Peer-to-Peer Networking and Applications (2025) 18:130
https://doi.org/10.1007/s12083-024-01868-8

Integrating ABHA for authentication and key exchange: A hybrid security framework for smart healthcare in India

Riaz A. Khan[1] · Saba Mushtaq[2] · Sajaad A. Lone[1] · Rajesh Gupta[3] · Ayaz Hassan Moon[1]

Received: 13 September 2024 / Accepted: 21 November 2024

Abstract

Digital technologies enable huge potential for cultivating healthcare access and quality globally, including in India. The Internet of Things (IoT) allows connection between devices and healthcare specialists, thus enhancing healthcare delivery with reduced overheads such as manual intervention, time consumption and administrative cost. However, the incorporation of IoT technology in the healthcare sector has experienced obstacles due to security issues. These concerns involve unauthorized access arising from vulnerabilities in open wireless channels and the limitations of device abilities, which may hamper the performance of complex security algorithms. Existing solutions often rely on conventional security algorithms that incur high computational overhead. Moreover, the inclusion of non-unique identifiers as authenticating parameters, makes them vulnerable to security attacks including replay attack, identity collisions etc. Furthermore, the current solutions fail to balance adequately between security and efficiency, thus leading to increased energy consumption. Therefore, to address these challenges, we propose a minimally intrusive authentication scheme that integrates the Ayushman Bharat Health Account (ABHA) number – a unique identifier, with Physical Unclonable Function (PUF), and Zero-Knowledge Proof (ZKP) as the authenticating parameters. The scheme prevents from several security attacks including *replay attack, man-in-the-middle attack, impersonation and insider attack, eavesdropping and message modification attack, password guessing attack, DoS attack* alongside it provides *session key security* as well. Further it undergoes a wide range of evaluation and validation using the "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool, providing convincing evidence of its resilience against security threats. Since the scheme exploits lightweight techniques such as PUF, message digest, and ZKP, thus it yields lower cost overhead compared to traditional methods. Upon comparison, the scheme presents an average of 99.14 ms for computation cost and 1248 bits of communication cost which is far lesser than most of the existing schemes. Therefore, the proposed scheme outperforms many of the existing protocols in terms of complexity, communication and computation cost and presents a comprehensive solution for e-healthcare security.

Keywords IoT · Smart healthcare · Healthcare security · Authentication · Key establishment · Cryptography · ABHA number · PUF · ZKP

1 Introduction

The advent of technologies has offered a multitude of prospects to boost healthcare in India, a country grappling with challenges regarding accessibility, affordability, and quality. Amongst these technologies, the Internet of Things (IoT) stands out as a potential game-changer in transforming healthcare within India. Through the interconnectedness it nurtures among healthcare professionals, medical equipment, and IoT sensors, thus holding the capacity of providing high-quality healthcare facilities even in remote areas. Notably, the recent COVID-19 pandemic has acted as a catalyst for the swift expansion of IoT's role in healthcare [1].

This article is part of the Topical Collection: *2 - Track on Security and Privacy*

Guest Editors: Rongxing Lu

✉ Riaz A. Khan
riaz.khan@islamicuniversity.edu.in

[1] Islamic University of Science and Technology, Kashmir, India

[2] University of Kashmir, Kashmir, India

[3] Nirma University, Ahmedabad Gujrat, India

Published online: 26 March 2025