Notification No.: 558/2024

Date of Award:10/5/24

Name of Scholar: Manoj Kumar

Name of Supervisor: Prof. Syed Zeeshan Hussain

Name of Department/Centre: Computer Science

Topic of Research: A secured wireless body area Network based on IoT

Findings

The culmination of my Ph.D research, spanning seven chapters. The research summary is as follows-

Chapter 1 highlights the critical role of Wireless Body Area Networks (WBANs) in healthcare, enabling continuous monitoring and real-time data collection through wearable devices. However, WBAN technology faces numerous challenges, primarily concerning network design, data security, and privacy. Robust security measures are essential to address these challenges and overcome trust deficits, ensuring safe and effective implementation of WBANs in healthcare settings.

Chapter 2 reviews various key agreement schemes used in WBANs, analyzing their effectiveness against different types of attacks and performance parameters. Key agreement schemes are categorized into four classes and assessed based on parameters like data confidentiality and node authentication. The review reveals that many schemes neglect critical performance aspects, such as resource efficiency, DoS attack prevention, forward/backward secrecy, scalability, data integrity, unlinkability, and unforgeability, posing significant risks to WBAN security and functionality. The chapter identifies research gaps and emphasizes the need for optimized security measures tailored to the resource constraints of WBANs.

Chapter 3 addresses the limitations of existing cryptographic techniques in resource-constrained WBAN environments. This chapter proposes a lightweight mutual authentication-based key agreement scheme. Utilizing XOR operations and cryptographic hash functions, the protocol is designed to balance security and performance for WBANs. The proposed protocol aims to maintain continual parameter refreshment and session key generation, ensuring robust security without compromising the efficiency of body sensor nodes.

Chapter 4 details the verification framework and performance analysis of the proposed authentication protocol. Initial informal analysis identifies potential vulnerabilities, which are further scrutinized using formal methods like BAN logic and automated tools such as Scyther. The emphasis on balancing security with performance, addressing 15 key security parameters, ensures the protocol's robustness in communication and storage efficiency.

Chapter 5 explores the implementation of WBAN simulation scenario using Castalia 3.2 with OMNET++ framework. The simulator's enhancements, including a wireless channel model and a dedicated Healthcare Application Layer, facilitate the evaluation of WBANs. Simulation scenarios with five sensor nodes and a coordinator node are discussed, testing various protocols like one-hop star topology and MAC protocols. Castalia's modules offer a testbed for distributed algorithms in dynamic wireless channels, aiding in the assessment of WBAN performance metrics.

Chapter 6 discusses the integration of Edge Computing (EC) with IoHT, highlighting the benefits and security challenges. WBANs, despite their potential in healthcare, face limitations due to sensor capacity, necessitating cloud computing support. EC addresses latency and bandwidth issues, enhancing data translation, scalability, and storage. The chapter underscores the importance of robust security measures for IoHT's successful adoption, emphasizing ethical approaches to data security and privacy preservation.

Chapter 7 focuses on remote patient monitoring. This chapter reviews WBAN architecture, security challenges, and key agreement schemes. A proposed lightweight mutual authentication protocol is evaluated for its security and efficiency using BAN logic and Scyther tools. The chapter also explores the utility of the Castalia framework for WBAN simulation and discusses the integration of EC in healthcare to address sensor limitations and cloud support challenges. Emphasizing security and privacy, the chapter outlines strategies for achieving a secure and adaptable WBAN architecture.

The thesis highlights the transformative potential of IoT in healthcare, particularly through the use of WBANs. It addresses the critical challenge of securing sensitive medical data in resource-constrained environments. By proposing a lightweight mutual authentication protocol and advocating for efficient edge-cloud integration, the research provides solutions to enhance WBAN functionality and security. These advancements are crucial for the reliable and efficient operation of WBANs, ultimately contributing to improved healthcare delivery and patient outcomes.