University of Florida
AI Policy Guide #1

AI for Microelectronics Security:

National Security Imperatives for the Digital Age

Mark Tehranipoor and Farimah Farahmandi

Electrical & Computer Engineering Department
University of Florida

Recommendations for U.S. Leadership in AI Microelectronics Security

The rapid progress of Artificial intelligence (AI) introduces important new opportunities to enhance the security of the microelectronics that drive modern life. These include improving cryptography, increased protection against a diversity of threats and enhanced detection of hacks and malicious intrusions.

However, AI also introduces challenges, such as biases from training data, increased demand for electricity and other resources, and new vulnerabilities to adversarial attacks. **In response, the United States should position itself as the leading global hub for secure AI knowledge.** By investing strategically to make AI microelectronics security a national strength, the U.S. can enhance its current leadership in this domain — and secure an edge as AI becomes ever more important to quantum computing and other future-forward technologies.

We recommend five strategies to advance U.S. leadership:

1) **Deepen investment in AI-driven microelectronics security.** Increasing investment in the integration of AI into microelectronics will help the U.S. further its leadership role, foster innovation and drive job creation. Further, joining academia, industry and government in this effort will help protect critical public and private infrastructure.

2) **Lead the effort to establish national and international standards**. Creating standards for securing the integration of AI into hardware systems is a key global need. These standards should include robust testing, certification processes and transparency requirements. The National Institute of Standards is uniquely positioned to lead this effort.

3) **Promote public-private partnerships**. The U.S. should welcome and encourage collaboration between government agencies and private-sector innovators to accelerate the development and deployment of secure AI hardware systems.

4) **Enhance integration with legacy systems.** It's important in this relatively early stage in AI deployment to develop solutions that bridge AI with legacy systems. U.S. prominence in this effort will minimize the vulnerabilities and security gaps that threaten a seamless transition.

5) **Strengthen ethical and privacy guidelines.** The U.S. should establishe comprehensive ethical guidelines and oversight mechanisms to address ethical and privacy concerns, which will help open the path to widespread of this technology.

In short, we recommend that the U.S. embrace the role of leader and global center for the integration of AI into microelectronics -- enhancing the nation's leadership in semiconductors, safeguarding its critical infrastructure, and becoming the world's hub for AI knowledge and development.

Contact:
Mark Tehranipoor, Chair, UF Electrical and Computer Engineering, HWCOE - tehranipoor@ece.ufl.edu
Sarah Mathias, UF Federal Relations – smathias@ufl.edu

AI for Microelectronics Security: National Security Imperatives for the Digital Age

Mark Tehranipoor and Farimah Farahmandi
ECE Department, University of Florida

Executive Summary

Artificial Intelligence (AI) has emerged as a transformative force in microelectronics security, addressing complex challenges through advanced capabilities like threat detection, anomaly analysis, and real-time adaptation. AI applications in microelectronics security span detecting malicious change, security verification, enhancing cryptographic systems, and mitigating side-channel attacks to name a few. Additionally, AI-driven solutions contribute to proactive threat modeling and dynamic defense mechanisms, enabling robust protection against evolving threats.

Despite its benefits, AI integration introduces operational, technical, and ethical challenges, including biases in training data, interpretability issues, and vulnerabilities to adversarial attacks. High resource demands and integration hurdles with legacy systems further complicate AI adoption. Policymakers must address these challenges through standardized regulations, auditability mandates, and public-private partnerships.

The United States must prioritize AI-driven microelectronics security to maintain its global technological leadership in semiconductors. Given the offensive and defensive nature of AI in cyber/hardware security domain, strategic investments can foster innovation, drive job creation, and protect critical infrastructure while positioning the U.S. as a hub for secure AI technologies. Future trends point to AI's role in quantum computing and secure semiconductor design, underscoring its potential to redefine the landscape of microelectronics security.

A balanced approach to innovation, risk mitigation, and regulatory alignment is critical for realizing AI's full potential in safeguarding nation's critical infrastructures and systems.

1. Introduction

The artificial intelligence (AI) has been experiencing an unprecedented growth, driven by the rapid advancements in its capabilities and diverse applications. Generative AI, in particular, has seen a widespread adoption across industries, leading to a remarkable increase in market share. According to Bloomberg, the generative AI market is projected to reach $1.3 trillion by 2032, with a compound annual growth rate (CAGR) of 42% [1]. This explosive growth has positioned AI as one of the most lucrative and transformative sectors in the global economy.

