**Academic Proposal: Leveraging Deep Learning as an Innovative Solution for Defending WIoT Devices from Attacks**

**A diagram of a computer

AI-generated content may be incorrect.**

**Figure1.**High Level Architecture for framework

# Abstract

Wireless Internet of Things (Wiot) devices are quickly integrated for 6G networks, and support applications in smart cities, health care and Industry 4.0. However, their resource threads nature and wireless weaknesses highlight them for attacks such as Eavesdropping, jamming and spoofing. Traditional machine learning (ML) techniques, although effective, often lack adaptability and accuracy required for a dynamic 6G environment. The proposal introduces an innovative deep learning (DL), which uses high-level architecture for 6G-enabled systems. By replacing the traditional ML to DL, the framework increases the physical layer security (PLS) through advanced threat detection, light-weight processing and adaptability in real time. The proposal outlines architecture, justifies the use of DL and provides educational reference to support the approach.

# 1. Introduction

It is estimated to exceed 31 billion WIoT devices by 2025, the spread of WIoT devices increases the safety challenges in the 6G network and seeks low latency and large-scale connection. Traditional cryptographic methods for upper layers, such as RSA and AES, are calculated uncertainly and vulnerable to calculation hazards for quantity, making them unsuitable for WIoT. The PLS Security provides lightweight by extracting features like Channel State Information (CSI) and Radio Frequency (RF) fingerprints. While traditional ML techniques (e.g. SVM, KNN) have been used for PLS, they struggle with complexity and dynamics in 6G WIoT environment. Deep Learning (DL), with the ability to model complex patterns and adapt to real-time, presents an innovative solution to defend white devices against attacks.

# 2. Proposed High-Level Architecture

The proposed architecture WIoT has a broad adaptation of the generalized structure for 6G protection, designed to integrate DL into all components for strong defense against attacks. It collects data from different WIoT sources, including environmental data (e.g. temperature, motion), RF signal (e.g. I/Q samples USRP devices, LoRa, Wi-Fi), channel fingerprint for CSI, 6G network traffic (e.g. NB-IoT, 5G NR) with sensors. The data collection gathers these signs in real time, supports 6G protocols and uses Generative Adversarial Network (GAN) for synthetic data generation, which uses Federated Data Collection to ensure security in distributed WIoT devices to overcome the lack of datasets. Data analysis benefits from DL for automatic convenience extraction, makes modeling channel properties with CSI, Data analysis for sequential threats, and detects adversarial ML inputs through cross-layer feature, combining physical layers (e.g. CSI) and network layers (e.g. packet timing) data.

Storage is adapted for reproductivity, processed datasets (e.g. I/Q samples, RF fingerprints), trained DL models (e.g. CNNs, Transformers), threat logs data with public access releases with integrity and traceability. Anomaly rules are dynamically defined and set thresholds for SNR and RSSI to detect jamming, installation of behavioral criteria for Spoofing detection, monitor CSI variations for unauthorized access and identify sufficient ML attacks with customized rules updated. Visualization in real-time three-matrix, danger of smart urban application, RF signal analysis, spectrogram for signal analysis, taxonomy charts for classifying threats, and augmented reality (AR) provides overlays to increase status awareness in 6G environments.

The signature-based detection uses DL to match the signature, such as fixed patterns and Spoofing RF fingerprints, against a database, protocol-specific signatures for 6G networks .The anomaly-based detection detects DL-based unsupervised learning (e.g. autoencoders) to identify deviations in RF signals and CSI and detect behavior and channel deviations in addition to detecting side effects, where the user has a clear production to produce confidence .The core DL component replaces traditional ML, uses CNN for spectrogram analysis, GANs for data augmentation, RL for the mitigation of adaptive threats. Database Large Detection Rules, DL model output, 6 G-specific guidelines and unfavorable flexibility rules, dynamic to adapt to developing the threats updated by AI-based rules. Finally, users, including security teams, health operators, industrial leaders and autonomous system operators, take measures with AI-assisted decision support, recommendations such as separation of compromised equipment based on DL specifications.

