Archives available at journals.mriindia.com

International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347-2820

Volume 14 Issue 02, 2025

Deep Learning and Optimization Approaches in Secure AI for 6G Mobile Devices: Deep Kronecker Neural Network Optimized with Hybrid Cat Hunting Optimization to Combat Side-Channel Attacks: A Review

Khaldun Mulyadi
Associate Professor, Department of Electrical and Computer Engineering, Vindhya College of Engineering Systems, India
Email: khaldun.mulyadi@vces-in.org

Peer Review Information

Submission: 20 July 2025

Revision: 10 Aug 2025

Acceptance: 26 Aug 2025

Keywords

6G Mobile Networks, Side-Channel Attacks, Deep Kronecker Neural Networks, Hybrid Cat Hunting Optimization, Secure AI, Deep Learning Security

Abstract

The advancement of sixth-generation (6G) communication networks is expected to enable intelligent, ultra-low latency, and high-speed mobile systems powered by Artificial Intelligence (AI). However, the integration of AI into resource-constrained mobile devices introduces critical security challenges, particularly vulnerability to side-channel attacks (SCAs), which exploit physical leakages such as power consumption and electromagnetic emissions to extract sensitive information. Traditional cryptographic defenses are insufficient to mitigate these threats, necessitating advanced AI-driven security mechanisms.

This paper presents a comprehensive review of deep learning and optimization approaches for secure AI in 6G mobile devices, focusing on Deep Kronecker Neural Networks (DKNN) optimized using Hybrid Cat Hunting Optimization (HCHO). DKNN architectures leverage Kronecker product representations to reduce model complexity while maintaining high-dimensional learning capability. The integration of HCHO enhances parameter optimization, improving detection accuracy and convergence speed.

The study reviews recent developments from 2020–2023, highlighting the effectiveness of hybrid deep learning and metaheuristic optimization in combating SCAs. Results indicate that DKNN-HCHO models outperform conventional approaches in terms of accuracy, computational efficiency, and robustness. Future directions include lightweight model design, federated learning integration, and explainable AI for secure and scalable 6G systems.

Introduction

The emergence of 6G communication networks represents a transformative milestone in wireless communication, promising unprecedented capabilities such as terabit-per-second data rates, ultra-low latency, and seamless integration of artificial intelligence (AI) into network operations. These advancements are driven by the increasing demand for intelligent applications, including autonomous systems, smart healthcare, industrial automation, and immersive extended reality (XR) environments.

A key feature of 6G networks is the integration of AI at the edge, enabling real-time decision-making and intelligent service delivery. Mobile devices in 6G environments are no longer passive endpoints but active participants in data processing and network management. This shift toward AI-driven edge computing introduces

new security challenges, particularly in protecting sensitive data processed on resource-constrained devices.

One of the most critical security threats in this context is side-channel attacks (SCAs). Unlike traditional cyberattacks, SCAs exploit physical characteristics of devices, such as power consumption, electromagnetic radiation, and timing information, to infer sensitive information such as cryptographic keys. These attacks are particularly dangerous in 6G environments due to the widespread deployment of IoT devices and edge nodes, which often lack robust security mechanisms.

Traditional security solutions, including encryption and authentication protocols, are insufficient to defend against SCAs because they do not address physical leakage. Therefore, there is a growing need for AI-driven security mechanisms capable of detecting and mitigating such attacks in real time.

Deep learning has emerged as a powerful tool for enhancing security in wireless networks. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Deep Neural Networks (DNNs) have been widely used for intrusion detection, anomaly detection, and malware classification. However, these models often require large amounts of data and computational resources, making them less suitable for resource-constrained mobile devices.

To address these challenges, researchers have proposed Deep Kronecker Neural Networks (DKNN), which leverage Kronecker product-based architectures to reduce model complexity while maintaining high accuracy. DKNN models are particularly effective in handling high-dimensional data, making them suitable for analyzing side-channel signals.

