Neuromorphic-Enabled Security for IoT

Soheil Salehi*, Tyler Sheaves*, Kevin Immanuel Gubbi*, Sayed Arash Beheshti†, Sai Manoj P D†,
Setareh Rafatirad*, Avesta Sasan*, Tinoosh Mohsenin‡, and Houman Homayoun*
*Electrical and Computer Engineering Department, University of California Davis, Davis, CA 95616
†Electrical and Computer Engineering Department, George Mason University, Fairfax, VA 22030
‡Computer Science and Electrical Engineering Department, University of Maryland Baltimore County, Baltimore, MD 21250
*{ssalehi, tsheaves, kgubbi, srafatirad, asasan, hhomayoun}@ucdavis.edu;†{sbehesht, spudukot}@gmu.edu;‡tinoosh@umbc.edu;

2022 20th IEEE Interregional NEWCAS Conference (NEWCAS) | 978-1-6654-0105-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/NEWCAS52662.2022.9842256

***Abstract*—Hardware attacks on resource-constrained IoT devices are evolving rapidly. These threats have become a significant concern due to the increase of IoT devices used in applications such as human health, public transportation, autonomous vehicles, defense, and environmental monitoring. Recent studies show the potential of using deep learning to steal user data by monitoring hardware features and side-channel information. Additionally, machine learning (ML) approaches have recently been widely adopted in IoT applications. Advanced platforms demand novel circuits and architectures that can yield several orders of magnitude improvements in energy consumption in ML applications while maintaining consistent accuracy. Neuromorphic computing leveraging digital, mixed-signal, and analog processing has been shown to be a promising candidate due to energy, wire count, and area efficiency. Thus, an effective cutting-edge hardware approach for neuromorphic computing to perform rapid, energy-efficient, and secure supervised and unsupervised learning at the IoT edge is sought. Here we discuss the challenges and potential benefits of using neuromorphic computing modules for security at the IoT edge. The intersection of neuromorphic computing and hardware security serves many IoT domains in mission-critical and privacy-preserving applications.**

***Index Terms*—Neuromorphic Computing, Machine Learning, Hardware Security, IoT, Supply Chain Security, Side-Channel Attack, Reverse Engineering.**

I. Introduction

The number of Internet of Things (IoT) devices has been estimated to surpass 75 billion by 2025 [1]. Furthermore, state-of-the-art hardware attacks on resource constrained IoT devices are evolving very rapidly [1], [2]. Security threats have become a significant concern due to the rapid increase of IoT devices used in applications such as human health, public transportation, autonomous vehicles, and environmental monitoring. For instance, due to limited resources within IoT devices, such as implantable medical devices, adversaries can gain access to private patient information or cause malfunction and disrupt the function of the device, which in case of medical implants can have life-threatening consequences [2]. Moreover, recent advancement in the hardware security community have shown that advanced threats and attacks involving IoT cannot be effectively mitigated using conventional rule-based defense solutions [3]. Additionally, inter- and intra-connectivity of IoT devices leaves them vulnerable to network security threats, such as network intrusion attempts [3]. Thus, novel effective mitigation mechanisms are sought for on-line and accurate threat detection using unsupervised Machine Learning (ML) approaches. A recent study shows high accuracy of detecting malware using ML based models [4]. An accuracy of 99.69% in detecting malware was achieved by [5]. Intrusion detection is another aspect of creating a secure IoT device. The work in [6] does a comprehensive study on ML based intrusion detection approaches.

Furthermore, one of the main challenges in the field of ML is that Deep Learning (DL) approaches require significant computing power, energy consumption, and storage needs [3]. The computational demands of DL techniques in IoT devices have been studied by Venkataramani et al. in [7]. Hardware acceleration, approximate computing and emerging post-CMOS devices are approaches that can potentially lead to more energy-efficient embedded systems. Neuromorphic processing can provide high performance and low power ML platforms, which can be a promising candidate for learning and inference within resource constrained IoT edge devices [8]. Benefits of alternatives to von-Neumann architectures are sought for emerging applications such as IoT and hardware-aware intelligent edge devices, as well as the application of hardware-enabled security [3], [9]. Authors in [10] propose a brain-inspired architecture called Hierarchical Temporal Memory (HTM), that is capable of detection Hardware Trojans (HTs) during run-time without the need for a golden chip, a chip that is fabricated in a trusted facility and is assumed to have no HTs. ML-assisted approaches have also been introduced to keep up with the increasing demands of faster and efficient security assessment at run-time [11]. Thus, countermeasures are necessary to prevent and mitigate these powerful attacks.

