Journal of Global Research in Electronics and Communication
Volume 1, No. 11, November 2025
Available Online at: www.jgrec.info
RESEARCH PAPER

A Deep Review of Hardware Trojan Identification Methods in System-on-Chip Architecture

Dr. Sunita Dixit
Professor
Department of Computer Science & Engineering
St. Andrews Institute of Technology & Management
Gurgaon
bhardwajsunita23@gmail.com

***Abstract*—Hardware Trojans (HTs) have become one of the most important dangers to the modern integrated circuits, particularly as System-on-Chip (SoC) designs are becoming both larger and more complex and dependent on globalized supply chains. Such malicious modifications may undermine functionality, cause sensitive information to get stolen, or provide backdoors that may remain unnoticed, and that means that effective detection methods are necessary to ensure that modern hardware platforms are secure. The higher diversification of chip architectures such as digital, analog or mixed-signal, RF as well as biochips also contributes to increased pressure on the security mechanisms that are robust and adaptive. A broad overview of hardware Trojan detection methods is presented in this work, especially paying attention to machine learning (ML) and deep learning (DL) development. Look at the pre-silicon (static and dynamic) verification schemes, post-silicon (side channels) and the new smart detection schemes that make use of the power, electromagnetic, timing, and PUF-based signals. Other issues that were identified in the survey are the computational overhead, data limitations and the cross-platform generalization problems. Overall, the work provides the existing advancement and trace the way to advance further research to enhance trusted SoC design and the security of hardware.**

Keywords*—Computer Hardware, Hardware Trojan Detection, Detection Techniques, Integrated Circuit (IC), System-on-Chip (SoC).

I. INTRODUCTION

Computer hardware includes both the internal workings of the system, such as the CPU and memory, and the outward workings, such as the display and input devices, such as keyboards and monitors. These elements serve as the basis for software operation because they are made to handle, store, and exchange data. A semiconductor material called silicon is used to create integrated circuits (ICs), also known as chips. Transistors, which are tiny electronic components, are produced within the silicon and linked together using interconnects laid on top of the silicon surface. The integration principle is crucial in today's quickly changing electronic environment. This idea is best embodied by system-on-chips (SoCs), which represent a revolution in semiconductor architecture by combining numerous functions onto a single silicon chip [1]. It has been an amazing journey from the simple origins of integrated circuits to the sophisticated designs of SoCs today [2]. They are now the foundation of a wide variety of electronic devices, powering the operation of medical equipment, IoT devices, smart devices, and automotive systems.

As in the software industry [3]. Hardware projects can include the integration of modules developed by third parties, in addition to the complete outsourcing of device production [4]. This outsourcing helps to reduce development costs and is a reflection of the globalization on the hardware industry [5] supply chain. However, it is possible for hardware devices to be compromised by malicious third parties or for consumers to be tricked into purchasing a counterfeit device. Hardware Trojans, or malicious alterations of integrated circuits (ICs), are a growing security threat in the IC business. ICs with these Trojans may malfunction, disclose private data, or have other dire repercussions [6]. As a result, industry, academics, government, and the military have all been concerned about hardware Trojans. Numerous investigations on detection techniques have been carried ever since the initial hardware Trojan research was released. On the other hand, not much research has been done on how Trojans are actually used. The viability of Trojan insertion in real-world situations must be understood in order to create trustworthy detection and defensive methods.

The IC Trojans are implemented through illicit alterations to chips during the third-party manufacturing process; these modifications intentionally compromise the integrity of the chips to enable potential exploits, such as surveillance, control, or interception of confidential keys or internal chip data [7]. Trojan horses can be hard to spot in today's increasingly complex processors as their inner workings are neither programmable nor observable beyond silicon. They may also lie dormant for long stretches of time, only coming up at designated times as needed. Consequently, creating noninvasive methods to analyze ICs [8]. Detecting Trojans has been recognized as an important area of study. The goal is to present a new method for detecting Trojans that makes use of multimodal spatial thermal and power estimations after silicon processing. Infrared emissions from the silicon die's reverse side may be used to thermally characterize chips [9]. After processing, precise spatial power maps can be generated.

A. *Structure of the Paper*

The structure of the paper is as follows: Section II provides a description of SoC security fundamentals and types of chips. Section III examines significant hardware security threats and vulnerabilities of the supply chain. Section IV describes pre-silicon and post-silicon Trojan detection methods. Section V introduces recent studies of detection based on Trojan detection. Section VI ends with the most important findings and recommendations of the future.

