AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

ISSN 2581 – 3781

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(4)

REVIEW ARTICLE

Review of Emerging Trends in Security-Driven Verification for High-Speed Interconnects (PCIe, CXL, AMBA)

Dr. Parth Gautam*
Associate Professor, Mandsaur University, Mandsaur
Department of Computer Sciences and Applications
Email-parth.gautam@meu.edu.in

Received: 08-10-2025; Revised: 02-11-2025; Accepted: 14-12-2025

Abstract*—The new developments in security-focused verification of high-speed interconnects, including PCIe, CXL and AMBA, highlight the urgent requirement to have a sound verification structure that incorporates both performance and protection in the contemporary computing structure. As heterogeneous platforms, cloud computing applications, and data-intensive applications continue to evolve at a rapid pace, these interconnects are the key to the secure and efficient communication. Security-related verification is moving beyond more traditional correctness checks to incorporate methods that characteristically deal with vulnerabilities, reduce the danger, and make certain that protocols are adhered to. Formal verification, hardware/software co-verification and runtime monitoring approaches are also being increasingly integrated with adaptive machine learning-based approaches in order to detect anomalies and enhance resilience to new threats. Moreover, the use of lightweight authentication, encryption and active threat modeling are increasingly becoming a part of the verification process and the mechanisms of trust are introduced at the first steps of design. The article sheds light on an extensive overview of the current state-of-the-art approaches demonstrating the changes in verification frameworks that are bent on the protection of data integrity, preventing unauthorized access, and ensuring reliability of the systems. This innovation indicates paradigm shift of holistic verification to ensure that performance, scalability, and security are brought together, thus formulating a groundwork of interconnect systems that can support not only efficiency, but also resilience in various operational environments in the future.

***Keywords*–High-speed interconnects, PCIe, CXL, AMBA, security-driven verification, hardware/software co-verification.**

I. INTRODUCTION

The modern computing systems are mostly based on high-speed interconnects which allow efficient communication between processors, accelerators, memory modules and peripheral devices [1]. Cloud computing and artificial intelligence (as well as the scaling of computing platforms to the needs of data intensive applications) imply that the reliability and security of these interconnects is as important to their functionality as performance [2][3]. The secure and verified operation is now the key requirement because the vulnerabilities on the interconnect level may be extended to the large-scale systems, endangering the data integrity and the overall system reliability.

In this environment, PCI Express (PCIe) has become the most popular standard of high-speed data transportation, which is the driving force in computing, networking, and AI-driven workloads [4]. The extensive use of PCIe indicates it as an important facilitator of system performance, but also poses it to a large spectrum of verification obstacles. The demand to have powerful methodologies that confirm functionality and security in heterogeneous deployments has increased as the PCIe market remains to expand at a high rate. Security-based verification is the vital factor in countering such risks like side-channel vulnerabilities [5], misuse of protocols, and unauthorized access, as it is necessary to make the PCIe systems scalable and trustworthy.

In addition to PCIe, Compute Express Link (CXL) is also quickly becoming a groundbreaking technology in interconnect, engineered to both scale out cache coherence as well as allow more sophisticated memory pooling [6]. CXL provides the possibilities of better utilization and performance in large-scale data centers by enabling the disaggregated and shared memory resources in thousands of endpoints. These benefits, however, also present new challenges in the verification, specifically [7], in ensuring the integrity of data, performance isolation, and protocol compliance under heavy loads. Security-related strategies to check CXL verification are necessary to provide coherent operation at memory hierarchies and protection against possible CXL exploits aiming at compromise of cache coherence and pool memory configurations.

The Arm AMBA AXI interconnect is a complementary standard that is used extensively in system-on-chip (SoC) design to enable an efficient data transfer and communication in between processors, accelerators, and peripheral devices [8]. Although AXI has always been performance-oriented, comparatively less attention has been given to the security implication of the use. Recent studies point to the fact that it is important to include verification strategies that are not limited to functional correctness, but also access control, the weak point of bus sharing, and a possible risk of memory corruption. AMBA interconnects must have security-based verification schemes as there is a need to provide a reliable protection system at both IP and system levels.

