ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Harnessing AI for Advanced Cybersecurity in System on Chip Design a Compendious Study

Rajat Suvra Das

Senior Director, Business Development, L&T Technology Services, USA

ABSTRACT

System-on-Chip (SoC) designs are becoming increasingly intricate as they integrate various components and functionalities onto a single chip. This intricacy brings forth new vulnerabilities and attack surfaces, presenting a challenging task to ensure robust cybersecurity. Although previous studies have explored different AI approaches, there is a need to delve into the complexities of modern SoCs and propose practical methods to secure these systems, thereby aiding researchers in mitigating potential threats. The primary objective of this paper is to uncover the opportunities that emerge from utilizing AI techniques in SoC designs to fortify cybersecurity defenses. Subsequently, the study aims to deliberate on the complexities involved in integrating AI with SoC and provide appropriate recommendations to address these intricacies. This review paper will identify and discuss the technical, architectural, and implementation challenges faced by researchers and practitioners when incorporating AI into SoC designs for cybersecurity purposes. Moreover, it will suggest with potential solutions and strategies to effectively tackle these challenges. Furthermore, it aims to aid future researchers by offering potential research directions to enhance security in AI-SoC through innovative solutions. By identifying gaps in current literature and highlighting areas that require further exploration, this paper will guide future researchers in developing advanced and secure AI-SoC systems for cybersecurity applications. Overall, this review paper will contribute to the existing body of knowledge by providing a comprehensive analysis of the impact that integrating AI and SoC has on cybersecurity and foster advancements in AI-SoC systems that effectively enhance cybersecurity measures.

***Corresponding author**

Rajat Suvra Das, Senior Director, Business Development, L&T Technology Services, USA.

Received: December 07, 2023; **Accepted:** December 13, 2023; **Published:** December 21, 2023

Keywords: Artificial Intelligence, Chip, Cybersecurity, Integrated Circuits, System on Chip

Introduction

The rapid pace at which technology is advancing has consistently reshaped the landscape of digital innovation. At the core of this setup is the progress of electronic components, specifically in terms of their integration and connectivity. Accordingly, the Integrated Circuits have played a significant role in the development of technologies like tablets, cameras and smartphones. Initially, ICs were simple and consisted of a transistor and capacitor with three resistors. However, advancements in fabrication technology have allowed for the creation of ICs with numerous transistors, known as System on Chip (SoC) [1]. The SoC represents the pinnacle of this progress by integrating not only transistors, but also complete functional systems, inclusive of memory, Input/output (I/O) systems, processors and periodically the network interfaces into a chip. This level of integration can be compared to fitting an entire computer system onto a tiny chip. The objective was not just to reduce size but also to enhance efficiency, minimize the consumption of power and elevate the complete performance of the electronic system.

Concurrently, as the Internet of Things (IoT) endures to magnify, the demand for SoCs with various connectivity options are growing, leading towards a truly interconnected world. Alongside the pursuit of miniaturization, the forthcoming SoC technology will be influenced by the increasing need for Machine Learning (ML) and Artificial Intelligence (AI) capabilities in electronic devices [2]. Consequently, an increasing number of SoCs is anticipated with specialized AI and ML hardware, such as Tensor Processing Units (TPUs) and Neural Processing Units (NPUs). These dedicated processors will enable devices to efficiently perform intricate AI and ML tasks, resulting in the development of more smart and capable devices [3,4]. Concurrently, with the expanding number of connected devices and the rise of IoT, manufacturers are placing utmost importance on confirming the security of such devices [5]. Considering this, researchers have attempted to use different approaches to develop a reliable SoC model using AI.

In the paper by Gookyi et al. various authentication methods and encryption methods are used along with a key exchange or generation protocol [6]. Further, according to Marco Ciaffi, the combination of the security capabilities embedded in CPU architecture, along with additional hardware and software layers, allows SoC designers to create a design that inherently incorporates security measures. The RISC-V architecture, developed during the AI era and in response to the security concerns of today, offers an open-source solution that benefits from public scrutiny and engineering expertise. Moreover, the architecture includes a programmable memory attribute that allows designers to assign memory regions as read-only, write-only, or unrestricted for access. Overall, by leveraging the security capabilities of CPU architectures and employing complementary hardware and software layers, SoC designers can develop a design that

seamlessly integrates security measures. The suggested RISC-V architecture, with its open-source nature and compatibility with AI and modern security demands, provides an ideal platform for achieving this objective.

