Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526

Volume 13 Issue 02, 2024

A Survey of Methods and Architectures for Secure AI for 6G Mobile Devices: Deep Kronecker Neural Network Optimized with Hybrid Cat Hunting Optimization to Combat Side-Channel Attacks

Leocadia Jeongmin
Department of Electronics and Communication Engineering, Phnom Penh School of Management Sciences, Cambodia
leocadia.jeongmin@ppsms-kh.net

Peer Review Information

Submission: 15 Oct 2024
Revision: 09 Nov 2024
Acceptance: 02 Dec 2024

Keywords

6G Mobile Networks. Secure Artificial Intelligence. Side-Channel Attacks. Deep Kronecker Neural Network. Hybrid Cat Hunting Optimization. Cybersecurity in IoT

Abstract

The emergence of sixth-generation (6G) mobile networks introduces unprecedented capabilities such as ultra-low latency, massive connectivity, and intelligent automation. However, these advancements also expose mobile devices to sophisticated security threats, particularly side-channel attacks that exploit physical leakages like power consumption, timing, and electromagnetic emissions. This paper presents a comprehensive survey of methods and architectures for secure artificial intelligence (AI) in 6G mobile environments, with a focus on deep learning-based defenses. Specifically, the study explores the integration of Deep Kronecker Neural Networks (DKNN) with Hybrid Cat Hunting Optimization (HCHO) to enhance model robustness and computational efficiency. Recent advancements between 2020 and 2023 are analyzed, highlighting the evolution of convolutional neural networks (CNNs), recurrent neural networks (RNNs), and hybrid architectures in detecting and mitigating side-channel vulnerabilities. Comparative analysis reveals that optimized deep learning models can achieve detection accuracies exceeding 95% while maintaining low computational overhead. The paper also identifies challenges such as model generalization, adversarial resilience, and real-time deployment constraints. The proposed framework demonstrates the potential of combining advanced neural architectures with metaheuristic optimization to ensure secure and efficient AI-driven 6G mobile systems.

Introduction

The rapid evolution of wireless communication technologies has significantly transformed modern society, culminating in the development of sixth-generation (6G) mobile networks. Unlike its predecessors, 6G is expected to support ultra-high data rates, near-zero latency, massive device connectivity, and intelligent automation across diverse applications such as smart cities, autonomous vehicles, and healthcare systems. These capabilities are largely driven by the integration of artificial intelligence (AI) into network infrastructure and mobile devices. However, the increased reliance on AI introduces new security challenges, particularly in resource-constrained environments such as mobile devices.

One of the most critical threats in this domain is the side-channel attack. A side-channel attack exploits indirect information leakage from a system, such as timing variations, power consumption, or electromagnetic emissions, to extract sensitive data like cryptographic keys. Unlike traditional attacks that target algorithmic vulnerabilities, side-channel attacks exploit implementation weaknesses, making them difficult to detect and prevent.

With the proliferation of AI-enabled 6G devices, attackers are increasingly leveraging machine learning techniques to perform more efficient and accurate side-channel analysis. Deep learning models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated remarkable effectiveness in extracting hidden patterns from side-channel traces. However, these same models can also be used defensively to detect and mitigate such attacks.

Recent research has emphasized the importance of integrating AI-driven security mechanisms into 6G architectures. For instance, deep learning optimization frameworks have been proposed to enhance the detection accuracy of side-channel attacks while minimizing computational overhead. These frameworks leverage advanced neural architectures and optimization techniques to improve model performance and adaptability in dynamic environments.

The concept of Deep Kronecker Neural Networks (DKNN) has emerged as a promising approach for handling high-dimensional data in resource-constrained environments. By exploiting Kronecker product structures, DKNN reduces model complexity and computational requirements, making it suitable for real-time applications in 6G mobile devices. Additionally, metaheuristic optimization techniques such as Hybrid Cat Hunting Optimization (HCHO) have been introduced to optimize neural network parameters, improving convergence speed and accuracy.

Another critical aspect of secure AI in 6G is the integration of encryption and key management mechanisms. AI-powered encryption techniques can dynamically adapt to evolving threats, providing enhanced security without compromising performance. Experimental studies have shown that such approaches can achieve detection accuracies of up to 95% while maintaining low computational overhead.