© JGREC 2025, All Rights Reserved

II. Security of System-on-Chip Designs

In recent years, the chip industry has grown substantially, and chip design has branched out beyond conventional circuits. Several new types of innovative chips have emerged in recent years to address the wide variety of demands, including artificial intelligence (AI) chips, biochips, radio-frequency integrated circuits (RF IC), and advanced microsystems (AMS) chips [10]. However, the impact of HTs is starting to show up on these new chips.

A. Types of Chips

Chips are also called Integrated Circuit (IC) which are very important part of any hardware and there are different types of chips like AMS IC and Bio Chip. These chips are explained below:

1) AMS/RF IC

An analog/mixed-signal (AMS) circuit is different from a digital one in terms of its construction [11]. The AMS circuit known as the radio-frequency integrated circuit (RF IC) integrates digital and analogue components. Alternately, the AMS circuit can use either an analogue trigger in conjunction with a digital payload or an analogue trigger in conjunction with an analogue payload. HTs target opamps, oscillators, filters, and bias generators.

2) Bio Chip

Micro-total analysis systems, upon which BoC systems are built, minimize and consolidate all sample analysis methods into one device, allowing for thorough microscale analysis. Normal laboratory operations, including analyte detection, sample injection, mixing, reaction, separation, and enrichment, must be able to be performed [12]. As a result of their versatility, these systems often have complex designs with several components, allowing them to operate in either an active or passive capacity. In most cases, though, as illustrated in Figure 1, there are four primary components to the experimental setup: the inlet unit, which introduces the sample into the microchip; the reacting unit, which carries out the necessary reactions; the analysis unit, where biosensors detect physicochemical reactions; and the data processing unit, which transforms the resulting signals into output signals.

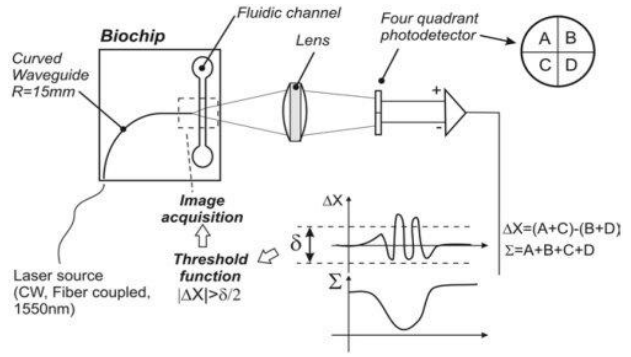

Fig. 1. Working Principle of Biochip

B. Hardware Security Threats

The exponential growth of high-performance computing platforms, systems integrated into vital infrastructure, and Internet of Things (IoT) devices has created formidable obstacles to hardware security [13]. Important information, operational stability, and user privacy are at risk from threats such as hardware Trojans (HTs), side-channel assaults (SCAs), and IC cloning, which undermine the trustworthiness, reliability, and integrity of electronic systems [14]. Growing reliance on globally dispersed supply networks makes these vulnerabilities much more severe. Interchip communication devices (ICs) can be vulnerable to hardware Trojans, design defects, and unauthorized access when they are handled by untrusted parties during design, manufacturing, assembly, and distribution.

- **Hardware Vulnerabilities:** Hardware vulnerabilities include RTUs, HMIs, PLCs, and smart devices that communicate with a SCADA system's main terminal [15]. An HMI is typically used in a SCADA setting to monitor all smart devices. In today's SCADA networks, these highly advanced HMIs can be customized to monitor a system's current state. Operators may receive information about particular sensors and the condition of control systems. Additionally, the HMI offers a way to make any necessary remedial action easier. Since HMIs are a major target inside SCADA systems, they should be air-gapped or isolated on a reliable network due to the risks they provide.

III. Security Vulnerabilities and the Emergence of Hardware Trojans

HT can be applied at various IC life cycle stages. The presence of HT risks when each pair of parties in the IC market model interacts. There is no assurance that foundries won't introduce a certain kind of HT into the chips during the fabrication process [16]. Untrusted employees or other parties who have access to the manufacturing process could pose a threat to chips made in foundries. For instance, by purposefully or inadvertently altering the dopant level or the mask layout during the sample or mass production, a Trojan can be inserted into the IC. Furthermore, foundries might contract with a third party to generate the masks, which could include malicious mask macros. Additionally, harmful algorithms that gather important data in IPs and SoCs may be present in software tools created by EDA [17] suppliers. Regardless of the reliability of the design team, the source of the EDA tools, or IP providers, logic implementations inferred by these tools may perform more than is necessary. Adversaries could use this unanticipated vulnerability to carry out attacks.

