning, data mining for IoT-based systems': 'Research Anthology on Machine Learning Techniques, Methods, and Applications' (IGI Global, 2022), pp. 447-471

21 Kashyap, R.: 'Machine learning for internet of things': 'Research Anthology on Artificial Intelligence Applications in Security' (IGI Global, 2021), pp. 976-1002

22 Nair, R., Alhudhaif, A., Koundal, D., Doewes, R.I., and Sharma, P.: 'Deep learning-based COVID-19 detection system using pulmonary CT scans', Turkish Journal of Electrical Engineering and Computer Sciences, 2021, 29, (8), pp. 2716-2727

23 Nair, R., Singh, D.K., Yadav, S., and Bakshi, S.: 'Hand Gesture Recognition system for physically challenged people using IoT', in Editor (Ed.)^(Eds.): 'Book Hand Gesture Recognition system for physically challenged people using IoT' (IEEE, 2020, edn.), pp. 671-675