VHDL Based Firewall Implementation Using XC9572 CPLD

Yogita N. Dubey[1], Kashish R. Janole[2], Shruti D. Bijwe[3], Tejaswini M. Khandre[4]. Sakshi V. Rathod[5]
Dr. Nilesh N. Kasat[6]
[1,2,3,4,5]*Projectee Scholar, Department of E&TC, Sipna COET, Amravati, Maharashtra, India*
[6] *Professor in E&TC Dept., Sipna COET Amravati Maharashtra*

***Abstract*—This project designs a high-speed hardware firewall using VHDL on a CPLD (Xilinx XC9572). Unlike software firewalls that can slow down due to heavy network traffic, this hardware firewall filters data directly at the logic gate level, enabling Realtime and low-latency security. The system continuously scans 8-bit incoming data patterns and checks for a malicious pattern '10101010'. If this pattern is detected, the data is blocked and a red LED turns on. If the data is safe, it is allowed to pass and a green LED turns on. The design was created using Xilinx ISE Design Suite and programmed onto the CPLD using the JTAG interface. The results show that CPLDs can be used as fast and reliable embedded hardware security filters.**

***Index Terms*—CPLD, Embedded Systems Security, Hardware Firewall, Network Security, VHDL, Xilinx XC9572**

I. INTRODUCTION

XC9572 CPLD means implementing digital logic circuits on a programmable chip developed by Xilinx. VHDL allows designers to describe digital hardware behaviour and structure, making it suitable for implementing hardware-based security mechanisms [1]. The XC9572 CPLD contains programmable logic blocks that can be configured to perform operations such as control logic, decoding, and digital system design in embedded and electronic applications [2-3]. With the exponential growth of internet-connected devices, the necessity for robust security in digital communication systems has become more critical than ever before [1]. Network firewalls constitute the first line of defence against cyber threats, unauthorized access, and malicious payloads attempting to breach an internal network structure. Historically, firewalls have been predominantly software-based, executing sequential filtering algorithms on general-purpose microprocessors. While software firewalls are highly flexible and capable of handling complex rulesets, they inherently suffer from performance bottlenecks when confronted with Gigabit and Terabit network speeds.

To address these latency issues, network engineers and cybersecurity experts have increasingly turned to hardware-accelerated solutions. Hardware firewalls execute their packet-filtering logic directly at the silicon level, enabling high-speed packet filtering with minimal latency [1–2], utilizing parallel processing structures to evaluate multiple data streams instantaneously. Devices such as Field Programmable Gate Arrays (FPGAs) and Complex Programmable Logic Devices (CPLDs) are at the forefront of this transition. While FPGAs offer massive logic capacity suitable for enterprise-grade unified threat management, CPLDs such as the Xilinx XC9572 provide a cost-effective and fast solution for implementing embedded hardware security systems [2–3].

In this project, a foundational hardware firewall is designed using Very High-Speed Integrated Circuit Hardware Description Language (VHDL) and practically implemented on a CPLD development board. The primary objective is to demonstrate real time data inspection and filtering without relying on any underlying operating system, achieving nanosecond latency in decision-making.

II. BACKGROUND AND LITERATURE REVIEW

The concept of shifting security protocols from the application layer down to the physical or data link

layer is not entirely new, but it has gained significant traction with the advent of high-speed broadband and Internet of Things (IoT) devices. Early firewall solutions relied heavily on software packet-sniffing tools (like iptables or pf) which analyse packet headers through CPU interrupt handling. However, as link speeds increased from 10 Mbps to 10 Gbps, software-based inspection triggered heavy CPU load, often becoming the bottleneck in network throughput.

Researchers have proposed various Application Specific Integrated Circuit (ASIC) and FPGA-based designs to tackle this bottleneck. ASICs offer the ultimate performance but lack updatability—a critical flaw given the dynamic nature of cyber threats. FPGAs successfully bridge this gap by offering reprogrammable hardware. However, FPGAs require an external boot ROM to load their configuration upon power-up, slightly complicating the embedded design. CPLDs present an optimal middle ground for specific, localized security tasks. The Xilinx XC9572, employed in this project, features non-volatile Flash-based programmable logic. This means the firewall logic is instantly available upon power-up ('instant-on' capability), making it exceptionally suitable for mission critical embedded systems where boot-time vulnerabilities cannot be tolerated. By implementing the firewall logic on a CPLD, the system achieves deterministic timing, ensuring that malicious packets are blocked predictably and securely.

III. SYSTEM ARCHITECTURE AND HARDWARE REQUIREMENTS

The development of the CPLD-based firewall necessitates a carefully selected array of hardware components, functioning cohesively to simulate a network data stream and the subsequent filtering process. The overarching architecture is designed to be self-sufficient and observable [4].