Subsequently, the RISC-V ISA's custom extensions permit for developing specialized instructions that enhance the efficiency of cryptographic algorithms. By leveraging these instructions, hackers without authorization encounter increased difficulty in circumventing the system. Further, to streamline the process of integrating custom extensions and security components, Andes Technology offers the Andes Custom Extensions (ACE) tool. This powerful tool significantly reduces the time required for implementation and verification [7]. Despite the significant endeavours of existing works in leveraging AI at SOC level to enhance cybersecurity, there exist a need to undertake a review in this regard so as to unveil the complexities of the contemporary SoCs and suggesting with probable approaches to secure this system by assisting researchers in mitigating potential threats.

Significant Contributions

- To delineate the two way impact of AI-SoC and unveil the possibilities of enhancing cybersecurity using AI at SoC by undertaking a comprehensive review.
- To deliberate the challenges involved in integrating AI with SoC and provide suitable suggestions to mitigate such intricateness.
- To assist future researchers with probable research directions so as to enlighten security in AI-SoC with innovative solutions.

Paper Organization

Paper is organized as follows with section 2 discussing the review method, section 3 presenting the integration of AI-SoC, section 4 exposing improved cybersecurity with AI integrated SoC, section 5 deliberating challenges and future suggestions in this area and section 6 presenting concluding remarks of the study.

Review Methodology

Survey was undertaken through the use of Google Scholar. Research Articles have been fetched from publishers like Research gate, IEEE etc. Stepwise process involved in finalizing the entire studies are provided in Figure 1.

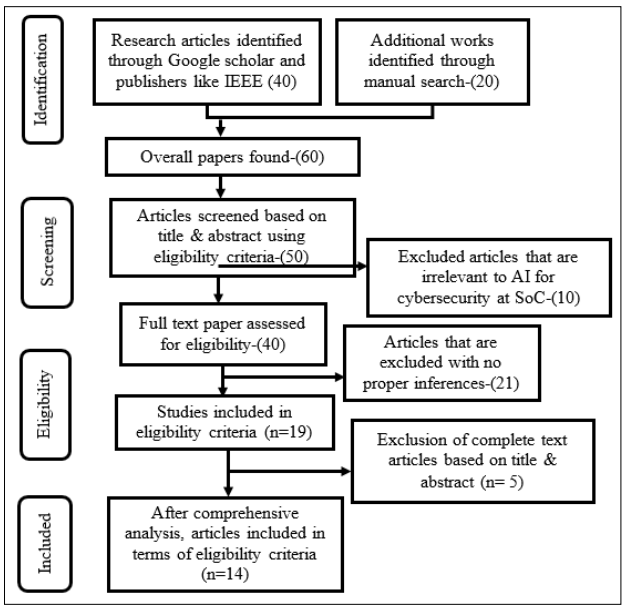

Figure 1: Selection of Articles Based on PRIMSA Guidelines

As shown in figure 1, appropriate articles that have been considered in the present study completely rely on PRISMA guidelines. Relevant and suitable publications have been taken from recent studies (≥) 2018 being considered and publications (<2018) being exempted. In such case, relevant and suitable citations have been considered from research articles (from 2018 to 2023). Primarily, a total of 40 research works have been found through e-database (Google Scholar) and from publishers (namely IEEE, Researchgate etc). In addition, 20 articles have been explored through manual searching. Overall, 60 papers have been found. Subsequently, 50 research works have been screened based on the title and abstract, wherein, 10 articles have been excluded. Following this screening, 40 research works have been exposed. Among them, 21 research articles having unsuitable inferences have been disregarded. Then, 19 papers have been considered based on eligibility. Among them, 5 papers have been excluded based on abstract and title. Lastly, the studies that have been refined based on the concept have been explored to be 14.