A. IC Supply Chain Vulnerabilities

Critical infrastructure, military applications, the food and pharmaceutical sectors, and other similar fields are especially vulnerable to the catastrophic impacts of counterfeit integrated circuits (ICs). The drive toward globalization is one of the key elements increasing the scope of the counterfeit issue [18]. The latter is motivated by the need to reduce expenses in order to obtain a competitive edge and has led to a notable increase in outsourcing levels. The complexity of the supply chain has increased dramatically due to the increased number of firms engaged and the necessity to distribute the chain over more levels. This transformation of the supply chain architecture has given birth to several major concerns pertaining to the counterfeiting problem:

- **Visibility:** The intricacy of the buyer-supplier network makes it more difficult to evaluate the integrity of purchased ICs, since participants have limited access to and control over upstream stages.

© JGREC 2025, All Rights Reserved

- **Traceability:** Separately identifying each bought IC becomes a challenge due to the dispersed and shared tracking data between participating firms.
- **Accountability:** There are insufficient ways to hold companies responsible for the part of the supply chain processes they manage.

B. Trojan Insertion Points in IC Development

A device Trojans are dangerous, undesired, and intentional modifications to electrical circuits. The Trojan can be injected at several levels of abstraction by a malevolent entity that is present at any point in the IC design or manufacturing process in order to accomplish destructive outcomes. This highlights the necessity of defining hardware Trojan in relation to various adversarial models. Trojans come from three distinct sources: foundries, SoC integrators, and 3PIP vendors. One or more of these entities may introduce a Trojan. Hardware Trojans may be present in third-party intellectual property that a SoC developer or design firm purchases [19]. Depending on whether the IP is hard (GDSII), firm (netlist-level), or soft (RTL-level), the Trojan's impact and design can change. A foundry can reverse-engineer the design to add, alter, or remove gates and manufacture Trojans because they have access to all of the design's layers.

IV. Hardware Trojan Detection Strategies and SOC Design

Trojan detection and integrated circuit (IC) security are closely related. The methods used to identify post-silicon Trojans can be categorized as destructive or non-destructive. Any form of integrated circuit (IC) reverse engineering could be seen as a notoriously destructive method that produces very certain results but renders the chip useless after processing. Nevertheless, non-destructive procedures offer more reliable results (i.e., less dependence); the chip remains usable even after the analysis is completed [20]. The timeline of recently suggested detection methods is displayed in Figure 2, along with some of the notable solutions that attracted a lot of attention from the scientific community.

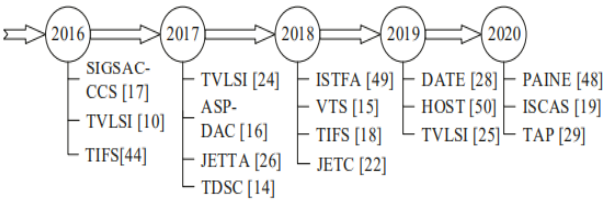

Fig. 2. Timeline of recently proposed hardware Trojan detection techniques.

A. Design-Time (Pre-Silicon) Detection Technique

Several methods for checking the security of SoCs have been made for the pre-silicon stage of the design process. These techniques are shown in Figure 3. Dynamic and static security verification are the two main categories into which these methods fall. The detailed taxonomy is illustrated in Figure 4. Static security verification methods focus on analyzing the RTL codes of an SoC design without applying any test vectors. This analysis can be conducted through manual or automated code reviews, where the RTL code is examined for potential security issues and vulnerabilities. Moreover, static verification-based methods include property-driven formal verification techniques [21]. In such techniques, a mathematical representation of the design is created and verified against various security properties and requirements.

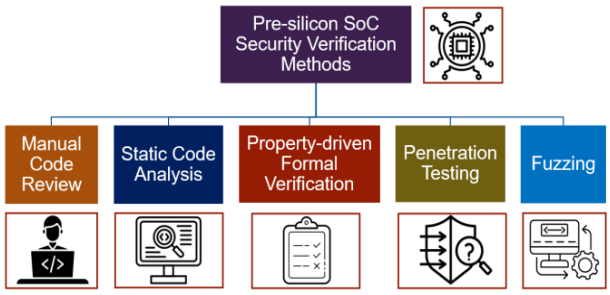

Fig. 3. Pre-silicon SoC security verification techniques.

Pre-silicon (design-time) identification in order to ensure the security of a SoC before it is manufactured, design-time techniques include human code review, automatic code analysis, formal methods for verifying security properties, penetration testing to simulate attack scenarios, and fuzzing to find hidden vulnerabilities through random input generation.

