International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 7, July 2024)

Artificial Intelligence based Security Solution For Data Encryption in VLSI Applications

[1]Chhavi Baghmare, [2]Prof. Nitesh Kumar

[1]Research Scholar, Dept. of Electronics and Comm. Engineering, Sagar Institute of Research & Technology, Bhopal, India,
[2]Assistant Professor, Dept. of Electronics and Comm. Engineering, Sagar Institute of Research & Technology, Bhopal, India

***Abstract*— In the era of ubiquitous computing, ensuring data security in Very Large Scale Integration (VLSI) applications has become increasingly critical. This paper explores the application of artificial intelligence (AI) in enhancing data encryption mechanisms within VLSI systems. AI-based security solutions offer adaptive and robust approaches to protect sensitive information against evolving cyber threats. This review provides a comprehensive overview of current AI techniques employed in data encryption for VLSI applications, including machine learning algorithms, neural networks, and hybrid models. We examine the advantages and limitations of these techniques, along with their impact on performance, power consumption, and security. The paper also discusses the challenges and future research directions in integrating AI with VLSI for robust data encryption, aiming to provide insights into developing next-generation secure VLSI systems.**

Keywords—AI, VLSI, Decryption, Encryption, Security.

I. INTRODUCTION

With the rapid advancement of technology and the proliferation of connected devices, data security has become a paramount concern, especially in Very Large Scale Integration (VLSI) applications. VLSI technology, which integrates millions of transistors onto a single chip, is foundational to modern electronic systems, encompassing applications from consumer electronics to critical infrastructure. As the complexity and connectivity of VLSI systems increase, so does their vulnerability to security breaches and cyber-attacks. Ensuring the confidentiality, integrity, and availability of data within these systems is crucial.

Traditional data encryption methods, while effective, often struggle to keep pace with the sophistication of contemporary cyber threats. The static nature of conventional encryption algorithms can make them predictable and vulnerable to advanced attacks. This has led to the exploration of artificial intelligence (AI) as a means to enhance the security of data encryption in VLSI applications. AI, with its ability to learn from data, adapt to new threats, and optimize processes, presents a promising avenue for developing more robust and dynamic security solutions.

AI-based security solutions for data encryption leverage various techniques, including machine learning algorithms, neural networks, and hybrid models that combine multiple AI approaches. Machine learning algorithms can analyze patterns in data and detect anomalies that may indicate security breaches. Neural networks, particularly deep learning models, can learn complex representations of data and generate more secure encryption keys. Hybrid models, which integrate different AI techniques, can offer enhanced security by combining the strengths of individual methods.

One of the primary advantages of AI-based encryption is its adaptability. Unlike static algorithms, AI models can continuously learn from new data and evolving threats, allowing them to dynamically adjust their encryption strategies. This adaptability is particularly beneficial in VLSI applications, where the operating environment and threat landscape can change rapidly. Additionally, AI-based solutions can optimize encryption processes to balance security, performance, and power consumption, which is crucial for the resource-constrained nature of VLSI systems.

However, integrating AI with VLSI for data encryption also presents several challenges. The computational complexity of AI models can lead to increased power consumption and latency, which are critical constraints in VLSI applications. Ensuring the reliability and robustness of AI models in diverse and dynamic environments is another significant challenge. Furthermore, the security of AI models

themselves must be considered, as they can be susceptible to adversarial attacks that manipulate the model's inputs to produce incorrect outputs.

Despite these challenges, the potential benefits of AI-based security solutions for data encryption in VLSI applications are substantial. By leveraging AI, it is possible to develop more secure, efficient, and adaptable encryption mechanisms that can protect sensitive data against sophisticated cyber threats. The integration of AI with VLSI technology represents a promising frontier in the quest for enhanced data security.