Convergence of AI and SoC-A Two Way Impact

In the contemporary era, AI is found to significantly revolutionize the execution and designs of SoC. The basic SoC model is shown in figure 2 that encompass of processors, memories and interconnects. AI with SoC concept delineates the seamless inclusion of AI operations into SoC's hardware framework. In this case, the chip turns to be a centre to execute the tasks and processes of AI. Primary intention lies in permitting the capabilities of smart processing within compact SoC confines. Integration of AI with SoC comprise of a range of methods, permitting the inclusion and adaptation of AI approaches into special SoC architecture. Such an inclusion is instigated by the realization that, traditional SoC designs might face hurdles in dealing with the computational necessities of advanced AI enabled applications [8]. Consequently, engineers and investigators endeavoured to optimize the SoC models for accelerating the operations of neural network, confirming a symbiotic association amongst underlying hardware and AI. This integration involves adapting AI approaches to fit the processing abilities and resource constraints of SoC. This adaptation seems to be vital in striking the correct balance amongst the computational complexity and distinct constraints comprised by the power, thermal restrictions and power in SoC designs. It could also be utilized for designing and developing effectual solutions for extensive applications namely hardware acceleration, memory optimization, power optimization, security etc [9].

For Example, Chandrasekaran in the study has intended to minimize the test time of SoC through AI based test scheduling approaches [10]. Test scheduling of SoC attains the ideal values corresponding to the parameters of test time. This assists in reducing the chip's test cost. High test time occurs owing to the usage of large size of memory. Considering this pitfall, an objective functionality has been applied to attain the tuning parameters under diverse load conditions of d695 and p22810 SoC benchmark circuit. Further, AI based nature inspired methods have been used to undertaken effectual test scheduling. The considered AI algorithms include Ant Colony Optimization (ACO), Bat Algorithm, Artificial Bee Colony (ABC), Firefly Algorithm (FA) and Modified ACO (MACO). Outcomes revealed the better performance of Bat algorithm. Similarly, the research has endorsed evolutional methodologies for performing test scheduling so as to minimize time and cost [11]. Accordingly, ALO (Ant Lion Optimization) and dragonfly have been executed to accomplish test time optimization. The suggested algorithms have been estimated for several Test Access Approach widths. Under varying Test Access Approach widths. Outcomes

revealed the better performance of dragonfly in comparison to the other considered approaches.

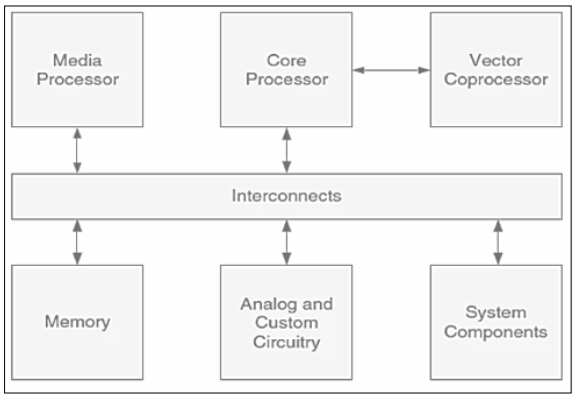

Figure 2: Fundamental SoC Model

Further, to optimize the latency rate, the study has used Deep Neural Network (DNN) method upon edge devices with the use of multi-processor system on the chip [12]. Experimentations have revealed that, the use of edge-devices for AI inferences have been superior when compared to cloud execution of similar network for latency optimization as well as energy efficacy of the system. Results revealed that, the suggested system could enhance the computational ability of DNNs with the use of Digital Signal Processor (DSP) and Logic Gates (LGs) on FPGA and use of ARM processing to co-ordinate and control purposes.

Subsequently, ensuring the cybersecurity of embedded systems have turned as a significant challenge in the advancement of IoTs, Cloud computing, and different renowned applications. Security of these FPGA- heterogeneous SoCs are crucial to enabling the development of secure implementation environments for sensitive applications by the embedded system designers. To achieve this, extending the ARM TrustZone based technology in SoCs seems to be a viable solution, provided that security can be ensured. Nevertheless, the current enhancement of ARM TrustZone seems to be insecured. In accordance with this, the study has presented evidence of multiple existing threats, revealing the potential for using them to compromise system security, potentially resulting in severe consequences. The paper describes six successful attacks undertaken on a typical software and hardware system, but it should be noted that diverse attack paths are also conceivable. Consequently, designers who intend for developing sensitive applications on these heterogeneous SoCs must prioritize the complete system security from the initial stages of the design process [13].