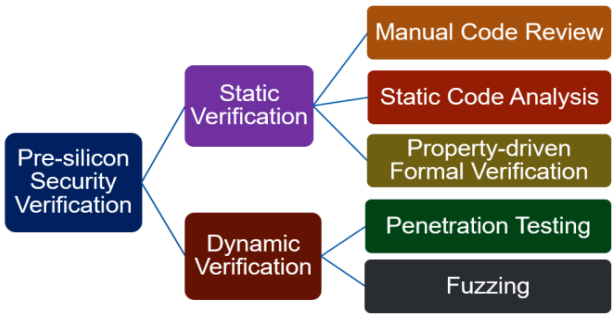

Fig. 4. Taxonomy of SoC security verification techniques at the pre-silicon stage.

Pre-silicon security verification is a combination of both static and dynamic techniques that ensure that vulnerabilities are detected during a pre-fabrication phase. Manual code review, automated code analysis, and formal property checks are employed in the process of performing statistical verification to identify structural and logical defects at an early stage. Dynamic verification uses penetration testing and fuzzing to provide attack scenarios and unforeseen inputs, which are designed to expose runtime security vulnerabilities in the design.

B. Power Side Channel Trojan Technique

Post-silicon hardware Trojan (HT) detection could be achieved, for example, by analyzing signals from power-side channels. Without physically accessing the chip's internal structure, this approach can detect HT symptoms by analyzing the power consumption patterns of integrated circuits (ICs) while they are operating [22][23]. Using sophisticated machine learning algorithms on datasets like the "Power and Electromagnetic Side-Channel Signals of Hardware Trojan Benchmarks," one can detect subtle changes or outliers in power traces that point to malicious modifications. This method improves scalability and versatility by detecting HTs using pattern recognition and feature extraction spanning time, frequency, and wavelet domains, instead of relying on standard golden reference ICs.

C. Intelligent Detection and Trusted Soc Design

Machine learning (ML) frameworks for detecting hardware trojans, including support vector machines (SVMs), decision trees (DTs), and reinforcement learning, have used

© JGREC 2025, All Rights Reserved

RTL-level verification to identify patterns in Verilog/VHDL conditional statements that could compromise security. Machine learning models that self-reference and undergo dynamic post-processing can now be used as a substitute for golden reference chips, enabling the non-destructive identification of Trojans in commercially available components. Physically unclonable function-based encryption is one of several approaches being investigated as potential defenses against Trojan horses and authentication methods that could compromise secure silicon systems. Trickery at the design stage makes it more difficult to prevent hardware Trojan injection or other intrusive ways of attack [24]. The TroLLoc framework reduces on-die security pitfalls after design by combining logic obfuscation with secure placement/routing. Recent research identifies possible weaknesses in logic locking methods, including the possibility of unintentional data leaking and key recovery attacks [25]. To test the efficacy of logic-locking methods, AI-assisted vulnerability evaluations are being developed.

1) Progression of Trojan Detection in SoCs

Hardware Trojan problem designs, classifications, and defenses have been covered in a number of great surveys. Extensive analyses have brought attention to intricate HT risks and demonstrated workable defenses against attacks throughout the PLD and ASIC life cycles. The security and trust challenges linked to FPGA-based systems, as well as the necessary solutions, have been covered in earlier research. New categories of detection and counterattack methods were introduced, and taxonomies of HT risks were clarified by more research. Reviews have also examined current protection strategies and detailed particular HT risks encountered during IC development procedures [26]. Some investigated whether Trojan insertions and similar defence measures could be implemented at any point in the IC development and production process, while others looked at possible trends for the future, current technology, and lessons learnt from HT related issues.

2) Data Sources and Signal Modalities for Detection

Side-channel information, or the exterior physical characteristics made evident by the circuit's operation, includes time consumption, energy expenditure, and electromagnetic information [27]. A collection of intrinsic physical characteristic data is generated by the original circuit operating in the same experimental setting. Similarly, the original circuit's side-channel data and the additional physical data produced by the hardware Trojan module are different. One way to tell if a hardware Trojan is present in a circuit is to compare this difference [28]. Hardware Trojan detection research is shifting its focus to side-channel analysis due to its accuracy, speed, and low cost.

V. Literature Review

This literature review highlights Recent studies that highlight the growing use of ML and DL techniques for detecting Hardware Trojans in SoC designs. These methods improve accuracy, scalability, and post-deployment monitoring by analyzing system behaviors and side-channel patterns. However, challenges such as computational overhead, data variability, and limited cross-platform generalization remain.