A. Xilinx xc9572 cold development board

The core processing engine of this firewall is the Xilinx XC9572 CPLD. The Xilinx XC9572 CPLD contains programmable logic blocks and microcells that can be configured to implement custom digital logic circuits [5,6]. Its architecture is based on advanced Flash technology, granting it thousands of program/erase cycles. Its primary advantage for this project lies in its pin-to-pin propagation delay of just 7.5 nanoseconds, allowing the firewall filtering logic to execute at blistering speeds. The development board houses the CPLD, necessary voltage regulators (usually stepping down an external power supply to the required 5V or 3.3V logic levels), and a breakout of input/output pins for peripheral interfacing.

B peripheral interfaces: switches and led

To simulate the arrival of network data, an 8-position Dual In-line Package (DIP) switch is interfaced with the input pins of the CPLD. Each switch toggle represents a single bit in an 8-bit data sequence, effectively acting as an ingress data port. To visualize the firewall's Realtime decision-making process, Light Emitting Diodes (LEDs) serve as output indicators. When the user configures a safe sequence on the DIP switches, a green 'Allow' LED is illuminated. When an unauthorized or malicious sequence is entered, a red 'Block' LED activates immediately.

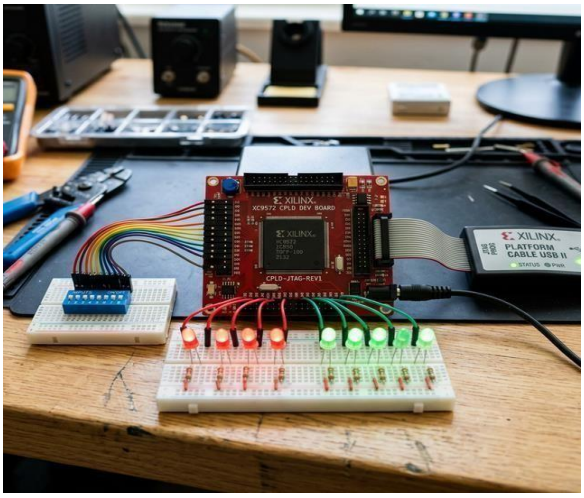

Figure 1: Hardware setup showing the CPLD

C. Jtag programming interface

The configuration generated on the host computer must be transferred to the XC9572's non-volatile memory. The Joint Test Action Group (JTAG) interface is commonly used for programming and debugging CPLD and FPGA devices [7,8]. A JTAG programming cable connects via USB to the host workstation and connects to the dedicated TMS, TDI, TDO, and TCK pins on the CPLD board, providing a direct pipeline to flash the bitstream configuration.

Figure 2: JTAG programming cable used for configuring the XC9572 CPLD

IV. SOFTWARE ENVIRONMENT

The translation of conceptual firewall rules into physical logic gates requires a specialized suite of electronic design automation (EDA) tools. The project extensively utilizes the Xilinx ISE (Integrated Synthesis Environment) Design Suite. ISE provides a comprehensive workflow spanning from initial code entry to final device programming.

The firewall's logic is described exclusively using VHDL (Very High-Speed Integrated Circuit Hardware Description Language). VHDL allows the designer to define the behaviour of the circuit concurrently. Unlike sequential programming languages like C or Python, VHDL instructions are evaluated simultaneously, which is exactly why hardware firewalls can process multiple rules in parallel without suffering from execution delay.

Once the code is synthesized and fitted onto the specific CPLD
architecture, the IMPACT programming tool (bundled within the ISE suite) is utilized to transfer the final `. jed` (JEDEC) programming file to the physical hardware via the JTAG link.

