International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A RECONFIGURABLE HARDWARE ARCHITECTURE OF AHB PROTOCOL USING MACHINE LEARNING TECHNIQUE IN ASIC AND FPGA

V L PRASANNA DHULIPUDI
Department of electronics and communication engineering, Puducherry technological University
East coast road, pillaichavady, Puducherry, 605014
Email-id: prasannadhulipudi14@gmail

Dr G. Sivaradje
Department of electronics and communication engineering, Puducherry technological University
East coast road, pillaichavady, Puducherry, 605014
Email-id: shivaradje@ptuniv.edu.in

Abstract:

In modern ASIC and FPGA systems, integrating Machine Learning (ML) techniques is essential for achieving high accuracy, speed, and power efficiency in applications such as large-scale data processing and automotive systems. This work presents a versatile hardware architecture that combines an ML-driven Support Vector Machine (SVM) with a high-speed AHB protocol and Floating Point (FP) operations. Efficient communication is enabled through I2C and I2S interfaces, while an AHB-to-APB bridge ensures seamless connectivity between the Fabric Reconfigurable Multi-Processor (FDPM) and its peripherals.

To enhance system security, the design integrates SHA-256 and AES algorithms, and Double-Precision Floating Point (DPFP) arithmetic operations are employed to improve ML computation accuracy. The architecture, developed in Verilog HDL, undergoes verification using LINT and Spyglass CDC tools. ASIC synthesis is performed using the DC Compiler, and FPGA implementation utilizes Vivado Design Suite 2018.1, validated on a Zynq processor via the SDK tool. Experimental results show an 18% increase in throughput, a 21% power reduction, and a 34% latency decrease, demonstrating the design's efficiency for ML-based hardware applications.

Keywords: AHB/APB Protocols, ASIC/FPGA, Double Precision Floating Point (DPFP), SVM, FDPM and ML.

1. INTRODUCTION

Cyberspace encompasses a broad spectrum of innovative ideas and recent advancements in network applications, digital wireless technologies, and the Internet of Things. Experts in technical strategy, security, government, military, commerce, and entrepreneurship use this term to describe the global technology ecosystem. Scholars also adopt this concept, extending its applicability to Internet-connected devices [1]. Through this expansive network, individuals engage

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

in various activities such as commerce, idea expression, information sharing, social support, entertainment, and creative media participation [2]. Despite its immense potential for development, cybersecurity remains the least regulated and managed area in human history, posing a significant threat to information confidentiality. The success achieved by the realms of business and information technology has led to unprecedented levels of assaults, including computer viruses, hacker attacks, and intrusions by malicious software. As new scientific discoveries and technical advancements emerge, Internet security continually faces challenges. Quantum computers pose a threat to traditional cryptographic systems like RSA [3] and ElGamal [4] due to their unique vulnerabilities. Quantum technology addresses the discrete logarithm problem (DLP) and integer factoring problem, making these traditional systems susceptible. To address this concern, the author suggests developing cryptosystems that do not rely on discrete logarithms, emphasizing the necessity for information safety in the future Internet's cyberspace. The fundamental concept of security in cyberspace entails implementing measures at every level and in every direction of a network to identify and address security concerns. While quantum cryptography is a relatively young field, the threats it poses to existing cyberspace security cannot be ignored. In 1994, mathematician Shor devised a quantum algorithm [5] capable of efficiently solving the discrete logarithm and integer factorization problems in the time domain using quantum computing. The absence of a well-established standard approach within the Turing machine paradigm to tackle these issues is a crucial consideration. Cryptography and network security play vital roles in ensuring the safety of information systems [6]. Quantum cryptography, a noteworthy subset that combines physics and encryption, leverages principles like Heisenberg's uncertainty and the concept of quantum no-cloning to secure private conversations [7]. Research into quantum cryptography protocols is essential to address future Internet cyberspace security challenges, particularly with the potential advent of quantum computing machines. The study also explores FPGA-based dynamically reconfiguration systems [8].

Due to their remarkable performance and energy efficiency, FPGAs have garnered significant attention for developing dynamically reconfigurable multiprocessor systems, offering adaptability in modifying hardware for various applications. In a study conducted in [9], they introduced a dynamically reconfigurable multiprocessor system based on FPGAs aimed at enhancing Convolutional Neural Networks (CNNs) for object recognition tasks. The system demonstrated an impressive speedup of up to 16 times compared to a CPU-based implementation. Moreover, its reconfigurability for different CNN models allowed optimization for diverse object recognition tasks. Another noteworthy study in [10] presented an innovative approach to FPGA-based hardware security using machine learning. This system employed a neural network to identify malicious attacks on the hardware and dynamically reconfigure the FPGA to counteract the attack. The system's efficacy was evaluated on an FPGA-based AES encryption module, demonstrating the ability to detect and mitigate fault injection attacks with a high level of accuracy. In [11], they explore the emerging paradigm of "networks-on-chip (NoCs)" in semiconductor-based communications. They specifically focus on buffer less NoCs, which offer advantages such as reduced space and power consumption.

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

However, buffer less NoCs present new challenges in scheduling that need to be addressed to maximize their capacity. The authors provide initial observations and hypotheses regarding the capabilities of buffer less NoCs. They propose optimal periodic schedules for buffer less NoCs with a traffic pattern of full exchange, making them well-suited for distributed-programming paradigms and congestion control strategies. Additionally, the study introduces greedy scheduling algorithms for common traffic patterns that are both efficient and effective, avoiding potential stalemates and often outperforming standard online greedy algorithms. Through network simulations, the authors quantitatively demonstrate the speedup achieved by their proposed methods, showcasing up to a 35 percent throughput enhancement on a torus network [12].

2. LITERATURE SURVEY

In [13], the focus is on on-chip routers that typically incorporate buffers designated for specific input or output ports. This shared queue approach proves more effective, resulting in improved throughput even under high network load conditions. The proposed router reduces latency by enabling packets to leave shared queues during periods of light traffic demand. In [14], they delve into the concept of Wavelet Networks (WNs), also known as WNs, which are characterized as self-teaching and self-organizing systems. Despite the proven utility of WNs in various applications, their potential in process control and identification domains has not been extensively explored. The research focuses on translating WNs onto the SIMD digital architecture of an FPGA to accelerate computations. This digital architecture, employing a linear approximation of the wavelet transfer function for various mother wavelet functions, is validated as a generic approximation for accurately identifying nonlinear SISO functions. In [14] present an FPGA-based image processing architecture, outlining a framework formed by hardware skeletons. Hardware skeletons are parameterized descriptions of task-specific architectures that utilize hardware-specific optimizations. The framework offers a variety of alternative skeletons for the same task, some of which are formatted for different data types. FPGAs are leveraged for real-time image processing applications, capitalizing on spatial and temporal parallelism, subject to considerations on the system's processing mode and hardware limitations. The article discusses generic approaches for addressing limitations in image processing processes and efficient mappings for these procedures.