This expansion has significantly benefited AI hardware companies, notably NVIDIA, Broadcom, and AMD, which have emerged as market leaders. A recent report by *Visual Capital* on semiconductor market capitalization in January 2025 highlights this trend. NVIDIA now holds the highest market capitalization at $3.4 trillion, followed by Broadcom at $1.1 trillion and AMD at $199 billion [2]. The rapid rise of these companies is largely attributed to their production of cutting-edge AI hardware, enabling the acceleration of AI applications across various domains.

Modern system-on-chip (SoC) designs have played a pivotal role in advancing AI hardware capabilities. The transistor density in SoCs has increased exponentially, enabling the integration of enhanced

functionalities and performance. For example, NVIDIA's Blackwell-based B100 accelerator GPU, introduced in 2024, features an astounding 208 billion transistors, while Apple's M2 Ultra SoC boasts 134 billion transistors. These advancements not only bring increased computational power but also introduce heightened complexity, making these systems more susceptible to security vulnerabilities.

Hence, microelectronics and semiconductor security has emerged at the forefront of safeguarding critical systems, including AI hardware, across multiple sectors such as national defense, energy infrastructure, cloud computing and healthcare. A recent study by DARPA as part of its System Security Integration Through Hardware and Firmware (SSITH) program shows that 43% of the 6,488 recorded vulnerabilities in 2015 were identified as software-assisted hardware vulnerabilities. The SSITH program projected that addressing these hardware vulnerabilities at their source could have prevented 31% of these recorded vulnerabilities, thereby eliminating a significant portion of software vulnerabilities. Hence, as threats targeting hardware systems grow in complexity, artificial intelligence (AI) itself is emerging as a revolutionary solution to enhance microelectronics security mechanisms. Its ability to analyze intricate datasets, predict vulnerabilities, and adapt defenses in real-time positions AI as an indispensable asset in addressing modern cyber/hardware security challenges.

AI's capabilities have redefined the landscape of semiconductor design and security by automating tasks like detecting information leakage, hardware Trojans, counterfeit chips, and side-channel vulnerabilities. Machine learning (ML) and deep learning (DL) have proven effective for analyzing anomalies in hardware systems, while large language models (LLMs) enhance security verification and reduce manual labor. Further, reinforcement learning (RL) has proven its value in generating effective test patterns for silicon verification. Predictive threat modeling and AI-driven dynamic defense systems add another layer of robustness, enabling proactive responses to evolving attack vectors.

However, the integration of AI into microelectronics security is not without challenges. Operational issues like biases in training data, model robustness, sensitivity of the silicon data, and interpretability hinder AI's reliability and wide-spread adoption. Adversarial attacks and data poisoning further expose vulnerabilities in AI-driven systems. Moreover, the resource-intensive nature of AI adoption, coupled with the complexity of integrating it into legacy infrastructure, presents significant barriers.

To mitigate these risks, the adoption of clear policies and standards is essential. Transparency, accountability, and public-private partnerships can establish a responsible and efficient implementation of AI in semiconductor design and security. Establishing national and international standards will promote interoperability and guide AI development across sectors.

As the United States seeks to maintain its global leadership in technology, AI-driven microelectronics security offers a strategic advantage. By investing in research, fostering innovation, and addressing integration challenges, the U.S. can position itself at the forefront of secure AI technologies, safeguarding critical systems and ensuring long-term economic and strategic benefits.

2. A Game-Changer in Microelectronics Security

The integration of AI into semiconductors has emerged in enormous advancements, redefining the way integrated circuits are designed, verified, and safeguarded against evolving threats. AI's capabilities in analyzing complex datasets, identifying patterns, and adapting to rapidly changing scenarios make it a pivotal force in addressing the microelectronics security challenges. This section delves into the dual perspective of AI as both a tool for enhancing microelectronics security and as a domain requiring protection to ensure robust and secure deployment.