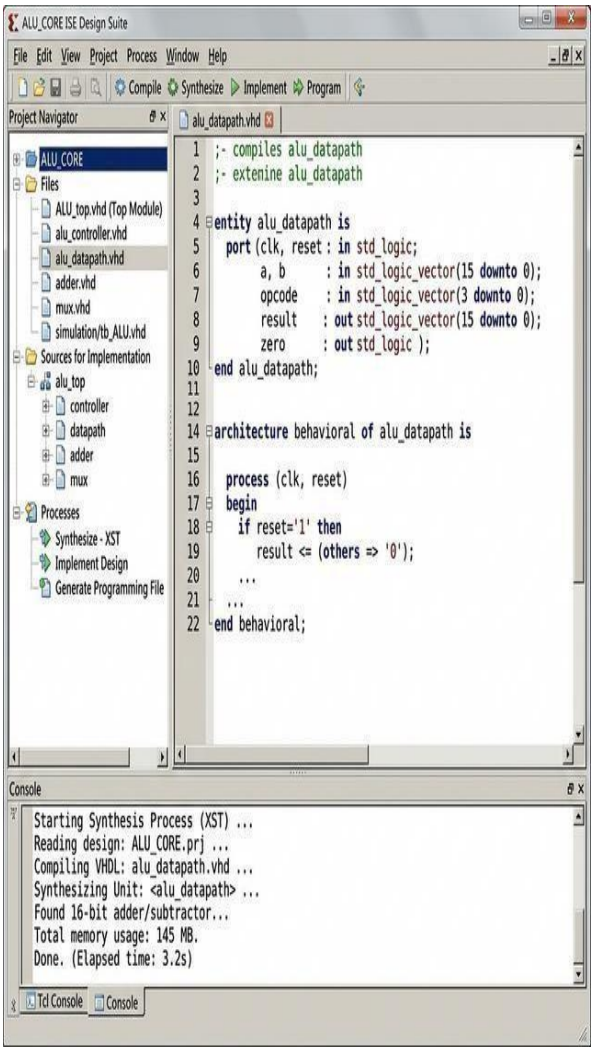

Figure 3: Xilinx ISE Design Suite Interface for VHDL Synthesis.

V. WORKING OF THE SYSTEM AND METHODOLOGY

The primary function of this custom hardware firewall is pattern recognition across an incoming 8bit bus. The filtering mechanism constitutes a concurrent comparator logic block built inside the XC9572 macro cells [8,9].

The system operates on a continuous monitoring mechanism, where the input data stream is sampled in real-time through the DIP switch interface. Each bit of the 8-bit input is simultaneously fed into the comparator logic implemented within the CPLD macro cells. This eliminates the need for sequential data processing and ensures immediate evaluation of the incoming data pattern.

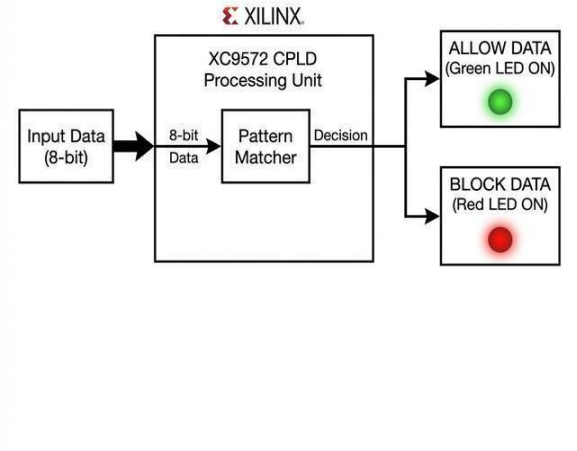

Figure 4: Architecture Block Diagram of the VHDLBased Firewall.

In the physical implementation, the 8-bit DIP switches map directly to the defined input ports in the VHDL entities (e.g., IN_DATA (7 down to 0)). The system checks this incoming data vector continuously against a predefined malicious packet signature to detect and block unauthorized patterns [8,9]. For the scope of this demonstration, the binary pattern 10101010 (representing alternating logic highs and lows, or 0xAA in hexadecimal) is flagged as unpermitted data. The internal logic employs a comparator equation. The moment the input data precisely matches the '10101010' vector, the comparator output transitions from logic LOW to logic HIGH. This transition is tied to a routing multiplexer that forces the system to drop the packet and simultaneously output a logic HIGH to the designated pin driving the RED 'Block' LED. Concurrently, the GREEN 'Allow' LED is driven LOW, confirming the prevention of data traversal.
If the comparator evaluates to false (meaning the input data is any of the other 255 possible 8-bit combinations), the system natively allows the data structure to proceed. In this state, the RED LED is pulled LOW, and the GREEN LED is driven HIGH.

Moreover, the architecture is inherently scalable, supporting future enhancements such as multi-pattern detection, wider data buses, and integration with external communication protocols. This makes the design adaptable for deployment in advanced embedded security systems and real-time network filtering applications.