In [15] focus on a nonlinear switching continuous system (NSCS) with time-delayed data and propose a defect detection approach based on machine learning are applied to the model's database for fault detection and isolation. The study validates the proposed approach on the "three-tank system," a benchmark problem, demonstrating the efficacy of the time-delayed “Unscented Kalman Filter (TD-UKF)” and Machine Learning-based fault detection. The research suggests that time skews in measurements impact fault detection, and the machine learning algorithm exhibits higher precision and lower false positive rates compared to previous statistical approaches. The study's findings can be applied to various industrial systems for improved problem detection with enhanced precision and broader coverage. In the work of [16], they address the integration of modern reinforced blocks, such as carry blocks and DSP (Digital Signal Processing) blocks, into contemporary heterogeneous FPGA

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

layouts. These specialized blocks play a crucial role in enhancing designs with heavy arithmetic requirements. The study notes that a diverse array of data path patterns can be implemented using these reinforced blocks, each configurable in different ways.

To address this challenge, the authors propose the utilization of "graph neural networks (GNN)" to automatically learn operation mapping patterns. This approach aims to overcome the deficiencies in existing HLS tools and enhance accuracy in estimating resource utilization and latency. This innovative use of GNNs is positioned as a solution to improve the effectiveness of high-level synthesis tools in accommodating and optimizing designs with reinforced blocks like carry and DSP blocks in modern heterogeneous FPGA layouts. In [17], emphasized the need for adaptive logic over an Application-Specific Integrated Circuit (ASIC) for picture compression. After researching various Discrete Wavelet Transform (DWT) designs, the folded DWT design was chosen. The study includes a determination of the required number of storage elements for each wavelet coefficient. The original SPIHT method was modified and parallelized for computation, with the architecture built on the foundation of fixed-order SPIHT. This modification was designed specifically for implementation in adaptive hardware. In [18] address the enhanced parallelism in the data flow architecture as a universal solution for "Deep Neural Network (DNN)" acceleration. [18]. In [19] focuses on high-dimensional bioinformatics data, suggesting GPUs and FPGAs for high-performance computing in this domain. The study highlights the benefits of FPGA dynamic partial reconfiguration (DPR) in recent years, allowing modification of specific sections within the device. The authors propose a dynamic multi-classifier architecture, combining FPGA utilization with DPR for processing bioinformatics data. In bioinformatics, applying multiple classification algorithms to the same dataset is preferred for a more trustworthy consensus judgment. The study emphasizes the efficiency gained by utilizing FPGAs and DPR in this bioinformatics data processing, compared to standard personal computers [20].

In summary, the integration of FPGA-based dynamically reconfigurable multiprocessor systems with machine learning algorithms has demonstrated significant potential for accelerating various tasks such as object recognition, encryption, and medical picture segmentation. This combination not only enhances performance but also adds an additional layer of security to protect against hostile assaults [21]. The versatility of FPGA-based systems is particularly evident in applications like medical image segmentation and image encryption, where the adaptability and reconfigurability of the hardware play a crucial role. Moreover, the research indicates that FPGA-based dynamically reconfigurable multiprocessor systems offer robust hardware security measures against malicious attacks. By leveraging the inherent capabilities of FPGAs and incorporating dynamic reconfiguration, these systems can effectively defend against unauthorized intrusions and ensure the integrity of sensitive data. Overall, the findings suggest that the marriage of FPGA-based dynamically reconfigurable multiprocessor systems with machine learning algorithms holds promise for improving both system performance and security across various applications [22]. This research contributes to advancing the capabilities of computing systems, making them more efficient, adaptable, and resilient in the face of evolving technological challenges [23].

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This work highlights the significance of FPGA-based dynamically reconfigurable multiprocessors with security enhancements using machine learning (ML) techniques, particularly in applications such as large data processing, automotive electronics, and driverless vehicles [19]. The proposed chapter introduces a reconfigurable hardware design featuring a Support Vector Machine (SVM) from ML, a Zynq processor, high-speed Advanced High-performance Bus (AHB) protocol, Floating Point (FP) operations, and the ability to communicate with low-speed protocols like I2C and I2S. This design aims to maintain high performance and low latency [24].

The work evaluates and designs an Application-Specific Integrated Circuit (ASIC)-based run-time reconfigurable architecture that facilitates dynamic core deployment for transmitting data between the processor and peripherals. The focus is on creating an architecture that supports and accelerates ML classifiers running between general-purpose processors and peripherals on target FPGAs through reconfiguration [25]. The use of AHB protocol, AHB to Advanced Peripheral Bus (APB) bridge, and security methods between the FDPM and peripherals is employed to maximize throughput with low latency. AES and SHA-256bit IPs are integrated to secure the proposed system from potential assaults, with AES ensuring memory security and threat detection. The suggested system utilizes DPFP arithmetic for ML applications and is designed to read and communicate data from slower peripherals like I2C and I2S. The Zynq processor and SDK tool validate hardware-software data transmission [25]. The results of the study demonstrate an 18% throughput improvement, a 21% reduction in power consumption, and a 34% delay reduction compared to state-of-the-art approaches, emphasizing the effectiveness of the proposed FPGA-based dynamically reconfigurable multiprocessor system with enhanced security using ML techniques [26].

The proposed chapter emphasizes the advantages of utilizing a Multiprocessor with NoC (Net chapter on Chip) for on-chip communications and interconnections, specifically highlighting the benefits of a hybrid approach that combines buffered and buffer-less routing. The key focus is on achieving energy efficiency, reduced power consumption, lowered space requirements, and improved throughput for complex designs, catering to the evolving needs of cloud computing and the Internet of Things [27]. The chapter suggests that a significant reduction in energy consumption can be achieved by decreasing the size of input and output buffers in a Multiprocessor with NoC routing, without compromising overall system performance. The reduction in buffer sizes is particularly beneficial for real-world applications with low traffic volume. By decreasing the amount of Multiprocessor with NoC routing, the speed of the router can be increased, leading to reduced latency.

The proposed design simplifies router architecture by eliminating complex buffer allocation and management techniques, with a focus on supporting buffer-less routing algorithm design. The absence of certain functionalities such as quality of service, different traffic classes, and congestion awareness in the design of net chapters is acknowledged, but the chapter aims to address these challenges in future work [28]. The hybrid Multiprocessor with NoC approach, which combines buffered and buffer-less methods, is designed to effectively manage congestion and achieve energy efficiency. The chapter highlights the use of a Trace-driven simulator,

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

demonstrating a 17% average improvement in application performance, a 24% improvement at best, a 13% improvement in fairness, and a 38% reduction in power usage compared to standard buffered Multiprocessor and NoC results [29]. Furthermore, the chapter introduces the MaS (Multidirectional Adaptive Switching) algorithm, emphasizing its role in enabling energy-efficient, in-order delivery without receiver buffering. The proposed MaS system outperforms the BLESS-Worm system in terms of power usage reduction, packet delay reduction, and lower buffer requirements at the receiver end. Simulations indicate up to an 80% reduction in buffer needs compared to BLESS-Worm, with less stringent buffer requirements [30]. In conclusion, the proposed chapter underscores the potential of a hybrid Multiprocessor with NoC approach to address the challenges posed by growing data volumes and processing speeds, achieving both energy efficiency and effective handling of massive data through the optimal use of available resources and congestion management.