In order to address the aforementioned need and to increase the security of IoT applications, the development of an effective neuromorphic platform using emerging beyond-CMOS memristive devices could bridge the efficiency gap, and allow for on-line learning and high accuracy and effective inference within an energy- and area-efficient, scalable, and reconfigurable hardware architecture. To advance the approaches previously proposed in the literature, a new class of neuromorphic chips, which enable high-throughput on-chip learning via established approaches for artificial neural network processing are required. Mixed-signal techniques combined with in-memory compute geared to the demands of neuromorphic processing can be combined in a field-programmable and run-time adaptable platform [12]–[15]. Utilization of reprogrammable weights within the neuromorphic chip architecture can realize adaptable precision and accuracy as well as increased security

978-1-6654-0105-0/22/$31.00 ©2022 IEEE

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:04:51 UTC from IEEE Xplore. Restrictions apply.

as elaborated in this work. This cross-cutting beyond-von Neumann view of ML is explored within the context of real-time decision-making from data observations within resource constraint IoT applications.

II. Background

Recent studies show potential of using DL to understand the underlying behavior of the hardware by monitoring features, such as Hardware Performance Counters (HPCs), and side-channel information, such as power, electromagnetic emission, heat, computational timing, memory accesses, etc. [16], [17]. Additionally, Integrated Circuit (IC) counterfeit attacks can attain information from the design by micro-probing the circuit to extract information about the layout and functionality of the design. Moreover, attackers can extract information regarding the design by inserting faults, such as bit flips, and observe the behavior of the circuit. On the other hand, previous works on non-von Neumann in-memory computing and signal processing using emerging beyond-CMOS devices have shown significant improvements in terms of area and energy-efficiency while maintaining comparable performance with conventional von Neumann computing approaches due to their near-zero standby power, non-volatility, high integration density, low-power operation, fabrication feasibility, and reduced data movement [12], [13], [15], [18]–[23].

Furthermore, Recent advances to hardware integration and realization of highly efficient analog computing approaches have inspired novel circuit and architectural-level innovations that consider device-level constraints for IoT applications wherein lifetime energy, device area, and manufacturing costs are highly constrained. Additionally, recently ML approaches have been widely used in IoT applications to increase security [24]–[26]. However, there is an increasing demand for novel circuits and architectures that can yield several orders of magnitude improvements in energy consumption of ML applications while maintaining high accuracy and security. Furthermore, neuromorphic computing leveraging analog processing has been shown to be energy, wire-count, and area efficient [27]. However, the pathways from its software simulation to realizable neuromorphic chips using mixed-signal approaches are underexplored. More recently, neuromorphic hardware architectures have been proposed that include custom silicon, such as IBM's TrueNorth [28] and Intel's Loihi [29], as well as some exploratory schemes using emerging devices such as spintronics, memristors, or phase-change devices as shown in Table I. In 2022, the automobile manufacturer Mercedes has incorporated BrainChip's Akida neuromorphic chip in their latest concept car called Vision EQXX. Mercedes has claimed that the use of neuromorphic computing has helped extending the range by reducing power dissipation[1]. Furthermore, in 2022 Samsung released the world's first Magnetic Random Access Memory (MRAM)-based In-Memory Computing