In addition to model design, optimization plays a crucial role in enhancing the performance of deep learning models. Metaheuristic algorithms, such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Ant Colony Optimization (ACO), have been widely used to optimize model parameters. Among these, Hybrid Cat Hunting Optimization (HCHO) has gained attention due to its ability to balance exploration and exploitation, leading to faster convergence and improved performance.

The integration of DKNN with HCHO provides a robust framework for detecting and mitigating side-channel attacks in 6G mobile devices. This hybrid approach combines the efficiency of Kronecker-based neural networks with the optimization capabilities of metaheuristic algorithms, resulting in improved accuracy, reduced computational cost, and enhanced energy efficiency.

This paper aims to provide a comprehensive review of deep learning and optimization approaches for secure AI in 6G mobile devices, with a focus on DKNN-HCHO models. The main contributions of this paper include:

- A detailed analysis of side-channel attacks in 6G environments
- A review of deep learning-based security mechanisms
- An overview of optimization techniques for model enhancement
- A comparative analysis of existing approaches
- Identification of research gaps and future directions

Literature Review

The rapid integration of Artificial Intelligence (AI) into 6G mobile networks has introduced new security challenges, particularly in protecting edge devices from side-channel attacks (SCAs). Between 2020 and 2023, significant research efforts have been directed toward developing deep learning-based and optimization-driven solutions to detect and mitigate such threats. This section provides a comprehensive and chronological review of these advancements.

Literature Review – Year 2020: Foundations of Deep Learning-Based SCA Detection

The year 2020 marked a foundational phase in applying deep learning techniques to side-channel attack detection. Researchers primarily focused on leveraging Convolutional Neural Networks (CNNs) and autoencoders to analyze side-channel signals such as power traces and electromagnetic emissions.

Maghrebi et al. (2020) demonstrated that deep learning models could automatically extract features from raw side-channel traces without manual preprocessing. Their work showed that CNNs significantly outperform traditional machine learning techniques in identifying leakage patterns, achieving higher classification accuracy.

Similarly, Zaid et al. (2020) proposed a methodology for applying deep learning to side-channel analysis, emphasizing the importance of model architecture and dataset quality. Their findings highlighted that deeper networks improve detection performance but at the cost of increased computational complexity.

Autoencoder-based models were also explored for anomaly detection. These models learned normal device behavior and identified deviations indicative of potential attacks. While effective, they suffered from high false-positive rates in noisy environments.

Despite these advancements, the models developed in 2020 faced several limitations:

- High computational and memory requirements
- Limited adaptability to dynamic attack patterns
- Dependence on large labeled datasets

These challenges motivated further research into hybrid and optimized models.

Literature Review – Year 2021: Emergence of Hybrid Deep Learning Models

In 2021, research shifted toward hybrid deep learning architectures to improve detection accuracy and adaptability. Combining multiple neural network paradigms enabled better handling of complex and time-dependent side-channel data.

Kim (2021) introduced a CNN-RNN hybrid model, which combined spatial feature extraction with temporal sequence learning. This approach significantly improved the detection of time-dependent leakage patterns in side-channel traces.

Researchers also explored Long Short-Term Memory (LSTM) networks to capture temporal dependencies in power and electromagnetic signals. LSTM-based models demonstrated improved performance in detecting sequential attack patterns.

In addition, optimization techniques such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) were introduced to enhance model performance. These methods optimized hyperparameters such as learning rate, network depth, and weight initialization, resulting in improved convergence and accuracy.

Another important development was the introduction of **transfer learning**, which allowed models trained on one dataset to be adapted to another, reducing the need for large labeled datasets.

However, 2021 models still faced several challenges:

- Increased model complexity
- Longer training times
- Difficulty in real-time deployment on mobile devices

These limitations led to the exploration of more efficient architectures.

Literature Review – Year 2022: Optimization-Driven and Distributed Security Approaches

The year 2022 marked a significant transition toward optimization-driven and distributed security frameworks. Researchers focused on improving model efficiency, scalability, and robustness through advanced optimization techniques.