3.PROPOSED HIGH THORUGHPUT AND LOW POWER HYBRID RECONFIGURABLEMULTIPROCESSOR AT SOC SYSTEM

In this work, a review of the previous chapter on reconfigurable FPGAs and their applications in artificial intelligence is briefly presented. It is noted that while there is a considerable amount of literature on FPGAs, there is a limited number of research studies specifically focusing on the implementation of artificial intelligence in FPGAs. The chapter introduces the concept of “Reduced Deflection Chipper” (ReDC), a buffer-less deflection router that utilizes two Partially Disjoint Networks (PDNs) to generate efficient results at output ports. The preferred design chosen from the PDNs is expected to enhance performance, providing increased efficiency. The discussion then shifts to on-chip communication using a Network-on-Chip (NoC)-equipped multiprocessor, emphasizing the need for lower power consumption in chips. The implementation of buffer-less multiprocessors with NoCs is explored, highlighting the challenge of scheduling to achieve full capacity. The chapter proposes an approach that focuses on creating periodic schedules for buffer-less on-chip net chapters with complete-exchange data-flow patterns. Greedy scheduling techniques are employed for expected traffic patterns to avoid deadlocks and outperform online greedy algorithms.

Received: October 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

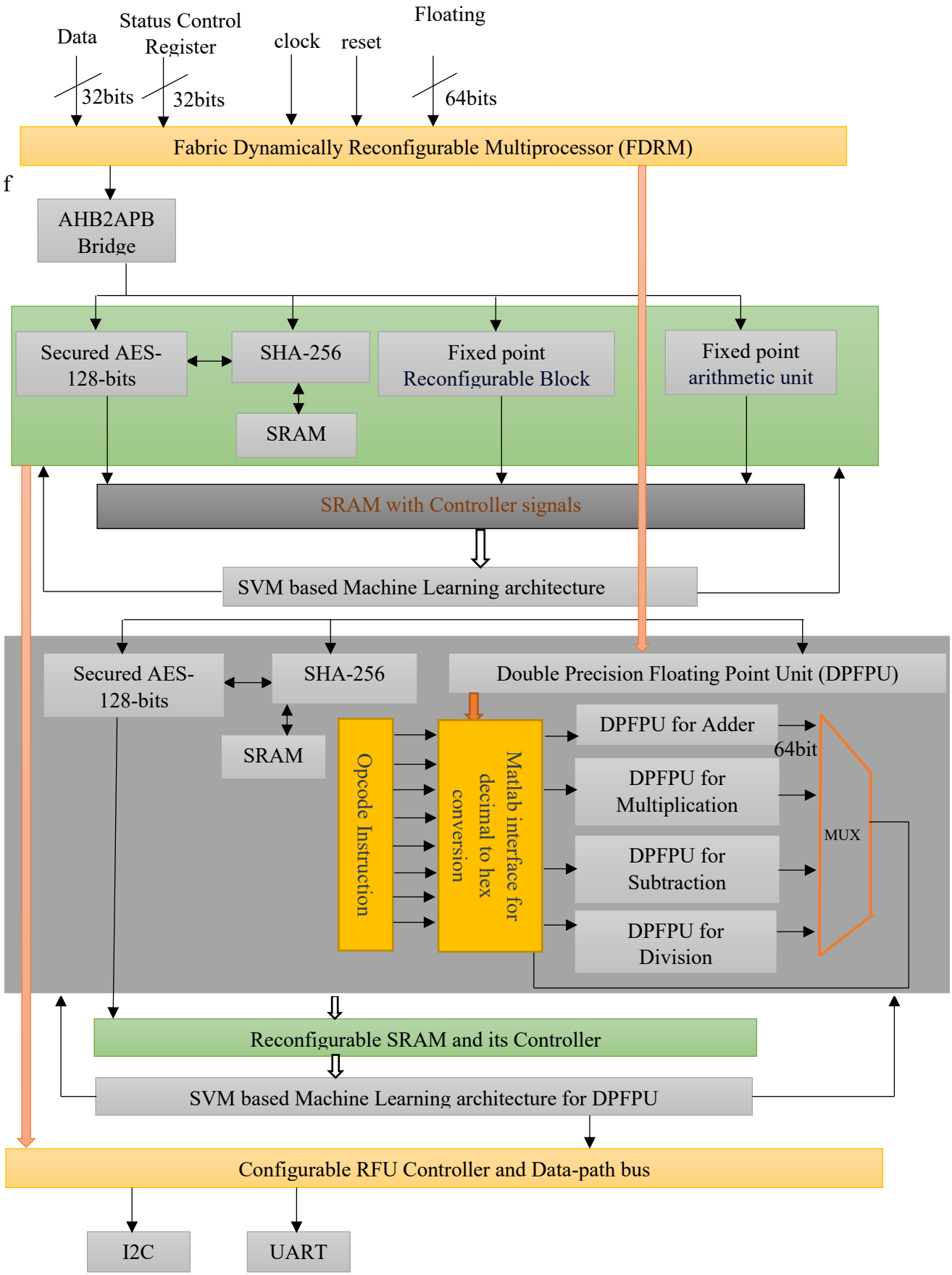

Figure 1: Proposed hybrid reconfigurable multiprocessor for multipurpose applications at SoC level.

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Simulations are mentioned to support the efficiency of the suggested approaches, with a particular focus on a torus net chapter. The integration of photonic waveguides is proposed to address power constraints and speed limitations on semiconductors. The combination of high-radix multiprocessors with NoCs and on-chip waveguides is expected to enhance performance. The BLOCON approach is introduced to maximize silicon photonics use, and the SIDRRM scheduling algorithm and DIPA route allocation strategy are proposed solutions to address the challenges in Clos network routing. The chapter also delves into the topic of fault-tolerant buffer-less multiprocessors with NoCs, introducing FTDR-H and FTDR routers that aim to reduce chip area usage and improve transient fault performance. The QORE design, featuring Multi-Function Control (MFC) buffers, is recommended for its ability to reverse propagate faults and achieve lower power consumption. The RoShaQ design is presented as a low-latency router that outperforms the VC router in terms of delay, throughput, and energy consumption. Experimental findings demonstrate the suggested technique's speed and its ability to outperform uniform buffer allocation.