Not only AI assists SoC in diverse applications. It is a two-way impact, where, SoC also assists AI in diverse applications. AI algorithms like Deep Learning (DL) methods utilize NNs which could differ in size in accordance with the requirements of applications in real-time. Taking this into account, the study includes a solution termed SoC to accelerate DNNs [14]. In this case, an ARM processor manages the complete implementation. It also delegates computational tasks to the hardware accelerator. System has been executed on SoC development board. Empirical outcomes have revealed that, the system has accomplished a speed of nearly 22.3 in comparison to operating a network on dual core cortex-ARM A9 processor. A mathematical modelling has also been presented for computing the overall implementation time for different network size. System has been assessed using the recognition of Epileptic Seizure as the case-study. Outcomes revealed the better performance of the suggested system with regard to clock-frequency, scalability and execution time.

Enhancing Cybersecurity with AI Integrated SoCs

The use of SoC technology has become prevalent in modern computing integrated circuits to improve the processing and communication capabilities on a single chip. SoCs may face functionality issues, information leakage, Denial of Services (DoS) attacks, hardware Trojan Horses, and other security threats. Verifying the security of SoCs adds another layer of complexity, especially when considering the diverse applications and evolving use cases of IoT devices. Failing to comprehensively verify the security of SoCs in IoT devices can possess severe consequences, including privacy breaches, damage to business reputation, and even endangering lives. Detecting and pinpointing hardware Trojan Horses is highly challenging due to their discreet behaviour, which necessitates the development of efficient and scalable security validation approaches [15].

Even a simple HT can be exploited by attackers to gain unauthorized access to the Network-on-Chip (NoC) backbone of the processor, thereby compromising the communication patterns within the system. In light of these concerns, the research study has demonstrated that embedding single or multiple HTs within NoC of a many or multi-core processor can result in the leakage of sensitive information about traffic patterns to external attackers [16]. Constructing an AI system demands high performance encompassing of low power, high security and effectual processors. Figure 3 explores a high-level model of a secured NN processor SoC utilized in AI applications. This processor SoC could be extensively secured while executing with reliable IP.

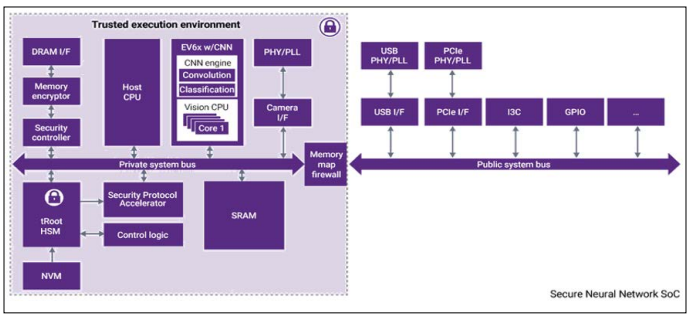

Figure 3: Reliable Environment with a Designware IP in Securing NN-SoCs for AI Applications

Further, leveraging Machine Learning (ML) techniques, these attackers can infer the applications running on the processor by analyzing the HT payload data. To mitigate such attacks, the suggested defense mechanism has integrated a randomized routing algorithm relying on Simulated Annealing. This algorithm has attempted to obfuscate the attacker's ability to accurately infer user profiles. Experimental results substantiate the effectiveness of the suggested randomized routing algorithm, showcasing a significant reduction in the attacker's accuracy in identifying user profiles. The accuracy has dropped from over (98%) to (<15%) in many or multi-core systems.

Selecting suitable SoC is crucial for determining the appropriateness for developing a reliable application. Further, the utilization of cutting-edge cryptographic operations on FPGA to explore design space has afforded improved power and area consumption requirements. The suggested approach has also employed the optimization technique, Genetic Algorithm (GA) to evaluate the effectiveness of SoC with enhanced cryptographic algorithms, thus

ensuring device security. In order to verify the outcomes produced by the GA model on the hardware devices, security benchmarks have been implemented and the execution time and performance has been carefully analyzed. The accuracy of the algorithm has been determined using the confusion matrix method, resulting in an achieved accuracy of 89.66% [17].