1.1 Structure of the paper

The structure of the paper is like this: In Section II, we are going to discuss the basic principles of fast interconnects (PCIe, CXL, AMBA). In Section III, the new security-related verification trends will be discussed, among them, AI/ML, HW/SW co-verification, and automated test generation. The major security problems consisting of data integrity, confidentiality, authentication, access control, and protocol vulnerabilities will be illustrated in Section IV. Some research summaries and verification techniques are given in Section V, and Section VI does go into the key points and future directions.

II. HIGH-SPEED INTERCONNECTS

Speaking on a broader perspective, a "high-speed inter-connect" is the one in which the time taken by the propagating signal to travel between its end points cannot be neglected. An obvious factor that influences this definition is the physical extent of the interconnect [9]; the longer the inter-connect, the more time the signal takes to travel between it send points. Smoothness of signal propagation suffers once the line becomes long enough for the signal's rise/fall times to roughly match its propagation time through the line [10]. Then the interconnect electrically isolates the driver and the receivers which no longer act as loads directly on the driver. Instead, within the time of the signal's transition between its high and low voltage levels, the impedance of interconnect becomes the load for the driver and also the input impedance to the receivers. This causes a number of transmission line effects, including reflections, overshoot, undershoot, crosstalk, and modelling of such requirements the integration of EM and circuit modelling.

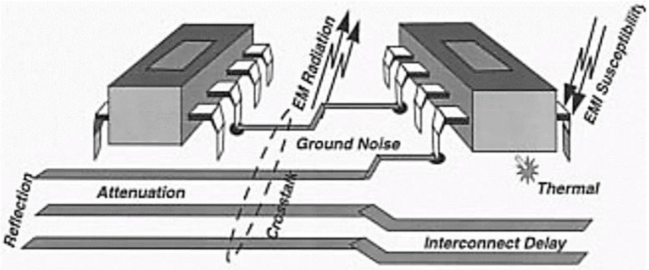

Figure. 1. High-speed interconnect effects

A. PCI Express (PCIe)

According to the PCIe industry-standard roadmap, PCIe 5.0 will provide more efficiency in 5G, AI, and network computing requirements, since its bandwidth is increased to 32.0 Gb/s. The I/O bandwidth doubles every three years in PCI Express. This drives PCIe fabric topology, as it is the main architecture in the current PC industry [11]. PCIe 5.0 products were introduced to the market. Intel™ introduced PCIe 4.0 and PCIe 5.0 solutions to the PC industry, which can provide systems with better performance, as shown in Figure 2. The PCIe 5.0 and PCIe 6.0 technology roadmaps have been verified in other high-speed serial bus protocols

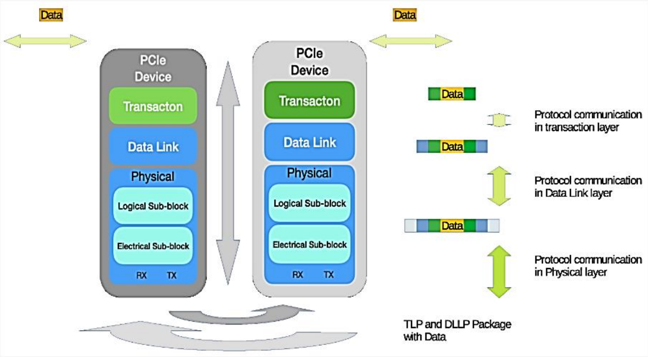

Figure 2. PCIe layers

B. Compute Express Link (CXL)

The original CXL supports coherency and memory semantics on devices that are connected directly to a host. This enables fine-grained heterogeneous processing of shared data structures for CPUs and accelerators as well as cost-effective scale-up for memory bandwidth and capacity [12]. Just like PCIe, CXL is an asymmetric protocol. Root complex (RC) is found in the host processor, one per CXL link, and is connected to a device which is an End Point. Cache Coherency is coordinated by the host processor. Software configures the system through instructions executing in the host processor, which generates the configuration transactions to access each device [13]. CXL is natively x16, x8, and x4 link widths but in degraded mode it is x2 and x1. Degraded mode A PCIe link can also automatically switch to a reduced width and/or frequency to overcome the unexpectedly high error rate on a particular lane. CXL has a data rate of 32.0 GT/s and 64.0 GT/s native, with 16.0 GT/s and 8.0 GT/s data rates supported in degraded mode.