In conclusion, this section provides an overview of diverse topics ranging from buffer-less routers to fault-tolerant designs and thermal considerations in multiprocessors with NoCs. The suggested approaches and designs aim to optimize performance, reduce power consumption, and enhance the efficiency of on-chip communication systems. The suggested architecture, as depicted in Fig.1, However, due to the cache being internally located within the Zynq, direct probing for monitoring is not possible. To address this limitation, a solution involves storing data in external memory, allowing the Zynq processor to access the data as needed and facilitating the disablement when required. In this proposed architecture, the customized accelerator is capable of accessing external cache memory, in addition to the internally placed Block RAM (BRAM). To enhance the accessibility between the accelerator and DDR memory, a high-speed and size-trimmed cache IP is introduced, establishing direct connections between them. This configuration aims to facilitate efficient data access between DDR and the accelerator for specified addresses. The suggested design also incorporates an additional AHB with a counter, timer, and an interface to the Zynq and peripherals for seamless data transmission. The AHB system communicates directly with the host interface, providing system-level cache access, unaligned byte strobe, and low latency. This integration is intended to optimize the overall performance and data transfer efficiency within the architecture.

The proposed architecture's multiprocessor core generates data and addresses, transmitting them via the AHB to APB bridge to interface with slower peripherals like I2C and I2S. These peripherals are used to transfer audio signals between the processor and audio processing algorithms, enhancing performance with minimal latency. The AHB to APB bridge optimizes clock cycles during 'setup' and 'access' states to match the audio and interface modules' speed, increasing performance and reducing data/packet losses. It includes a Transmit FIFO (Tx-FIFO) with a depth of 256 to store 32-bit packets, later read by serial peripherals. Serial protocols convert the data into serial bits transferred to GPIO through FPGA PMOD connectors for external device interfacing. The master sends serial bits and a serial clock for slave synchronization. The I2C Slave controller

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

core interfaces a microprocessor with an I2C master device, offering parametrized FIFO depth and a standard APB interface to the SoC. The controller core includes various status bit flags for quick software (SW) and Intellectual Property (IP) lookup, covering FIFO overruns, underruns, invalid register access to configuration/status register space, receiving a 19.2 MHz standard io_clock input, and receiving serial clock (scl) of up to 5MHz from the I2C master. The I2C slave is capable of 7/10-bit addressing. Clock stretching is supported by the I2C slave only in open-drain mode. The I2C Slave bridge facilitates communication between the microprocessor and the master device, receiving data from the microprocessor for transmission to the I2C master and vice versa. The ML-based SVM accelerator architecture features input/output and weights buffers for efficient processing. A specialized 3D-NoC redistributes output packets through a multi-banked input buffer, reducing off-chip memory traffic. Independent processing elements (PEs) for SVM and 3D-NoC operations are managed by a central control module, optimizing SVM processing and on-chip resource utilization.

3. RESULTS AND DISCUSSIONS

Mesh topology forms the network connections in the tiny multipurpose processor to validate the Multiprocessor with NoC, which is tested through various analyses. Network-on-Chip (NoC) technology is gaining global attention for facilitating communication between System-on-Chips (SoCs). This research chapter focuses on modelling synchronous Multiprocessor with NoCs on FPGAs. The initial trial involves designing and implementing the synchronous circuit in standard FPGAs, including designing the workflow, testing it, and evaluating its performance. FPGAs are utilized to build the best-effort Multiprocessor with NoC to meet specific requirements, incorporating switches, system connections, and multiprocessors with NoCs. The primary Multiprocessor-NoC handshake in the 4-stage system uses UART and memory, with the OCP Interface as the main protocol. To demonstrate real-time design, an architectural model technique is employed. A miniature multipurpose processor model is created to showcase the intended Multiprocessor with NoC. A 3x3 Multiprocessor with NoC, UART protocol, and VHDL simulation is constructed and tested on the Artix-7 FPGA kit. The testing procedures involve the use of Chip Scope software instruments, including Virtual Input/Output (VIO) and Integrated Controller (ICON), to depict data movement from its origin to its destination. Data transfer efficiency is monitored using metrics such as Packet Delivery Ratio (PDR), latency, slices, Look-Up Tables (LUTs), Flip-Flops (FFs), and area. Traffic Pattern Generators are employed to generate packets, resulting in improvements of 12% in LUTs, 7% in flip-flops, 23% in throughput, and 26% in latency.

The process involves building and testing direct traffic generators using traffic supply and sink signals. Data packets are transmitted to a new data store, and sink signals are compared to the data for input/output pairing. The Multiprocessor with NoC architecture (Figure 2) transports network packets after secret key exchange using NoC-based multiprocessors. Routers use data and handshake signals, and address-specific acknowledgements increment an asynchronous counter, storing incremental values in memory. The output channel demultiplexer controls data packet processing stored in ROM for FPGA processing via JTAG. Data extraction and

Received: October 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

verification are done using the Chip Scope Pro tool and VIO core, which monitors and records FPGA signal data for debugging and testing. In the scenario depicted in Figure 2, after user authentication, the sender requests a private key for AES-128 encryption based on data sensitivity levels: Non-sensitive, Sensitive, and Most-sensitive. Non-sensitive data isn't encrypted, while AES-128 and AES-256 are used for Sensitive and Most-sensitive data, respectively. Given the time-consuming nature of encrypting large datasets, especially in the Cloud, the solution uses the AES Encryption algorithm within the MapReduce framework. This parallel and distributed processing model enhances efficiency in handling large volumes of data, making cryptographic operations faster and more suitable for securing data in cloud environments.

The provided table compares the current and proposed 3x3 Synchronous Network-on-Chip (NoC) Multiprocessor configurations. It includes various parameters such as Slice Register, Slice LUTs, LUT FF, Delay, Power, Frequency, Throughput, and Latency. Here's a summary of the data shown in Table 1. The proposed configuration shows significant improvements in terms of Slice Register, Slice LUTs, and Power consumption compared to the referenced configurations ([17] and [22]). The Delay in the proposed configuration is remarkably reduced, going from microseconds to nanoseconds. The Frequency is maintained at 594.229MHz in the proposed configuration.