Security attacks primarily targeted the computing cores. However, contemporary attacks now exploit the vulnerability of the NoC interconnect to inject unwanted traffic. This poses a significant security risk for physical systems that rely on sensory feedback and control signals. Modifying these signals maliciously generates abnormal traffic patterns, directly impacting the system's operation and performance. To address this issue, the research has attempted to detect abnormal traffic patterns, signifying potential attacks, in NoC data through the utilization of Spiking Neural Networks [18]. Specific focus has been provided on exploring the susceptibilities of Denial-of-Service (DoS) attacks and assess the impact of attack duration on detection rates. The results have revealed that the start time of attacks is not a crucial parameter. Regardless of when the attack(s) commence during an application's execution, they can be detected. However, the temporal duration of the attack plays a significant role, as longer attacks have a higher probability of detection. Attacks that last around 30% of the complete time for data exchange can be successfully detected. Furthermore, the preliminary investigation has denoted that multiple attacks of substantial duration can also be detected.

Significant Role of NPUs Integrated with AI in SoC Design for Cybersecurity

In the realm of cybersecurity, NPUs play a significant role when combined with AI in SoC designs. NPUs are specialized hardware components crafted to expedite AI computations, particularly neural network operations. They are finely tuned to perform intricate mathematical calculations necessary for AI algorithms, such as deep learning. Within the realm of cybersecurity, NPUs can be harnessed to amplify the capabilities of AI systems in multiple ways [19]. Here are a few instances:

- **Intrusion Detection:** NPUs can be deployed to scrutinize network traffic in real-time, pinpointing patterns or irregularities that may signify potential cyber threats. By swiftly and efficiently processing massive volumes of data, NPUs enable expedited detection and response to security breaches.
- **Malware Detection:** NPUs can be trained to identify patterns and distinctive characteristics of known malware, facilitating efficient recognition and categorization of malicious software. This aids in the identification and mitigation of potential threats before they inflict harm.
- **Behavioural Analysis:** NPUs can analyze user behavior and network activity in order to establish normal patterns and identify any deviations that may indicate unauthorized access or suspicious activities. This empowers proactive threat detection and prevention.
- **Anomaly Detection:** NPUs can be employed to detect abnormal patterns or behaviors within a system or network. By continually monitoring and analyzing data, NPUs are capable of identifying unusual activities that may imply a security breach or an ongoing attack.

By integrating NPUs into SoC designs, AI-powered cybersecurity systems can leverage accelerated processing capabilities, enabling real-time analysis and response to potential threats. This fusion of AI and NPU technology enhances the overall security stance of systems, delivering improved protection against cyber threats.

Challenges in AI-SoC Integration and Future Suggestions

The infusion of AI into SoC designs presents significant opportunities for transforming various industries. However, this integration is not devoid of obstacles. This article will delve into eight common key challenges (identified after a precise review) that necessitate attention in order to effectively implement AI in SoCs.

- **Hardware Constraints:** A primary challenge in merging AI and SoCs lies in the limitations of hardware. AI algorithms often demand substantial computational power and memory resources, which may surpass the capabilities of conventional SoCs. To overcome this hurdle, it is crucial to design effectual hardware accelerators such as Field-Programmable Gate Arrays (FPGAs) or Graphics Processing Units (GPUs) to proficiently manage AI workloads.
- **Power Usage:** Incorporating AI into SoCs can lead to an augmented power consumption. AI algorithms require significant computational resources, leading to amplified energy requirements. Effectively addressing this challenge involves the development of power-effective architectures and the optimization of algorithms for minimizing power usage without negotiating performance.
- **Algorithm Complexity:** AI approaches are intrinsically complex, necessitating intricate mathematical models and extensive training data. The integration of such approaches into SoCs poses a challenge due to the limited availability of computational resources. Hence, future investigators must focus on developing efficient algorithms that strike a balance between accuracy and computational efficiency.
- **Data Management:** AI methods heavily rely on enormous data for training and inference. Managing and preserving this data within the SoC constraints can be perplexing. Effective data management techniques, such as on-chip memory optimization, quantization, and compression are vital for the successful inclusion of AI in SoCs.
- **Real-Time Processing:** Numerous AI applications, such as self-driving cars or robotics, necessitate the ability to process data in real-time. It is a significant challenge to achieve real-time performance within the limited resources of SoCs. To overcome this obstacle, it is crucial to design efficient parallel processing architectures and optimizing algorithms to reduce latency during inference.
- **Security and Privacy:** Integrating AI into SoCs introduces potential vulnerabilities, making the privacy and security aspect critical. Adversarial attacks, data breaches, and unauthorized access to AI models are some of the risks associated with AI integration. To safeguard AI-enabled SoCs, it is vital to implement robust security measures such as encryption, anomaly detection and authentication.
- **Interoperability and Standardization:** The lack of interoperability and standardization across AI frameworks and SoC models pose a significant challenge. Different AI frameworks may have varying requirements and compatibility issues with SoCs. To facilitate seamless integration and interoperability between AI and SoCs, it is necessary to establish industry-wide standards and protocols.

