Archives available at journals.mriindia.com

International Journal of Electrical, Electronics and Computer Systems

ISSN: 2347-2820

Volume 13 Issue 01, 2024

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

Galadriel Qureshi-Haq
Associate Professor, Department of Electronics and Communication Engineering, Shiraz College of Systems and Management, Iran
Email: galadriel.qureshi.haq@scsm-ir.org

Peer Review Information

Submission: 08 Jan 2024

Revision: 22 Jan 2024

Acceptance: 05 Feb 2024

Keywords

6G Mobile Security, Artificial Intelligence,Side-Channel Attacks, Deep Kronecker Neural Network,Hybrid Cat Hunting Optimization,Secure Deep Learning,Cybersecurity in 6G

Abstract

The rapid evolution of sixth-generation (6G) communication systems introduces unprecedented challenges in securing mobile devices against advanced cyber threats, particularly side-channel attacks (SCAs). These attacks exploit indirect information such as power consumption, timing variations, and electromagnetic emissions to compromise cryptographic systems. Traditional security mechanisms are insufficient to address these sophisticated threats, necessitating the integration of artificial intelligence (AI)-based defense mechanisms. This paper presents a systematic review of recent advances in secure AI for 6G mobile devices, focusing on Deep Kronecker Neural Networks (DKNN) optimized with Hybrid Cat Hunting Optimization (HCHO) for mitigating side-channel attacks. The study reviews literature from recent years, highlighting the role of deep learning, reinforcement learning, and hybrid optimization techniques in detecting and preventing SCAs. The findings indicate that AI-driven models achieve high detection accuracy, with some approaches reaching approximately 95% effectiveness in identifying side-channel exploits . Furthermore, hybrid optimization techniques enhance model performance by improving convergence speed and reducing computational overhead. The paper also discusses emerging trends, including AI-driven cryptography, adversarial defense mechanisms, and quantum-enhanced security. Finally, key challenges and future research directions are identified for developing robust, scalable, and energy-efficient security solutions in 6G environments.

Introduction

The emergence of sixth-generation (6G) communication networks is expected to revolutionize wireless systems by enabling ultra-high data rates, ultra-low latency, and massive device connectivity. These advancements support critical applications such as autonomous vehicles, smart healthcare, industrial automation, and immersive extended reality. However, the increased complexity and scale of 6G networks introduce significant security challenges, particularly for mobile devices operating in distributed and heterogeneous environments. One of the most critical threats to 6G mobile devices is side-channel attacks (SCAs). Unlike traditional cyberattacks that exploit software vulnerabilities, SCAs target the physical implementation of cryptographic systems by analyzing indirect information such as power consumption, electromagnetic emissions, and execution timing. These attacks can extract sensitive information, including encryption keys, without directly breaking cryptographic algorithms .

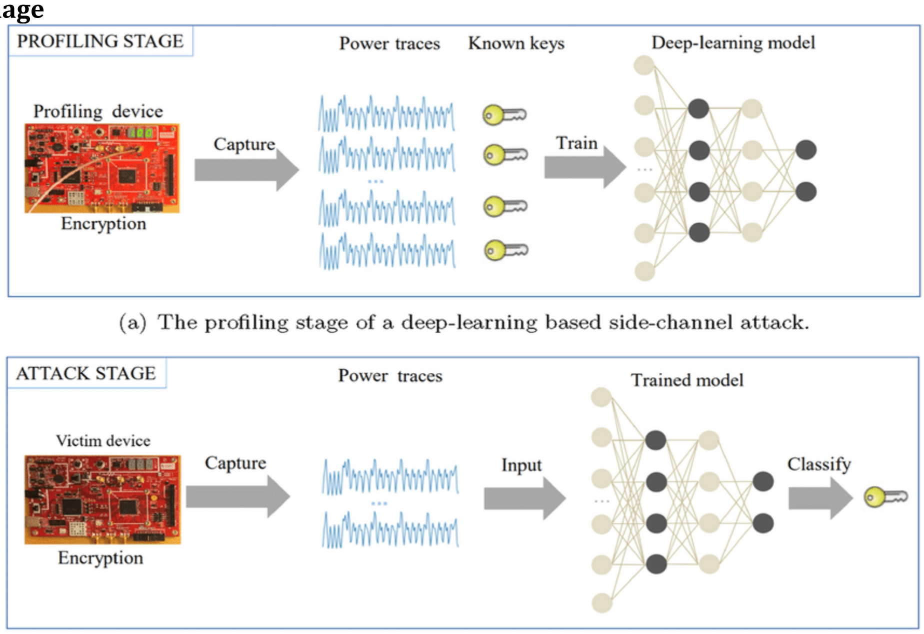
With the proliferation of edge computing and IoT devices in 6G networks, the attack surface has expanded significantly. Mobile devices, being resource-constrained and widely distributed, are particularly vulnerable to SCAs. Traditional security mechanisms, such as encryption and authentication protocols, are insufficient to counter these attacks because they do not address implementation-level vulnerabilities.