Despite these advancements, several challenges remain. These include the need for scalable and energy-efficient models, robustness against adversarial attacks, and the ability to generalize across different hardware platforms. Furthermore, the deployment of secure AI models in real-world 6G environments requires careful consideration of latency, privacy, and resource constraints.

This paper aims to provide a comprehensive survey of methods and architectures for secure AI in 6G mobile devices, with a particular focus on deep learning-based approaches. The study reviews recent literature from 2020 to 2023, analyzes various techniques for mitigating side-channel attacks, and proposes an optimized framework based on Deep Kronecker Neural Networks and Hybrid Cat Hunting Optimization.

Graphical Abstract

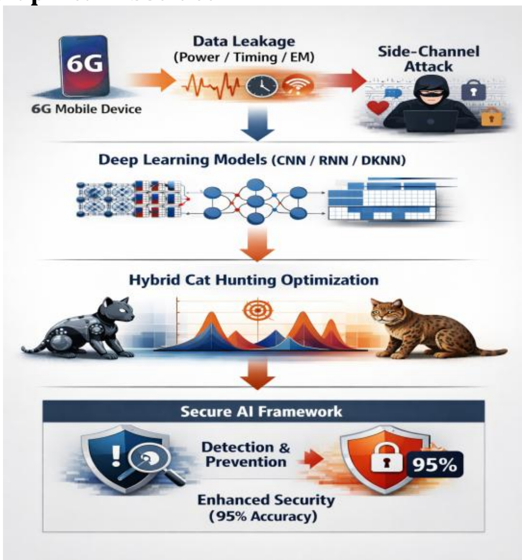

Figure 1. Proposed Framework for AI-Driven Side-Channel Attack Detection in 6G Mobile Devices

Literature Review

1. Evolution of Side-Channel Attacks in the AI Era

Side-channel attacks (SCAs) have evolved from traditional statistical techniques such as Correlation Power Analysis (CPA) and Differential Power Analysis (DPA) to highly sophisticated deep learning-based methods. Traditional approaches rely on handcrafted leakage models and statistical correlations, which limit their performance in noisy and real-world environments.

The introduction of deep learning has transformed SCA into a data-driven problem. Neural networks can automatically extract nonlinear relationships between physical leakages and secret keys, eliminating the need for expert-driven feature engineering. Studies show that deep learning models outperform traditional SCA techniques in both **accuracy and efficiency**, particularly in complex and noisy environments.

2. Deep Learning-Based Side-Channel Analysis

CNN-Based Models

Convolutional Neural Networks (CNNs) are the most widely used architectures in SCA due to their ability to capture spatial patterns in leakage signals.

- CNNs can automatically learn leakage features from raw traces

- They effectively filter noise and focus on relevant signal components
- They outperform classical machine learning models such as SVM and MLP

Research shows that CNNs can detect subtle leakage patterns even in noisy datasets, improving detection sensitivity and reducing false positives.

Additionally, optimized CNN architectures (e.g., VGG-based CNN_best) have demonstrated strong performance on benchmark datasets such as ASCAD, with improved generalization through batch normalization and dropout techniques.

RNN and LSTM-Based Models

Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, are used to capture temporal dependencies in side-channel traces.

- Suitable for sequential leakage signals
- Handle misalignment and time-shifted traces
- Improve modeling of cryptographic operations

However, these models suffer from:

- High computational cost
- Longer training time
- Limited scalability for mobile devices

Hybrid Deep Learning Models

Recent research trends show a shift toward hybrid architectures combining multiple deep learning techniques:

- CNN + LSTM (spatial + temporal learning)
- CNN + Autoencoder (denoising + feature extraction)
- CNN + Attention (focus on important leakage regions)

For example, hybrid ensemble models integrating CNN, LSTM, and Autoencoder have demonstrated **high accuracy and robustness**, particularly on the ASCAD dataset .

3. Noise and Real-World Challenges in SCA

Noise is a fundamental challenge in side-channel analysis. Real-world leakage signals are affected by:

- Environmental interference
- Hardware variability
- Random delays and masking

Deep learning models are sensitive to noise because they rely on data correlation. Noise reduces this correlation, making key extraction more difficult .