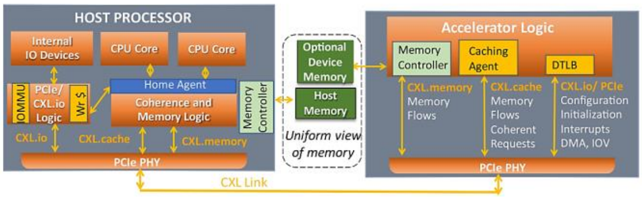

Figure. 3. Dynamic multiplexing of three protocols on PCIe physical layer with CXL

Figure 3 illustrates how CXL offers full interoperability with PCIe, since it uses the PCIe stack. A CXL device will initiate link training with the PCIe Gen 1 Data Rate of 2.5 GT/s and negotiate CXL as the operating protocol with the alternate protocol negotiation mechanism specified by the PCIe 5.0 and PCIe 6.0 specifications in case the link partner can support CXL.

C. Advanced Microcontroller Bus Architecture (AMBA)

AMBA bus architecture consists of three components, namely Advanced High-Performance Bus (AHB), Advanced System Bus (ASB), Advanced Peripheral Bus (APB). AMBA AHB or ASB is high performance bus and has higher bandwidth [14]. So, the components requiring higher bandwidth like High Bandwidth on chip RAM, High-performance ARM processor, High Bandwidth Memory Interface and DMA bus master are connected to the AHB or ASB. AMBA APB is low bandwidth and low performance bus in figure 4. So, the components requiring lower bandwidth like the peripheral devices such as UART, Keypad, Timer and PIO (Peripheral Input Output) devices are connected to the APB [15]. The bridge connects the high performance AHB or ASB bus to the APB bus. So, for APB the bridge acts as the master and all the devices connected on the APB bus acts as the slave. The component on the high-performance bus initiates the transactions and transfer them to the peripherals connected on the APB. So, at a time the bridge is used for communication between the high-performance bus and the peripheral devices.

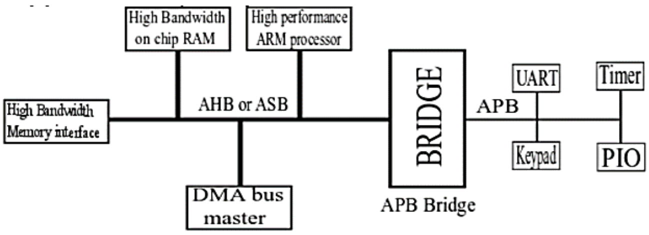
High Bandwidth on chip RAM
High performance ARM processor
High Bandwidth Memory interface
AHB or ASB
DMA bus master
BRIDGE
APB Bridge
APB
UART
Timer
Keypad
PIO

Figure 4: AMBA Bus Architecture

III. EMERGING TRENDS IN SECURITY-DRIVEN VERIFICATION

With the established standards of interconnection, including PCIe, CXL, AMBA, and others, security-oriented verification is becoming more integrated with comprehensive integrity, encryption, and authentication schemes, AI-assisted verification, and oblivious memory access models [16][17]. For example, IDE (Integrity and Data Encryption) is now a requirement for CXL 2.0 with full AES-GCM-based encryption, replay protection, and key exchange with SPDM/CMA/DOE protocols for both the TX and RX channels. Security enhancements for CXL memory are also taking place, for example, Shield CXL will provide physical tamper resistance by sealing CXL memory packages to provide confidentiality, integrity, and freshness in the event of a physical attack [18]. To deal with the growing complexity in verification, AI-based verification schemes that log end-to-end debugs of encrypted CXL traffic and aiding in root-cause analysis, are under development.

A. AI/ML-Based Verification

The process of comparing the performance of a model with some predetermined norms or standards is called validation [19]. This is done because it is essential due to a number of reasons:

1. **Accuracy:** It is important to ensure that models provide predictive accuracy to ensure that users are confident in the model and that the results are desired. False models may cause serious mistakes, particularly in the cutthroat world of health and money.
2. **Fairness:** AI/ML systems are trained regularly on past data, which is prone to stereotypes [20]. These biases will also have to be evaluated and mitigated by the validation process to avoid the discriminatory results that might affect the marginalized groups.
3. **Robustness:** meaning AI/ML models should be resilient to the changes in the input data. Strong validation models verify the capacity of a model to be consistently predictive across various scenarios [21], adversarial attacks and unknown inputs.
4. **Generalization:** The capability of a model to make predictions on new, unobservable data is a major indicator of a model that is effective. Validation frameworks should test the performance of the models in external data to test their ability to be applicable in real-world settings.