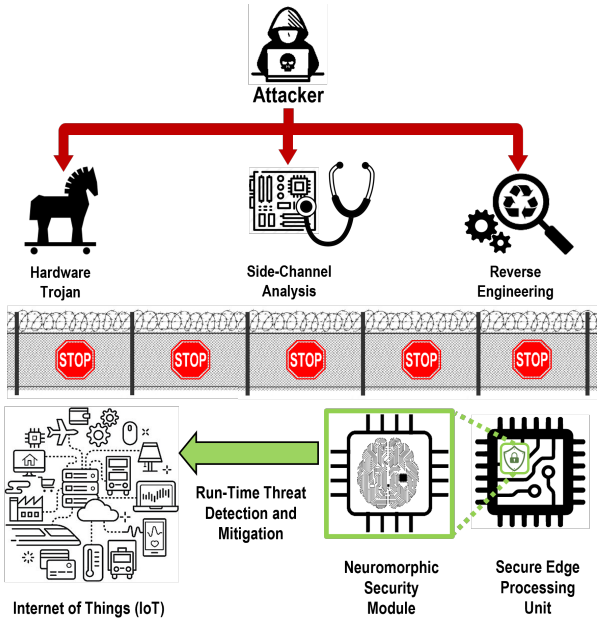

Fig. 1: Neuromorphic-Enabled Security for IoT

(IMC)[2]. These neuromorphic processors can achieve orders of magnitude energy-efficiency compared to traditional von-neumann computing approaches and are considered promising candidates for machine learning acceleration at the edge. The applications of the such neuromorphic-enebled security module spans mobile devices, autonomous vehicles, robotics, wearables, and so on [30].

III. Neuromorphic-Enabled Security for IoT

The advantages of mixed-signal processing on a single die to realize neuromorphic architectures could yield orders of magnitude reduction in energy consumption. A circuit-level-to-architecture-level approach is sought to integrate front-end signal processing and ML operations within a low-footprint reconfigurable fabric that enables mixed-signal processing. Using emerging technologies within IoT and neuromorphic circuits to utilize more effective intrinsic switching behaviors of the devices at-hand, reductions in energy and execution time can be achieved [24], [25]. Since die fabrication cost is a key constraint for IoT devices, in-the-field configuration can allow a single die to be optimized for multiple applications while avoiding the fabrication overhead costs. Therefore, technology-specific advantages of new emerging devices should be exploited for leveraging the cooperating benefits of well-established CMOS devices. Thus, we can leverage the new and powerful prospect of technology heterogeneity both at design-time and at run-time to develop energy-efficient, reliability-aware, and secure computing systems. In this paper, we explore the impact of an effective cutting-edge hardware approach for neuromorphic computing to perform rapid, energy-efficient, and secure supervised and

[1]https://www.eetimes.com/mercedes-applies-neuromorphic-computing-in-ev-concept-car/

[2]https://news.samsung.com/global/samsung-demonstrates-the-worlds-first-mram-based-in-memory-computing

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:04:51 UTC from IEEE Xplore. Restrictions apply.

unsupervised learning at the IoT edge. The applications of neuromorphic chips in IoT include but are not limited to secure and privacy-preserving IoT applications such as smart healthcare, autonomous vehicles, and smart cities, as well as energy-efficient edge computing utilizing ML algorithms.

In particular, neuromorphic chips can enable on-chip security against insider and outsider threats using ML-based anomaly detection, Physical Unclonable Functions (PUFs), and trojan detection, network intrusion detection, with on-line learning that provides orders of magnitude performance improvement compared to the state-of-the-art approaches. Inside every computing chip, there are many node activities that can leak critical information, especially, if there is an active attack or threat. Thus, critical nodes can be located and observed using a low-power neuromorphic chips that performs ML anomaly detection algorithms to monitor the behavior of these nodes and produce a warning in case of an anomaly or outlier behavior detection in run-time. Additionally, Ensemble Learning algorithms may be coupled with neuromorphic hardware to maximize performance and accuracy of anomaly detection. Neuromorphic chips leveraging emerging devices would enable on-line training and weight updates to the network without dramatic memory operation and resource consumption. The context diagram of such neuromorphic-enabled security module for IoT is shown in Figure 1.

Neuromorphic chips are dense and stacked in a 3D structure on top of the baseline CMOS devices. Thus, reverse engineering can be significantly challenging without damaging the neighborhood devices during the reverse engineering process. Additionally, countermeasures such as the one proposed in [31] have been used to prevent probing and reverse engineering attacks on neuromorphic architecture. However, there is a possibility of reverse engineering attacks if the attacker gains physical access to the neuromorphic chip and can extract the proprietary algorithm. In particular, if an attacker attains physical access to the neuromorphic chip, he/she can apply inputs and observe output behavior to extract the weights and their relationship with the inputs and eventually gain access to the algorithm being performed to replicate the design. This becomes significantly more important since the neuromorphic chips are usually designed using modular approach and replicated manner and access to one architecture module can reverse engineer other modules as well. Some countermeasures to mitigate such attacks are proposed in the literature [32].