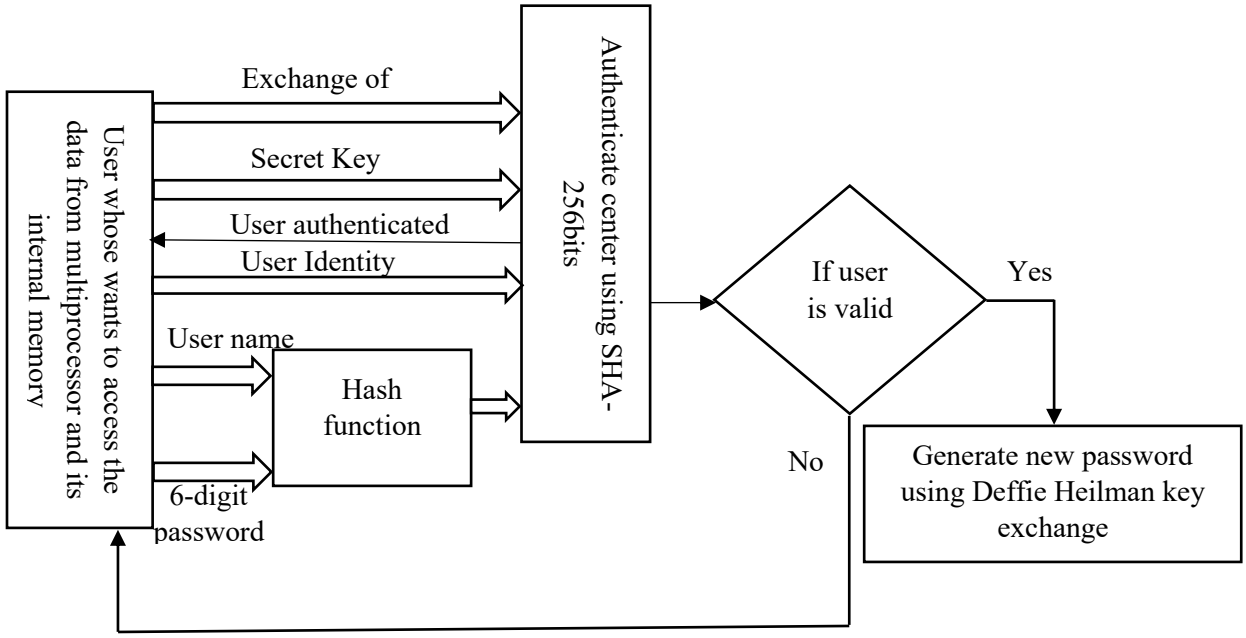

Figure 2: Authentication of user by exchange of their secrete keys after validation using SHA-256

Throughput sees a substantial increase in the proposed configuration, reaching 6.37GB/s. Latency in the proposed configuration is 2.006ns, indicating a relatively fast data processing time. The provided information also discusses the implementation details, such as data imposition into the ROM for data modification, the use of the AES Encryption algorithm, and the consideration of asynchronous and synchronous modes in the Multiprocessor with NoC architecture. Additionally, challenges and potential solutions related to

Received: October 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FPGA prototyping and deadlock prevention methods are highlighted.

Table 1: Comparison of existing and proposed hybrid multiprocessor along security algorithms

Terms	**[2]**	**[3]**	**Proposed**
Slice Register	27170	11250	9501
Slice LUT's	27179	6150	4981
LUT FF	6722	6434	4921
Delay (ns)	10.11	49ns	3.91
Power (mW)	2100	11.5	9.5
Frequency (MHz)	2000	100	2310
Throughput (Gbps)	3.1	235.20	6.37

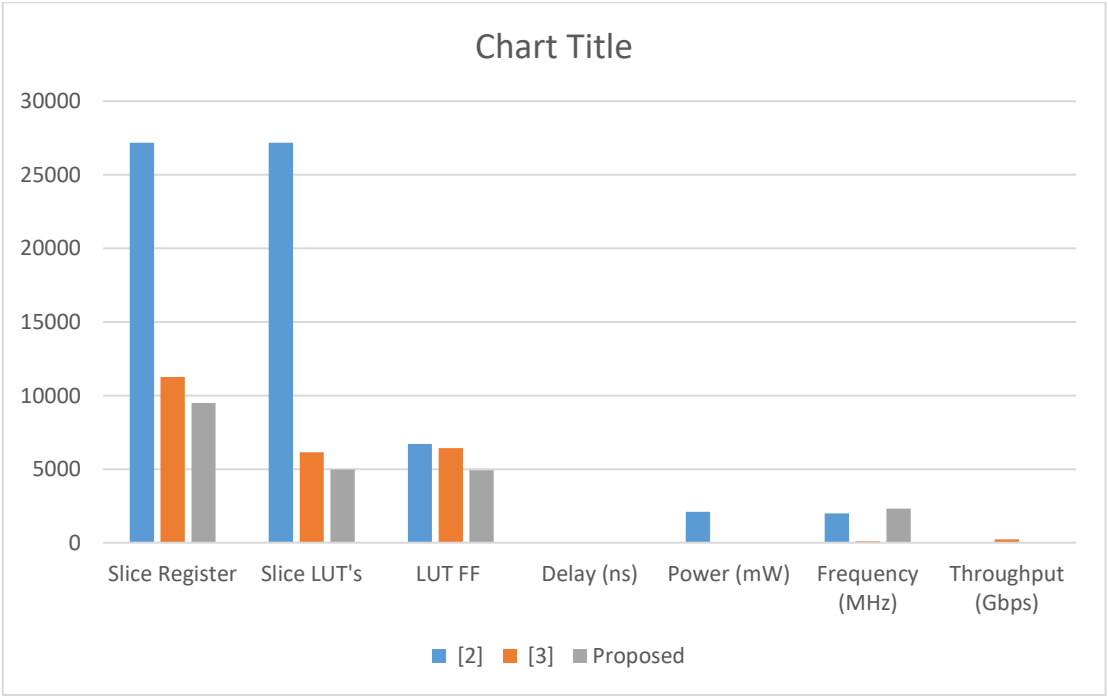

Figure 3: Synthesis report of proposed design in terms of hardware utilizations

Received: October 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

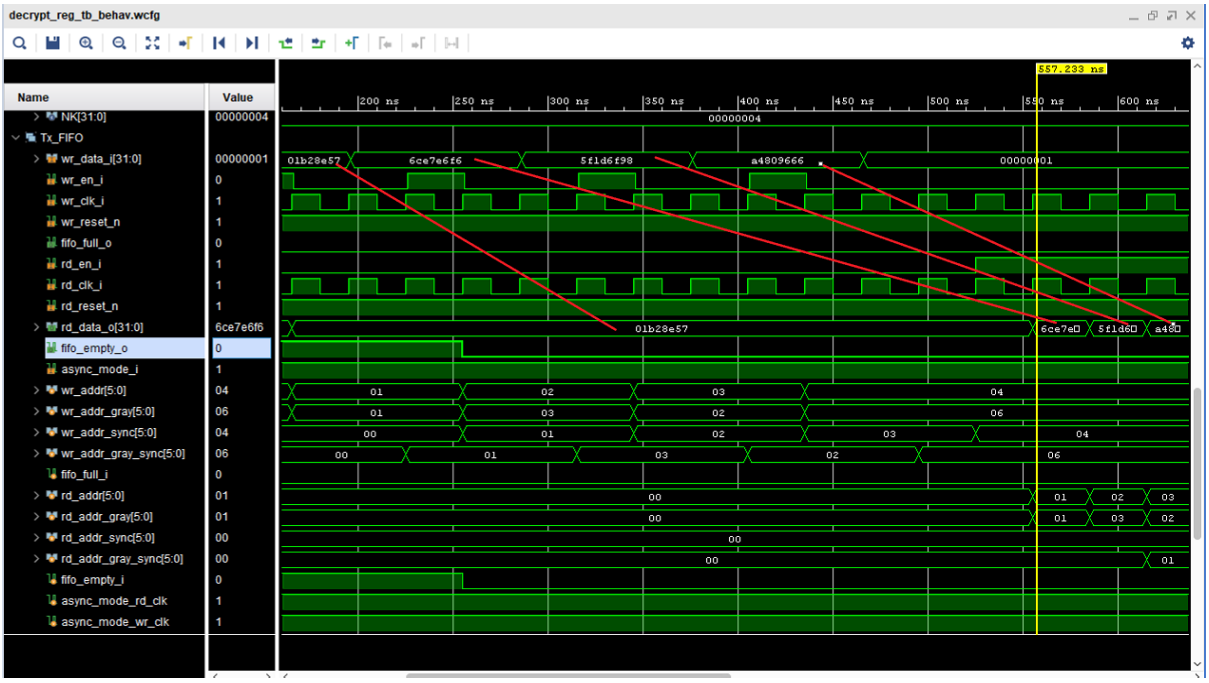

Figure 4: Simulated results of top-level Security system of data encryption and decryption