John et al. (2025) employed machine learning algorithms alongside side-channel analysis to detect hardware that was not in use. Trojan horses. Collected power consumption data from an Artix FPGA running an AES-128 algorithm that included various Trojan insertions. Experimental results show that applying machine learning directly to power consumption traces allows for effective Trojan detection without extensive feature extraction. Among the classifiers evaluated, the Random Forest model achieved a detection accuracy of 98%, outperforming existing methods. The K-Nearest Neighbors (KNN) classifier also showed strong performance, achieving an accuracy of 97%. The proposed method reduces preprocessing requirements, lowers computational costs, and improves noise robustness, thereby enabling the post-deployment detection of Trojans in integrated circuits [29].

Saraf, Kulkarni and Niamat (2025) presented a DL-based framework for detecting hardware Trojans in ICs using SCA and Challenge-Response Pairs (CRPs) from Ring Oscillator Physical Unclonable Functions (ROPUFs). A Trojan-infected ROPUF is implemented on an Artix7 FPGA using VHDL in the AMD Xilinx Vivado Design Suite. Power, voltage, and current traces are collected using Keysight DC power analyzers under Trojan-active and Trojan-inactive states to assess the impact of Trojan circuits. The study employs advanced DLAs, including CNN, RNN, LSTM, and DCN, to analyze subtle variations in the collected datasets [30].

Hemavathy, Jagadeesh and Bhaaskaran (2025) The suggested framework has been shown to have an average execution time of 40.184 ms for Trojan identification. The suggested framework has been tested with two metrics: use scale and digest uniqueness. Use scale shows how Trojans affect the resource used, while digest uniqueness varies from 45.3% to 55% and indicates the presence of Trojans. Computation and communication expenses are also used to validate the authentication protocol's performance. Burrows-Abadi-Needham (BAN) logic and informal techniques are used in the formal analysis of the authentication protocol to verify its resilience to hardware-based attacks [31].

Tahghigh and Salmani (2024) introduced a novel method for reference-free HT detection in manufactured ICs, leveraging Gaussian mixture models (GMMs) with power side-channel signals. Experimental results, conducted on AES-128 with various hardware Trojans, demonstrate an accuracy exceeding 95.52%. To be introduced for the first time, to the best of knowledge, proposed GMM-based HT detection method also provides a probabilistic framework, attributing evolving probability values to individual side-channel measurements to indicate potential HT activation. Consequently, it becomes feasible to ascertain with a high level of confidence whether a manufactured design has been tampered with an HT [32].

Rusu et al. (2024) introduced several solutions for the multivariate extension of a previously designed single-response adaptive pre-silicon integrated circuit verification approach employing machine learning algorithms. These techniques aim to achieve the most accurate identification of worst-case circuit behavior through simultaneously modeling multiple electrical parameters (EP). The usefulness of the proposed methods was verified by extensive testing on several synthetic test functions that were designed to simulate the operation of actual circuits. Through testing on a physical Low Dropout Voltage Regulator (LDO) circuit, can verify the reliability and precision of the algorithms [33].

Dakhale et al. (2023) proposed a method for HT detection that is based on the VGG-Net architecture. Using the

© JGREC 2025, All Rights Reserved

Advanced Encryption Standard (AES) benchmarks T500, T600, T700, T800, and T1600, the model achieves an average accuracy of 91.2%, with individual scores of 93%, 87%, 100%, and 76%. It outperforms the state-of-the-art versions in the AES-T600, AES-T700, AES-T800, and AES-T1600 benchmarks [34].

Zhang et al. (2022) suggested an innovative technique that uses electromagnetic radiation differences to identify hardware Trojans. When the electromagnetic radiation of the suspect IC differs from that of the authentic IC in the designated mode by more than the threshold, a hardware Trojan is deemed to be present. Experiments on hardware Trojan detection in FPGA demonstrate that the suggested technique may successfully differentiate between the radiation emission of Trojan IC and authentic IC [35].

Table I summarizes recent research on Hardware Trojan detection strategies in System-on-Chip (SoC) architectures. The studies are organized according to study topic, methodology, major findings, obstacles, and potential future research areas.