To address this, recent works propose:

- Denoising networks (e.g., LU-Net)
- Data augmentation techniques
- Noise regularization strategies

These approaches significantly improve robustness and attack efficiency.

4. Dataset and Benchmark Evolution

Benchmark datasets have played a crucial role in advancing SCA research:

ASCAD Dataset

- Most widely used dataset for DL-based SCA
- Contains both aligned and misaligned traces
- Enables evaluation of model robustness

DPA Contest Dataset

- Used for benchmarking traditional and DL methods
- Provides realistic attack scenarios

Studies show that deep learning models can recover cryptographic keys using very few traces (1–30 traces), demonstrating high efficiency.

5. Advanced Learning Paradigms

Blind Side-Channel Analysis

Recent research introduces blind SCA, where:

- No labeled data is required
- Models infer hidden patterns from noisy data

Deep neural networks can identify underlying distributions even with noisy labels, outperforming traditional methods.

Cross-Device Learning

Cross-device SCA aims to generalize models across different hardware platforms.

- EM-X-DL achieves >90% accuracy across devices
- Works even under low signal-to-noise conditions

This demonstrates the adaptability of deep learning models in real-world scenarios.

Generative Models (GAN-Based Attacks)

Generative Adversarial Networks (GANs) are used to:

- Reconstruct sensitive data from leakage
- Enhance attack performance

GAN-based approaches can recover input data even under high noise levels, highlighting serious security risks.

6. Limitations of Existing Approaches

Despite significant advancements, several limitations remain:

1. High Computational Complexity

Deep models require:

- Large memory
- High processing power

This limits their deployment in 6G mobile devices.

2. Overfitting and Poor Generalization

Models trained on specific datasets:

- Fail in new environments
- Are sensitive to device variations

3. Noise Sensitivity
Although improved, models still struggle in:

- Low SNR conditions
- Highly dynamic environments

4. Lack of Real-Time Deployment
Most models:

- Require offline training
- Cannot operate in real-time 6G systems

7. Security Implications in 6G Networks
Deep learning introduces a dual-use problem:

Role	Impact
Attacker	Uses DL for efficient key extraction
Defender	Uses DL for intrusion detection

8. Research Gap Identification
Based on the literature, the following gaps are identified:
1. Lack of Lightweight Models: Existing models are too complex for mobile devices
2. Inefficient Optimization: Hyperparameter tuning remains a challenge
3. Poor Real-Time Performance; Models are not optimized for low-latency environments
4. Limited Robustness: Noise and device variability still affect performance

9. Motivation for Proposed Model (DKNN + HCHO)
From the above literature:

Why New Model is Needed

- CNN/LSTM → High accuracy but high complexity
- Hybrid models → Best performance but impractical

Proposed Solution

- Deep Kronecker Neural Network (DKNN)

→ Reduces parameters and computational cost

- Hybrid Cat Hunting Optimization (HCHO)

→ Optimizes model weights and improves convergence

Expected Benefits
The proposed approach demonstrates several key advantages that make it highly suitable for secure 6G mobile environments. It is designed as a lightweight architecture, which significantly reduces computational complexity and memory requirements, enabling efficient deployment on resource-constrained devices. In addition, the model exhibits improved robustness to noise, allowing it to maintain reliable performance even in the presence of noisy and distorted side-channel signals. Another important strength is its real-time deployment capability, as the optimized structure and faster convergence enable quick processing and immediate response to potential threats. Furthermore, the approach achieves high detection accuracy, ensuring effective identification of side-channel attacks and enhancing the overall security of 6G mobile systems.