Wang et al. (2022) explored the use of metaheuristic optimization algorithms for enhancing deep learning models. Techniques such as Ant Colony Optimization (ACO), Grey Wolf Optimization (GWO), and Whale Optimization Algorithm (WOA) were applied to optimize neural network parameters, improving detection accuracy and reducing training time.

Hybrid optimization methods began to gain attention, combining multiple algorithms to balance exploration and exploitation. These approaches achieved faster convergence and better global optimization compared to single-method techniques.

Another major development in 2022 was the adoption of federated learning (FL) for secure AI. FL enabled distributed model training across multiple devices without sharing raw data, addressing privacy concerns in 6G networks. This approach was particularly useful for mobile devices, where data is generated locally.

Researchers also explored edge-based security frameworks, where detection models were deployed directly on mobile devices or edge nodes. This reduced latency and enabled real-time threat detection.

Despite these advancements, several challenges persisted:

- Communication overhead in federated learning
- Complexity of hybrid optimization algorithms
- Limited interpretability of optimized models

Literature Review – Year 2023: Advanced DKNN and Hybrid Optimization Models

In 2023, research advanced toward efficient and scalable architectures, particularly focusing on Deep Kronecker Neural Networks (DKNN) and hybrid optimization techniques such as Hybrid Cat Hunting Optimization (HCHO).

DKNN models leverage the Kronecker product to represent high-dimensional weight matrices in a compressed form. This reduces the number of parameters while maintaining model accuracy, making DKNN particularly suitable for resource-constrained 6G mobile devices.

Recent studies demonstrated that DKNN models achieve:

- Reduced computational complexity
- Lower memory consumption
- High accuracy in detecting side-channel attacks

To further enhance performance, researchers integrated DKNN with metaheuristic optimization algorithms. Among these, HCHO emerged as a promising technique due to its ability to effectively balance exploration and exploitation.

HCHO combines the hunting behavior of cats with hybrid optimization strategies, enabling efficient search of the solution space. When applied to DKNN, HCHO optimizes:

- Network weights
- Hyperparameters
- Feature selection

This integration significantly improves detection accuracy and reduces convergence time.

Additionally, 2023 research emphasized robustness against adversarial attacks, where attackers attempt to deceive AI models. Advanced models incorporated adversarial training techniques to improve resilience.

The concept of AI-native security frameworks also gained attention, where security mechanisms are embedded directly into AI models rather than added as external layers.

Thematic Evolution of Secure AI in 6G

Based on the reviewed literature, the evolution of secure AI for 6G can be categorized into four phases:

1. Deep Learning Foundation (2020)

- CNNs and autoencoders for SCA detection
- High accuracy but high complexity

2. Hybrid Learning Phase (2021)

- CNN-RNN and LSTM models
- Improved temporal analysis

3. Optimization and Distribution Phase (2022)

- Metaheuristic optimization and federated learning
- Enhanced scalability and privacy

4. Efficient Hybrid Intelligence Phase (2023)

- DKNN + HCHO models
- High efficiency, robustness, and scalability

Research Gaps Identified

Despite significant progress, several critical gaps remain:

1. **Lightweight Model Design**
   Many models are too complex for mobile devices
2. **Real-Time Detection**
   High latency limits practical deployment
3. **Adversarial Robustness**
   AI models remain vulnerable to adversarial attacks
4. **Data Scarcity**
   Limited availability of labeled SCA datasets
5. **Explainability**
   Lack of transparency in deep learning models

Summary

The literature from 2020–2023 demonstrates a clear progression from basic deep learning models to advanced hybrid architectures optimized with metaheuristic algorithms. The integration of DKNN with HCHO represents a significant advancement in secure AI for 6G mobile devices, offering a balance between accuracy, efficiency, and scalability.

Comparative Table

Year	Technique	Advantages	Limitations
2020	CNN, Autoencoders	High accuracy	High complexity
2021	CNN-RNN Hybrid	Temporal learning	Training cost
2022	Metaheuristic Optimization	Faster convergence	Parameter tuning
2023	DKNN + HCHO	High efficiency, robust	Implementation complexity

Comparative Analysis

DKNN-HCHO models outperform traditional deep learning approaches by reducing computational complexity while maintaining high accuracy. Hybrid optimization improves convergence and robustness, making these models suitable for real-time deployment.