This paper provides a comprehensive review of current AI techniques employed in data encryption for VLSI applications. We examine various machine learning algorithms, neural network architectures, and hybrid models, evaluating their effectiveness, advantages, and limitations. The review also addresses the impact of AI-based encryption on performance, power consumption, and security. Furthermore, we discuss the challenges and future research directions in this field, offering insights into the development of next-generation secure VLSI systems. By exploring the intersection of AI and VLSI, this paper aims to contribute to the advancement of robust and adaptive data encryption solutions that can meet the demands of modern electronic systems.

II. LITERATURE REVIEW

A. K. Mishra et al.,[1] The Internet of Things (IoT) has a significant impact on the transportation industry. Autonomous vehicles (AVs) were created to make daily activities easier by hauling goods, distributing packages, and easing traffic. The AVs had a wide range of uses and comprised land vehicles, aerial vehicles, and maritime vehicles. The Cyber Security (CS) enabled data transfer autonomous driving was set up by them to facilitate the solution of this challenge. A network acts as the mediator, downloading data of the transmitter to the autonomous car. For additional safety, the CS -based method Advanced Encryption Standard (AES) is involved to decrypt the data, which is transferable to cypher text.

K. Shahbazi et al.,[2] presented architecture includes 8-bit datapath and five main blocks. It is designed two specified register banks, Key-Register and State-Register, for storing the plain text, keys, and intermediate data. To reduce the area, Shift-Rows is embedded inside the State-Register. To adapt the Mix-Column to 8-bit datapath, we design an optimized 8-bit block for Mix-Columns with four internal registers, which accept 8-bit and send back 8-bit. Also, a shared optimized Sub-Bytes is employed for the key expansion phase and encryption phase. To optimize Sub-Bytes, we merge and simplify some parts of the Sub-Bytes. To reduce power consumption, we apply the clock gating technique to the design.

M. Risso et al.,[3] focuses on Temporal Convolutional Networks (TCNs), a convolutional model for time-series processing that has recently emerged as a possible option to more complicated recurrent designs. TCNs have emerged as a promising alternative to more complex recurrent architectures as a result of recent developments. We provide the first NAS tool that specifically addresses the optimisation of the most unusual architectural characteristics of TCNs, namely dilation, receptive-field, and the amount of features in each layer. This tool is intended to be used in the design of TCNs. The strategy that has been presented looks for networks that provide favourable trade-offs between the precision of their results and the amount of parameters and operations they need, which enables efficient deployment on embedded platforms. Additionally, its primary characteristic is that it is simple and undemanding in terms of the level of search complexity, which enables it to be used even with constrained hardware resources.

Z. Chen et al.,[4] Physical Unclonable Function, often known as PUF, is a Nano or lightweight security primitive that may be used for device authentication in the Internet of Things. On the other hand, every single strong PUF instance is had to retain a minimum of 106 trustworthy challenge-response pairs in the centre nodes. This necessitates an excessive storage cost due to the fact that centres link enormous distant PUFs. An obfuscation-feedback-shift-register (OFSR) PUF is conceived, constructed, and implemented in this short. The PUF is made up of certain weak PUF cells that collaborate with an obfuscation mechanism.

D. Xu et al.,[5] provide a decryption strategy for ring-BinLWE that is based on 2's complement ring and aims to be more precise and secure than previous methods. The re-derived decryption function shows a considerable improvement in the decoding rate over the prior decryption function, increasing it by a factor of fifty percent. In addition, on the basis of the proposed decryption function, high-performance and Nano or lightweight hardware designs for terminal devices in the IoT are respectively provided. These hardware architectures are scalable and may be readily modified to ring-BinLWE hardware deployment with various parameter sets.

K. Alhaj et al.,[6] In a wide range of real-world applications using artificial intelligence (AI), convolutional neural networks, often known as CNNs, have been shown to be very successful. The layer depth of CNN, on the other hand, becomes deeper as user applications get more complex. This results in a significant rise in the number of operations as well as the amount of memory used. Because of the enormous quantity of intermediate data that is created, there is an excessive amount of data transit between the memory and the processing cores, which causes a significant bottleneck. In-memory computing (IMC) is an attempt to circumvent this barrier by doing computations directly inside the memory itself.