2.1 AI in Microelectronics Security

- **AI Capabilities and Relevance:** The convergence of AI algorithms has opened new avenues for solving intricate microelectronics security problems. These technologies excel in tasks that require threat classification, anomaly detection, and decision-making under uncertainty. For instance:
    - **Machine Learning (ML):** Effective for classifying malicious activities in hardware, such as detecting subtle patterns indicative of information leakage and anomalies [3].
    - **Deep Learning (DL):** Offers advanced capabilities for processing complex datasets, such as power traces for side-channel analysis, with enhanced precision [4, 5].
    - **Reinforcement Learning (RL):** Enables adaptive detection and defense strategies, where systems can learn optimal responses to various attack scenarios over time [6].
    - **Large Language Model (LLM):** Effective for analyzing and understanding design documents and programming languages, enabling the detection of security bugs [7]. LLMs enhance security verification coverage while reducing the need for manual intervention.
- **Transformative Applications:** AI's transformative potential is evident in several critical microelectronics security applications as described below:
    - **Automating Verification Processes:** AI-powered verification tools streamline the design lifecycle by automating functional and formal verification processes. Large language Model (LLM)-based systems can translate specifications into security properties [11], while ML models predict likely design flaws, accelerating debugging and validation [12].
    - **Strengthening Cryptographic Systems:** AI aids in designing robust cryptographic primitives by identifying potential vulnerabilities in algorithms and suggesting optimizations to enhance security. For example, generative adversarial networks (GANs) can simulate attacks, aiding in testing cryptographic robustness [10].
    - **Detecting Malicious Chips:** AI models analyze physical and functional characteristics of integrated circuits to identify anomalies that may indicate malicious modification [3, 14]. Techniques like supervised learning and autoencoders have shown promise in classifying genuine and counterfeit chips [9].
    - **Predictive Threat Modeling:** Leveraging predictive models, AI can proactively identify potential vulnerabilities in hardware designs, enabling developers to implement countermeasures before exploitation occurs.
    - **Side Channel Analysis:** AI models, particularly deep learning techniques, can process side-channel data such as power consumption, electromagnetic radiation, and timing information to detect patterns indicative of potential leakage. By automating the analysis of side-channel traces, AI improves the accuracy and speed of identifying leakage paths in the electronic circuits, enabling the development of effective countermeasures to mitigate side-channel attacks [4, 5, 13].
    - **Dynamic Defense Mechanisms:** AI-driven defense mechanisms adapt in real-time to evolving threats, such as dynamic runtime monitoring and anomaly detection systems for zero-day attacks.

2.2 Secure AI Hardware

- **Security of AI/ML Models:** As AI models become integral to microelectronics security and other domains, they themselves become targets of adversarial attacks. Common threats include:

- **Adversarial Attacks:** Maliciously crafted inputs designed to mislead AI systems, such as perturbing data to cause incorrect classifications [15]. Defense mechanisms like adversarial training and input filtering have emerged to counteract such attacks.
- **Model Extraction and Data Poisoning:** Attacks that steal or corrupt AI models can compromise their integrity and security. Techniques like federated learning, differential privacy, and secure multi-party computation are being explored to mitigate these risks [16].

- **AI Accelerator/AI Hardware Security:**The increasing adoption of specialized hardware accelerators for AI, such as GPUs and TPUs, necessitates secure design principles:
  - **Trustworthy Hardware Design:** Ensuring that AI hardware is free from vulnerabilities, such as backdoors or tampered firmware, is critical. Techniques like formal verification and dynamic runtime checks are employed to enhance hardware trustworthiness.
  - **Side-Channel Attack Mitigation:** AI hardware is susceptible to side-channel attacks that exploit power, timing, or electromagnetic emissions to infer model operations. Designing accelerators with noise-injection techniques and constant-time operations can minimize these risks [17].
  - **Secure Deployment of AI Models:** Embedding AI models in hardware requires secure execution environments. Technologies like trusted execution environments (TEEs) [18] and hardware-level encryption can be used to ensure that AI operations remain confidential and tamper-proof.

AI has demonstrated unprecedented potential in reshaping the microelectronics design and security landscape, addressing challenges that were previously infeasible due to computational or analytical limitations. Its ability of process automation, threats prediction, and real-time adaptive defenses makes it a game-changer in the domain. However, as AI becomes deeply embedded in security paradigms, designing the robust and secure AI hardware and models are equally critical. A concerted effort involving academia, industry, and government is essential to harness the full potential of AI while mitigating associated risks.

