PLOS ONE

RESEARCH ARTICLE

A lightweight and robust authentication scheme for the healthcare system using public cloud server

Irshad Ahmed Abbasi[1,2☯*], **Saeed Ullah Jan**[3☯], **Abdulrahman Saad Alqahtani**[4☯], **Adnan Shahid Khan**[2☯], **Fahad Algarni**[4☯]

1 Department of Computer Science, College of Science and Arts Belqarn, University of Bisha, Sabtul-Alaya, Saudi Arabia, **2** Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan, Malaysia, **3** Higher Education Department of Khyber Pakhtunkhwa at Govt. College Wari Dir Upper, Wari, Khyber Pakhtunkhwa, Pakistan, **4** Department of Computer Science, College of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia

☯ These authors contributed equally to this work.
* aabasy@ub.edu.sa

Citation: Abbasi IA, Jan SU, Alqahtani AS, Khan AS, Algarni F (2024) A lightweight and robust authentication scheme for the healthcare system using public cloud server. PLoS ONE 19(1): e0294429. https://doi.org/10.1371/journal.pone.0294429

Editor: Vincent Omollo Nyangaresi, Jaramogi Oginga Odinga University of Science and Technology, KENYA

Received: September 19, 2023

Accepted: November 1, 2023

Published: January 30, 2024

Peer Review History: PLOS recognizes the benefits of transparency in the peer review process; therefore, we enable the publication of all of the content of peer review and author responses alongside final, published articles. The editorial history of this article is available here: https://doi.org/10.1371/journal.pone.0294429

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Abstract

Cloud computing is vital in various applications, such as healthcare, transportation, governance, and mobile computing. When using a public cloud server, it is mandatory to be secured from all known threats because a minor attacker's disturbance severely threatens the whole system. A public cloud server is posed with numerous threats; an adversary can easily enter the server to access sensitive information, especially for the healthcare industry, which offers services to patients, researchers, labs, and hospitals in a flexible way with minimal operational costs. It is challenging to make it a reliable system and ensure the privacy and security of a cloud-enabled healthcare system. In this regard, numerous security mechanisms have been proposed in past decades. These protocols either suffer from replay attacks, are completed in three to four round trips or have maximum computation, which means the security doesn't balance with performance. Thus, this work uses a fuzzy extractor method to propose a robust security method for a cloud-enabled healthcare system based on Elliptic Curve Cryptography (ECC). The proposed scheme's security analysis has been examined formally with BAN logic, ROM and ProVerif and informally using pragmatic illustration and different attacks' discussions. The proposed security mechanism is analyzed in terms of communication and computation costs. Upon comparing the proposed protocol with prior work, it has been demonstrated that our scheme is 33.91% better in communication costs and 35.39% superior to its competitors in computation costs.

1. Introduction

The effective handling of stored information gathered from different patients has widely been implemented for research, investigation, and treatment in the healthcare system. This sensitive data is collected with the help of wearable devices embedded inside the human body. The network-enabled devices are connected to the public network over several methods like IEEE

Funding: The authors are thankful to the Deanship of Scientific Research, University of Bisha (SA) for supporting this work through grant number UB-GRP-65-1444.

Competing interests: The authors have declared that no competing interests exist.

802.15.4 port, IEEE 802.16, WiFi, or WiMAX [1]. The sensor has limited low-power battery storage capacity while performing high computation by generating tremendous output, which requires substantial computing power, massive storage capacity, and real-time processing [2]. For this purpose, a public cloud server offers affordable, flexible, high-performance computing, virtualized storage, and software applications for the healthcare system or patient at home [3]. It is cost-effective, scalable, and available for data-driven pervasive healthcare systems; other service providers can also take benefit by demanding the same high-speed online services from it so that to provide high-quality treatment, effective communication of healthcare personnel with patients, doctors, nurses, pharmacists, and other staff members [4].

A medical information system stored in public cloud services can support the healthcare system for numerous delivery services. This facility is made possible by physiological monitoring devices for patients at home directly or with the doctors at a clinic or in the e-healthcare industry [5]. The public cloud server is mature for the interaction and enhanced sharing of valuable information between various medical institutions, hospital systems, and respective care providers. Such a healthcare system is preferred to reduce costs and make efficient processes, preserving the medical record's privacy and patient's identity [6]. Patients' concerns about losing their privacy are a significant hurdle to adopting cloud-based healthcare systems since they may feel uneasy and lack confidence in the service providers to keep their identities a secret. The transmission of patient information through an insecure internet needs to be secure, and patient privacy is preserved [7]. Thus, a public cloud server's stored medical information system needs a strong authentication technique to protect accessibility, confidence, and authenticity [8].

Similarly, cloud computing must be implemented to meet the tremendous output generated by numerous IoT in the healthcare system, which requires constant availability and storage [9]. Cloud computing is a potential paradigm in computing that transfers the hardware and software platform to outside service providers (e-healthcare systems) who provide the healthcare facilities to its users (patients) at a significantly lower cost. Cloud computing has much potential for improving the e-healthcare system to ease end-users lives—the cloud transfers patient-sensitive data to healthcare enterprises for management by physicians, labs, research and associated tasks. In general, an e-health cloud is a platform that manages and stores vast amounts of health data from various healthcare providers [10].

Furthermore, attention is required owing to the ubiquitous output of thousands of wearable devices in the healthcare system and the production dispatch for storing it in the public cloud server. As thousands of Internet-of-Medical-Things (IoMT)/sensors generate the result, transmitted to the server for storage requires proper authentication; otherwise, no one builds trust in it due to a lack of privacy, security, and continuous changes in patient conditions which may cause massive mobility issues [11]. All these issues and challenges are due to the need for an appropriate authentication scheme. Therefore, a reliable authentication protocol for such a sensitive environment is much needed to support the accurate authentication of each device, exact data stored in the server, low end-to-end delay, integrity, confidentiality, and low energy consumption. So that, to ensure the privacy of patient security of stored information and deny control of the resources by any fraudulent user. The main contributions of this research work for such a system are as follows:

- An ECC-based lightweight authentication protocol has been proposed to securely provide services to the end-user in the cloud-enabled healthcare system.
- A fuzzy extractor method is used to design the proposed protocol to make the authentication process more secure, and the system shows uniqueness while performing any task. An adversary cannot forge, extract, or collide the hash image generated from user biometrics in combination with a random key extracted before authentication.