B. Hardware and Software Verification

To test the hardware (HW) and debugging software (SW) running in the highly integrated system on chip (SOC) poses technical problems [22]. The processor cores embedded in the SOC are no longer visible, as there are no more pins to connect the in-circuit emulator (ICE) and logic analyzer (LA) for debugging and analysis [23]. ICE and LA, the address, data, and control bus are needed to debug, which are not visible in the SOC [24]. In addition to verifying hardware functionality, the methodology must take into account the growing amount of software used in consumer electronic products. The topics addressed in this section are the following:

- HW/SW verification environment and method
- Soft Prototype
- Verification and authentication
- Rapid Prototyping System
- FPGA based design
- Development of computer printed circuits
- Software Testing

The HW/SW verification procedure and software prototype is demonstrated by a debugging case of the Universal Asynchronous Transmitter and Receiver (UART) utility that was used during the planning.

C. Automated Test Generation for Security

Automated security testing ranges from generating random input (fuzzing) to security testing based on models [25]. The presented approach targets the generation of interaction sequences according to protocols used in IoT systems, the typical domain of MBT. However, instead of developing a full model, a list of commands (e.g., protocol messages) is specified and a test generator from functional testing is applied to create interaction sequences [26]. Sequence generation methods are built on random generation techniques, search based, genetic algorithm, reinforcement learning techniques. Testing using feedback directed online is to identify viable sequences, as well as discourage the production of illegal sequences that break protocol restrictions. This approach creates sequences by executing each selected command during test generation and evaluating the feedback (response of the SUT) before adding them to the sequence. Thus, the approach is able to generate long valid sequences (positive tests) that achieve a deep coverage of internal states as well as sequences that lead to an invalid command call after a number of valid interactions (negative tests).

IV. SECURITY CHALLENGES IN HIGH-SPEED INTERCONNECTS

The communication between computer systems is facilitated by high-speed interconnects such as PCIe, CXL and AMBA [27]. Their intricacy and widespread nature present a range of security issues that pose a threat to system integrity, confidentiality, and availability. These interconnects exist on the hardware-software divide, which differs from traditional communication links [28]. Attacking an interconnect is appealing because the attacker can focus on exploiting weaknesses in the design process of protocols, access control, and media of transmission.

- **Data Confidentiality:** The transmissions are not encrypted and hence the sensitive information will be vulnerable to interception and tampering.
- **Vulnerabilities in Protocol Implementations:** Design oversight and specification incompleteness may be used to carry out malicious activities.
- **Side-Channel Attacks:** Timing variation, power analysis, and leakage of electromagnetic may be used to deduce information.
- **Scalability of Security Measures:** It is a major challenge to have good protection without affecting the interconnect performance.
- **Denial-of-Service (DoS) Attacks:** The perpetrators may use the restrictions of bandwidth and resources, which interfere with communication and slows down the work of the entire system.

A. Data Integrity and Confidentiality Issues

Fast interconnects including PCIe, CXL and AMBA are now stapled ingredients in contemporary computing platforms so that processors, accelerators, and memory subsystems can communicate effectively [29]. Nonetheless, their increasing sophistication and use in diverse settings has raised major apprehensions concerning data integrity and confidentiality. Unauthorized data modification, replay attack, or injection of malicious transactions in communication can be grounds of integrity issues resulting in corrupted computation or malfunction of systems. Equally, confidentiality threats arise due to side-channel leakage, snooping threats, or due to an inadequate separation in shared interconnect settings, sensitive information, like encryption keys, user data, or proprietary algorithms, is exposed [30]. The requirement of low-latency and high-bandwidth communication can further increase these challenges and restrict the viability of the traditional heavy-weight cryptographic protection background, the increasingly common practice amongst designers is to deploy lightweight cryptographic mechanisms, runtime monitoring, and hardware-based access control policies to alleviate these risks. However, the attainment of an optimum trade-off between high security assurances and system performance is still a research issue in the checking of the high speed interconnects.