TABLE I. SUMMARY OF RECENT STUDIES ON HARDWARE TROJAN DETECTION TECHNIQUES

Reference	Study On	Approach	Key Findings	Challenges / Limitations	Future Directions
John et al. (2025)	ML-based Trojan detection with power traces on Artix FPGA (AES-128)	ML on power-consumption traces to detect Trojan	Applied ML classifiers (RF, KNN) to Trojan detection 98% and 97% accuracy; does not need heavy feature extraction	low power usage and high tolerance to noise May need good-trace collection	Expand to deep-learning, test on larger FPGA/ASIC datasets, real-world deployment
Saraf, Kulkarni & Niamat (2025)	DL-based Trojan detection based on SCA + ROPUF (Artix7 FPGA)	CNN, RNN, LSTM, DCN on power/voltage/current trace measured with Keysight	analyzers Deep models were able to capture fine differences in traces	effective Trojan-active vs. inactive detection large datasets	high compute, complex model training required to be discovered
Hemavathy, Jagadeesh & Bhaaskaran (2025)	Trojan identification & authentication protocol evaluation	Proposed framework with utilization scale + BAN logic	validation 40.184 ms avg. identification time; digest uniqueness 45.3-55% identity validation protocol;	limited hardware diversity in use	more protocol side-focused; not as diverse hardware collections as possible
Tahghigh & Salmani (2024)	Reference-free HT detection of AES-128 ICs	using GMMs on power SCA data Gaussian Mixture Models	on power SCA data Achieved >95.52% accuracy	probabilistic detection of HT activation likelihood May not work with very noisy signals	very large signal-to-noise ratios between manufacturing batches
Rusu et al. (2024)	Multivariate ML based pre-silicon IC verification	ML modeling of a variety of electrical parameters to make a worst-case prediction	Accurate consistency over many synthetic functions; verified on actual LDO circuits	Only focuses on pre-silicon stage only	Extend to post-silicon SCA, no post-silicon verification established
Dakhale et al. (2023)	HT detection with VGG-Net on AES Trojan benchmarks	Deep CNN (VGG-Net) classification on AES T500-T1600	Accuracy: 93, 87, 100, 100, 76 (mean 91.2) better than previous models	HT detection with VGG-Net on AES	Develop lightweight model specially CNN
Zhang et al. (2022)	FGPA based Trojan detection	difference analysis and Electromagnetic radiation	Effectively difference in Trojan vs. genuine IC by thresholds	Sensitive to environmental noise; requires calibrated EM setup	Improve noise filtering; develop portable EM-based detection tools

VI. CONCLUSION AND FUTURE WORK

In the modern System-on-Chip (SoC) designs, hardware Trojan detection has become a more critical concern as security vulnerabilities are being increased by the chip complexity and the process of globalization. Recent developments made in the area of ML- and DL-based methods were also discussed in the context of this study to gain insight into their efficiency in both design-time and post-silicon detection conditions. The reviewed papers indicate that machine learning classifiers, deep neural networks, probabilistic models, and post-deployment detection based on side-channels are crucial to improving accuracy, noise robustness, and capabilities of detection. The use of Random Forest-based trace analysis, DL techniques involving the use of ROPUF variables, and GMM-based reference-free classification have high potential for public deployment, whereas EM-based and multivariate verification techniques focus on the digital and analog worlds. Also, metrics such as digest uniqueness and utilization scale also reinforce authentication structures. Although these are improved, there are still constraints, such as high computational needs, sensitivity to environmental noise, poor cross-platform generalization, and high-quality datasets are required.

It is the direction of future research to make lightweight and explainable AI models, which can run effectively on-chip and at the same time have high detection accuracy. The growth of standardized benchmark databases, in particular, of mixed-signal and real-world hardware, will assist in enhancing the generalization of models. Adaptive and multimodal detection frameworks are also required, which incorporates power, EM, timing and PUF metrics in order to enhance resistance to changing Trojans. The further development of trusted SoC will involve integrating safe design automation tools, improving logic-locking validation and evaluation of the real-time post-deployment monitoring methods.

REFERENCES

[1] U. A. Korat and A. Alimohammad, "A Reconfigurable Hardware Architecture for Principal Component Analysis," *Circuits, Syst. Signal Process.*, vol. 38, no. 5, pp. 2097–2113, 2019, doi: 10.1007/s00034-018-0953-y.

[2] M. Gupta, S. Gupta, and P. Aswal, "Comprehensive Analysis of System on Chips: Architecture, Applications, and Future Trends," Oct. 2024. doi: 10.22541/au.172977161.13847266/v1.

[3] Y. Macha and S. K. Pulichikkunnu, "A Survey of DevOps Practices for Machine Learning and Artificial Intelligence Workflows in Modern Software Development," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, pp. 200–208, 2024, doi: 10.56472/25832646/JETA-V4I3P121.