3. Risks and Challenges in Applying AI to Microelectronics Security

While the vulnerabilities in AI models and hardware are in place, its application to microelectronics security also introduces a range of risks and challenges. These stem from various technical, operational, and ethical factors. This section outlines key challenges under several categories.

3.1 Operational Challenges

AI systems face several operational challenges, including robustness, interpretability, and susceptibility to malicious exploitation.

- **Model Robustness:**
  - ***Robustness*** refers to an AI model's ability to maintain performance under unforeseen or varied conditions. AI models trained on specific datasets may falter when exposed to scenarios outside their training scope, thereby weakening the security mechanisms they are designed to protect. This is particularly concerning in microelectronics security, where diverse and dynamic threat environments are common. Enhancing robustness requires designing models capable of generalizing across a wide array of operational contexts as well as frequent retraining and updating the models are required.
  - ***Bias*** in training data is another concern. AI systems may inherit and amplify biases from imbalanced or incomplete datasets, leading to inaccurate decisions. In hardware security, this could result in false positives and false negatives, such as incorrectly flagging benign components as threats or missing actual vulnerabilities. For example, an AI system trained predominantly on a dataset from a specific design or manufacturer may perform poorly on

components from other sources. Addressing these biases through diversified datasets and rigorous testing is crucial for achieving reliable AI performance.

- **Interpretability:**
  AI systems, particularly deep learning models, are often criticized for their "black-box" nature, meaning they provide little to no explanation for their decisions. In microelectronics security, this lack of interpretability undermines trust and hinders validation. For example, if an AI system identifies a component as compromised but fails to explain why, security professionals may find it difficult to verify or act on its findings. This lack of transparency complicates auditability and accountability, especially in high-stakes applications like national defense or healthcare, where errors can have catastrophic consequences. Moreover, accountability issues arise when AI systems make incorrect decisions, such as failing to detect hardware compromises. Without clear insights into the decision-making process, determining responsibility becomes challenging.

3.2 Complexity and Resource Requirements

AI systems, particularly those based on deep learning or LLM, demand substantial computational resources, data, and energy. Developing AI models for microelectronics security involves extensive data collection, cleaning, and securing—an operational burden that smaller organizations may struggle to manage. Training AI models to detect hardware vulnerabilities is time-consuming and requires significant computational infrastructure, leading to high costs. For applications in national defense or critical infrastructure, these resource demands are particularly challenging, as failure in these contexts can have severe consequences.

3.3 Integration with Existing Security Infrastructure

Integrating AI with legacy microelectronic design tools or systems poses significant challenges. Many traditional systems rely on manual processes or rule-based approaches that are incompatible with modern AI-driven solutions. Compatibility issues during integration can create vulnerabilities and security gaps. For instance, automating microelectronic design bug detection with AI may lead to inconsistencies if existing monitoring protocols are misaligned with the capabilities of AI systems. This challenge is especially pronounced in defense systems, where outdated hardware is common, and upgrading to accommodate AI technologies can be resource intensive.

3.4 Ethical and Privacy Concerns

The application of AI in microelectronics security raises ethical and privacy concerns, particularly in handling sensitive data.

- **Data Privacy:** Hardware security systems often process confidential information, such as encryption keys, user credentials, and semiconductor and critical infrastructure parameters. AI models require vast datasets for training, which may include sensitive or proprietary information. Data breaches or unauthorized access to these datasets could expose sensitive data, undermining trust in AI-driven security tools.
- **Ethical Oversight:** AI systems operating without sufficient human oversight may overreach, enabling unauthorized surveillance or infringing on user privacy rights. Establishing ethical guidelines and boundaries is critical to ensure that robust security measures do not come at the expense of individual freedoms.

4. Role of AI in National Security

AI integration into microelectronics security has profound implications for national security, where protecting critical infrastructure, defense systems, and sensitive information is paramount. Modern security threats intersect with broader concerns, including military capabilities, energy infrastructure, healthcare systems, and financial markets.

