Framework for Health Data Security within Smart Healthcare

Rida Tahir (ridatahir712@gmail.com)

Short Report

Keywords:

Posted Date: February 1st, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2524909/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Abstract

E-health solutions can be used to monitor patients at any time and from any location. Patient's health and recovery status are constantly monitored using mobile communication. In these kinds of systems, the privacy, authenticity, and validity of patients' health records must be protected. To protect e-health systems in a digital network context, effective access control and transmission are necessary. Because of the resource-constrained design of the digital network environments, traditional access control techniques are unable to safely route e-health services. This work proposes an innovative and upgraded authentication scheme that attempts to address the obstacles associated with the confidentiality and protection of patients’ sensitive data through robust encryption management. A well-organized and lightweight access control mechanism is also a goal of the suggested model.

1. Introduction

In today's environment, e-health is thought to be the most potential technology. E-health systems enable huge groups of patients to be monitored for a range of diseases anywhere at time and from any location. The continuing load on caregivers to keep track of their patients' health is also taken into account. E-health systems transform the way patients' health is monitored by lowering the associated costs [1, 2]. Medical devices (sensors, for example) are placed throughout the body and collect data from the patient before transmitting it to medical centers. E-health systems cannot be developed in the healthcare sector without adequate security. It is critical to ensure that only approved users can access, read, and change data in e-health systems. The information in such kinds of systems is sensitive, and any unauthorized change or update of sensitive information can result in negative consequences. By implementing access control procedures, e-health systems can be made safer [3, 4]. We aim to develop a digital healthcare safety model based on the Internet of Things. A model for addressing protection aspects of IoT services is presented, and it is tested on smart devices to answer the safety needs for IoT environments.

2. Literature Review

In order to improve human living standards, technological advancements have enabled the adoption of innovative solutions. Data on health-related issues has been gathered and analyzed from a variety of sources by experts investigating the advancement of technologies [5]. Consequently, the advancement of unified medical technologies can potentially increase patient satisfaction and efficiency at every level of the health sector. Introducing innovative solutions to electronic-health (eHealth) systems and applications can overcome specific issues that exist in conventional healthcare systems [6, 7] by ensuring robust patient safety practices, universal access to data, remote outpatient monitoring, instant clinical treatments, and distributed digital records. The use of these systems can improve quality of life for patients and promote collaboration, as well as increase patient experience, lower costs, and boost the effectiveness of e-healthcare. In addition, defined e-Health as a high-tech sector that uses the Internet, networking, and health to provide assistance to stakeholders and users. By integrating and advancing new technologies, e-health addresses long-standing issues, reduces costs, and improves quality by
integrating health technology and global health. Meanwhile, the Internet of Things (IoT) is making it possible for users to access shared resources such as computers, devices connected to the internet, applications, and infrastructure. Thus, IoT-connected models, equipment, and systems are becoming more prevalent. In addition, IoT’s widespread implementation parallels the evolution of interconnected telecommunications, including computational intelligence in health, business, manufacturing, and operational processes. To make the adoption of healthcare data technology, solutions, and overall e-Health systems effective and secure, security mechanisms must be highly efficient and robust. The widespread usage of IoT systems has supported investigation and innovation in IoT technology, which now includes a variety of architectures to be used in healthcare systems. With the Internet of Things, e-Health systems have the ability to communicate data related to health via networks, devices, apps, and services [12, 13].

When connected as adaptable, flexible, and effective patient health systems, IoT developing innovative technologies reinforce one another’s abilities. Integration offers advantages over traditional systems, including ease of adoption, increased data security, easy access to records, and energy savings over traditional technologies. The Internet of Things can be used to enhance health services as well as encourage scientific research. Connecting people, applications, databases, and storing health data are the main functions of IoT-based e-Health systems [14].

New innovations in computing continue to move beyond the existing system, introducing multiple security vulnerabilities to transmitted or saved data. IoT-based digital healthcare systems applied as e-Health systems were designed with interoperability, multiple technical specifications, networking protocols, and technical specifications in mind. In appropriate protocols and standards, web technologies, networking protocols, and hardware design are all incorporated. A reliability test demonstrated that interoperability between diverse IoT devices, standards, and protocols could be established in an e-Health system and used continuously on the Web, proving the architecture’s reliability. Build a smart e-Health platform based on a dispersed intermediate layer of intellectual ability between sensor nodes and the Web [15]. In order to address mobility, energy consumption, adaptability, and reliability concerns, people took advantage of the increased availability of current healthcare technologies. This reduced the load on sensors, networking, and distant health centers. In order to successfully implement their e-Health system, the UT-Gate gateway provided superior functionalities, including an IoT-based Early Warning System and health monitoring system with improved overall structure, intellectual capacity, effectiveness, efficiency, interconnection, safety, and consistency. Integrating smart IoT devices with a web platform provides access to patient data. It is easier for doctors to address patients’ health concerns on time by collecting the data required to assess their health on time. Developed a four-step architecture for e-Health systems, including devices, data aggregation, data management, and data processing. They described the applications for which the system would be useful, as well as the technology required to make it operational, and the advantages and constraints associated with it [16].