Discussion

The integration of deep learning and optimization techniques for securing AI in 6G mobile devices represents a significant advancement in addressing modern cyber-physical threats, particularly side-channel attacks (SCAs). The literature clearly demonstrates that deep learning has transformed the landscape of SCA detection by enabling automatic feature extraction from raw leakage signals such as power traces and electromagnetic emissions. Unlike traditional statistical or template-based methods, deep learning models can learn complex nonlinear relationships, significantly improving detection accuracy and robustness.

Recent studies indicate that convolutional neural networks (CNNs) and deep neural networks (DNNs) are highly effective in identifying leakage patterns, even under noisy conditions. However, deep learning-based SCA systems still face challenges such as overfitting, slow convergence, and sensitivity to noise . These limitations have motivated the development of improved architectures incorporating attention mechanisms, denoising modules, and hybrid learning frameworks.

The introduction of Deep Kronecker Neural Networks (DKNN) addresses several of these challenges by reducing model complexity through Kronecker-based tensor decomposition. DKNN models significantly reduce the number of

parameters while preserving representational power, making them highly suitable for resource-constrained 6G mobile devices. This is particularly important in edge computing environments, where computational resources and energy are limited.

Optimization techniques play a crucial role in enhancing the performance of deep learning models. Metaheuristic algorithms such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and Whale Optimization have been widely used. However, the emergence of Hybrid Cat Hunting Optimization (HCHO) introduces a more efficient mechanism for balancing exploration and exploitation in the search space. By mimicking the hunting behavior of cats, HCHO enables faster convergence and improved global optimization, which is critical for tuning deep learning models.

The combination of DKNN and HCHO provides a robust framework for secure AI in 6G. This hybrid approach achieves:

- Reduced computational complexity
- Improved convergence speed
- Enhanced detection accuracy
- Better energy efficiency

Another important observation is the increasing focus on **noise resilience and denoising techniques**. Noise significantly affects side-channel signal quality, reducing model performance. Advanced architectures such as LU-Net and Inception-based models have been proposed to improve denoising and feature extraction, thereby enhancing attack detection performance .

Furthermore, the literature highlights the growing importance of **adversarial robustness**. Attackers can manipulate input data to deceive AI models, leading to incorrect predictions. Recent research has introduced adversarial training and model obfuscation techniques to improve resilience against such attacks.

Despite these advancements, several challenges remain:

1. Computational Overhead – Even optimized models may require significant processing power
2. Data Scarcity – Limited availability of labeled SCA datasets affects model training
3. Real-Time Deployment – Achieving low-latency detection remains difficult
4. Security vs Performance **Trade-off** – Enhancing security often increases computational cost

In addition, the emergence of **AI-native 6G architectures** introduces new security requirements. AI models are now embedded across network layers, increasing the attack surface. This necessitates the development of integrated security frameworks that combine detection, prevention, and response mechanisms. Overall, the discussion highlights that while deep learning and optimization techniques have significantly improved SCA detection, achieving **scalable, lightweight, and secure AI systems** remains an open research challenge.

Conclusion

This paper presented a comprehensive review of deep learning and optimization approaches for securing AI in 6G mobile devices, with a particular focus on Deep Kronecker Neural Networks (DKNN) optimized using Hybrid Cat Hunting Optimization (HCHO). The study examined the evolution of side-channel attack detection techniques from traditional machine learning models to advanced deep learning and hybrid optimization frameworks.

The findings indicate that deep learning has significantly enhanced the ability to detect and mitigate side-channel attacks by enabling automatic feature extraction and pattern recognition. CNNs, RNNs, and hybrid architectures have demonstrated strong performance in analyzing complex side-channel signals. However, these models often suffer from high computational complexity and limited scalability.

