Brought to you by INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Scopus

Back

Optimizing Internet of Things security: Artificial neural networks algorithms performance in authentication and authorization via physical layer features

Engineering Applications of Artificial Intelligence • Article • 2026 •
DOI: 10.1016/j.engappai.2026.115408

Istiaque Ahmed, Kazi [a] ; Tahir, Mohammad [b, c] ; Jiangbin, Zheng [a] ; Lau, Sian Lun [d] ; Habaebi, Mohamed Hadi [e] ; +1 author

[a] School of Software, Northwestern Polytechnical University, Shaanxi, 710129, China

Show all information

0
Citations

Full text Export Save to list

Document Impact Cited by (0) References (57) Similar documents

Abstract

The increasing dependence on the Internet of Things (IoT) across various sectors necessitates enhanced security mechanisms, particularly for authentication and authorization (AA) processes. Owing to their dynamic nature and resource constraints, IoT networks are vulnerable to various security breaches, underscoring the need for robust cybersecurity solutions. This study aims to optimize IoT security by evaluating the performance of Artificial Neural Network (ANN) algorithms in this era of Artificial Intelligence (AI) for AA, utilizing physical layer (PHY-layer) attributes, such as device temperature, antenna orientation, Received Signal Strength Indicator (RSSI), and Link Quality Indicator (LQI). Ten different ANN algorithms in Machine Learning (ML), including both classical and recent optimization techniques, were evaluated for their ability to improve convergence rates

and minimize errors. These methods were assessed using performance metrics such as convergence epochs, Mean Squared Error (MSE), and correlation coefficients (R-values). The results indicate that the Bayesian Regularization (BR) and Levenberg–Marquardt (LM) algorithms outperformed the others, with the lowest MSE and highest R-values, demonstrating superior performance in IoT AA tasks. This study offers significant insights into the selection of ANN algorithms for robust IoT security and contributes to the development of more reliable and adaptive security solutions for IoT networks. Future work will focus on integrating these optimized algorithms into federated learning systems to enhance the scalability and adaptability of IoT network security mechanisms in evolving network environments. © 2026 Elsevier Ltd.

Author keywords

Artificial intelligence; Artificial neural networks; Authentication; Authorization; Cybersecurity; Internet of Things; Machine learning; Network security

Indexed keywords

Engineering controlled terms

Antennas; Cybersecurity; Federated learning; Internet of things; Learning algorithms; Learning systems; Machine learning; Mean square error; Network layers; Network security; Neural networks; Optimization; Physical layer; Secure communication

Engineering uncontrolled terms

Artificial neural network algorithm; Authentication and authorization; Cyber security; Machine-learning; Mean squared error; Networks security; Neural-networks; Performance; Physical layers; Security mechanism

Engineering main heading

Authentication

Corresponding authors

Corresponding author: K. Istiaque Ahmed

Affiliation: School of Software, Northwestern Polytechnical University, Shaanxi, 710129, China