With body sensor network technology, data is transmitted and received through cloud computing via lightweight wireless sensor nodes that have the Internet of Things built in. Confidentiality and safety
protocols are evaluated to ensure the safety of the health system and the confidential information of patients. Cloud computing and IoT devices are increasingly used in e-health systems, presenting challenges, possibilities, and constraints. According to them, authentication is crucial to ensure the safety of IoT and e-Health systems, and they presented a method for protecting these systems that is more efficient and intuitive. IoT-cloud-based apps enhance flexibility, extensibility, and cost reduction for startups through pay-as-you-go cloud hosting services [17].

Several studies of IoT-enabled e-Health systems have developed effective security procedures with crucial software components to enable precise and reliable data transmission among sensors. Aside from safety and confidentiality, IoT-based e-Health platforms should be developed with high accuracy and efficiency, so that any quantity of data can be analyzed and transferred as quickly as possible. Among the most significant safety and security features of IoT-enabled Health technologies are information security, data integrity, availability of services, traceability, identification, security systems, and non-repudiation. It is clear that more attention needs to be paid to the safety and privacy issues of IoT-cloud-based e-Health systems, even though several studies have examined these issues with different combinations of solutions. When attackers or man-in-the-middle attacks (MITM) get access to complete patient data through insecure procedures for e-Health infrastructure, their security is compromised. Patients, doctors, and other participants can be protected by developing a safe method for IoT-based e-Health platforms [18].

Digital e-Health Concept:

As novel technologies and standards which were not viable a decade ago are being developed, advanced e-Health systems are transforming healthcare through empowering individuals. It's challenging to specify digital e-Health systems even though new ideas are continuously being developed, and all these concepts will ultimately become new core elements of advanced health care systems, as shown in [19], which analyses and compared studies of digital healthcare IoT systems through examining the safety precautions integrated within healthcare IoT network.

By studying various frameworks and discussing the potentially IoT systems to improve healthcare, the analysis comes to the findings that safety is guaranteed for healthcare systems. Researchers have found that embracing digital healthcare can lead to improved diagnoses in numerous applications. Data-driven treatment services will be significantly enhanced thanks to IoT-enabled sensors that provide doctors with the data they need. E-Health systems, information retrieval, characteristics, and individual health monitoring will all benefit from big data [20].

They discussed the genuine potential of Smart e-Health technologies and the health domain, as well as the benefits and drawbacks of privacy and safety solutions within the perspective of big data in health. In addition, there was a paper discussing IoT's utility in the context of digital health and how security ideas can be incorporated into IoT digital healthcare. The researchers proposed an IoT-based solution that could help with healthcare. Gave a comprehensive assessment and analysis of the literature regarding safety and confidentiality challenges within Healthcare.
Healthcare safety and confidentiality challenges. Researchers then presented the benefits of the safety and confidentiality strategies, tools, and frameworks employed in Healthcare. It also discussed Industry and showed how it relates to healthcare. They discussed healthcare application contexts and how to use Industry techniques to healthcare. To deliver the most important advantages, services, and advancements throughout the field of health [21].

A collection of basic concepts in modern e-Health system is as follows:

2.1.1. Ambient Assisted Living (AAL): is the use of smart things in an aided living atmosphere for caring and helping elders in becoming more self-sufficient. Distant monitors can use AAL software to gather, manage, and evaluate patient activities, allowing them to respond swiftly to crises and effectively examine issues of mistreatment.

2.1.2. Wearable Gadgets: are devices with incorporated devices and embedded devices, including smart wristbands, smartwatches, necklaces, and glasses. The IEEE 802.11 standard bandwidth is used by the majority of such gadgets. Peer-to-peer networking is a method of storing information about activities across many devices. With its decentralized structure, healthcare may enhance visibility among patients and doctors, provide productive communication across health resources using intelligent rules, and prevent breakdown and data loss.

Issues with EHR:

The medical sector has evolved dramatically in the last decade as a result of technological transformation. The days of keeping, storing, and retrieving patient data in big file folders inside a healthcare setting are long gone. The overall transition of a data storage system to an electronic health record (EHR) is one of the most remarkable advancements in the health industry. The most prevalent challenges with Electronic Health Records (EHR) which caregivers experience, as well as their resolutions, are discussed in this article [22].