The introduction of DKNN provides an effective solution by reducing model parameters while maintaining high accuracy. This makes DKNN particularly suitable for resource-constrained 6G mobile devices, where computational efficiency is critical. When combined with HCHO, DKNN models achieve improved optimization, faster convergence, and enhanced robustness.

The integration of optimization techniques into deep learning models represents a key advancement in secure AI. Hybrid optimization algorithms such as HCHO enable efficient parameter tuning, improving model performance without significantly increasing computational cost. This is essential for real-time deployment in 6G environments.

The study also highlights the importance of addressing challenges such as noise resilience, adversarial robustness, and data scarcity. Advanced architectures incorporating denoising and attention mechanisms have shown promising results in improving model performance.

Despite these advancements, several challenges remain. The limited availability of quantum and edge hardware, high computational requirements, and security vulnerabilities in AI models must be addressed to enable practical deployment. Additionally, ensuring data privacy

and model interpretability is critical for building trustworthy AI systems.

Future research should focus on:

- Developing lightweight and energy-efficient models for mobile devices
- Integrating federated learning for privacy-preserving training
- Enhancing adversarial robustness of AI models
- Exploring explainable AI techniques for improved transparency
- Implementing hybrid quantum-classical security frameworks

In conclusion, DKNN-HCHO models represent a promising direction for securing AI in 6G mobile devices. By combining efficient neural architectures with advanced optimization techniques, these models provide a scalable and robust solution for combating side-channel attacks. Continued research and technological advancements will be essential for realizing secure and intelligent 6G communication systems.

References

Maghrebi, H., Portigliatti, T., & Prouff, E. (2020). Breaking cryptographic implementations using deep learning techniques. https://doi.org/10.1007/978-3-030-42068-0_3

Zaid, G., Bossuet, L., Habrard, A., & Venelli, A. (2020). Methodology for efficient CNN architectures in SCA. https://doi.org/10.46586/tches.v2020.i1.1-38

Benadjila, R., et al. (2020). Deep learning for side-channel analysis. https://doi.org/10.1007/s13389-019-00216-z

Kim, J., et al. (2021). CNN-based side-channel analysis. https://doi.org/10.46586/tches.v2019.i3.148-179

Ito, A., et al. (2021). Imbalanced data in SCA. https://doi.org/10.1109/TIFS.2021.3077287

Kubota, T., et al. (2021). Deep learning SCA on AES. https://doi.org/10.1016/j.micpro.2021.103383

Alam, M., et al. (2021). ML-based SCA detection. https://doi.org/10.1145/3437801

Wang, S., et al. (2022). Optimization in DL security. https://doi.org/10.1016/j.future.2022.01.012

Ou, Y., & Li, L. (2022). Deep learning SCA methods. https://doi.org/10.1007/s11704-021-1173-7

Chang, L., et al. (2022). Deep learning SCA analysis. https://doi.org/10.3390/app12168246

Kwon, D., et al. (2022). Optimization for SCA. https://doi.org/10.1109/ACCESS.2022.3142290

Ahmed, A. A., et al. (2023). CNN-based SCA detection. https://doi.org/10.5755/j02.eie.32479

Do, N. T., et al. (2023). DL-based SCA performance. https://doi.org/10.1049/ise2.12100

Hu, F., et al. (2023). Denoising autoencoder SCA. https://doi.org/10.1109/TIFS.2023.3245678

Li, L., & Ou, Y. (2023). Block cipher SCA models. https://doi.org/10.1016/j.jocs.2023.102078

Berreby, Y. E., & Sauvage, L. (2023). Efficient DL architectures for SCA. https://doi.org/10.48550/arXiv.2309.13170

Huang, H., et al. (2025). DL-based improved SCA. https://doi.org/10.3390/electronics1501018

Yang, M., et al. (2025). Deep learning power analysis. https://doi.org/10.3390/electronics15010018

Feng, T., et al. (2025). CNN with attention for SCA. https://doi.org/10.1007/s42452-025-06854-0

Picek, S., et al. (2023). SoK: Deep learning SCA survey. https://doi.org/10.1145/3560821