Furthermore, we believe that utilizing ensemble learning algorithms will make it more complicated for attacks to be successful due to the increase in the complexity of the ML algorithm being performed on the neuromorphic chip. Researchers in [33] discuss the feasibility of using ensemble learning to detect malware in real-time by using minimal hardware. By using a smaller number of boosted HPCs, authors in [33] show promising latency reduction in detecting malware. These results further validate our claim. Moreover, utilizing beyond-CMOS devices provide low-power operation which makes it increasingly difficult for attackers to utilize power side channel analysis to extract secret information. However,

TABLE I: Neuromorphic Accelerators

	Domain	Technology	Neurons	Area	Energy
SpiNNaker [34]	Digital	130nm	1000	102 mm^2	27 nJ
BrainScaleS [35]	Analog	180nm	8 to 512	50 mm^2	174 pJ
Loihi [29]	Digital	14nm (FinFET)	1024	60 mm^2	105.3 pJ
TrueNorth [28]	Digital	28nm	256	430 mm^2	27 pJ
Chen et al. [36]	Digital	10nm FinFET	2330	1.72 mm^2	1.7 uJ
Yin et al. [37]	Digital	28nm (Simulated)	1306	1.65 mm^2	773 nJ

the devices used to store weights within the neuromorphic chip can be vulnerable to soft and hard failures caused due to applying high current values, resulting in unwanted bit flips or, in the worst case, device malfunction and change in the behavior of the device. As a possible mitigation approach for such attacks, the utilization of current limiting circuits to prevent device malfunction in the neuromorphic chips could be integrated into the solution. Additionally, using multi-level weights can further mitigate reverse engineering attacks due to the increase in the complexity of the weights assigned by the ML algorithm in the neuromorphic architecture. Moreover, as the accuracy of the algorithm running on the neuromorphic chip increases, the attacker's job to reverse engineer and replicate the algorithm becomes increasingly easier. Thus, to mitigate such attacks, a neuromorphic chip can provide adaptive accuracy to cause confusion for attackers, as shown effective in [32]. It is important to note that the adaptive nature of neuromorphic chips allow for flexible coverage for attack mitigation as new security threats such as new HTs emerge.

Although, almost all recent implementations of neuromorphic processing are performed using traditional CMOS technology, there has been significant research on utilization of emerging technologies and devices such as magnetic tunnel junctions, memristors, phase-change, ferroelectric, and other advanced technologies [30]. While emerging devices have not garnered widespread commercial usage, we believe that the significant efficiency advantages gained by using emerging devices in neuromorphic settings could be a major catalyst for industry-wide adoption.

IV. Discussion

Neuromorphic-enabled security could benefit from the inherent scalability of neuromorphic computers and increasing the number synapses and neurons will provide more processing power and speed. The neuromorphic chips can be stacked in a modular fashion similar to SpiNNaker and Loihi [30]. The event-driven nature of neuromorphic-enabled security as well as its massively parallel processing capabilities will allow for energy and resource efficient computation whenever data is available considering the sparsity of spikes. Moreover, the processing and storage elements within the neuromorphic-enabled security can be the same. Furthermore, the focus of the research has been on advancements in materials, devices, and technologies. However, significant effort is required to develop novel neuromorphic algorithms to run on neuromorphic hardware [30]. New algorithms are sought to narrow the gap between accuracy of neuromorphic computing and deep learning approaches. To enable the advancement of

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:04:51 UTC from IEEE Xplore. Restrictions apply.

neuromorphic algorithm development, we need to address the need for developing software tools and hardware platforms as well as make them accessible to the research community.

Currently, there are limited number of tools and hardware platforms for neuromorphic computing, which are mostly available via cloud access. Additionally, it is important to note that the current tools available have limited applications, suffer from slow speeds, and their performance drops as the design scales. Last but not least, lack of proper benchmark suits or unified metrics to comprehensively evaluate new neuromorphic algorithms and decide what hardware implementation could potentially offer superior performance given the needs of the algorithm [30]. This is extremely important because current benchmarks and metrics are tailored for evaluating deep learning approaches. Utilizing these benchmarks can result in an unfair comparison with neuromorphic methods, thus not fully demonstrating the advantages of the neuromorphic computing.