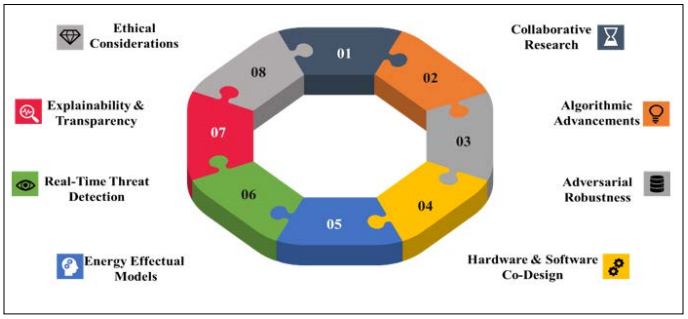

Figure 4: Supplementary Probable Research Directions

Ethical and Legal Considerations: As AI becomes more prevalent in SoCs, ethical and legal considerations come to the forefront. Addressing issues like bias in AI algorithms, transparency, and accountability is imperative. To ensure responsible AI integration in SoCs, it is essential to develop ethical guidelines and regulatory frameworks. In light of the aforementioned challenges and the objective of ensuring a promising future for AI at SoC for cybersecurity, the following (as shown in figure 4) are some other future recommendations for researchers. The Table 1 describes overview indication of the various conventional models in the chip designing.

Table 1: Overview Indication of the Existing Studies on the Chip Designing

References	Method	Algorithm	Parameters	Outcome
[9]	DL	AI-SoC	• Algorithmic adaptation • Accelerator type • Parallel processing • Resource allocation • Learning rate	• Power consumption-15% • Latency-20% • Throughput-25% • Learning rate-30% • Efficiency-10%
[12]	ML	DNN-GPU Cluster	• Energy efficiency • Security	• Power consumption-215.8W • Latency-83S • Throughput-187 Img/S
[14]	DL	DNN	• No of hidden layers • No of input nodes • Weight of the network	
[16]	ML	GAN (Generative Adversarial Network)	Security and production	Accuracy >98% to <15%
[17]	ML	GA (General Algorithm)	• Latency • Performance • Throughput	• Latency-1.05S • Performance-0.92 • Throughput -117.85 Mbps

From the various existing studies, AI methods specifically Machine learning methods and Deep learning methods was experimented and presented in the various research. Different learning methods were depicted and experimented with various algorithms and it is keenly described in tabular column.

Conclusion

The study aimed to undertake a review leveraging AI to enhance cybersecurity at SoC level. To perform this, the study followed PRISMA guidelines to fetch relevant papers. The review described the bi-directional impact of AI and SoC. Further, the study also uncovered the possibilities in improving cybersecurity with AI at SoC. Through this analysis, challenges involved in incorporating AI with SoC was discussed. Finally, suitable suggestions were provided to resolve this intricateness. From the review, it was found that, integrating AI into SoCs presents immense potential for transforming diverse industries. Nevertheless, successful implementation requires overcoming several challenges. By addressing hardware limitations, power consumption, algorithm complexity, data management, real-time processing, security and privacy concerns, interoperability, and ethical considerations, it is probable to pave the way for seamless AI integration into SoCs. Through continuous efforts to enhance efficiency and considering ethical implications, these challenges can be overcome, unlocking the full potential of AI in SoC designs. Also, by focusing on these suggested advancements, researchers can contribute to the promising future of AI in SoCs for cybersecurity that will pave the way for advanced and secure AI-powered cybersecurity systems.

