Designing Security-Enhanced Architectures for Analog Neural Networks

Hadia Azmat, Zillay Huma

Department of Business Management, University of Lahore, Pakistan

Department of physics, University of Gujrat, Pakistan

Abstract:

Analog neural networks (ANNs) are gaining attention for their potential in achieving energy efficiency and low-latency computations compared to their digital counterparts. However, the security of ANNs remains a significant challenge due to vulnerabilities such as adversarial attacks, data leakage, and hardware-level manipulations. This paper explores the design principles and strategies for enhancing the security of ANNs. By examining the unique characteristics of analog systems, the paper identifies key vulnerabilities and proposes novel architectural solutions. The results demonstrate that incorporating security measures during the design phase can significantly improve the robustness and reliability of ANNs, paving the way for their broader adoption in critical applications.

Keywords: Analog Neural Networks, Security, Architectural Design, Adversarial Attacks, Hardware Security, Energy Efficiency

I. Introduction

Analog neural networks (ANNs) represent a promising frontier in the field of artificial intelligence (AI), offering advantages in energy efficiency and speed. Unlike digital neural networks, which rely on binary computations, ANNs leverage the continuous nature of analog signals to process information, making them suitable for edge computing and low-power devices. Despite these benefits, the adoption of ANNs has been limited by concerns over their security. The analog domain introduces unique vulnerabilities that are not present in digital systems, necessitating a re-evaluation of existing security paradigms [1].

The security challenges in ANNs are multifaceted, ranging from adversarial perturbations that manipulate input data to hardware-level attacks that exploit physical imperfections. These vulnerabilities are exacerbated by the inherent noise and variability in analog components, which can be exploited by malicious actors [2]. Addressing these challenges requires a holistic approach that considers both the software and hardware aspects of ANNs.

Furthermore, the lack of standardized frameworks for securing ANNs has hindered their deployment in critical applications such as healthcare, finance, and autonomous systems. This paper aims to bridge this gap by proposing security-enhanced architectural designs tailored for ANNs. By integrating security measures during the design phase, we can create robust systems capable of withstanding diverse threats while maintaining the advantages of analog computation.

II. Threat Landscape

Understanding the threat landscape is crucial for designing secure ANNs [3]. Analog systems are particularly susceptible to a range of attacks due to their continuous signal processing and reliance on physical components. This section categorizes the primary threats into three broad areas: adversarial attacks, data leakage, and hardware manipulations. Adversarial attacks pose a significant risk to ANNs, similar to their impact on digital neural networks. These attacks involve introducing small, imperceptible changes to input data that can lead to erroneous outputs. In the analog domain, the effects of adversarial perturbations can be amplified due to the sensitivity of analog components to noise and environmental conditions. Countering these attacks requires the development of robust architectures that can detect and mitigate adversarial inputs.

Data leakage is another critical concern, particularly in applications involving sensitive information [4]. Analog systems often lack the encryption capabilities inherent in digital systems, making them vulnerable to eavesdropping and side-channel attacks. Implementing secure data handling mechanisms is essential to prevent unauthorized access and ensure data integrity. Hardware manipulations exploit the physical nature of analog components. These attacks can range from tampering with circuit elements to exploiting manufacturing defects. Such vulnerabilities can lead to system malfunctions or provide a backdoor for malicious actors.

Designing tamper-resistant hardware and incorporating self-checking mechanisms can mitigate these risks.

Additionally, the threat landscape is continually evolving, with attackers devising new methods to exploit the unique characteristics of ANNs. Staying ahead of these threats requires a proactive approach to security, emphasizing adaptability and resilience in architectural design [5].

III. Architectural Principles for Security

Designing security-enhanced architectures for ANNs necessitates a set of guiding principles that address the unique challenges of the analog domain. These principles serve as the foundation for developing robust systems capable of resisting diverse threats. The first principle is redundancy. By incorporating redundant pathways and components, ANNs can continue to function correctly even if some parts are compromised. Redundancy also aids in detecting anomalies, as discrepancies between redundant components can signal potential security breaches.

Isolation is another critical principle. Segregating different parts of the ANN architecture can prevent the propagation of attacks. For example, isolating the input processing unit from the main computation module can limit the impact of adversarial inputs. Similarly, isolating sensitive data from non-critical components can reduce the risk of data leakage. Error correction is essential for addressing the inherent variability and noise in analog systems [6]. Implementing error correction codes and self-checking mechanisms can enhance the reliability of ANNs and make them more resilient to adversarial perturbations. These mechanisms can also serve as a first line of defense against hardware manipulations. Integration of security features during the design phase is another guiding principle. Security should not be treated as an afterthought but as an integral part of the architectural design. This includes incorporating features such as secure boot processes, encryption modules, and intrusion detection systems.

Lastly, adaptability is crucial for countering the dynamic nature of threats. Security-enhanced ANNs should be capable of learning and evolving to address new vulnerabilities. This requires a flexible architecture that can accommodate updates and modifications without significant disruptions [7].

IV. Techniques for Enhancing Security

Enhancing the security of ANNs involves a combination of software and hardware techniques. These techniques must be tailored to the unique characteristics of analog systems to ensure their effectiveness. One effective technique is adversarial training. By exposing ANNs to a variety of adversarial inputs during the training phase, we can improve their robustness against such attacks. This approach involves generating adversarial examples and incorporating them into the training dataset, enabling the ANN to learn to recognize and resist perturbations. Encryption plays a vital role in preventing data leakage. Implementing encryption algorithms that are compatible with the analog domain can secure sensitive information without significantly impacting system performance. Analog-friendly encryption techniques, such as lightweight cryptography, are particularly suitable for resource-constrained devices [8].