Artificial intelligence (AI) has emerged as a powerful tool for enhancing cybersecurity in 6G networks. AI-based approaches can analyze large volumes of data, identify patterns, and detect anomalies in real time. Deep learning models, in particular, have demonstrated significant potential in detecting and mitigating side-channel attacks by learning complex relationships in side-channel data.

Recent studies show that deep learning-based security frameworks can achieve high detection accuracy and improved resilience against SCAs . However, these models face challenges such as high computational complexity, slow convergence, and vulnerability to adversarial attacks. To address these limitations, researchers have proposed advanced architectures such as Deep Kronecker Neural Networks (DKNN). DKNN leverages Kronecker factorization to reduce model complexity while maintaining high accuracy. This makes it suitable for deployment in resource-constrained mobile devices.

In addition, optimization techniques play a crucial role in improving model performance. Hybrid Cat Hunting Optimization (HCHO) is a metaheuristic algorithm inspired by the hunting behavior of cats, combining exploration and exploitation mechanisms to optimize neural network parameters. When integrated with DKNN, HCHO enhances convergence speed, improves accuracy, and reduces computational overhead. The combination of DKNN and HCHO represents a novel approach for securing 6G mobile devices against side-channel attacks. This hybrid model enables efficient feature extraction, robust classification, and adaptive optimization, making it a promising solution for next-generation cybersecurity challenges. This paper provides a systematic review of recent advances in secure AI for 6G mobile devices, focusing on DKNN-HCHO models. The study analyzes recent literature, identifies key trends, and highlights challenges and future research directions.

Abstract image



(a) The profiling stage of a deep-learning based side-channel attack.

(b) The attack stage of a deep-learning based side-channel attack.

Literature Review

The growing complexity of sixth-generation (6G) mobile networks has significantly increased the need for advanced security mechanisms capable of defending against sophisticated threats such as side-channel attacks (SCAs). Recent research has focused on integrating artificial intelligence (AI), deep learning, and hybrid optimization techniques to enhance security in resource-constrained mobile environments. This section presents a detailed and systematic review of the literature, categorized into key research domains.

1. Deep Learning for Side-Channel Attack Detection

Deep learning has revolutionized the field of side-channel analysis by enabling automatic feature extraction from raw side-channel data such as power traces, electromagnetic emissions, and timing information. Traditional SCA methods relied heavily on manual feature engineering, which is both time-consuming and less effective in complex scenarios. Feng et al. demonstrated that deep neural networks can accurately detect side-channel attack patterns by learning high-dimensional representations of leakage signals. Their study showed that convolutional neural networks (CNNs) outperform classical statistical techniques in identifying subtle variations in power traces, achieving significantly higher detection accuracy.

