HCIS Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) Open Access

Human-centric Computing and Information Sciences (2026) 16:39
DOI: https://doi.org/10.22967/HCIS.2026.16.039
Received: April 22, 2025; Accepted: July 25, 2025; Published: July 15, 2026

Blockchain-Based Lightweight Anonymous Authentication Scheme for Security Enhancement in Internet of Medical Things Environment

Zaid Ameen Abduljabbar[1,2,3,*], Vincent Omollo Nyangaresi[4,5], Mohammed Abdulridha Hussain[1], Junchao Ma[2,6,*], Mustafa A. Al Sibahee[7], Zaid Alaa Hussien[8], Abdulla J.Y. Aldarwish[1], Ali Hasan Ali[9,10,11], Ahmed Ali Ahmed[7], and Husam A. Neamah[12]

Abstract

The Internet of Medical Things (IoMT) has continued to revolutionize the healthcare sector, resulting in reduced costs and improved quality of treatment. To facilitate real-time remote patient monitoring, biosensors frequently interact with medical systems over the public Internet. This connectivity, however, exposes the IoMT environment to a myriad of privacy and security threats. Although past research has proposed numerous security techniques to address these challenges, most of these solutions fail to provide an adequate balance between security and performance. In this paper, we propose a robust IoMT security scheme that leverages elliptic curve cryptography and one-way hashing operations to achieve low communication, energy, and computation overhead. Formal security analysis using a random oracle model demonstrates the robustness of the negotiated session keys. In addition, semantic security analysis confirms that our scheme mitigates various typical IoMT cyber threats, such as desynchronization, forgery, impersonation, and ephemeral secret leakage attacks. A comparative performance evaluation verifies that the proposed protocol incurs the lowest execution, energy, and communication costs. Specifically, it reduces computation and energy costs by 19.04%, increases supported functionalities by 69.23%, and lowers communication overheads by 8.7%. These efficiencies make our scheme ideal for deployment in IoMT devices with limited energy, processing and communication capabilities.

Keywords

IoMT, Security, Authentication, ECC, Privacy, Biosensor

***Corresponding Author:** Zaid Ameen Abduljabbar (zaid.ameen@uobasrah.edu.iq), Junchao Ma (majunchao@sztu.edu.cn)
[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[2]Guangdong Laboratory of Artificial Intelligence and Digital Economy (SZ), Shenzhen, China
[3]Department of Business Management, Al-Imam University College, Balad, Iraq
[4]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya
[5]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tami lnadu, India
[6]School of Artificial Intelligence, Shenzhen Technology University, Shenzhen, China.
[7]Department of Management and Marketing, College of Industrial Management for Oil and Gas, Basrah University for Oil and Gas, Basrah, Iraq
[8]Information Technology Department, Management Technical College, Southern Technical University, Basrah, Iraq
[9]Department of Mathematics, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[10]Technical Engineering College, Al-Ayen University, Thi-Qar, Iraq
[11]Institute of Mathematics, University of Debrecen, Debrecen, Hungary
[12]Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Debrecen, Hungary