- Electronic health records are extremely important:

EHR stands for electronic health records, and it is used to keep track of a patient's information. All patient-centered records can be accessed by approved individuals at any time, trying to make the medical process simpler. The healthcare professional has direct accessibility to the patient's entire health record, including diagnosis, treatment choices, follow-ups, medication issues, laboratory test data, and many others. Because of the many advantages it offers, including hospital billing operations and doctor credential activities, EHR has become a crucial resource for hospitals and independent health professionals all over the globe. Patients and physicians benefit from it by improving their health conditions while reducing healthcare costs. Healthcare errors are reduced, diagnoses are more accurate, and care is of higher quality. As a result, patients have more contact with their doctors, and the quality of care is higher [23].
• **Data Security:**

Another significant issue with EHR implementation is security and data protection issues. Among users, data vulnerability as a result of a natural crisis or cyberattack is a common concern. To ensure the safety of health data, a comprehensive strategy has been developed under the legal requirement. When a safety violation occurs, the corporation may face legal actions and be required to pay huge amounts of money to rectify the situation. As a consequence, the company's major responsibility is to ensure the EHR's data protection.

Electronic health records are intended to make the process more efficient. The interface, on the other hand, may be challenging to manage when the EHR is designed by developers with insufficient consideration of how it would be used in real-world scenarios. It means that person may take much longer than necessary to enter basic data or find the appropriate records [24, 25].

### 3. The Health Data Security Framework's Fundamental Architecture

Traditional medical care faces risks towards the security, administration, and exchange of health and individual data because of the proliferation of healthcare activities and data. The conceptual model is partitioned into two parts: an intelligent medical data administrator as well as a smart health monitoring accredited supervisor. The conceptual model inhibits and assures individual healthcare data cryptography, safety authorization control, and the secrecy of health data generated by each center point. The suggested health data security model is depicted in Fig. 2.

The health data security model is made up of 3 parts:

- A localized health services provider who changes the patient's health records and sends them to the intelligent health certifying supervisor by a health entity.
- A intelligent medical care certified supervisor is a verification entity that produces, distributes, and manages keys and also acts as access control and data mediator.
- A intelligent medical data supervisor is an identity verification entity that encrypts, saves, and disperses private and health-related data.

Through dividing operations into the intelligent medical data manager, which gives details cryptography, and certified manager, which is willing to take responsibility for medical data access control, this framework seeks to autonomously conduct the authentication and encryption of health data provided to local hospitals. The following is a description of each layer's role within the suggested safety structure.

### A layer of Safety for Healthcare Devices:

The health devices security layer assures that the activities done by digital health gadgets are available, secure, and private. The physical safety of a device safeguards it from tampering and theft by deploying intrusion detection and anti-theft devices.
The layer of Security for Healthcare Communications:

Data is exchanged among devices using the networking functionality of IoT systems. Elements of IoT networks can be incorporated using the communication functionality that provides compatibility across various devices. The degree of safety needed for IoT applications’ communication functions should be developed in light of vulnerabilities to these data transmissions.

A layer of Information Safety:

The vulnerability assessment layer gathers and processes the system’s entire system information from devices and network activity to identify and react to any safety breaches or system risks. Its goal is to discover system processes in real-time, identify probable known attacks, and develop safeguards in the case of an intrusion.

• Threat Measuring: Receives and manages data on the safety state of the treatment of diseases based on intrusion behavioral patterns and access control policies.

• Threat Assess: This method looks for activities or trends that could lead to safety flaws or risks in a given system. This step involves the analysis of malevolent behavior and rule-based analysis. By monitoring use trends in the system, the malevolent behavior analysis finds irregular activity after understanding behavior patterns. The rule-based analysis identifies particular occurrences which do not happen in regular systems and assesses safety risks depending on the rules established.

4. Conclusion

E-health systems transform the way patients’ health is monitored by lowering the associated costs. Medical devices (sensors, for example) are placed throughout the body and collect data from the patient before transmitting it to medical centers. E-health systems cannot be developed in the healthcare sector without adequate security. It is critical to ensure that only approved users can access, read, and change data in e-health systems. The information in such kinds of systems is sensitive, and any unauthorized change or update of sensitive information can result in negative consequences. A digital healthcare safety model based on IoT is the goal of this research. In this paper, we outline the safety requirements for IoT environments and present and test a model for building protection aspects for IoT services.

References


7. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: A systematic review. SN Appl. Sci. 2020, 2, 139. [CrossRef].


20. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. J. Ind. Inf. Integr. 2020, 18, 100–129. [CrossRef]


Figures
Figure 1

Architecture of smart health.
Figure 2

Conceptual EHR data safety framework.