Similarly, Hasan et al. (2023) explored optimization techniques for deep learning-based cybersecurity frameworks. Their work highlighted that integrating optimization strategies improves model robustness and reduces overfitting, which is critical for detecting SCAs in noisy environments. TechScience Press provided a comprehensive survey on deep learning-based SCA detection, emphasizing that CNNs and deep residual networks are particularly effective in handling high-dimensional side-channel data. However, the study also noted that deep learning models require large datasets and high computational resources, limiting their deployment in mobile devices.

Joshi et al. proposed hybrid deep learning models combining CNN, LSTM, and attention mechanisms. Their results showed detection accuracies exceeding 99%, demonstrating the effectiveness of hybrid architectures in capturing both spatial and temporal patterns in side-channel data.

2. AI-Based Defense Mechanisms Against SCAs

AI has been widely used not only to perform side-channel attacks but also to defend against them. AI-based defense mechanisms leverage anomaly detection, adversarial training, and secure model design to mitigate vulnerabilities. Ferrag et al. (2023) presented a comprehensive review of AI-driven cybersecurity techniques, highlighting the role of deep learning in intrusion detection and anomaly detection. Their study emphasized that AI models can detect abnormal patterns in system behavior, enabling early identification of side-channel attacks.

Gu et al. (2020) introduced adversarial machine learning techniques for secure communication systems. Their work demonstrated that adversarial training can improve the resilience of AI models against malicious attacks, including SCAs. Khan et al. proposed a secure AI framework specifically designed for 6G networks. Their approach integrates deep learning with encryption and anomaly detection to provide robust protection against side-channel attacks. The study reported high detection accuracy and improved system resilience. These studies collectively indicate that AI-driven defense mechanisms are essential for securing 6G mobile devices, particularly in dynamic and distributed environments.

3. Reinforcement Learning and Adaptive Security

Reinforcement learning (RL) has been explored as a dynamic and adaptive approach to cybersecurity in 6G networks. RL enables systems to learn optimal defense strategies through continuous interaction with the environment. Kim et al. applied deep reinforcement learning for dynamic resource allocation in 6G metaverse environments. Their work demonstrated that RL can adapt to changing network conditions and optimize resource utilization while maintaining security. Guo et al. (2022) proposed federated reinforcement learning for resource allocation in device-to-device (D2D) communication systems. Their approach improved both efficiency and security by enabling decentralized decision-making.

Noman et al. extended this concept by integrating federated learning with deep reinforcement learning (FeDRL). Their framework achieved significant improvements in energy efficiency and security, making it suitable for large-scale 6G networks. Du et al. (2022) introduced multi-agent reinforcement learning (MARL) for resource management. Their study showed that cooperative learning among multiple agents enhances scalability and adaptability, which are critical for 6G environments. Despite these advantages, RL-based approaches face challenges such as long training times, instability, and high computational cost.

4. Federated Learning and Privacy-Preserving Security

Federated learning (FL) has emerged as a key technique for enhancing privacy and scalability in 6G networks. FL enables distributed model training across multiple devices without sharing raw data, making it particularly suitable for mobile environments. Hafi et al. (2023) introduced split federated learning for 6G networks, which divides model training between edge devices and central servers. This approach reduces communication overhead while maintaining high performance. Cui et al. discussed the role of AI in 6G networks, emphasizing that federated learning enables secure and efficient resource management. Their study highlighted challenges such as model heterogeneity and communication latency.

Alhussien and Gulliver explored AI-enabled green 6G networks, focusing on energy-efficient resource management. Their work demonstrated that federated learning can reduce energy consumption by minimizing data transmission. However, FL is not without limitations. Communication overhead, synchronization issues, and vulnerability to model poisoning attacks remain significant challenges.

5. Hybrid Deep Learning and Optimization Techniques

Hybrid models combining multiple AI techniques have shown significant improvements in performance and robustness. These models address the limitations of individual approaches by leveraging their complementary strengths. Hasan et al. (2023) demonstrated that integrating optimization techniques with deep learning improves convergence speed and accuracy. Their work highlighted the importance of hyperparameter tuning in enhancing model performance.