Using Neuromorphic-enabled security for IoT edge devices comes with its challenges. Security of the neuromorphic chip, achieving similar accuracy to state-of-the-art ML hardware counterparts, lacking good benchmark datasets and evaluation metrics that could measure efficient real-world performance are a few of these challenges. A head-to-head comparison between SNN and ANN accelerators in [38] reaffirms the advantages of using Neuromorphic computing hardware. Although the accuracy of SNN accelerators compared to ANN accelerators, as observed in [38], is lower, recent advances in SNN accelerators have shown significance improvement in inference accuracy of SNN accelerators. Moreover, the study was done on small-scale chips and networks. Neuromorphic chips provide significant improvement in terms of power and area of performing ML algorithms, however, increase in shared resource usage and modular design of such architectures makes them vulnerable to malicious security attacks [39]. HT insertion is another form of attack that can result in vulnerability of the neuromorphic architecture.

Moreover, presence of HPCs for increased observability for performance monitoring and testing of the circuit can make the design vulnerable to hardware attacks. Side-channel analysis can be done on devices to extract side-channel leakage information via power, electromagnetic emissions, timing, and memory side-channels, which may leak critical information. Welch's t-test, also known as variance test, has been most commonly used for detection of side-channel leakage [40]. The work done in [16], [17], [33] show that HPCs are effective means to determine the presence of malware, and that malware can be detected with far lower latency as more HPC metrics are observed. These works perform post-processing ML models on powerful host systems to detect the presence of malicious software/firmware, which would incur a large cost at the edge. This motivates the use of tightly coupled neuromophic platforms in IoT edge devices. This could reduce intrusion/malware detection to an order of a few picojoules per synaptic operation. In case of using neuromorphic-enabled security for IoT, security of neuromorphic chips from the hardware perspective is significantly important and on its own is a topic of research [39]. Herein, we discuss some of the potential threat models and attack scenarios that could affect the integrity of the neuromorphic chips:

- **Side-Channel Attacks**: To launch such attacks, the adversary requires physical access to the supply voltage and electromagnetic emission traces of the neuromorphic chip. Additionally, success of this attack requires that the adversary have knowledge of the algorithm used for spiking encoding as well be the ability to modify the algorithm inputs.
- **Fault Injection Attacks**: Physical access to the neuromorphic chip is required to perform fault injection attacks. The adversary needs to decapsulate the neuromorphic chip, locate the region of interest on the layout, apply inputs, and observe outputs' behavior.
- **Probing Attacks**: The adversary requires physical access of the neuromorphic chip to locate memory components and generate inputs and observe the behavior of the hardware and switching of transistors.
- **Focused Ion Beam Attacks**: Physical access to the neuromorphic chip is needed so that the adversary can decapsulate the IC and locate the region of interest on the layout. Then, the attacker can steal model-specific information, such as the weights stored in the neuromorphic chip, if no physical countermeasures are implemented in the front or back side.

Integrating neuromorphic chips in IoT may also introduce attack surfaces. It is still an open question whether or not meaningful data can be extracted directly from power or electromagnetic signatures. Typical power side-channel attacks aim to extract sensitive data from correlated power traces. In the context of neuromorphic ICs, the most useful side-channel information corresponds to mapping regions of chip activity to known operations. This concept is analogous to mapping brain activity with specific human functions.

V. Conclusion

In this work we have explored the feasibility, and potential security applications, of modern neuromorphic platforms in IoT edge settings. We have shown that these platforms show great promise in narrowing efficiency and response time costs of security counter-measures in embedded platforms. This analysis supports development of future modules which could provide run-time and on-chip security using learning-based anomaly detection against insider and outsider threats with rapid and efficient on-line learning.

Acknowledgment

This work was supported in part by the National Science Foundation through Computing Research Association for CIFellows #2030859.

References

[1] W. Zhou, Y. Jia, A. Peng *et al.*, "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, 2019.

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:04:51 UTC from IEEE Xplore. Restrictions apply.

[2] K. Yang, D. Blaauw, and D. Sylvester, "Hardware designs for security in ultra-low-power iot systems: An overview and survey," *IEEE Micro*, vol. 37, no. 6, pp. 72–89, 2017.

[3] M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security on neuromorphic computing system," in *2017 International Joint Conference on Neural Networks (IJCNN)*, 2017, pp. 3830–3837.

[4] K. Shaukat, S. Luo, V. Varadharajan *et al.*, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222 310–222 354, 2020.

[5] X. Pei, L. Yu, and S. Tian, "Amalnet: A deep learning framework based on graph convolutional networks for malware detection," *Computers Security*, vol. 93, p. 101792, 2020.

[6] K. A. da Costa, J. P. Papa, C. O. Lisboa *et al.*, "Internet of things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[7] S. Venkataramani, K. Roy, and A. Raghunathan, "Efficient embedded learning for iot devices," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016, pp. 308–311.