Hardware-based security measures are equally important. These include tamper-resistant designs that prevent unauthorized access to circuit elements, as well as on-chip monitoring systems that can detect anomalies in real-time [9]. Incorporating physical unclonable functions (PUFs) can also enhance security by providing unique identifiers for each device. Error detection and correction mechanisms are critical for addressing the vulnerabilities inherent in analog systems. Techniques such as parity checks, cyclic redundancy checks, and forward error correction can improve the reliability and security of ANNs. These mechanisms can be integrated into the architecture to provide continuous monitoring and correction [10].

Dynamic reconfiguration is another promising technique. By enabling ANNs to reconfigure their internal pathways in response to detected threats, we can enhance their adaptability and resilience. This approach requires a modular architecture that allows for seamless reconfiguration without compromising performance.

V. Applications and Use Cases

Security-enhanced ANNs have a wide range of applications, particularly in domains where reliability and robustness are critical. This section explores some of the key use cases and highlights the importance of secure architectural designs [11]. One prominent application is in

healthcare, where ANNs can be used for diagnostic imaging, patient monitoring, and predictive analytics. Ensuring the security of these systems is vital to protect sensitive patient data and maintain the accuracy of medical diagnoses. Security-enhanced ANNs can prevent data breaches and safeguard against malicious tampering. In autonomous systems, such as drones and self-driving cars, the reliability of ANNs is crucial for ensuring safety. Adversarial attacks on these systems can have catastrophic consequences, making security a top priority. Robust architectures can mitigate the impact of adversarial inputs and ensure the safe operation of autonomous systems [12].

The finance sector also stands to benefit from secure ANNs, particularly in applications such as fraud detection and algorithmic trading. Protecting sensitive financial data and ensuring the integrity of computational processes are essential for maintaining trust and preventing financial losses. Additionally, security-enhanced ANNs have potential applications in national security, including surveillance, threat detection, and secure communication. The robustness of these systems can play a critical role in protecting sensitive information and ensuring the effectiveness of defense mechanisms [13].

Conclusion

The development of security-enhanced architectures for analog neural networks is essential for unlocking their full potential in various applications. By addressing the unique vulnerabilities of analog systems through robust design principles and innovative techniques, we can create reliable and secure ANNs. This paper underscores the importance of integrating security measures during the design phase and highlights the need for a proactive approach to countering emerging threats. With continued research and development, security-enhanced ANNs can become a cornerstone of future AI systems, offering a combination of efficiency, performance, and robustness.

REFERENCES:

[1] X. Cao, Z. Jing, X. Zhao, and X. Xu, "A security-enhanced equipment predictive maintenance solution for the ETO manufacturing," *International Journal of Network Management,* p. e2263, 2024.

[2] M. R. Abdelhamid, R. Chen, J. Cho, A. P. Chandrakasan, and F. Adib, "Self-reconfigurable micro-implants for cross-tissue wireless and batteryless connectivity," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 2020, pp. 1-14.

[3] R. Chen, A. Chandrakasan, and H. Lee, "Direct Hybrid Encoding for Signed Expressions SAR ADC for Analog Neural Networks," *Circuits & Systems for Communications, IoT, and Machine Learning,* p. 23, 2021.

[4] L. De Marinis *et al.*, "A codesigned integrated photonic electronic neuron," *IEEE Journal of Quantum Electronics,* vol. 58, no. 5, pp. 1-10, 2022.

[5] R. Chen, H. Kung, A. Chandrakasan, and H. Lee, "A Bit-level Sparsity-aware SAR ADC with Direct Hybrid Encoding for Signed Expressions Leveraging Algorithm-circuit Co-design," *Circuits, Systems, and Power Electronics,* p. 23, 2022.

[6] B. Liu *et al.*, "Frequency-Domain Inference Acceleration for Convolutional Neural Networks Using ReRAMs," *IEEE Transactions on Parallel and Distributed Systems,* 2023.

[7] R. Chen, "Activity-Scaling SAR with Direct Hybrid Encoding for Signed Expressions for AIoT Applications," Massachusetts Institute of Technology, 2021.

[8] R. Chen, H. Kung, A. Chandrakasan, and H.-S. Lee, "A bit-level sparsity-aware SAR ADC with direct hybrid encoding for signed expressions for AIoT applications," in *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, 2022, pp. 1-6.

[9] J. Liu, B. Cheng, Z. M. Enciso, S. Davis, and N. Cao, "CIPUF: Towards On-chip Learnable Anomaly Detection with Compute-In-PUF Architecture," in *Proceedings of the 29th ACM/IEEE International Symposium on Low Power Electronics and Design*, 2024, pp. 1-6.

[10] R. Chen, A. Chandrakasan, and H.-S. Lee, "Sniff-sar: A 9.8 fj/c.-s 12b secure adc with detectiondriven protection against power and em side-channel attack," in *2023 IEEE Custom Integrated Circuits Conference (CICC)*, 2023: IEEE, pp. 1-2.

[11] R. Chen, H. Wang, A. Chandrakasan, and H.-S. Lee, "RaM-SAR: a low energy and area overhead, 11.3 fj/conv.-step 12b 25ms/s secure random-mapping SAR ADC with power and EM side-channel attack resilience," in *2022 IEEE Symposium on VLSI Technology and Circuits (VLSI Technology and Circuits)*, 2022: IEEE, pp. 94-95.

[12] R. Chen, "Analog-to-Digital Converters for Secure and Emerging AIoT Applications," Massachusetts Institute of Technology, 2023.

[13] K. P. Seng and L.-M. Ang, "Embedded intelligence: State-of-the-art and research challenges," *IEEE Access,* vol. 10, pp. 59236-59258, 2022.