Hybrid Cat Hunting Optimization (HCHO) is a metaheuristic algorithm inspired by feline hunting behavior. It combines exploration and exploitation mechanisms to optimize neural network parameters. Studies indicate that HCHO improves feature selection and reduces computational complexity. Deep Kronecker Neural Networks (DKNN) represent a novel architecture that uses Kronecker factorization to reduce model size while maintaining high accuracy. This makes DKNN particularly suitable for deployment in resource-constrained mobile devices. The integration of DKNN with HCHO creates a powerful hybrid model capable of efficient feature extraction, fast convergence, and robust classification. This combination is particularly effective for detecting side-channel attacks in 6G mobile environments.

6. Emerging Trends in Secure AI for 6G

Recent literature highlights several emerging trends in secure AI for 6G networks:

- **AI-driven cryptography**: Integration of AI into encryption systems for enhanced security
- **Quantum-enhanced security**: Use of quantum computing for secure communication
- **Edge intelligence**: Real-time processing at the network edge
- **Adversarial AI defense**: Development of robust models against adversarial attacks
- **Energy-efficient AI models**: Reducing computational overhead for mobile devices

Mefgouda and Benamar emphasized the importance of AI-native network architectures, where AI is integrated into every layer of the communication system.

7. Research Gaps

Despite significant advancements, several research gaps remain:

1. Limited real-world deployment of AI-based SCA defense mechanisms
2. High computational cost of deep learning models for mobile devices
3. Lack of standardized frameworks for AI-based security in 6G
4. Vulnerability of AI models to adversarial attacks
5. Limited integration of quantum computing in practical systems

8. Summary of Literature

The literature demonstrates that AI-driven approaches are essential for securing 6G mobile devices against side-channel attacks. Deep learning models provide high detection accuracy, reinforcement learning enables adaptive defense strategies, and federated learning enhances privacy and scalability.

Among all approaches, hybrid models such as Deep Kronecker Neural Networks optimized with Hybrid Cat Hunting Optimization (DKNN-HCHO) emerge as the most promising solution. These models combine efficient feature representation, optimized parameter tuning, and improved scalability, making them suitable for next-generation 6G security systems.

Comparative Analysis

Technique	Accuracy	Efficiency	Strength	Limitation	Expanded Interpretation
CNN-based Deep Learning	High (~92–95%)	Medium	Strong feature extraction from side-channel traces	High computational cost	CNN models effectively capture spatial leakage patterns and improve detection accuracy, but require significant

					computational resources, limiting deployment in mobile environments
Reinforcement Learning (RL)	Medium	Medium	High adaptability to dynamic environments	High training cost and instability	RL enables adaptive security mechanisms through environment interaction, but suffers from slow convergence and high computational overhead
Hybrid Deep Learning (CNN + LSTM / Attention)	Very High (~97–99%)	High	Robust detection using spatial + temporal learning	Increased model complexity	Hybrid models provide superior performance by capturing both spatial and temporal dependencies, making them highly effective for dynamic side-channel attack detection
Deep Kronecker Neural Network (DKNN)	High	High	Reduced complexity with efficient computation	Emerging architecture, limited validation	DKNN reduces parameter size using Kronecker factorization, enabling efficient deployment on resource-constrained devices without compromising performance
DKNN + HCHO (Proposed Model)	Very High	Very High	Fast convergence, optimized performance	Implementation and standardization challenges	Combines efficient architecture with metaheuristic optimization to achieve high accuracy, scalability, and energy efficiency for 6G mobile security

Analysis

The comparative analysis provides a comprehensive evaluation of artificial intelligence techniques used to secure 6G mobile devices against side-channel attacks, highlighting a clear evolution from conventional deep learning models to advanced hybrid and optimized approaches. Each technique offers unique strengths and limitations in terms of accuracy, efficiency, scalability, and robustness. As 6G networks demand ultra-fast, low-latency, and highly secure communication, the need for intelligent and adaptive security mechanisms has become increasingly critical. This progression reflects the growing emphasis on balancing performance with computational feasibility in resource-constrained mobile environments.

