FPGA - BASED BORDER INTRUSION DETECTION SYSTEM

WINTER INTERNSHIP REPORT : DECEMBER 2025

INTERNSHIP REPORT SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR ASSESSMENT AND AWARD OF CREDITS FOR THE COURSE UNDER THE AUTONOMOUS REGULATIONS OF SRI ESHWAR COLLEGE OF ENGINEERING, COIMBATORE AFFILIATED TO ANNA UNIVERSITY, CHENNAI

INTERNSHIP REPORT

Submitted by

KARTHIBAN S T-722824106067

PRAVIN A-722824106121

BATCH 2024 – 2028

Under the Guidance of

NANDITHA N VARMA

ADHOC FACULTY

DEPARTMENT OF VLSI

NIELIT CALICUT

Sri Eshwar College of Engineering

(An Autonomous Institution)

Kinathukadavu (Tk), Coimbatore - 641 202, Tamil Nadu

Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai

FPGA - BASED BORDER INTRUSION DETECTION SYSTEM

INTERNSHIP REPORT SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR ASSESSMENT AND AWARD OF CREDITS FOR THE COURSE UNDER THE AUTONOMOUS REGULATIONS OF SRI ESHWAR COLLEGE OF ENGINEERING, COIMBATORE AFFILIATED TO ANNA UNIVERSITY, CHENNAI

WINTER INTERNSHIP REPORT : DECEMBER 2025

INTERNSHIP REPORT

Submitted by

KARTHIBAN S T-722824106067

PRAVIN A-722824106121

BATCH 2024 – 2028

Under the Guidance of

NANDITHA N VARMA

ADHOC FACULTY

DEPARTMENT OF VLSI

NIELIT CALICUT

Sri Eshwar College of Engineering

(An Autonomous Institution)

Kinathukadavu (Tk), Coimbatore - 641 202, Tamil Nadu

Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai

Sri Eshwar College of Engineering
Coimbatore | Tamilnadu
An Autonomous Institution
Affiliated to Anna University, Chennai

INTERNSHIP COMPLETION CERTIFICATE

This is to certify that the internship project entitled "**FPGA-BASED BORDER INTRUSION DETECTION SYSTEM** " was carried out by PRAVIN A - 722824106121 during the short-term internship programme, in partial fulfilment of the requirements for the award of the Internship Certificate.

The work presented in this Internship Project Report is a record of original work carried out by the student under my supervision and guidance in the Department of VLSI, NATIONAL INSTITUTE OF ELECTRONICS & INFORMATION TECHNOLOGY, Calicut

To the best of my knowledge, the work is genuine and has not been submitted elsewhere for any other academic or professional purpose.

----------	----------
SIGNATURE	**SIGNATURE**
Mr. SREEJEESH S G **SENIOR TECHNICAL OFFICER** **DEPARTMENT OF VLSI** **NIELIT CALICUT**	**NANDITHA N VARMA** **ADHOC FACULTY** **DEPARTMENT OF VLSI** **NIELIT CALICUT**

Submitted for the **as a part of winter Internship** held during the period from 01.12.2025 to 26.12.2025.

CANDIDATE'S DECLARATION

I, PRAVIN A hereby declare that the report entitled DIGITAL SYSTEM PROTOTYPING USING FPGA's which is being submitted to Department of VLSI in **National Institute of Electronics & Information Technology, Calicut** is our authentic work carried out during internship.

I declare that my work has not been submitted in part or in full to any other university or institution for the award of any certificate.

PRAVIN A

QUALITY POLICY

To establish a system of Quality Enhancement, which would on a continuous basis evaluate and enhance the quality of teaching – learning, research and extension activities of the institution, leading to improvements in all processes, enabling the institution to attain excellence.

INSTITUTE VISION

To be recognized as a premier institution, grooming students into globally acknowledged engineering professionals.

INSTITUTE MISSION

- Providing outcome and value-based engineering education
- Nurturing research and entrepreneurial culture
- Enabling students to be industry ready and fulfill their career aspirations
- Grooming students through behavioural and leadership training programs
- Making students socially responsible

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

DEPARTMENT VISION

To groom students into futuristic and globally competent Electronics and Communication engineering professionals.