B. Authentication and Access Control

Authentication and access control is important to protect fast interconnects (e.g., PCIe, CXL, and AMBA). They safeguard confidentiality and integrity of the information passing through the interconnect by making sure that the system resources are only accessed by authenticated users and devices [31]. In conjunction with layered access policies, authentication and access control can limit possible unauthorized actions and prevent privilege escalation, as well as hacks and tampering. An effective design should ensure a balance in the two areas of security and low latency to prevent the possible performance bottlenecks.

- Interconnect resources should be accessible to only authenticated devices and users.
- Eliminate unauthorized operations and privilege escalation attacks.
- Have fine grained access policies and role based access policies to enable secure communication.
- Reduce the potential of data leakage and ill intentional interference.
- Strike a right balance between high security and performance.

C. Protocol Implementations Vulnerabilities

The security issue of high-speed interconnects such as PCIe, CXL, and AMBA has many vulnerabilities in protocol implementations. Such vulnerabilities are usually caused by a lack of compliance with the protocol specification, design, or insufficient validation in development [32]. High-speed interconnect standards are complex, and even minor issues can cause subsystem components to be vulnerable to attacks, including packet injection, unauthorized access, and data corruption. In addition, as these protocols evolve to incorporate new features and higher bandwidth, the attack surface increases in size and hence places the system at greater risk of security vulnerabilities [33]. Such security vulnerabilities may endanger the confidentiality of information, the integrity of information, but may also endanger availability of the system leading to severe performance degradation. The rigorous verification, systematic compliance testing, fuzzing, and currently formal security verification are important to ensure effective and secure implementation of protocol specifications.

V. LITERATURE OF REVIEW

This literature review identifies the trend of the security-driven checks in CXL, PCIe and AMBA interconnects, including that of secure memory design, systematic bug checks, access control frameworks and side-channel vulnerabilities, and outlining performance, integration and scalability limitations with future research directions.

Choi *et al.*, (2025) the CXL-based memory as a secure main memory device, while removing the conventional memory. In the conventional DDRx memory, to provide confidentiality, integrity, replay protection, and obliviousness, costly mechanisms such as counter-based integrity trees and location shuffling by ORAM (Oblivious RAM) are used. Such mechanisms incur significant performance degradation in the current DDR-based memory systems, and their costs increase as the capacity of the memory increases. To mitigate the performance degradation, the prior work proposed an obfuscated channel for a secure memory module enclosing its controller in the package [34].

Zonta-Roudes *et al.*, (2024) Arm Advanced extensible Interface (AXI) protocol is a common on-chip interconnect protocol that is used by processors and accelerators, memories, and other IPs. The AXI implementations have any bugs which threaten the correctness of the chip. Buggy or non-compliant third-party IPs can use AXI implementation bugs to bypass the security mechanisms of the whole system. Identifying AXI implementation bugs is challenging because the incomplete specifications allow room for implementation-specific behavior in performant designs. expect is a systematic approach for analyzing AXI implementations to detect functional and security violations [35].

Restuccia *et al.*, (2023) Aker is an access control design and verification design framework of on-chip access control. The very heart of AKER is the access control wrapper (ACW) - a fast, but low-overhead, hardware unit that arbitrates dynamically on-chip communications. AKER disseminates ACWs throughout the SoC and programs them to undertake local access control. To ensure that the ACWs are correctly integrated and configured, AKER has offered a tool to generate firmware and a security verification methodology, which is property-driven. Security verification AKER ensures that the ACW acts correctly on IP level [36].

Kim *et al.*, (2023) a new side-channel attack using the IOTLB with devices. Devious uses PCIe devices with DMA capabilities, including NIC with RNIC and GPU, in order to present the attack. Thus, our attack has no influence on CPU caches or TLB in a victim's machine. Implementing Devious is not trivial as microarchitectural internals of the IOTLB of Intel processors are hidden. overcome this by reverse-engineering the IOTLB and disclose its hidden architectural properties. Use two IOTLB-based primitives of timing attacks on a GPU and an RNIC. Next, illustrate realistic attacks on co-located VMs of hardware-assisted isolation, and remote machines connected via the RDMA network. They can also discuss possible mitigations against the proposed side-channel attack [37].

Side *et al.*, (2022) a new exploitable side-channel vulnerability that ubiquitously exists in systems equipped with modern GPUs. This vulnerability is due to measurable contention caused on the host-GPU PCIe bus. To demonstrate the exploitability of this vulnerability, they conduct two case studies. the vulnerability to build a cross-VM covert channel that works on virtualized NVIDIA GPUs. To the best of our knowledge, this is the first work that explores covert channel attacks under the circumstances of virtualized GPUs. The covert channel can reach a speed up to 90 kbps with a considerably low error rate [38].