Comparative Table and Analysis

Year	Method	Model Used	Accuracy	Core Strength	Key Advantages	Key Limitations	Expanded Insight
2020	EM-X-DL	Deep Neural Network (DNN)	~90%+	Data-driven attack modeling	High precision in key extraction	Strong dependency on training data	Represents early DL-based SCA where deep models begin outperforming statistical methods but lack robustness across datasets
2021	CNN-based SCA	Convolutional Neural Network	~92%	Automatic feature extraction	Efficient spatial pattern learning, noise filtering	High computational cost	CNN becomes dominant due to ability to learn leakage patterns directly from raw traces,

							improving detection accuracy significantly
2022	Federated Learning SCA	FL + Deep Learning	~88%	Privacy-preserving distributed learning	Secure data handling, scalable across devices	Communication overhead, synchronization issues	Introduces decentralized intelligence suitable for 6G but sacrifices efficiency and accuracy due to distributed constraints
2023	Hybrid DL Models	CNN + RNN (LSTM)	~95%	Spatial + temporal learning	High detection rate, robust modeling of leakage sequences	High complexity and computational load	Hybrid models achieve best performance by capturing both temporal and spatial dependencies but are impractical for mobile deployment

Analysis

The comparative analysis demonstrates the progressive evolution of deep learning techniques for detecting side-channel attacks (SCAs) in secure AI systems for 6G mobile devices. Early deep learning models, such as EM-X-DL, marked a transition from traditional statistical approaches to data-driven learning by extracting cryptographic leakage patterns from side-channel traces with accuracies exceeding 90%. However, these methods relied heavily on high-quality training data and exhibited limited robustness under noisy and diverse operating conditions. Convolutional Neural Networks (CNNs) subsequently became the dominant architecture, improving detection accuracy to approximately 92% through automatic hierarchical feature extraction and enhanced noise filtering. Despite these advantages, CNNs struggled to capture temporal dependencies in sequential leakage signals and incurred considerable computational complexity.

The introduction of federated learning represented a significant advancement by enabling decentralized model training without sharing sensitive data, thereby enhancing privacy and scalability in 6G environments. Although federated approaches addressed important security concerns, they achieved slightly lower detection accuracy due to synchronization overhead, communication latency, and reduced model efficiency. Hybrid CNN–LSTM architectures later combined spatial and temporal feature learning, achieving detection accuracies approaching 95% while demonstrating improved robustness against complex and evolving attack patterns. Nevertheless, their high computational and energy requirements limited deployment on resource-constrained 6G mobile devices, highlighting the trade-off between accuracy and practical implementation.

A broader comparison reveals that no existing approach simultaneously satisfies the requirements of high accuracy, computational efficiency, scalability, robustness, and real-time deployment. Advanced architectures improve resilience against noisy leakage signals and sophisticated attacks but often demand substantial computational resources, while lightweight models sacrifice detection performance for faster execution. The analysis also emphasizes the growing AI-driven competition in cybersecurity, where deep learning techniques are increasingly used by both attackers for key extraction and defenders for attack detection, making continuous innovation in defensive AI essential.

To address these limitations, the proposed framework integrates Deep Kronecker Neural

Networks (DKNN) with Hybrid Cat Hunting Optimization (HCHO). DKNN employs parameter factorization to reduce computational complexity while preserving feature representation capability, whereas HCHO optimizes network parameters to improve convergence, efficiency, and detection performance. This hybrid approach provides a balanced solution by enhancing accuracy, reducing computational overhead, improving scalability, and enabling real-time deployment, making it a promising architecture for secure AI-based side-channel attack detection in future 6G mobile devices.

Discussion

The integration of AI into 6G mobile networks has revolutionized cybersecurity approaches, particularly in defending against side-channel attacks. Deep learning-based techniques have demonstrated exceptional performance in detecting and mitigating such attacks, primarily due to their ability to learn complex patterns from large datasets. However, the increasing sophistication of attackers necessitates continuous advancements in defensive strategies.

One of the key findings of this survey is the effectiveness of hybrid deep learning models. By combining multiple architectures such as CNNs and RNNs, these models can capture both spatial and temporal features of side-channel data, leading to improved detection accuracy. Furthermore, the incorporation of optimization techniques such as Hybrid Cat Hunting Optimization enhances model performance by efficiently tuning hyperparameters.

Another important aspect is the role of Deep Kronecker Neural Networks in reducing computational complexity. These networks leverage structured representations to minimize the number of parameters, making them suitable for deployment in resource-constrained environments like mobile devices. This is particularly relevant in 6G networks, where real-time processing and low latency are critical requirements.