References

1. Clark G, Raniwala H, Koppa M, Chen K, Leenheer A, et al. (2023) Nanoelectromechanical Control of Spin–Photon Interfaces in a Hybrid Quantum System on Chip. Nano Letters https://pubs.acs.org/doi/10.1021/acs.nanolett.3c04301.
2. Kumar D (2022) The Artificial intelligence in Power Systems. International Journal of Innovative Research in Computer Science & Technology 10: 319-322.
3. Chahal S (2023) Harnessing AI and machine learning for intrusion detection in cyber security. International Journal of Science and Research 12: 2639-2645.
4. Elgendy M (2023) Emerging System-on-a-Chip Trends. Azom https://www.azom.com/article.aspx?ArticleID=23158.
5. Frąckiewicz M (2023) The Future of System on a Chip (SoC) Technology: Trends and Predictions.
6. Zhu X, Hu C, Lu Y, Wang Z, Xue H (2023) Lightweight Cryptographic Simulation of Power IoT Fused with Bayesian Network Algorithms. EAI Endorsed Transactions on Scalable Information Systems 10: e1-e1.
7. Marco Ciaffi JM (2021) Building security into an AI SoC using CPU features with extensions. Embedded https://www.embedded.com/building-security-into-an-ai-soc-using-cpu-features-with-extensions/.
8. Lavanya S, Mythili K, Kannimuthu DS (2020) An Integration of Big Data Analytics and Cyber Security-A Panoramic Survey. International Journal of Advanced Research in Engineering and Technology (IJARET) 11.
9. Chelladurai CC, Kuluchamy P, Santhavaliyan S, Samraj T (2023) Integrating AI-Driven on-Chip Neural Networks into SOC Architectures. ICTACT Journal On Microelectronics 9: 1640-1645.
10. ChandrasekaranG, Periyasamy S, Panjappagounder Rajamanickam K (2020) Minimization of test time in system on chip using artificial intelligence-based test scheduling techniques. Neural Computing and Applications 32: 5303-5312.
11. Chandrasekaran G, Karthikeyan P, Kumar NS, Kumarasamy V (2021) Test scheduling of system-on-chip using dragonfly and ant lion optimization algorithms. Journal of Intelligent & Fuzzy Systems 40: 4905-4917.
12. Omidsajedi SN, Reddy R, Yi J, Herbst J, Lipps C, et

al. (2021) Latency optimized Deep Neural Networks (DNNs): An Artificial Intelligence approach at the Edge using Multiprocessor System on Chip (MPSoC). Mobile Communication-Technologies and Applications 1-6.

13. Benhani E, Bossuet L, Aubert A (2019) The Security of ARM TrustZone in a FPGA-based SoC. IEEE Transactions on Computers 68: 1238-1248.
14. Shehzad F, Rashid M, Sinky MH, Alotaibi SS, Zia MYI (2021) A scalable system-on-chip acceleration for deep neural networks. IEEE Access 9: 95412-95426.
15. Farahmandi F, Huang Y, Mishra P (2020) System-on-Chip Security Vulnerabilities. Springer https://www.springerprofessional.de/en/system-on-chip-security-vulnerabilities/17421832.
16. Dhavlle A, Ahmed MM, Mansoor N, Basu K, Ganguly A, et al. (2023) Defense against On-Chip Trojans Enabling Traffic Analysis Attacks based on Machine Learning and Data Augmentation. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems https://ieeexplore.ieee.org/document/10130691.
17. Krishnamoorthy R, Krishnan K (2021) Security Empowered System-on-Chip Selection for Internet of Things. Intelligent Automation & Soft Computing 30.
18. Madden K, Harkin J, McDaid L, Nugent C (2008) Adding Security to Networks-on-Chip using Neural Networks. 2018 IEEE Symposium Series on Computational Intelligence (SSCI) https://ieeexplore.ieee.org/document/8628832.
19. (2023) What is an NPU and how does it help with AI? Chillblast https://www.chillblast.com/blog/what-is-an-npu-and-how-does-it-help-with-ai.