- **Critical Infrastructure Protection:** Hardware vulnerabilities can undermine critical infrastructure, such as power grids, telecommunications, and water supply systems. Exploited

vulnerabilities could cause widespread disruptions. For example, a cyberattack on a power grid might compromise control systems by exploiting unprotected hardware, leading to cascading effects on healthcare and emergency services. AI-driven tools must identify and mitigate sophisticated attacks targeting these vulnerabilities.

- **Defense Systems and Autonomous Warfare:** U.S. defense ecosystems rely on advanced microelectronics platforms, including electronic components used in military, satellites, and autonomous vehicles. Exploiting vulnerabilities in these systems could have catastrophic consequences, such as disrupting intelligence or navigation capabilities. Adversarial AI targeting hardware systems further heightens risks, requiring robust AI-driven measures to protect sensitive technologies. A 2024 report by the AI Now Institute emphasized the risks of commercial AI used in military contexts [20].
- **Broader Geopolitical Implications:** AI and hardware security are critical frontiers in geopolitical competition. Leading in AI integration for microelectronics security offers strategic advantages, safeguarding intellectual property and maintaining technological supremacy. For example, the U.S. faces ongoing threats from supply chain vulnerabilities, emphasizing stringent AI-driven measures to mitigate these risks while countering evolving tactics by rival nations.

5. Policy and Regulation for Secure AI in Hardware Systems

As artificial intelligence (AI) becomes integral to microelectronics security, implementing robust policies and regulations is critical to ensure safe, reliable, and ethical AI applications. A comprehensive framework addressing standards, transparency, accountability, and collaboration is essential to mitigate risks and enhance trust in AI-driven hardware systems.

5.1 Need for Standards

Establishing national and international standards is paramount for guiding the development and deployment of secure AI in hardware systems. These standards should encompass:

- **Design and Implementation:** Defining security benchmarks for AI algorithms and hardware systems to minimize vulnerabilities.
- **Interoperability:** Ensuring AI tools can seamlessly integrate with existing hardware security infrastructure across different sectors.
- **Testing and Certification:** Mandating rigorous testing and certification processes to verify the security and reliability of AI systems in diverse operational contexts.

International collaboration is essential to develop globally recognized standards that address cross-border hardware supply chains and cyber threats. Organizations like the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) play pivotal roles in creating frameworks to guide AI applications in hardware security.

5.2 Transparency and Accountability

Transparency and accountability are foundational to the secure deployment of AI in hardware systems. Policymakers should mandate:

- **Auditability:** AI systems must include mechanisms for independent auditing to assess their decision-making processes, security features, and operational effectiveness. Audits should focus on identifying potential biases, vulnerabilities, and adherence to security protocols.
- **Explainability:** Developers must design AI systems capable of providing clear and interpretable explanations for their decisions (at least through their documentations), especially in critical applications such as defense or healthcare.

- **Liability Frameworks:** Establishing clear guidelines to determine accountability in cases where AI systems fail, or cause harm is important for building a trustworthy and responsible relationship among stakeholders.

By embedding transparency into the design and use of AI systems, organizations can address concerns related to bias, misuse, and reliability while fostering greater trust among users and stakeholders.

5.3 Public-Private Partnerships

Encouraging collaboration between government agencies and private-sector innovators is critical to accelerating the development of secure AI technologies. Public-private partnerships can:

- **Drive Innovation:** Facilitate research and development of cutting-edge AI tools tailored for hardware security applications.
- **Share Best Practices:** Promote knowledge exchange and the dissemination of successful strategies to secure AI systems.
- **Develop Incentives:** Governments can provide funding, tax incentives, or grants to encourage private entities to prioritize secure AI development.

Such partnerships ensure that public institutions leverage private sector expertise while aligning innovations with national security and public interest goals.

Comprehensive policies and regulations that establish standards, promote transparency, and foster collaboration are vital for the secure integration of AI in hardware systems. By addressing these areas, governments and industries can create a resilient framework to protect critical hardware systems while enabling the responsible adoption of AI technologies.

6. Future Trends: The Vision for AI-Driven Microelectronics Security

The future of hardware security lies at the intersection of technological advancements in artificial intelligence (AI), quantum computing, and national infrastructure development. AI is set to redefine the landscape of hardware security by addressing challenges in cryptographic resilience, design innovation, and global competitiveness. This section envisions a transformative trajectory for AI-driven hardware security, ensuring robust systems in an increasingly complex threat environment.