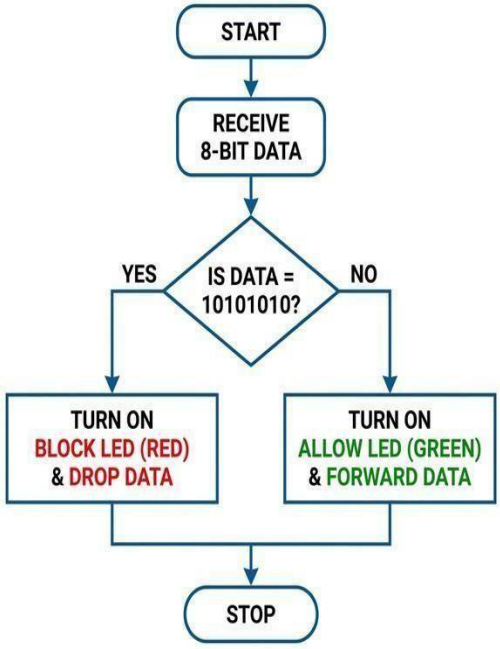

Figure 5: Operational Flowchart of the Data Filtering Logic

VI. VHDL IMPLEMENTATION STRATEGY

The VHDL design strategy for this project was to strike a balance between simplicity and operational robustness. An Entity was declared defining an 8-bit input vector (representing the data stream) and two single-bit outputs representing the Permit (Allow) and Deny (Block) states. The Architecture body leverages a simple combinatorial process block. Since the CPLD is primarily combinatorial logic optimized, the absence of a pervasive clock signal simplifies the design and essentially yields a zero-cycle latency filter. The matching evaluation propagates through the logic gates governed purely by the propagation delay traits of the XC9572 silicon.

VII. SYSTEM ADVANTAGES

The migration from a software appliance to a CPLD driven hardware
Appliance yields numerous architectural and functional advantage:

- High-Speed Data Filtering: Processing takes place at the nanosecond scale, practically invisible to upstream network components. There is zero buffering delay.
- Real-Time Operation: The concurrent nature of VHDL ensures that the input is filtered simultaneously as it arrives, satisfying the criteria for strict real-time systems.
- Absolute OS Independence: By relying exclusively on logic gates rather than sequential commands requiring an operating system, the firewall is entirely immune to OS-level vulnerabilities, exploits, memory leaks, and stack overflows.
- Low Power Consumption: CPLDs, lacking the heavy overhead of large processors and DDR memory banks, consume minimal wattage, making them perfect for battery-operated nodes.
- Instant Readiness: Powered by Flash memory, the XC9572 firewall is fully operational milliseconds after power is applied, intercepting threats immediately during cold boots.

VIII. INDUSTRIAL AND COMMERCIAL APPLICATIONS

Owing to its streamlined latency and robust nature, this CPLD-based firewall design is applicable to various vital sectors

- Network Security Appliances: Functioning as a highspeed inline pre-filter layer that silently drops obvious bad IP headers or traffic profiles before they reach the main software-based Deep Packet Inspection (DPI) servers.
- Routers and Industrial Switches: Embedding this logic into core network infrastructure appliances prevents DoS/DDoS amplification loops right at the port interface.
- Embedded IoT Devices: Providing a robust firewall layer for microcontrollers governing smart home networks and connected medical hardware [9,10].
- Automotive Networks: Securing the CAN-Bus networks in modern vehicles against malicious diagnostic port injections [9,10].

IX. CONCLUSION

In conclusion, this project successfully demonstrates the concept, design, and practical implementation of a highspeed hardware firewall using VHDL and a Xilinx XC9572 CPLD. By offloading the pattern recognition algorithms from software processing to hardware combinatorial execution, the system achieves remarkable real-time data inspection capabilities. Testing with the designated '10101010' malicious 8-bit signature confirmed immediate payload blockage alongside accurate status visualizations on the hardware testbed. While this implementation utilizes a simplified 8-bit signature architecture for demonstration purposes, the core logic structure can be inherently scaled. Future iterations could involve shifting to a more expansive FPGA to accommodate 64-bit or 128-bit payload signatures, enabling thorough packet header inspections, dynamic rule modifications, and integration into standard Ethernet physical layer (PHY) transceivers for real world gigabit traffic policing.

In addition, the architecture provides a strong foundation for future research in hardware-based intrusion detection systems. Enhancements such as dynamic rule configuration, multi-pattern recognition, and integration with higher-level network protocols can further extend the capabilities of the system.

REFERENCES

[1] Xilinx Inc., XC9500 CPLD Family Data Sheet, Xilinx Corporation, USA. Available: https://www.xilinx.com
[2] Douglas L. Perry, VHDL Programming by Example, 4th Edition, McGraw-Hill, 2002.
[3] S. Brown and Z. Vranesic, Fundamentals of Digital Logic with VHDL Design, 3rd Edition, McGrawHill Education, 2009.
[4] Xilinx Inc., ISE Design Suite User Guide, Xilinx Corporation.
[5] J. Bhasker, A VHDL Primer, 3rd Edition, Prentice Hall, 1999.
[6] William Stallings, Network Security Essentials: Applications and Standards, Pearson Education, 2017.
[7] R. Hinden and S. Deering, Internet Protocol Version 6 (IPv6) Specification, IETF RFC 8200.

[8] N. Weste and D. Harris, CMOS VLSI Design: A Circuits and Systems Perspective, Addison-Wesley, 2011.
[9] Behrouz A. Forouzan, Data Communications and Networking, McGraw-Hill Education.
[10] Xilinx Documentation, JTAG Boundary Scan and Programming Guide, Xilinx Inc.