Restuccia *et al.*, (2021) provides a property-driven security verification using MITRE common weakness enumerations. AKER verifies the SoC access control at the IP level to ensure the absence of bugs in the functionalities of the ACW module, at the firmware level to confirm the secure operation of the ACW when integrated with a hardware root-of-trust (HRoT), and at the system level to evaluate security threats due to the interactions among shared resources. The performance, resource usage, and security of access control systems implemented through AKER is experimentally evaluated on a Xilinx Ultra Scale+ programmable SoC, it is integrated with the Open Titan hardware root-of-trust, and it is used to design an access control system for the Open PULP multicore architecture [39].

Table 1 covers a comparative analysis of security-driven verification methods of PCIe, CXL, and AMBA that describe the methods, capabilities, issues, and future research directions in high-speed interconnects.

Table 1: Summary of a Study on Emerging Trends in Security-Driven Verification for High-Speed Interconnects (PCIe, CXL, AMBA)

Author	Study On	Approach	Key Findings	Challenges	Future Directions
Choi et al., (2025)	CXL-based secure memory	Obfuscated channel within secure memory module	Reduced performance overhead vs DDRx	Scaling cost with memory capacity; controller	Develop scalable low-overhead secure

			with ORAM/integrity trees	integration complexity	CXL memory with adaptive verification
Zonta-Roudes et al., (2024)	AXI protocol (AMBA) security verification	expect framework for systematic bug analysis	Detects functional and security violations in AXI implementations	Incomplete specifications leave ambiguity for compliant designs	Extend to heterogeneous SoCs; automate verification for third-party IPs
Restuccia et al., (2023)	On-chip access control verification (AKER)	Distributed access control wrappers + property-driven verification	Ensures ACWs are properly configured and verified at IP level	Integration complexity with hardware root of trust	Broaden verification to system-level resource sharing in SoCs
Kim et al., (2023)	PCIe side-channel via IOTLB (DevIOus)	Reverse-engineering Intel IOTLB + DMA attack primitives	Demonstrates practical IOTLB-based timing side-channel attacks	Hidden microarchitectural details hinder defense	Architect hardware-level mitigations for DMA-capable PCIe devices
Side et al., (2022)	PCIe bus contention side-channel (LockedDown)	PCIe host-GPU covert channel attack	Cross-VM covert channel with 90 kbps throughput and low error	PCIe contention inherently exploitable in GPUs	Build PCIe-aware security monitors; formal verification of bus contention
Restuccia et al., (2021)	Multi-level SoC access control (AKER with HRoT)	Property-driven verification using MITRE CWE	Validated access control at IP, firmware, and system level	High overhead in large SoCs; resource constraints	Explore lightweight verification; integrate into open-source SoC projects

VI. CONCLUSION AND FUTURE WORK

The high-speed interconnects have become key facilitators of the contemporary computing platforms like PCIe, CXL, and AMBA that can facilitate the heterogeneous integration, low-latency communication, and scalable performance. Simultaneously, they have become increasingly complex, which has led to an increase in the security issues they can present, including unauthorized access and data leakage as well as protocol-level vulnerabilities. New security-related verification, such as formal property checking, AI/ML-based test generation, hardware/software co-verification, etc., are tackling the area of concern with greater rigor and flexibility. In addition, the use of lightweight authentication systems and active modeling of threats can be used as examples of an increased awareness of security as a design time constraint, as opposed to an after-deployment feature. Altogether, the methods considered in the review demonstrate the achievements and the necessity to continue the innovation in the balance between performance efficiency and security assurance. However, the lack of benchmarking data and small scale deployment validation is a serious hindrance.

The research must be developed in the future through the creation of standardized benchmarks, practical datasets, and scalable validation platforms. Cross standard interoperability, automated verification pipelines and security conscious design practices will add additional confidence to next generation interconnect systems.

VII. REFERENCES

[1] N. Prajapati, "Review of Quantum Computing Advances and their Impact on Modern Cryptographic Security," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 5, 2025.