S. Charles et al.,[7] The limited availability of resources that are inherent to SoCs is a significant barrier to the development of effective security solutions against these types of assaults. In specifically, an eavesdropping attack is carried out when a router that is attacked with a Trojan replicates packets that are routed across the NoC and then reroutes the copied packets to an associated malicious programme that is operating on another IP in an effort to get private information. Although authenticated encryption may prevent attacks of this kind, the overhead it causes in systems on a chip with limited resources is unacceptable. In this piece, we will discuss a potential Nano or lightweight defence option that is based on digital watermarking methods.

R. Della Sala et al.,[8] presented a brand new Nano or lightweight Physical Unclonable Function (PUF) primitive that is compatible with FPGAs and is based on XOR gates. The XOR-PUF that has been suggested is the most compact FPGA-compatible PUF that has ever been published in the literature. It makes it possible to construct four PUF bits inside a single Configurable Logic Block (CLB) and has extremely high statistical performance. The design of the proposed PUF makes use of two cross-coupled XOR gates, each of which has the potential to take on the characteristics of either ring oscillators or SRAM cells depending on the specific configuration chosen.

J. Kaur et al.,[9] The Nano or lightweight architecture of ASCON makes use of a 320-bit permutation that is bit-sliced into five 64-bit register words in order to provide 128-bit level security. In this document, error detection algorithms for secure hardware implementations of ASCON are proposed for the first time. For both LUT and logic-based implementations of ASCON, the suggested techniques, which include signature, interleaved signature, and cyclic redundancy check approaches, are provided. These approaches are referred to as "signatures." The suggested error detection methods are further evaluated using two different FPGA families (Spartan-7 and Kintex-7), demonstrating that they achieve acceptable levels of space, power, and delay overheads. In addition, the suggested procedures provide a high error coverage, with a value of 99.99 percent, as shown by simulations run with 644,000 inserted faults. Therefore, the purpose of these techniques is to improve the reliability of the various ASCON designs.

F. Xu et al.,[10] The results of our practical investigations on AWS Lambda suggest that the unexpected performance of serverless DDNN training is mostly attributable to the resource constraint posed by Parameter Servers (PS) and the limited capacity of the local batches. We build and implement DNN, a cost-effective framework for function resource provisioning, in this article. Its purpose is to deliver predictable performance for serverless DDNN training workloads while simultaneously preserving the budget for provided functions. We create a Nano or lightweight analytical DDNN training performance model by using the PS network bandwidth and function CPU utilisation. This model enables us to design a DNN resource provisioning strategy, which is necessary in order to ensure DDNN training performance with serverless functions.

III. CHALLENGES

While AI-based security solutions offer promising advancements for data encryption in VLSI applications, several challenges must be addressed to fully realize their potential. These challenges span technical, operational, and ethical domains, requiring comprehensive strategies to overcome them effectively.

1. Computational Complexity

AI models, particularly deep learning algorithms, can be computationally intensive. Implementing these models within VLSI systems, which are inherently resource-constrained, poses significant challenges. The increased computational requirements can lead to higher power consumption and latency, adversely affecting the performance and efficiency of VLSI applications. Developing lightweight and efficient AI models that can operate within the limited resources of VLSI systems is a critical challenge.

2. Power Consumption

VLSI applications often operate in environments where power efficiency is crucial. The integration of AI-based

encryption techniques can lead to increased power consumption, which may not be sustainable for battery-powered or energy-sensitive devices. Balancing the need for robust security with the constraints of power consumption requires innovative approaches to optimize AI algorithms and hardware implementations.

3. Real-time Processing

Many VLSI applications, such as those in autonomous systems, medical devices, and real-time communication, require immediate data processing and encryption. Ensuring that AI-based encryption methods can meet the stringent real-time requirements without compromising security or performance is a significant challenge. Achieving real-time processing necessitates the development of fast and efficient algorithms capable of handling high-throughput data streams.