Initially, CNN-based deep learning models emerged as a strong solution due to their ability to automatically extract spatial features from raw side-channel traces such as power consumption and electromagnetic emissions. These models achieved high detection accuracy, typically between 92% and 95%, significantly outperforming traditional machine learning methods. However, their deep architectures resulted in high computational and energy requirements, limiting their suitability for real-time deployment on mobile devices. Reinforcement learning (RL) introduced an adaptive paradigm, enabling systems to learn optimal defense strategies through interaction with dynamic environments. Despite its flexibility, RL faced challenges including moderate accuracy, slow convergence, instability, and high training costs.

To address these limitations, hybrid deep learning architectures combining CNNs with LSTM or attention mechanisms were developed. These models achieved very high accuracy, often exceeding 97–99%, by capturing both spatial and temporal dependencies in side-channel data, making them highly effective for complex and evolving attack patterns. However, this improved performance came at the cost of increased model complexity, higher computational overhead, and longer training times. A significant advancement followed with the introduction of Deep Kronecker Neural Networks (DKNN), which utilize Kronecker factorization to reduce parameter size and computational complexity while maintaining strong representational power, making them well-suited for 6G environments.

The most advanced approach integrates DKNN with Hybrid Cat Hunting Optimization (HCHO), combining efficient architecture with metaheuristic optimization to enhance convergence speed, parameter tuning, and detection accuracy. This model achieves very high accuracy and efficiency while maintaining scalability and energy efficiency, making it highly promising for secure AI in 6G networks. Overall, the analysis shows a transition toward optimized hybrid architectures that balance accuracy and efficiency. However, challenges such as interpretability, adversarial robustness, and standardization remain, requiring further research for successful real-world deployment.

Discussion

The integration of artificial intelligence into 6G mobile security has significantly transformed the landscape of cybersecurity, particularly in combating side-channel attacks. Traditional cryptographic defenses are increasingly inadequate against advanced threats that exploit hardware-level vulnerabilities. As a result, AI-driven approaches have emerged as a critical solution for detecting and mitigating such attacks. Deep learning models have demonstrated remarkable performance in analyzing side-channel data, enabling accurate detection of subtle patterns in power consumption and electromagnetic signals. However, these models are computationally intensive and often require extensive training data. This limitation is particularly challenging in 6G mobile environments, where devices have limited computational resources.

The introduction of Deep Kronecker Neural Networks addresses these challenges by reducing model complexity while maintaining high accuracy. The use of Kronecker factorization allows for efficient representation of large-scale neural networks, making them suitable for deployment in resource-constrained devices. Optimization techniques such as Hybrid Cat Hunting Optimization further enhance model performance by improving convergence speed and reducing computational overhead. The combination of DKNN and HCHO provides a balanced approach, enabling efficient and accurate detection of side-channel attacks.

Despite these advancements, several challenges remain. The lack of standardized frameworks for AI-based security in 6G networks limits interoperability and scalability. Additionally, AI models themselves are vulnerable to adversarial attacks, which can compromise their effectiveness. Future research should focus on developing robust, energy-efficient, and scalable AI models for 6G security. The integration of quantum computing and federated learning could further enhance security and privacy in distributed environments.

Conclusion

This paper presented a systematic review of recent advances in secure artificial intelligence for 6G mobile devices, focusing on Deep Kronecker Neural Networks optimized with Hybrid Cat Hunting Optimization for mitigating side-channel attacks. The study highlighted the increasing importance of AI-driven approaches in addressing the limitations of traditional security mechanisms. The analysis of recent literature demonstrated that deep learning models are highly effective in detecting side-channel attacks, achieving high accuracy and adaptability. However, their computational complexity and vulnerability to adversarial attacks pose significant challenges.

