Scopus

Documents

Ahmed, K.I.[a] , Tahir, M.[b c] , Lau, S.L.[a] , Habaebi, M.H.[d] , Ahad, A.[e f] , Mughees, A.[a]

Trust-Aware Authentication and Authorization for IoT: A Federated Machine Learning Approach
(2024) *IEEE Internet of Things Journal*, .

DOI: 10.1109/JIOT.2024.3512657

[a] Sunway University, Department of Computing and Information Systems, Selangor, Petaling Jaya, 47500, Malaysia
[b] Turun Yliopisto, Department of Computing, University of TurkuFI-20014, Finland
[c] Chitkara University Institute of Engineering and Technology, Punjab, Rajpura, 140401, India
[d] International Islamic University Malaysia, IoT and Wireless Communication Protocols Lab, Department of Electrical and Computer Engineering, Selangor, Gombak, 53100, Malaysia
[e] Northwestern Polytechnical University, School of Software, Shaanxi, Xian, 710072, China
[f] Istanbul Technical University (ITU), Adjunct Scientific Research the Department of Electronics and Communication Engineering, Istanbul, 34467, Turkey

Abstract
The need for strong authentication and authorization (AA) security measures is growing with the proliferation of the Internet of Things (IoT). This paper presents an advanced trust-aware authentication and authorization system for IoT environments. Using real-world data collected from Zigbee Zolertia Z1 devices, a Federated Machine Learning model was developed that utilizes Physical Layer properties such as Received Signal Strength Indicator (RSSI), Link Quality Indicator (LQI), device Internal Temperature, device Battery Level, and device MAC address. The proposed solution for AA IoT utilizes a trust calculation algorithm based on Federated Learning (FL), which is suitable for IoT environments and enables data privacy and scalability. Incorporating device-specific information, such as internal temperature and battery level, helps a more nuanced evaluation of the device's status, improving the precision of trust calculations. The proposed architecture performs particularly well for unauthorized intrusion attempts modelled using spoofing, replay and Sybil attacks. Specifically, the proposed methodology can detect malicious AA activities classified as Writing + Reading attempts with 100% accuracy, demonstrating its effectiveness in protecting IoT devices from attacks. Furthermore, the model achieves 99.18% accuracy in reading access permissions and 99.99% accuracy in identifying Write + Read + Execute permissions, highlighting its reliability in implementing access control restrictions for improving security in IoT environments. This research helps improve IoT security by addressing crucial challenges in the ever-expanding world of networked devices. © 2014 IEEE.

Author Keywords
Access control; Artificial Neural Networks (ANN); Authentication; Authorization; Federated Learning (FL); Internet of Things (IoT); Machine learning (ML); Networking; Security; Trust; Trust Management

Correspondence Address
Tahir M.; Turun Yliopisto, Finland

Publisher: Institute of Electrical and Electronics Engineers Inc.

ISSN: 23274662
Language of Original Document: English
Abbreviated Source Title: IEEE Internet Things J.
2-s2.0-85212000514
Document Type: Article
Publication Stage: Article in Press
Source: Scopus