[4] V. T. Hayashi and W. V. Ruggiero, "Hardware Trojan Detection

© JGREC 2025, All Rights Reserved

in Open-Source Hardware Designs Using Machine Learning," *IEEE Access*, vol. 13, pp. 37771–37788, 2025, doi: 10.1109/ACCESS.2025.3546156.

[5] R. Patel, "Remote Troubleshooting Techniques for Hardware and Control Software Systems: Challenges and Solutions," *Int. J. Res. Anal. Rev.*, vol. 11, no. 2, pp. 933–939, 2024.

[6] M. Xue, C. Gu, W. Liu, S. Yu, and M. O'Neill, "Ten years of hardware Trojans: a survey from the attacker's perspective," *IET Comput. Digit. Tech.*, vol. 14, no. 6, pp. 231–246, Nov. 2020, doi: 10.1049/iet-cdt.2020.0041.

[7] K. Hu, A. N. Nowroz, S. Reda, and F. Koushanfar, "High-Sensitivity Hardware Trojan Detection Using Multimodal Characterization," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, New Jersey: IEEE Conference Publications, 2013, pp. 1271–1276. doi: 10.7873/DATE.2013.263.

[8] S. Gupta, "Systems used for Power-Constrained Testing of Digital Circuits: A Review of DFT and Power Management Integration," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 597–606, Aug. 2025, doi: 10.48175/IJARSCT-28675.

[9] V. Prajapati, "Improving Fault Detection Accuracy in Semiconductor Manufacturing with Machine Learning Approaches," *J. Glob. Res. Electron. Commun.*, vol. 1, no. 1, 2025, doi: 10.5281/zenodo.14935091.

[10] V. Panchal, "Mobile SoC Power Optimization: Redefining Performance with Machine Learning Techniques," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 13, no. 12, Dec. 2024, doi: 10.15680/IJIRSET.2024.1312117.

[11] C. Dong, Y. Xu, X. Liu, F. Zhang, G. He, and Y. Chen, "Hardware Trojans in Chips: A Survey for Detection and Prevention," *Sensors*, vol. 20, no. 18, Sep. 2020, doi: 10.3390/s20185165.

[12] C. Chircov, A. C. Bîrcă, A. M. Grumezescu, and E. Andronescu, "Biosensors-on-Chip: An Up-to-Date Review," *Molecules*, vol. 25, no. 24, Dec. 2020, doi: 10.3390/molecules25246013.

[13] S. K. Senthilkumar Thangavel, Arnav Kotiyal, Ancy Thomas, Harshal Patil, "Robust Authentication Protocols for IoT Devices in High-Density Networks," *2024 Int. Conf. Distrib. Syst. Comput. Networks Cybersecurity*, pp. 1–7, 2024.

[14] R. Parikh and K. Parikh, "Survey on Hardware Security: PUFs, Trojans, and Side-Channel Attacks," *Int. J. Eng. Res. Appl.*, vol. 15, no. 2, pp. 30–37, Jan. 2025, doi: 10.9790/9622-15023037.

[15] F. Basholli, B. Mema, D. Hyka, A. Basholli, and A. Daberdini, "Analysis of Security Challenges in SCADA Systems, a Technical Review on Automated Real-time Systems," in *Advanced Engineering Days (AED)*, 2023.

[16] H. Li, Q. Liu, and J. Zhang, "A survey of hardware Trojan threat and defense," *Integration*, vol. 55, pp. 426–437, Sep. 2016, doi: 10.1016/j.vlsi.2016.01.004.

[17] S. Grover, S. Yadav, S. K. Tiwari, and S. Ramachandran, "Engineering Robust AI Products Through Continuous Quality Assurance: A Framework for Testing, Monitoring, and Validation of Adaptive Live Learning AI/ML Systems in Dynamic Production Environments," *Int. J. Appl. Math.*, vol. 38, no. 2s, pp. 1092–1113, Oct. 2025, doi: 10.12732/ijam.v38i2s.710.

[18] L. Aniello, B. Halak, P. Chai, R. Dhall, M. Mihalea, and A. Wilczynski, "Anti-BlUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF," *Int. J. Inf. Secur.*, vol. 20, no. 3, pp. 445–460, Jun. 2021, doi: 10.1007/s10207-020-00513-8.

[19] B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "Benchmarking of Hardware Trojans and Maliciously Affected Circuits," *J. Hardw. Syst. Secur.*, vol. 1, no. 1, pp. 85–102, Mar. 2017, doi: 10.1007/s41635-017-0001-6.

[20] A. Jain, Z. Zhou, and U. Guin, "Survey of Recent Developments for Hardware Trojan Detection," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, IEEE, May 2021, pp. 1–5. doi: 10.1109/ISCAS51556.2021.9401143.