4. Model Reliability and Robustness

AI models used for encryption must be reliable and robust across diverse and dynamic environments. Variability in operational conditions, such as temperature changes and electromagnetic interference, can affect the performance of VLSI systems. Ensuring that AI models maintain their effectiveness and security under these varying conditions is essential. Additionally, the models must be resilient to adversarial attacks that attempt to exploit vulnerabilities in the AI algorithms.

5. Data Quality and Availability

High-quality data is essential for training effective AI models. In the context of VLSI applications, obtaining large and diverse datasets that accurately represent the operational environment and potential threats can be challenging. Limited availability of such data can hinder the development of robust AI-based encryption solutions. Furthermore, ensuring that the data used for training is free from biases and accurately labeled is crucial for developing reliable models.

IV. CONCLUSION

AI-powered encryption offers a promising avenue for securing data in VLSI applications. By leveraging machine learning's adaptability, AI can potentially generate stronger encryption algorithms, identify and respond to emerging threats more efficiently, and optimize key management for improved security within the physical constraints of VLSI circuits. This integration of AI and cryptography holds the potential to revolutionize data security in the ever-evolving world of VLSI design.

REFERENCES

1. A. K. Mishra, N. Tripathi, M. Vaqur and S. Sharma, "Artificial Intelligence based Security Solution for Data Encryption using AES Algorithm," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 1685-1690, doi: 10.1109/ICSCDS56580.2023.10104702.
2. K. Shahbazi and S. -B. Ko, "Area-Efficient Nano-AES Implementation for Internet-of-Things Devices," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 1, pp. 136-148, Jan. 2021, doi: 10.1109/TVLSI.2020.3033928.
3. M. Risso et al., "Nano or lightweight Neural Architecture Search for Temporal Convolutional Networks at the Edge," in IEEE Transactions on Computers, vol. 72, no. 3, pp. 744-758, 1 March 2023, doi: 10.1109/TC.2022.3177955.
4. Z. Chen et al., "A Nano or lightweight and Machine-Learning-Resistant PUF Using Obfuscation-Feedback-Shift-Register," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 11, pp. 4543-4547, Nov. 2022, doi: 10.1109/TCSII.2022.3193002.
5. D. Xu, X. Wang, Y. Hao, Z. Zhang, Q. Hao and Z. Zhou, "A More Accurate and Robust Binary Ring-LWE Decryption Scheme and Its Hardware Implementation for IoT Devices," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 8, pp. 1007-1019, Aug. 2022, doi: 10.1109/TVLSI.2022.3174205.
6. K. Alhaj Ali, A. Baghdadi, E. Dupraz, M. Léonardon, M. Rizk and J. -P. Diguet, "MOL-Based In-Memory Computing of Binary Neural Networks," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 7, pp. 869-880, July 2022, doi: 10.1109/TVLSI.2022.3163233.
7. S. Charles, V. Bindschaedler and P. Mishra, "Digital Watermarking for Detecting Malicious Intellectual Property Cores in NoC Architectures," in IEEE

Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 7, pp. 952-965, July 2022, doi: 10.1109/TVLSI.2022.3167606.

8. R. Della Sala, D. Bellizia and G. Scotti, "A Nano or lightweight FPGA Compatible Weak-PUF Primitive Based on XOR Gates," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 6, pp. 2972-2976, June 2022, doi: 10.1109/TCSII.2022.3156788.
9. J. Kaur, M. Mozaffari Kermani and R. Azarderakhsh, "Hardware Constructions for Error Detection in Nano or lightweight Authenticated Cipher ASCON Benchmarked on FPGA," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 69, no. 4, pp. 2276-2280, April 2022, doi: 10.1109/TCSII.2021.3136463.
10. F. Xu, Y. Qin, L. Chen, Z. Zhou and F. Liu, "λDNN: Achieving Predictable Distributed DNN Training With Serverless Architectures," in IEEE Transactions on Computers, vol. 71, no. 2, pp. 450-463, 1 Feb. 2022, doi: 10.1109/TC.2021.3054656.