Chapter 5
Federated Learning for Privacy-Preserving Healthcare Wearable Security

Grace Shalini T.
http://orcid.org/0000-0002-0016-3702
SRM Institute of Science and Technology, India

Pratham Shrivastav
http://orcid.org/0009-0008-5840-2084
SRM Institute of Science and Technology, India

Parthiv Gopa
http://orcid.org/0009-0009-5556-7841
SRM Institute of Science and Technology, India

ABSTRACT

The work demonstrates and performs a privacy-preserving multi-institutional multi-party end-to-end federated learning (FL) framework to detect security anomalies in multi-party data streams of healthcare wearables. The natural pipeline uses distributed non-identically-distributed (non-IID) telemetry to jointly train anomaly detectors on hospitals and device vendors across a secure environment without having to centralize raw patient data. The method includes time-varying deep neural network and client level differential privacy (DP-SGD), secure aggregation with efficient communication compressing update transmission. This work provides assumed yet reasonable multi-site outcomes to concretize feasibility, simulating what a production deployment would provide: on six institutions and 21,804 users

DOI: 10.4018/979-8-3373-7426-0.ch005

Copyright © 2027, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

generating 1.2 billion records, the DP-FL model achieves an AUROC of 0.943 ± 0.008 and an F1-score of 0.887 ± 0.011 when identifying the security -important anomalies such as spoofed sensors, tampered firmware, abnormal pairing, and suspicious connection events.

1. INTRODUCTION

The mobile biometrics of wearable devices have turned out to be the biggest biomedical distributed network of sensors of all time. These signals are being used to support clinical decision-making, triage, and many research applications in hospitals, insurers and device vendors, but are also exposing attack surfaces (Rani et al., 2023; Aminifar et al., 2024). The threat actors may spoof photoplethysmography (PPG) traces, disable or enable debug builds, make use of rogue pairing, or pivot off mobile apps into hospital networks. Classical security analytics require data to be aggregated at a central location, which is not acceptable in the healthcare industry because of the privacy rules and organizational risk conditions (Shirvani et al., 2024; Pati et al., 2024). Federated learning (FL) then presents an interesting alternative where instead of moving data out, it exchanges privacy-hardened model updates instead (Teo et al., 2024; Abbas et al., 2024).

There are, however, unique challenges in the integration of FL into wearable security. First, telemetry is non-IID: the cohorts are not age matched, nor comorbidity, brand of device or usage patterns. Second, with updates, information leaks unless defended through differential privacy and secure aggregation. Third, SOCs must have low-latency inference and actionable alerts that can be combined with the currently existing playbooks (Zhang et al., 2024; Grataloup & Kurpicz-Briki, 2024). This work prescribes an entire pipeline, threat model to SOC integration, which can meet these needs, and provide competitive detection performance and auditable privacy in it.

1.1 Contributions and Organization

The main contributions of this work are:

A comprehensive federated learning framework that addresses healthcare wearable security challenges including non-IID data distributions, intermittent connectivity, and strict privacy requirements. The Integration of differential privacy (DP-SGD) and secure aggregation and personalization layers to provide strong privacy guarantees ($\varepsilon \approx 3.5$) while still maintaining detection performance within 0.9 points from centralized training. The practical engaging of deployment considerations including (i) a SOC integration, (ii) mapping regulatory compliance (HIPAA, GDPR, DPDP

34 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/federated-learning-for-privacy-preserving-healthcare-wearable-security/413685

Related Content

Data Hiding Method Based on Inter-Block Difference in Eight Queens Solutions and LSB Substitution

Vinay Kumar, Abhishek Bansaland Sunil Kumar Muttoo (2014). *International Journal of Information Security and Privacy (pp. 55-68).*

www.irma-international.org/article/data-hiding-method-based-on-inter-block-difference-in-eight-queens-solutions-and-lsb-substitution/130655

FUR-HABE: A Hierarchical CP-ABE Scheme With Traceable Fine-Grained User Revocation for Cloud Storage

Xiaohui Yangand Ya'nan Tao (2025). *International Journal of Information Security and Privacy (pp. 1-25).*

www.irma-international.org/article/fur-habe/365602

Secure Agent Roaming under M-Commerce

Sheng-Uei Guan (2007). *Encyclopedia of Information Ethics and Security (pp. 571-578).*

www.irma-international.org/chapter/secure-agent-roaming-under-commerce/13527

Towards Autonomous User Privacy Control

Amr Ali Eldinand Rene Wagenaar (2007). *International Journal of Information Security and Privacy (pp. 24-46).*

www.irma-international.org/article/towards-autonomous-user-privacy-control/2469

Disassociations in Security Policy Lifecycles

Michael Lapkeand Gurpreet Dhillon (2015). *International Journal of Information Security and Privacy (pp. 62-77).*

www.irma-international.org/article/disassociations-in-security-policy-lifecycles/145410