[2] S. Narang and V. G. Kolla, "Next-Generation Cloud Security : A Review of the Constraints and Strategies in Serverless Computing," *Int. J. Res. Anal. Rev.*, vol. 12, no. 3, 2025.

[3] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.

[4] C. Tan, A. F. Donaldson, and J. Wickerson, *Formalising CXL Cache Coherence*, vol. 2, no. 1. Associationfor Computing Machinery, 2025. doi: 10.1145/3676641.3715999.

[5] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, pp. 229–238, 2025.

[6] Deepak Kumar Lnu, "AI-Driven Verification for Compute Express Link (CXL): Challenges, Innovations, and Future," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, pp. 2540–2557, 2025, doi: 10.32628/cseit25112728.

[7] V. Varma, "Secure Cloud Computing with Machine Learning and Data Analytics for Business Optimization," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, pp. 181–188, 2024, doi: 10.56472/25832646/JETA-V4I3P119.

[8] M. Zonta, N. Hinderling, and S. Shinde, "Xray: Detecting and Exploiting Vulnerabilities in Arm AXI Interconnects," *Proc. - Design, Autom. Test Eur. DATE*, 2025, doi: 10.23919/DATE64628.2025.10992968.

[9] 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.

[10] V. R. Kumbhare *et al.*, "High-Speed Interconnects: History, Evolution, and the Road Ahead," *IEEE Microw. Mag.*, vol. 23, no. 8, pp. 66–82, 2022, doi: 10.1109/MMM.2021.3136268.

[11] Y. Lin, J. Y. Jeng, Y. Y. Liu, and J. J. Huang, "A Review of PCI Express Protocol-Based Systems in Response to 5G Application Demand," *Electron.*, vol. 11, no. 5, pp. 1–25, 2022, doi: 10.3390/electronics11050678.

[12] D. Das Sharma, R. Blankenship, and D. Berger, "An Introduction to the Compute Express Link (CXL) Interconnect," *ACM Comput. Surv.*, vol. 56, no. 11, 2024, doi: 10.1145/3669900.

[13] 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.

[14] S. Sharma and S. M. Sakthivel, "Design and verification of AMBA AXI3 protocol," *Lect. Notes Electr. Eng.*, vol. 469, no. 21, pp. 247–259, 2018, doi: 10.1007/978-981-10-7251-2_26.

[15] U. A. Korat, P. Yadav, and H. Shah, "An efficient hardware implementation of vector-based odd-even merge sorting," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2017, pp. 654–657. doi: 10.1109/UEMCON.2017.8249010.

[16] V. Prajapati, "Cloud-Based Database Management : Architecture , Security , Challenges and Solutions," *J. Glob. Res. Electron. Commun.*, vol. 1, no. 1, pp. 7–13, 2025.

[17] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security : Challenges and Solutions," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 6–18, 2025, doi: 10.48175/IJARSCT-23902.

[18] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," vol. 9, no. 3, pp. 205–212, 2025.

[19] S. Garg, "AI/ML DRIVEN PROACTIVE PERFORMANCE MONITORING, RESOURCE ALLOCATION AND EFFECTIVE COST MANAGEMENT IN SAAS OPERATIONS," *Int. J. Core Eng. Manag.*, vol. 06, no. 06, pp. 263–273, 2019, [Online]. Available: https://ijcem.in/wp-content/uploads/AIML-DRIVEN-PROACTIVE-PERFORMANCE-MONITORING-RESOURCE-ALLOCATION-AND-EFFECTIVE-COST-MANAGEMENT-IN-SAAS-OPERATIONS.pdf

[20] N. Malali, "Model Validation and Governance for AI / ML in Actuarial Applications," *TIJER – Int. Res. J.*, vol. 12, no. 4, 2025, [Online]. Available: https://tijer.org/tijer/papers/TIJER2504026.pdf

[21] N. Malali and S. R. Praveen Madugula, "Robustness and Adversarial Resilience of Actuarial AI/ML Models in the Face of Evolving Threats," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, pp. 910–916, 2025, doi: 10.38124/ijisrt/25mar1287.

[22] G. Maddali, "Efficient Machine Learning Approach Based Bug Prediction for Enhancing Reliability of Software and Estimation," *Int. J. Res. Eng. Sci. Manag.*, vol. 8, no. 6, 2025.