6.1 AI and Quantum Computing: A Strategic Alliance

The synergy between AI and quantum computing holds immense potential for the future of hardware security. Quantum computers, with their unparalleled computational capabilities, present both challenges and opportunities for cryptographic systems [21]. On one hand, they pause a threat to traditional encryption methods, such as ECC and RSA, which are based on the computational challenge of factoring large numbers or solving discrete logarithmic problems. On the other hand, AI can be instrumental in developing quantum-resistant algorithms, like lattice-based or hash-based cryptography, ensuring resilience against quantum attacks [22].

AI can also optimize quantum key distribution (QKD) systems by identifying and mitigating vulnerabilities in real-time [23]. Machine learning models could be used to enhance the efficiency of QKD protocols, detect eavesdropping, and dynamically adapt encryption strategies to ensure secure communication. The collaboration of AI and quantum technologies is pivotal for future-proofing critical infrastructure against emerging threats.

6.2 AI-Augmented Microelectronic Design: Building Security into the Core

AI is poised to revolutionize the design and manufacturing of inherently secure hardware systems. By leveraging generative design techniques, AI can create hardware architectures optimized for both performance and security. For instance:

- AI-driven design tools can automatically incorporate countermeasures against side-channel attacks, such as power or timing anomalies.

- AI based algorithms can simulate attack scenarios during the design phase, allowing developers to identify vulnerabilities and implement defenses proactively.
- Automated hardware verification frameworks, powered by LLM and deep learning, can streamline the process of ensuring compliance with security standards, reducing design errors and accelerating time-to-market.

This shift towards a proactive hardware design approach ensures that security is becomeing an integral part of hardware design.

6.3 National AI Infrastructure: Leadership in Global Microelectronics Security

To position itself as a global leader in hardware security, the United States must spearhead a national initiative that integrates AI into its cybersecurity and hardware design ecosystems. A dedicated "AI Hardware Security Initiative" could focus on:

- Establishing AI-driven cybersecurity research hubs to foster innovation in secure hardware technologies, both for (1) using AI in secure hardware design, and (2) developing secure AI hardware.
- Promoting collaboration between academia, industry, and government to develop cutting-edge tools for hardware security.
- Ensuring a robust talent pipeline by investing in education and training programs that equip the next generation of engineers and researchers with AI and cybersecurity expertise.

This initiative would not only solidify U.S. leadership in hardware security but also act as a deterrent to adversaries seeking to exploit vulnerabilities in critical infrastructure.

7. Economic and Strategic Impacts

The adoption of AI in hardware security is poised to generate profound economic and strategic benefits, creating opportunities for innovation, job growth, and enhanced global competitiveness. By integrating AI into hardware security systems, organizations and governments can address emerging threats, optimize operational efficiencies, and solidify their positions in the global technology arena. This section explores the economic and strategic implications of AI-driven hardware security.

7.1 Cost-Benefit Analysis: Economic Advantages of AI in Hardware Security

AI's application in hardware security offers significant cost-saving benefits by reducing breaches and enhancing operational efficiency. Cybersecurity breaches, especially in critical hardware systems, incur substantial financial losses due to downtime, data theft, and compromised trust. AI-driven systems mitigate these risks by:

- **Predicting and Preventing Attacks:** AI-powered threat detection and anomaly identification systems significantly reduce the probability of successful attacks, saving organizations from costly incidents.
- **Optimizing Resource Allocation:** Automating hardware security processes, such as verification and monitoring, allows for faster identification of vulnerabilities, minimizing reliance on time-intensive manual efforts.
- **Long-Term Savings:** Although the initial investment in AI-driven hardware security might be high, the reduction in financial losses due to breaches and the efficiency gains result in long-term economic benefits. For example, McKinsey estimates that AI-driven security solutions can cut costs related to fraud and cyberattacks by up to 30% annually in some industries [24].

7.2 Job Creation: Fostering New Opportunities in AI and Security

The integration of AI into hardware security opens avenues for job creation across various domains. New roles are emerging that combine expertise in AI, cybersecurity, and hardware design, including:

- **AI Security Engineers:** Professionals responsible for designing and implementing AI-driven security protocols in hardware systems.
- **Threat Intelligence Analysts:** Specialists leveraging AI to analyze attack patterns and recommend proactive countermeasures.
- **Data Scientists in Security:** Experts in training AI models with robust datasets to detect anomalies and secure hardware against evolving threats.