[8] D. V. Christensen, R. Dittmann, B. Linares-Barranco *et al.*, "2022 roadmap on neuromorphic computing and engineering," *Neuromorphic Computing and Engineering*, 1 2022.

[9] M. E. Phillips, N. D. Stepp, J. Cruz-Albrecht *et al.*, "Neuromorphic and early warning behavior-based authentication for mobile devices," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, 2016, pp. 1–5.

[10] S. Faezi, R. Yasaei, A. Barua *et al.*, "Brain-inspired golden chip free hardware trojan detection," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2697–2708, 2021.

[11] M. Mushtaq, A. Akram, M. K. Bhatti *et al.*, "Machine learning for security: The case of side-channel attack detection at run-time," in *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2018, pp. 485–488.

[12] A. Tatulian, S. Salehi, and R. F. DeMara, "Mixed-Signal Spin/Charge Reconfigurable Array for Energy-Aware Compressive Signal Processing," in *2019 International Conference on Reconfigurable Computing and FPGAs, ReConFig 2019*. Institute of Electrical and Electronics Engineers Inc., 12 2019.

[13] S. Salehi and R. F. DeMara, "Adaptive Non-Uniform Compressive Sensing Using SOT-MRAM Multi-Bit Precision Crossbar Arrays," *IEEE Transactions on Nanotechnology*, vol. 20, pp. 224–228, 2021.

[14] S. Salehi and R. DeMara, "SLIM-ADC: Spin-based Logic-In-Memory Analog to Digital Converter leveraging SHE-enabled Domain Wall Motion devices," *Microelectronics Journal*, vol. 81, 2018.

[15] S. Salehi, A. Zaeemzadeh, A. Tatulian *et al.*, "MRAM-Based Stochastic Oscillators for Adaptive Non-Uniform Sampling of Sparse Signals in IoT Applications," in *Proceedings of the 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. Miami, FL, USA: IEEE, 9 2019, pp. 403–408.

[16] H. Wang, H. Sayadi, A. Sasan *et al.*, "Comprehensive evaluation of machine learning countermeasures for detecting microarchitectural side-channel attacks," in *Proceedings of the 2020 on Great Lakes Symposium on VLSI*, ser. GLSVLSI '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 181–186.

[17] H. Sayadi, Y. Gao, H. Mohammadi Makrani *et al.*, "Stealthminer: Specialized time series machine learning for run-time stealthy malware detection based on microarchitectural features," in *Proceedings of the 2020 on Great Lakes Symposium on VLSI*, ser. GLSVLSI '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 175–180.

[18] S. Salehi, R. Zand, A. Zaeemzadeh *et al.*, "AQuRate: MRAM-based Stochastic Oscillator for Adaptive Quantization Rate Sampling of Sparse Signals," in *Proceedings of the 2019 Great Lakes Symposium on VLSI (GLSVLSI)*. Tysons Corner, VA, USA: ACM, 2019, pp. 359–362.

[19] S. Sheikhfaal, S. D. Pyle, S. Salehi *et al.*, "An Ultra-Low Power Spintronic Stochastic Spiking Neuron with Self-Adaptive Discrete Sampling," in *Midwest Symposium on Circuits and Systems*, vol. 2019-August. Institute of Electrical and Electronics Engineers Inc., 8 2019, pp. 49–52.

[20] H. Wang, S. Salehi, H. Sayadi *et al.*, "Evaluation of Machine Learning-based Detection against Side-Channel Attacks on Autonomous Vehicle," *2021 IEEE 3rd International Conference on Artificial Intelligence Circuits and Systems, AICAS 2021*, 6 2021.

[21] S. Salehi, R. Zand, and R. F. DeMara, "Clockless Spin-based Look-Up Tables with Wide Read Margin," in *Proceedings of the 2019 Great Lakes Symposium on VLSI (GLSVLSI)*. Tysons Corner, VA, USA: ACM, 2019, pp. 363–366.

[22] M. Hossain, S. Salehi, D. Mulvaney *et al.*, "Embedded STT-MRAM Energy Analysis for Intermittent Applications using Mean Standby Duration," *2021 28th IEEE International Conference on Electronics, Circuits, and Systems, ICECS 2021 - Proceedings*, 2021.