The Figure 4 shown the simulated results of security system including encryption and decryption, the multiprocessor has generated the continuous 32-bits data and transmit to AHB2APB bridge through AXI interconnects, the bridge scales down the frequency required for AES engine. The engine processes all the 32-bit data's and transmits through I2C protocol after converting into parallel. These serial bits are input to receiver, the serial bits are converted into parallel and processed by AES- decryption to recovery the original data. The red lines shown in Figure 4 are 32-bits writing and encrypting and reading after from memory after decryption.

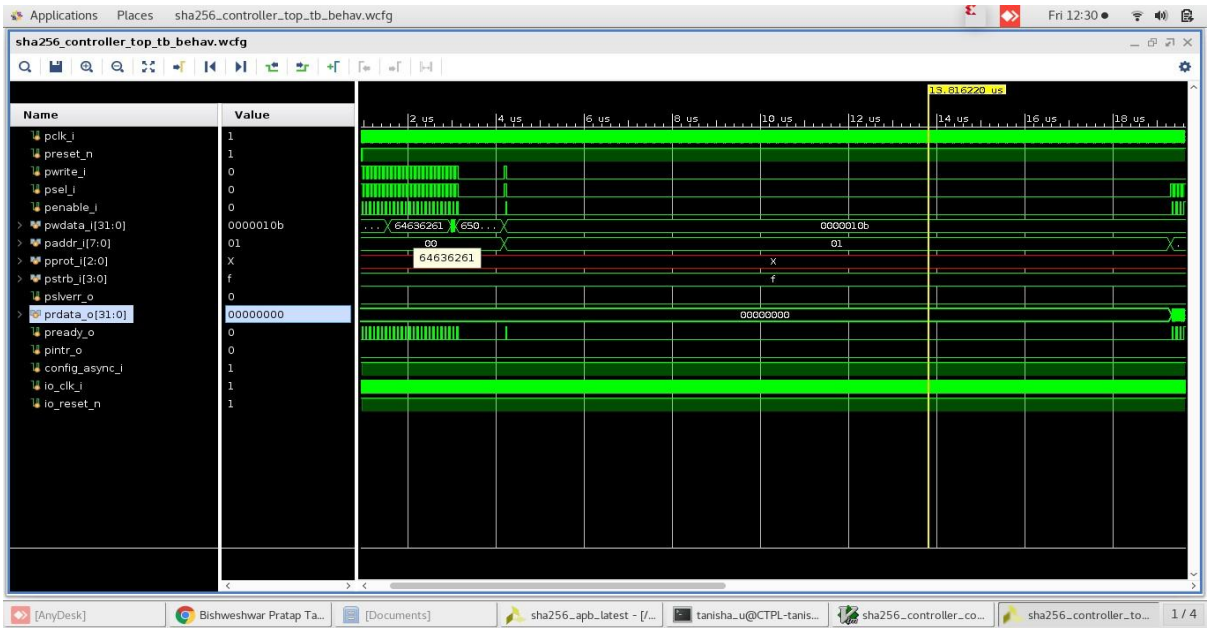

Figure 5: User Authentication using SHA-256bits to verify validity for accessing data from internal memories

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

SHA-256 is designed to produce a fixed-size output of 256 bits, which is 32 bytes shown in Figure 5. It is commonly used in various security applications and protocols to ensure data integrity and provide a secure means of verifying the authenticity of digital information. SHA-256 operates on a block of data and iteratively applies a series of mathematical operations, including bitwise operations, modular addition, and logical functions. It uses a Merkle–Damgård construction to process data in fixed-size blocks.

Input: SHA-256 takes an input message of any length and processes it in 512-bit blocks.

Padding: The message is padded to ensure its length is a multiple of 512 bits.

Initialization: The algorithm initializes eight working variables (hash values) to specific constants.

Compression: The message is processed in blocks, and each block updates the hash values through a series of operations.

Finalization: After processing all blocks, the hash values are concatenated to produce the final 256-bit hash.

SHA-256 is a highly secure cryptographic hash function, resistant to various attacks and providing a 256-bit hash value that makes brute-force attacks computationally infeasible. It is commonly used in digital signatures, certificate generation, and blockchain technology to secure transactions and blocks in cryptocurrencies like Bitcoin. Standardized by NIST, SHA-256 is widely adopted in security protocols and cryptographic systems, ensuring data integrity and security in digital communications and transactions. The DPFP-based Arithmetic Logic Unit (ALU) presented in this proposal encompasses four fundamental arithmetic operations: addition, subtraction, division, and multiplication. The Verilog Hardware Description Language (HDL) was employed for the design, and successful synthesis was accomplished using the "Vivado Design Suite 2018.1" software tool. Subsequently, the design underwent simulation using the ISim module within the same tool. The simulation results were then compared with the corresponding results obtained from the Matlab version, as detailed in Table 2 and its simulated results are shown in Figure 6.

Table 2: Comparison of simulated results in Vivado with Matlab simulated results.

Arithmetic Operation/Input values	Multiplication		Adder		Subtraction	
	Matlab	Verilog Simulation	Matlab	Verilog Simulation	Matlab	Verilog Simulation
In1: 124.56 In2: 451.986	40eb7d6c0980b242	40efabb9dc725c3d	4082045e353f7cee	4082045e353f7ced	c07476d0e5604189	c07476d0e5604189
In1:651.96	411f3115765fd8ae	411f3115765fd8ae	40966f47ae147ae2	40966f47ae147ae1	c0607ccccccccccc	c0607ccccccccccc

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In2:783.86						
In1:987.86 In2:345.86	4114da7509d49518	4114da7509d49518	4094d6e147ae147b	4094d6e147ae147b	4084100000000000	4084100000000000
In1:655.96 In2:788.86	411f95526c22680a	4114da7509d49518	40969347ae147ae2	40969347ae147ae1	c0609ccccccccccc	c0609ccccccccccc
In1:234.76 In2:563.86	4100289e30553261	4100289e30553261	4088f4f5c28f5c29	4088f4f5c28f5c29	c074919999999999a	c074919999999999a