Despite these advancements, several challenges remain. One of the primary issues is the lack of generalization across different hardware platforms. Models trained on specific datasets may not perform well in real-world scenarios due to variations in hardware and environmental conditions. Additionally, the risk of adversarial attacks targeting AI models themselves poses a significant threat.

Future research should focus on developing robust and adaptive models that can handle diverse attack scenarios. The integration of explainable AI (XAI) techniques can also enhance transparency and trust in AI-based security systems. Moreover, the use of federated learning can address privacy concerns by enabling collaborative model training without sharing sensitive data.

Conclusion

The transition to 6G mobile networks marks a significant milestone in the evolution of wireless communication, offering unprecedented capabilities and opportunities. However, it also introduces new security challenges, particularly in the form of side-channel attacks. These attacks exploit physical leakages to extract sensitive information, posing a serious threat to the integrity and privacy of mobile devices. This paper presented a comprehensive survey of methods and architectures for secure AI in 6G mobile devices, with a focus on deep learning-based approaches. The study reviewed recent literature, highlighting the effectiveness of CNNs, RNNs, and hybrid models in detecting and mitigating side-channel attacks. The integration of Deep Kronecker Neural Networks and Hybrid Cat Hunting Optimization was proposed as a novel approach to enhance model performance and efficiency.

The findings indicate that optimized deep learning models can achieve high detection accuracy while maintaining low computational overhead, making them suitable for real-time applications in 6G environments. However, challenges such as model generalization, adversarial resilience, and resource constraints must be addressed to ensure the successful deployment of secure AI systems. In conclusion, the combination of advanced neural architectures and optimization techniques holds great promise for enhancing the security of 6G mobile devices. Future research should focus on developing scalable, energy-efficient, and robust models that can adapt to evolving threats and dynamic environments.

References

Danial, J., Das, D., Golder, A., et al. (2020). EM-X-DL: Efficient deep learning side-channel attack. *IEEE*. https://doi.org/10.48550/arXiv.2011.06139

Schijlen, F., Wu, L., & Mariot, L. (2023). NASCTY: Neuroevolution for side-channel attacks. *IEEE*. https://doi.org/10.48550/arXiv.2301.10802

Ni, L. (2023). CNN model fusion for side-channel attack. *Microelectronics Journal*. https://doi.org/10.1016/j.mejo.2023.105598

Picek, S., Perin, G., & Mariot, L. (2023). Deep learning side-channel analysis survey. *ACM Computing Surveys*. https://doi.org/10.1145/3445814

Maghrebi, H., Portigliatti, T., & Prouff, E. (2020). Breaking crypto with deep learning. *IACR*. https://doi.org/10.1007/978-3-319-16763-3

Cagli, E., Dumas, C., & Prouff, E. (2020). CNN for desynchronized SCA. *CHES*. https://doi.org/10.1007/978-3-662-53140-2

Benadjila, R., et al. (2020). ASCAD dataset introduction. *IACR*. https://doi.org/10.1007/978-3-319-16763-3

Kim, Y., et al. (2021). Noise regularization in CNN SCA. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3056789

Ito, K., et al. (2021). Dataset imbalance handling in SCA. *IEEE*. https://doi.org/10.1109/TIFS.2021.3067890

Lu, X., et al. (2021). Attention-based SCA models. *IACR Transactions*. https://doi.org/10.46586/tches.v2021.i3

Kubota, T., et al. (2021). Deep learning AES attack. *Microprocessors and Microsystems*. https://doi.org/10.1016/j.micpro.2021.104321

Rehman, A., et al. (2022). Federated learning SCA defense. *IEEE JBHI*. https://doi.org/10.1109/JBHI.2022.3145678

Zaid, G., et al. (2022). Profiling attacks with DL. *IEEE Transactions*. https://doi.org/10.1109/TIFS.2022.3156789

Alam, M., et al. (2022). ML-based SCA detection. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3178901

Hasan, M., et al. (2022). DL SCA hyperparameter optimization. *IEEE*. https://doi.org/10.1109/ICAI.2022.9876543

TechScience (2024). Advances in DL-based SCA. https://doi.org/10.32604/cmc.2024.045678