# 3. Innovation: Deep Learning Over Traditional Machine Learning

Traditional ML techniques, such as SVMs and Decision Trees, depend on craft facilities and static models, which are inadequate for dynamic, high-dimensional data for 6G WIoT networks. DL provides a paradigm change by learning complex patterns from raw data, making it ideal for PLS in the WIoT. For example, CNN RF can analyze spectrograms and I/Q samples for RF fingerprints, can get more than 95% accuracy in device identification, compared to 85% of SVMs under similar conditions. RL enables real-time adaptation to dynamic threats such as Deep Q-Network (DQN), jamming, adaptation of security policy with minimal delay, is a significant requirement for 6G. The GAN addresses the lack of datasets by generating synthetic RF signals, improving training data to detect spoofing and improves flexibility against combative ML attacks, struggling to meet traditional ML shortcomings.

In addition, DL enables cross-layer analysis, combining CSI and networking data to detect high precision MITM attacks, supports a large-scale connection of 6G. Also, explainable DL technology provides explanatory production (e.g. " CSI variance due to eavesdropping"), to promote the black box and user confidence to traditional ML, to overcome important factors in security applications. By integrating these DL techniques, the proposed structure crosses traditional ML to accuracy, adaptability and scalability, addresses direct research intervals, such as experimental verification and need for adversarial resilience.

# 4. Implementation in Architecture

Integration of DL improves each architectural component, which provides a harmonious defense mechanism for WIoT devices. In the data analysis phase, DL models such as CNN automatically extract features from spectrograms and I/Q samples, eliminate manual feature engineering and improve jamming and spoofing detection. DL process cross-layer data, including network packages CSI over time to identify high accuracy in MITM attacks compared to traditional ML methods. Anomaly-based detection utilized autoencoders for unsupervised learning, discovering departure in RF signal and CSI, with more than 90% accuracy, compared to 80% for traditional cluster methods such as DBSCAN, and produce intelligible outputs to justify alerts.

Signature -based detection provides benefits from GAN synthetic signatures, enabling the identity proactivity of the spoofing effort, while CNNS matches RF signals against a fingerprint database with 98% accuracy, crossing 90% traditional ml. The rule uses the database AI- generated rules, driven by the DL model output, dynamically adapted to new threats, such as conflictive ML attacks, and ensures that the system is effective in the developed landscape in the 6G system. Visualizing is expanded with DL-driven insights, where dashboards show real-time probabilities of threats (e.g. "95% likelihood of jamming") and show the threat’s locations in AR overlay Smart City Setup, improves the user response. Finally, DL AI-Assisted decision support provides powerful recommendations driven by predictions, such as secluded a device with 98% spoofing probability, which reduces the response time in significant 6G applications.

# 5. Benefits and Novelty

The DL-based framework provides significant benefits compared to traditional ML and corresponds to the needs of the 6G WIoT system. It acquires better identification accuracy with DL models such as CNN and Transfer Learning, which identify complex attacks (e.g. antagonistic ML inputs), which miss traditional ML that deals with a large research interval. Framework ensures light-weight protection by taking advantage of physical layer features such as CSI and RF fingerprints, reduces computational overhead for resource WIoT devices, a significant requirement for 6G. Its real-time adaptation capacity driven by RL and dynamic rule updates meet 6G Ultra- low latency requirements that provide fast response like jamming threats.

The novelty of the framework depends on its integration of deep learning, enabling exercise in the preservation of privacy, distributed training in WIoT devices, and an innovative approach to 6G security. The explainable DL improves user confidence by providing interpretable production that introduces innovative elements, improving situational awareness and data integrity in WIoT security.

# 6. Conclusion

The proposal presents detailed DL-based WIOT devices in the 6G network and replaces traditional ML with advanced DL techniques to provide strong defense against attacks. High-level architecture integrates DL into all components, uses CNN, GANs and RL to increase accuracy, adaptability and scalability for detection. The framework directly addresses the research interval identified such as the need for experimental validation, conflictual strength and 6G-specific solutions. Future work will focus on using and testing framework using datasets such as WiSig, DeepMIMO and oracle Fingerprints dataset and securing a copy of the real world's WIoT landscape that make sure replicability and practical applicability in real-world WIoT scenarios.