Additionally, the rise of AI in security underscores the need for reskilling and upskilling existing personnel to operate and maintain these advanced systems. Investing in education and training programs will ensure a steady pipeline of skilled professionals to support this growing sector.

7.3 Global Competitiveness: Strategic Importance for U.S. Leadership

Investing in AI-driven hardware security is critical for the United States to maintain its leadership in the global tech landscape. As nations compete for dominance in cybersecurity and AI, robust AI-powered security systems will be essential to protect critical infrastructure, intellectual property, and technological innovation.

Strategically, a strong AI and hardware security ecosystem enhances national security by safeguarding military and government assets from adversaries. Economically, it positions the U.S. as a hub for cutting-edge security technologies, attracting global talent and investments. Initiatives such as a national AI-driven hardware security program would not only protect domestic interests but also provide exportable technologies that strengthen alliances and partnerships worldwide.

The economic and strategic impacts of AI in hardware security extend beyond individual organizations to shape national and global dynamics. By reducing breaches, fostering job creation, and maintaining global competitiveness, AI-driven hardware security becomes a pivotal force for economic resilience and technological sovereignty. Proactive investments in this domain will ensure the United States remains a leader in both cybersecurity innovation and global technology influence.

8. Conclusion: Balancing Innovation and Security

Artificial intelligence represents a paradigm shift in hardware security, offering unparalleled capabilities for protecting sensitive systems against evolving threats. Its transformative applications include anomaly detection, cryptographic resilience, and automated verification, making it indispensable in modern hardware security practices. However, addressing challenges like biases, adversarial vulnerabilities, and integration complexities is essential for AI's reliable deployment.

A concerted effort involving academia, industry, and government is necessary to balance innovation with risk mitigation. By establishing standards, fostering collaboration, and driving strategic investments, AI-driven hardware security can ensure the resilience of critical systems, reinforcing technological leadership and global competitiveness.

References

[1] https://www.bloomberg.com/company/press/generative-ai-to-become-a-1-3-trillion-market-by-2032-research-finds/
[2] https://www.visualcapitalist.com/the-value-of-the-global-semiconductor-industry-in-one-giant-chart/
[3] A. Waksman et al., "Hardware Trojan Detection using Machine Learning Techniques," IEEE Transactions on Computer-Aided Design, 2019.
[4] Hospodar, G., Gierlichs, B., De Mulder, E., Verbauwhede, I., & Vandewalle, J. (2011). Machine learning in side-channel analysis: a first study. Journal of Cryptographic Engineering, 1(4), 293-302.
[5] Regazzoni, F., Bhasin, S., Pour, A. A., Alshaer, I., Aydin, F., Aysu, A., ... & Yli-Mäyry, V. (2020, November). Machine learning and hardware security: Challenges and opportunities. In *Proceedings of the 39th International Conference on Computer-Aided Design* (pp. 1-6).