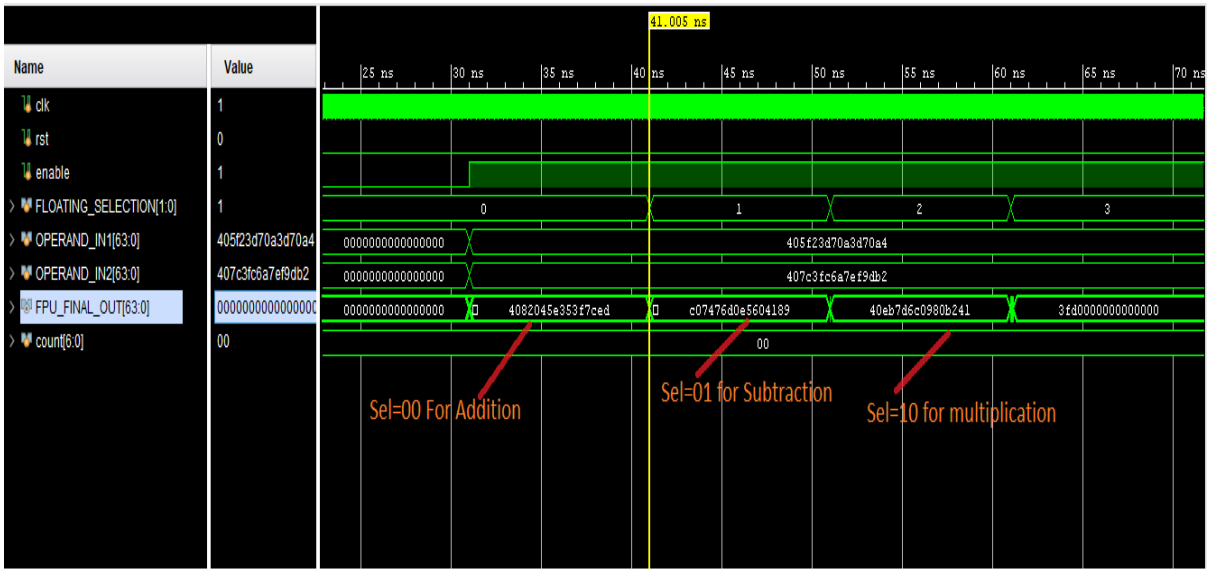

Figure 6: Simulated results of addition, subtraction and multiplication and their corresponding selection bits

The proposed work focuses on developing a highly efficient reversible DPFP subtractor, adder, and multiplication operations. Emphasizing minimal latency outputs, constant inputs, and minimal logic elements, the design achieves an impressive low latency of only 4 clock cycles. The advancements include the creation of eight-bit and 24-bit reversible subtractors using Ternary gates, aiming to reduce critical path delay. Additionally, 24-bit and 25-bit reversible shift registers and a 24-bit Leading Zero detector have been innovatively designed, contributing to the efficiency of ternary-based DPFP arithmetic operations. The work introduces an efficient architecture for multiple-precision fused double-precision floating-point (DPFP) arithmetic operations. This architecture supports various precisions, including quadruple, double, single, and half-precision operations, allowing for mixed-precision operations without significant area overhead. It enables Fused Multiply-Add (FMA) and 2-term dot-product operations with diverse precisions. Compared to conventional multiple-precision DPFP designs, the mixed-

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

precision DPFP architecture shows only a modest 23.5% increase in area, making it advantageous for applications requiring balanced precision for enhanced performance and accuracy. Additionally, the architecture supports half-precision DPFP operations and mixed-precision operations with just an 11.6% additional area compared to state-of-the-art designs, making it suitable for efficient processor designs or specialized hardware accelerators. The inclusion of parallel half-precision operations and support for mixed-precision operations enhances its applicability, particularly in accelerating low-power applications. Overall, the work presents a promising contribution to computing techniques, with potential applications in ultra-low-power digital circuits and quantum computers.

4. CONCLUSION

The research work demonstrates the effective use of Support Vector Machine (SVM) technology, optimized through Vivado Design Suite 2018 and high-level synthesis tools, to enhance packet identification accuracy while minimizing computing costs. The integration of block-level hardware with a Zynq processor, high-speed protocols, and AXI interconnects achieves scalability and superior performance. Testing confirms the design's functionality and potential for extensive data processing. Additionally, a hybrid multiprocessor with Network-on-Chip (NoC) improves service quality and energy efficiency under diverse application loads, addressing power and area concerns with buffer less routing to enhance latency, power consumption, and area overhead. The manuscript also explores the cryptographic foundations of AES, focusing on the trade-offs between 128-bit and 256-bit key sizes in terms of computational efficiency, security requirements, and technological challenges. It emphasizes the importance of selecting the appropriate key size for data confidentiality and integrity. Furthermore, the study delves into the Secure Hash Algorithm 256-bit (SHA-256), providing a comprehensive understanding of its principles, properties, and applications in information security. These findings offer valuable insights for professionals and researchers in cybersecurity and data processing.

REFERENCES

[1]. Yan, X., Huang, K., Meng, J. (2024). SoC Design. In: Wang, Y., Chi, MH., Lou, J.JC., Chen, CZ. (eds) Handbook of Integrated Circuit Industry. Springer, Singapore. https://doi.org/10.1007/978-981-99-2836-1_42

[2]. Kumar, V. B. Y., Deb, S., Gupta, N ., Bhasin, S., Haj-Yahya, J., Chatto padhyay, A. & Mendelson, A. (2020). Towards de signing a secure RISC-V system-on -chip : ITUS. Journal ofHardware a nd Systems Security, 4, 329-342. https://dx.doi.org/10.1007/s41635-020-00108-8

[3]. Prasanna, Viktor K.et.al, International Journal of Reconfigurable Computing, 2010/12/2, Reconfigurable Multiprocessor Systems: A Review 570279, VL - 2010, https://doi.org/10.1155/2010/570279

[4]. A. Zokaei, D. Truhachev and K. El-Sankary, "Memory Optimized Hardware Implementation of Open FEC Encoder," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol.

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

30, no. 10, pp. 1548-1552, Oct. 2022, doi: 10.1109/TVLSI.2022.3180554.

[5]. D. Alex, V. C. Gogineni, S. Mula and S. Werner, "Novel VLSI Architecture for Fractional-Order Correntropy Adaptive Filtering Algorithm," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 7, pp. 893-904, July 2022, doi: 10.1109/TVLSI.2022.3169010.

[6]. R. B. Chaurasiya and R. Shrestha, "Hardware-Efficient VLSI Architecture and ASIC Implementation of GRCR-Based Cooperative Spectrum Sensor for Cognitive-Radio Network," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 2, pp. 166-176, Feb. 2022, doi: 10.1109/TVLSI.2021.3114859.

[7]. T. Wang, C. Zhang, P. Cao and D. Gu, "Efficient Implementation of Dilithium Signature Scheme on FPGA SoC Platform," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 9, pp. 1158-1171, Sept. 2022, doi: 10.1109/TVLSI.2022.3179459.

[8]. S. M. Abbas, T. Tonnellier, F. Ercan, M. Jalaleddine and W. J. Gross, "High-Throughput and Energy-Efficient VLSI Architecture for Ordered Reliability Bits GRAND," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 6, pp. 681-693, June 2022, doi: 10.1109/TVLSI.2022.3153605.