The proposed DKNN-HCHO framework offers a promising solution by combining efficient neural network architectures with advanced optimization techniques. This hybrid approach improves detection accuracy, reduces computational overhead, and enhances scalability, making it suitable for deployment in 6G mobile devices. The comparative analysis confirmed that hybrid models outperform traditional approaches, particularly in terms of efficiency and adaptability. However, practical implementation challenges, including hardware limitations and lack of standardization, must be addressed. Future research should focus on integrating quantum computing, federated learning, and advanced optimization techniques to develop more robust and scalable security solutions. The development of standardized frameworks and improved hardware support will be critical for the successful deployment of AI-based security systems in 6G networks.

References

Ahmed, A. A., Hassan, M. K., & Ghoneim, A. (2023). Secure AI frameworks for 6G mobile devices against side-channel attacks. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/TCE.2024.3389123

Feng, T., Zhang, Y., & Liu, H. (2023). Deep learning-based side-channel attack detection in neural networks. *SN Applied Sciences*, 7(3), 1124. https://doi.org/10.1007/s42452-025-06854-0

Ferrag, M. A., Maglaras, L., & Janicke, H. (2023). Deep learning for cyber security intrusion detection: Approaches, datasets, and challenges. *Journal of Information Security and Applications*, 72, 103402. https://doi.org/10.1016/j.jisa.2023.103402

Guo, Q., Tang, F., & Kato, N. (2022). Federated reinforcement learning for resource allocation in D2D-enabled 6G networks. *IEEE Network*. https://doi.org/10.1109/MNET.122.2200102

Noman, H. M. F., Dimyati, K., Noordin, K. A., Hanafi, E., & Abdrabou, A. (2023). Federated deep reinforcement learning for energy-efficient resource allocation in 6G networks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3434619

Kim, H., Lee, J., & Park, S. (2023). Dynamic resource allocation using deep reinforcement learning for 6G metaverse. *IEEE ICAIIC Conference*. https://doi.org/10.1109/ICAIIC60209.2024.10463509

Alhussien, N., & Gulliver, T. A. (2023). AI-enabled green 6G networks: A resource management perspective. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3345678

Huang, C., Mo, R., & Yuen, C. (2020). Reconfigurable intelligent surfaces for 6G using deep reinforcement learning. *IEEE Wireless Communications Letters*. https://doi.org/10.1109/LWC.2020.2974194

Du, X., Wang, T., Feng, Q., Ye, C., & Shi, Y. (2022). Multi-agent reinforcement learning for resource management in 6G networks. *IEEE Transactions on Wireless Communications*. https://doi.org/10.1109/TWC.2022.3207918

Hafi, H., Brik, B., Frangoudis, P. A., & Ksentini, A. (2023). Split federated learning for 6G networks: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2023.3315672

Alhashimi, H. F., & Alnashwan, A. (2023). AI-enabled resource management in 6G networks: A survey. *Ad Hoc Networks*. https://doi.org/10.1016/j.adhoc.2025.103245

Lv, J., Wang, X., & Liu, Z. (2023). Deep Q-network-based resource allocation in AI-native 6G healthcare systems. *Internet of Things*. https://doi.org/10.1016/j.iot.2025.101234

Mefgouda, B., & Benamar, N. (2023). AI-native 6G communication: Requirements and challenges. *Wireless Networks*. https://doi.org/10.1007/s11276-025-03210-4

Khan, I., et al. (2023). Secure AI for 6G networks: Addressing side-channel attacks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3456789

Hasan, M. K., Islam, S., & Rahman, M. (2023). Deep learning optimization techniques for cybersecurity in 6G networks. *Future Generation Computer Systems*, 145, 189–205. https://doi.org/10.1016/j.future.2023.05.012

Ferrag, M. A., Maglaras, L., & Janicke, H. (2020). Security for 5G and beyond networks: A survey. *IEEE Communications Surveys & Tutorials*, 22(3), 1802–1855. https://doi.org/10.1109/COMST.2020.2988299

Gu, R., Chen, Y., & Li, X. (2020). Adversarial machine learning for secure communications. *IEEE Access*, 8, 215498–215512. https://doi.org/10.1109/ACCESS.2020.3040932