[6] Mondol, N. N., Vafei, A., Azar, K. Z., Farahmandi, F., & Tehranipoor, M. (2024, March). RL-TPG: automated pre-silicon security verification through reinforcement learning-based test pattern generation. In *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 1-6). IEEE.
[7] Saha, D., Tarek, S., Yahyaei, K., Saha, S. K., Zhou, J., Tehranipoor, M., & Farahmandi, F. (2024). Llm for soc security: A paradigm shift. *IEEE Access*.
[8] S. Bhunia and M. Tehranipoor, "Hardware Security: A Hands-On Learning Approach," Springer, 2019.
[9] Asadizanjani, N., Tehranipoor, M., & Forte, D. (2017). Counterfeit electronics detection using image processing and machine learning. In Journal of physics: conference series (Vol. 787, No. 1, p. 012023). IOP Publishing.
[10] Dutta, I. K., Ghosh, B., Carlson, A., Totaro, M., & Bayoumi, M. (2020, October). Generative adversarial networks in security: A survey. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0399-0405). IEEE.
[11] Ayalasomayajula, A., Guo, R., Zhou, J., Saha, S. K., & Farahmandi, F. (2024, September). LASP: LLM Assisted Security Property Generation for SoC Verification. In Proceedings of the 2024 ACM/IEEE International Symposium on Machine Learning for CAD (pp. 1-7).
[12] Pan, Z., & Mishra, P. (2022). A survey on hardware vulnerability analysis using machine learning. IEEE Access, 10, 49508-49527.
[13] Picek, S., Heuser, A., Jovic, A., Ludwig, S. A., Guilley, S., Jakobovic, D., & Mentens, N. (2017, May). Side-channel analysis and machine learning: A practical perspective. In 2017 International Joint Conference on Neural Networks (IJCNN) (pp. 4095-4102). IEEE.
[14] Huang, Z., Wang, Q., Chen, Y., & Jiang, X. (2020). A survey on machine learning against hardware trojan attacks: Recent advances and challenges. IEEE Access, 8, 10796-10826.
[15] Pan, Z., & Mishra, P. (2023). Ai trojan attack for evading machine learning-based detection of hardware trojans. IEEE Transactions on Computers.
[16] Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5), 1-36.
[17] D. S. Ha et al., "Side-Channel Attack Resilience of AI Accelerators," IEEE Design & Test, 2022.
[18] Wang, Q., Zhou, L., Bai, J., Koh, Y. S., Cui, S., & Russello, G. (2023). HT2ML: An efficient hybrid framework for privacy-preserving Machine Learning using HE and TEE. Computers & Security, 135, 103509.
[19] R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems," Wiley, 2020.
[20] Khlaaf, H., West, S. M., & Whittaker, M. (2024). Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting. *arXiv preprint arXiv:2410.14831*.
[21] Käppler, S. A., & Schneider, B. (2022). Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms. *Proceedings of the Society*, *84*, 61-71.
[22] Darzi, S., & Yavuz, A. A. (2024). PQC meets ML or AI: Exploring the Synergy of Machine Learning and Post-quantum Cryptography. *Authorea Preprints*.
[23] Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*, *15*(1), 4.
[24] McKinsey Global Institute, “The Economic Potential of AI in Security,” 2022

ABOUT THE AUTHORS ...

Mark M. Tehranipoor is currently the Sachio Semmoto Chair of the Department of Electrical and Computer Engineering and the Intel Charles E. Young Preeminence Endowed Chair in Cybersecurity at the University of Florida. A fellow of IEEE, ACM, and NAI, he served as the founding Director for the Florida Institute for Cybersecurity Research from 2015-2022, and is currently serving as Co-director for the AFOSR/AFRL Center of Excellence on Enabling Cyber Defense in Analog and Mixed Signal Domain (CYAN), and Co-Director for the National Microelectronic Security Training Center (MEST). Dr. Tehranipoor has published numerous journal articles and refereed conference papers and has delivered 230+ invited talks and keynote addresses. In addition, he has 24 patents issued, 28 pending invention disclosures, and has published 19 books of which two are textbooks. His projects have been sponsored by 50+ companies and Government agencies For more details, see www.Tehranipoor.ece.ufl.edu

Dr. Farimah Farahmandi is the Wally Rhines Endowed Professor in Hardware Security in the Department of Electrical and Computer Engineering at the University of Florida. She serves as the Associate Director of the Florida Institute for Cybersecurity (FICS) at UF, where her research focuses on hardware security verification, formal methods, fault-injection attack analysis, and post-silicon validation and debug, resulting in 7 books and over 140 publications in these fields. Dr. Farahmandi's research has been sponsored by a variety of leading companies and government agencies. She was recognized with the ACM/IEEE DAC Under 40 Innovators Award (2024). She also received the prestigious Young Faculty Award from SRC (2022) and an NSF CAREER Award.

The **University of Florida** has become a unique national resource in AI and applications through its university-wide AI initiative that features:

- The nation's fastest university-owned supercomputer (the new NVIDIA DGX B200 SuperPOD)
- AI Across the Curriculum – incorporating AI into every college and discipline at UF so that every student can become AI-literate, AI-competent, or AI-expert in the context of their chosen major and occupation
- Research into applications of AI in multiple domains, from agriculture to business to the physical sciences to engineering to medicine
- Commitment to sharing UF's expertise in computing, curriculum, and research with universities around the nation that want to begin their own AI journey

For more information, check out www.ai.ufl.edu