[23] P. B. P. Patel, Rutvik, "The Role of Simulation & Engineering Software in Optimizing Mechanical System Performance," *TIJER – Int. Res. J.*, vol. 11, no. 6, pp. 991–996, 2024.

[24] V. Panchal, "Mobile SoC Power Optimization : Redefining Performance with Machine Learning Techniques," *IJIRSET*, vol. 13, no. 12, 2024, doi: 10.15680/IJIRSET.2024.1312117.

[25] S. Marksteiner, R. Ramler, and H. Sochor, "Integrating threat modeling and automated test case generation into industrialized software security testing," *ACM Int. Conf. Proceeding Ser.*, 2019, doi: 10.1145/3360664.3362698.

[26] V. Shah, "A Systematic Review of Formal Methods for Reliable Network Testing and Verification," *Int. Res. J.*, vol. 8, no. 9, pp. 13–19, 2021.

[27] R. Patel, "'SECURITY CHALLENGES IN INDUSTRIAL COMMUNICATION NETWORKS: A SURVEY ON ETHERNET/IP, CONTROLNET, AND DEVICENET,'" *Int. J. Recent Technol. Sci. Manag.*, vol. 7, no. 8, pp. 54–63, 2022.

[28] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, pp. 853–858, 2023, doi: 10.56975/tijer.v10i6.158517.

[29] M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor, "Physical Layer Security: Authentication, Integrity, and Confidentiality," in *Physical Layer Security*, Cham: Springer International Publishing, 2021, pp. 129–150. doi: 10.1007/978-3-030-55366-1_6.

[30] V. Shah, "Network Verification Through Formal Methods : Current Approaches and Open Issues," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 90–94, 2021.

[31] S. W. Stark, A. T. Markettos, and S. W. Moore, "How Flexible is CXL's Memory Protection?," *Queue*, vol. 21, no. 3, pp. 54–64, Jun. 2023, doi: 10.1145/3606014.

[32] G. Sarraf, "Resilient Communication Protocols for Industrial IoT : Securing Cyber- Physical-Systems at Scale," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 694–702, 2021.

[33] H. Ghabri, G. Maatoug, and M. Rusinowitch, "Compiling symbolic attacks to protocol implementation tests," *Electron. Proc. Theor. Comput. Sci.*, vol. 122, pp. 39–49, Jul. 2013, doi: 10.4204/EPTCS.122.4.

[34] K. Choi, I. Kim, S. Lee, and J. Huh, "ShieldCXL: A Practical Obliviousness Support with Sealed CXL Memory," *ACM Trans. Archit. Code Optim.*, vol. 22, no. 1, pp. 1–25, 2025, doi: 10.1145/3703354.

[35] M. Zonta-Roudes *et al.*, "eXpect: On the Security Implications of Violations in AXI Implementations," in *Proceedings of the 43rd IEEE/ACM International Conference on Computer-Aided Design*, New York, NY, USA: ACM, Oct. 2024, pp. 1–9. doi: 10.1145/3676536.3676844.

[36] F. Restuccia, A. Meza, R. Kastner, and J. Oberg, "A Framework for Design, Verification, and Management of SoC Access Control Systems," *IEEE Trans. Comput.*, vol. 72, no. 2, pp. 386–400, 2023, doi: 10.1109/TC.2022.3209923.

[37] T. Kim, H. Park, S. Lee, S. Shin, J. Hur, and Y. Shin, "DevIOus: Device-Driven Side-Channel Attacks on the IOMMU," in *2023 IEEE Symposium on Security and Privacy (SP)*, IEEE, May 2023, pp. 2288–2305. doi: 10.1109/SP46215.2023.10179283.

[38] M. Side, F. Yao, and Z. Zhang, "LockedDown: Exploiting Contention on Host-GPU PCIe Bus for Fun and Profit," *Proc. - 7th IEEE Eur. Symp. Secur. Privacy, Euro S P 2022*, pp. 270–285, 2022, doi: 10.1109/EuroSP53844.2022.00025.

[39] F. Restuccia, A. Meza, and R. Kastner, "AKER: A Design and Verification Framework for Safe and Secure SoC Access Control," *IEEE/ACM Int. Conf. Comput. Des. Dig. Tech. Pap. ICCAD*, vol. 2021-Novem, pp. 1–9, 2021, doi: 10.1109/ICCAD51958.2021.9643538.