[9]. Y. Chen, H. Cui and Z. Wang, "An Efficient Reconfigurable Encoder for the IEEE 1901 Standard," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 9, pp. 1368-1372, Sept. 2022, doi: 10.1109/TVLSI.2022.3177239.

[10]. P. D. Sanzo and F. Quaglia, "On the Effects of Transaction Data Access Patterns on Performance in Lock-Based Concurrency Control," in *IEEE Transactions on Computers*, vol. 72, no. 6, pp. 1718-1732, 1 June 2023, doi: 10.1109/TC.2022.3222084.

[11]. A. F. Ajirlou and I. Partin-Vaisband, "A Machine Learning Pipeline Stage for Adaptive Frequency Adjustment," in *IEEE Transactions on Computers*, vol. 71, no. 3, pp. 587-598, 1 March 2022, doi: 10.1109/TC.2021.3057764.

[12]. G. Sisto *et al*., "Evaluation of Nanosheet and Forksheet Width Modulation for Digital IC Design in the Sub-3-nm Era," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 10, pp. 1497-1506, Oct. 2022, doi: 10.1109/TVLSI.2022.3190080.

[13]. Y. Li, Y. Wu, X. Zhang, J. Hu and I. Lee, "Energy-Aware Adaptive Multi-Exit Neural Network Inference Implementation for a Millimeter-Scale Sensing System," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 7, pp. 849-859, July 2022, doi: 10.1109/TVLSI.2022.3171308

[14]. R. Sharma, R. Shrestha and S. K. Sharma, "Low-Latency and Reconfigurable VLSI-Architectures for Computing Eigenvalues and Eigenvectors Using CORDIC-Based Parallel Jacobi Method," in *IEEE Transactions on Very Large Scale Integration (VLSI)*

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Systems, vol. 30, no. 8, pp. 1020-1033, Aug. 2022, doi: 10.1109/TVLSI.2022.3170526.

[15].E. Bank Tavakoli, A. Beygi and X. Yao, "RPkNN: An OpenCL-Based FPGA Implementation of the Dimensionality-Reduced kNN Algorithm Using Random Projection," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 4, pp. 549-552, April 2022, doi: 10.1109/TVLSI.2022.3147743.

[16].C. Butts, R. Jha, T. Messay-Kebede and D. Kapp, "Resilient Embedded Systems Designs via on the Fly Generation of Adaptive Degenerate Components Using Machine Learning," in *IEEE Transactions on Computers*, vol. 72, no. 5, pp. 1236-1246, 1 May 2023, doi: 10.1109/TC.2022.3204230.

[17].W. Jiang, X. Liao, J. Zhan, D. Adhikari and K. Jiang, "DESCO: Decomposition-Based Co-Design to Improve Fault Tolerance of Security-Critical Tasks in Cyber Physical Systems," in *IEEE Transactions on Computers*, vol. 72, no. 6, pp. 1652-1665, 1 June 2023, doi: 10.1109/TC.2022.3218987.

[18].M. N. Islam, R. Shrestha and S. Roy Chowdhury, "An Uninterrupted Processing Technique-Based High-Throughput and Energy-Efficient Hardware Accelerator for Convolutional Neural Networks," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 12, pp. 1891-1901, Dec. 2022, doi: 10.1109/TVLSI.2022.3210963.

[19].S. Walia, B. V. Tej, A. Kabra, J. Devnath and J. Mekie, "Fast and Low-Power Quantized Fixed Posit High-Accuracy DNN Implementation," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 1, pp. 108-111, Jan. 2022, doi: 10.1109/TVLSI.2021.3131609.

[20].B. Paul, T. K. Yadav, B. Singh, S. Krishnaswamy and G. Trivedi, "A Resource Efficient Software-Hardware Co-Design of Lattice-Based Homomorphic Encryption Scheme on the FPGA," in *IEEE Transactions on Computers*, vol. 72, no. 5, pp. 1247-1260, 1 May 2023, doi: 10.1109/TC.2022.3198628.

[21].K. Stangherlin and M. Sachdev, "Design and Implementation of a Secure RISC-V Microprocessor," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 11, pp. 1705-1715, Nov. 2022, doi: 10.1109/TVLSI.2022.3203307.

[22].X. Hu, M. Li, J. Tian and Z. Wang, "Efficient Homomorphic Convolution Designs on FPGA for Secure Inference," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 11, pp. 1691-1704, Nov. 2022, doi: 10.1109/TVLSI.2022.3197895.

[23].Z. Jiang, R. Wei, P. Dong, Y. Zhuang, N. C. Audsley and I. Gray, "BlueVisor: Time-Predictable Hardware Hypervisor for Many-Core Embedded Systems," in *IEEE Transactions on Computers*, vol. 71, no. 9, pp. 2205-2218, 1 Sept. 2022, doi: 10.1109/TC.2021.3125226.

[24].W. Jiang, X. Liao, J. Zhan, D. Adhikari and K. Jiang, "DESCO: Decomposition-Based Co-Design to Improve Fault Tolerance of

Received: October 15, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Security-Critical Tasks in Cyber Physical Systems," in *IEEE Transactions on Computers*, vol. 72, no. 6, pp. 1652-1665, 1 June 2023, doi: 10.1109/TC.2022.3218987.

[25].M. M. Rahman and S. Bhunia, "Practical Implementation of Robust State-Space Obfuscation for Hardware IP Protection," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 32, no. 2, pp. 333-346, Feb. 2024, doi: 10.1109/TVLSI.2023.3307027.

[26].B. Paul, T. K. Yadav, B. Singh, S. Krishnaswamy and G. Trivedi, "A Resource Efficient Software-Hardware Co-Design of Lattice-Based Homomorphic Encryption Scheme on the FPGA," in *IEEE Transactions on Computers*, vol. 72, no. 5, pp. 1247-1260, 1 May 2023, doi: 10.1109/TC.2022.3198628.

[27].Z. Lu *et al*., "An RRAM-Based Computing-in-Memory Architecture and Its Application in Accelerating Transformer Inference," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, doi: 10.1109/TVLSI.2023.3345651.

[28].M. D. Rote, Vijendran N and D. Selvakumar, "High performance SHA-2 core using the Round Pipelined Technique," *2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, Bangalore, India, 2015, pp. 1-6, doi: 10.1109/CONECCT.2015.7383912.

[29].. Sha, Z. Wang, M. Gao and L. Li, "Multi-Gb/s LDPC Code Design and Implementation," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 17, no. 2, pp. 262-268, Feb. 2009, doi: 10.1109/TVLSI.2008.2002487.

[30].A. P. Kakarountas, G. Theodoridis, T. Laopoulos and C. E. Goutis, "High-Speed FPGA Implementation of the SHA-1 Hash Function," *2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Sofia, Bulgaria, 2005, pp. 211-215, doi: 10.1109/IDAACS.2005.282972.

Received: October 15, 2025