[23] G. Kolhe, S. Salehi, T. D. Sheaves *et al.*, "Securing Hardware via Dynamic Obfuscation Utilizing Reconfigurable Interconnect and Logic Blocks," *Proceedings - Design Automation Conference*, vol. 2021-December, pp. 229–234, 12 2021.

[24] M. S. Alam, B. R. Fernando, Y. Jaoudi *et al.*, "Memristor based autoencoder for unsupervised real-time network intrusion and anomaly detection," in *Proceedings of the International Conference on Neuromorphic Systems*, ser. ICONS '19. New York, NY, USA: Association for Computing Machinery, 2019.

[25] Y. Chen, Z. Wang, A. Patil *et al.*, "A 2.86-tops/w current mirror cross-bar-based machine-learning and physical unclonable function engine for internet-of-things applications," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 6, pp. 2240–2252, 2019.

[26] L. Xiao, X. Wan, X. Lu *et al.*, "Iot security techniques based on machine learning: How do iot devices use ai to enhance security?" *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

[27] R. Zand and R. F. DeMara, "Snra: A spintronic neuromorphic reconfigurable array for in-circuit training and evaluation of deep belief networks," in *2018 IEEE International Conference on Rebooting Computing (ICRC)*, 2018, pp. 1–9.

[28] M. V. DeBole, B. Taba, A. Amir *et al.*, "Truenorth: Accelerating from zero to 64 million neurons in 10 years," *Computer*, vol. 52, no. 5, pp. 20–29, 2019.

[29] M. Davies, N. Srinivasa, T.-H. Lin *et al.*, "Loihi: A neuromorphic manycore processor with on-chip learning," *IEEE Micro*, vol. 38, no. 1, pp. 82–99, 2018.

[30] C. D. Schuman, S. R. Kulkarni, M. Parsa *et al.*, "Opportunities for neuromorphic computing algorithms and applications," *Nature Computational Science 2022 2:1*, vol. 2, no. 1, pp. 10–19, 1 2022.

[31] S. Kannan, N. Karimi, O. Sinanoglu *et al.*, "Security vulnerabilities of emerging nonvolatile main memories and countermeasures," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 1, pp. 2–15, 2015.

[32] C. Yang, B. Liu, H. Li *et al.*, "Security of neuromorphic computing: Thwarting learning attacks using memristor's obsolescence effect," in *Proceedings of the 35th International Conference on Computer-Aided Design*, ser. ICCAD '16. New York, NY, USA: Association for Computing Machinery, 2016.

[33] H. Sayadi, N. Patel, S. M. P.D. *et al.*, "Ensemble learning for effective run-time hardware-based malware detection: A comprehensive analysis and classification," in *2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*, 2018, pp. 1–6.

[34] S. B. Furber, F. Galluppi, S. Temple *et al.*, "The spinnaker project," *Proceedings of the IEEE*, vol. 102, no. 5, pp. 652–665, 2014.

[35] J. Schemmel, D. Brüderle, A. Grübl *et al.*, "A wafer-scale neuromorphic hardware system for large-scale neural modeling," in *2010 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2010, pp. 1947–1950.

[36] G. K. Chen, R. Kumar, H. E. Sumbul *et al.*, "A 4096-neuron 1m-synapse 3.8-pj/sop spiking neural network with on-chip stdp learning and sparse weights in 10-nm finfet cmos," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 4, pp. 992–1002, 2019.

[37] S. Yin, S. K. Venkataramanaiah, G. K. Chen *et al.*, "Algorithm and hardware design of discrete-time spiking neural networks based on back propagation with binary activations," in *2017 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, 2017, pp. 1–5.

[38] Z. Du, D. D. Ben-Dayan Rubin, Y. Chen *et al.*, "Neuromorphic accelerators: A comparison between neuroscience and machine-learning approaches," in *2015 48th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, 2015, pp. 494–507.

[39] J. Sepulveda, C. Reinbrecht, and J.-P. Diguet, "Security aspects of neuromorphic mpsocs," in *Proceedings of the International Conference on Computer-Aided Design*, ser. ICCAD '18. New York, NY, USA: Association for Computing Machinery, 2018.

[40] T. Schneider and A. Moradi, "Leakage assessment methodology," in *Cryptographic Hardware and Embedded Systems – CHES 2015*, T. Güneysu and H. Handschuh, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 495–513.

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:04:51 UTC from IEEE Xplore. Restrictions apply.