[21] R. Kibria, F. Farahmandi, and M. Tehranipoor, "A Survey on SoC Security Verification Methods at the Pre-silicon Stage," 2024.

[22] R. Patel, "Advancements in Renewable Energy Utilization for Sustainable Cloud Data Centers : A Survey of Emerging Approaches," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 5, pp. 447–454, 2023.

[23] N. P. Bhatta and F. Amsaad, "ML Assisted Techniques in Power Side Channel Analysis for Trojan Classification," *Cluster Comput.*, vol. 28, no. 3, Jun. 2025, doi: 10.1007/s10586-024-04715-w.

[24] R. Parikh and K. Parikh, "A Survey on AI-Augmented Secure RTL Design for Hardware Trojan Prevention," *J. Comput. Commun.*, vol. 13, no. 04, pp. 197–209, 2025, doi: 10.4236/jcc.2025.134013.

[25] V. Rajavel and R. Gahlot, "Advanced Fault Diagnosis of CMOS Circuit Design by Leakage Measurement in Nanometer Technology," in *2025 IEEE 5th International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI SATA)*, IEEE, May 2025, pp. 1–6. doi: 10.1109/VLSISATA65374.2025.11070065.

[26] Z. Huang, Q. Wang, Y. Chen, and X. Jiang, "A Survey on Machine Learning Against Hardware Trojan Attacks: Recent Advances and Challenges," *IEEE Access*, vol. 8, pp. 10796–10826, 2020, doi: 10.1109/ACCESS.2020.2965016.

[27] Pritesh B Patel, "Energy Consumption Forecasting and Optimization in Smart HVAC Systems Using Deep Learning," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 3, pp. 780–788, Jun. 2024, doi: 10.48175/IJARSCT-18991.

[28] W. Tang, J. Su, J. He, and Y. Gao, "A Deep Learning Method Based on the Attention Mechanism for Hardware Trojan Detection," *Electronics*, vol. 11, no. 15, Jul. 2022, doi: 10.3390/electronics11152400.

[29] A. K. John, S. T. Pitta, J. Dofe, and J. G. Pandey, "Hardware Trojan Detection with Machine Learning and Power Side-Channels: A Post-Deployment Analysis," in *2025 IEEE Conference on Communications and Network Security (CNS)*, IEEE, Sep. 2025, pp. 1–6. doi: 10.1109/CNS66487.2025.11195049.

[30] M. Saraf, A. R. Kulkarni, and M. Niamat, "Detecting Hardware Trojans: Deep Learning Solutions Combining PUF Metrics and Side-Channel Observations," in *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*, IEEE, Feb. 2025, pp. 1–5. doi: 10.1109/SATC65530.2025.11137155.

[31] S. Hemavathy, K. Jagadeesh, and V. S. K. Bhaaskaran, "Unified Security Framework Using Device-Specific Fingerprint: Mitigating Hardware Trojans and Authenticating Firmware Updates," *IEEE Access*, vol. 13, pp. 26897–26914, 2025, doi: 10.1109/ACCESS.2025.3538936.

[32] M. Tahghigh and H. Salmani, "Detecting Hardware Trojans in Manufactured Chips without Reference: A GMM-Based Approach," in *Proceedings of the 43rd IEEE/ACM International Conference on Computer-Aided Design*, New York, NY, USA: ACM, Oct. 2024, pp. 1–7. doi: 10.1145/3676536.3689919.

[33] A. Rusu, E. David, M.-D. Ţopa, V. Grosu, A. Buzo, and G. Pelz, "On Approaching Multivariate IC Pre-silicon Verification Using ML-based Adaptive Algorithms," in *2024 IEEE 30th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, IEEE, Jul. 2024, pp. 1–3. doi: 10.1109/IOLTS60994.2024.10616057.

[34] B. Dakhale, K. Vipinkumar, K. Narotham, S. Kadam, A. A. Bhurane, and A. G. Kothari, "Automated Detection of Hardware Trojans using Power Side-Channel Analysis and VGG-Net," in *2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS)*, IEEE, Apr. 2023, pp. 1–5. doi: 10.1109/PCEMS58491.2023.10136083.

[35] F. Zhang, D. Zhang, Z. Peng, Q. Ren, A. Chen, and D. Su, "Hardware Trojan Recognition based on Radiated Emission Characteristics," in *2022 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, IEEE, Sep. 2022, pp. 82–84. doi: 10.1109/APEMC53576.2022.9888518.

© JGREC 2025, All Rights Reserved