DEPARTMENT MISSION

- To impart quality education with moral and ethical values to develop competent engineers, leaders and successful entrepreneurs
- To establish state-of-art infrastructure and provide opportunities to update on emerging tools and technologies
- To empower the faculty towards excellence in teaching – learning, consultancy, research and development activities
- To foster socially relevant and industry oriented innovation among students.

PROGRAM EDUCATIONAL OBJECTIVES

- **PEO1:** Pursue career in multinational organizations, research organizations and core industries, higher studies at premier institutions and establish start-ups.
- **PEO2:** Acquire core competencies in Electronics and Communication Engineering and exposure to latest Electronic Design Automation (EDA) tools.
- **PEO3:** Exhibit professional skills and collaborative work experience

PROGRAM OUTCOMES

PO1: Engineering Knowledge: Apply knowledge of mathematics, natural science, computing, engineering fundamentals and an engineering specialization as specified in WK1 to WK4 respectively to develop to the solution of complex engineering problems.

PO2: Problem Analysis: Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions with consideration for sustainable development. (WK1 to WK4)

PO3: Design/Development of Solutions: Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required. (WK5)

PO4: Conduct Investigations of Complex Problems: Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions. (WK8).

PO5: Engineering Tool Usage: Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems. (WK2 and WK6)

PO6: The Engineer and The World: Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework, culture and environment. (WK1, WK5, and WK7).

PO7: Ethics: Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws. (WK9)

PO8: Individual and Collaborative Team work: Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.

PO9: Communication: Communicate effectively and inclusively within the engineering community and society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations considering cultural, language, and learning differences

PO10: Project Management and Finance: Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one's own work, as a member and leader in a team, and to manage projects and in multidisciplinary environments.

PO11: Life-Long Learning: Recognize the need for, and have the preparation and ability for i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change. (WK8)

PROGRAM SPECIFIC OUTCOMES

- **PSO1**:Interpret and design electronic systems using internet of things, VLSI technology and efficient signal processing and computing algorithms.
- **PSO2:**Apply knowledge to solve challenges in communication systems and networks.

ABSTRACT

This internship project focuses on the design, development, and implementation of an **FPGA-Based Intelligent Border Intrusion Detection and Tamper Monitoring System** intended to provide a reliable and real-time security solution for monitoring multiple protected zones. The primary objective of the project was to create a hardware-oriented system capable of detecting unauthorized intrusions, dynamically classifying threat levels, and identifying potential sensor tampering or sabotage. The system was designed using **Verilog Hardware Description Language (HDL)** and implemented on an **FPGA platform**, following a structured digital design methodology. A **Finite State Machine (FSM)** architecture was employed to control system operation, enabling smooth transitions between different operational states such as Safe, Alert, and High Alert based on real-time sensor inputs. The design supports monitoring of multiple zones simultaneously, with a priority-based zone detection mechanism to highlight the most critical intrusion area. To improve system robustness, a **time-based tamper detection mechanism** was incorporated, allowing the system to identify abnormal sensor behaviour such as signal jamming or prolonged constant inputs. An **arm/disarm control feature** was added to ensure that intrusion detection is active only when authorized, closely reflecting real-world security system requirements. For effective visualization and debugging on physical hardware, a **clock divider** was integrated to slow down the system clock, enabling human-perceivable LED indications without affecting the core logic. Comprehensive simulation and verification were performed using **Vivado design and simulation tools**, supported by an exhaustive testbench that validated all functional scenarios including single-zone intrusion, multi-zone coordinated attacks, alert escalation and downgrade, tamper detection, system reset, and disarm conditions. The system was successfully deployed on FPGA hardware and demonstrated stable and correct behavior under all tested conditions. Through this internship, significant hands-on experience was gained in FPGA design flow, FSM-based control logic, hardware debugging, timing analysis, and verification techniques, thereby strengthening both theoretical understanding and practical skills relevant to **VLSI, digital system design, and embedded hardware development**.

INTERNSHIP PROJECT REPORT

Table of Content

1.Introduction

1.1. Organization Background

The **National Institute of Electronics & Information Technology (NIELIT), Calicut** is a premier institution under the **Ministry of Electronics and Information Technology (MEITY), Government of India**, established to promote education, training, and research in the fields of electronics, information technology, and emerging digital technologies. NIELIT functions as an autonomous scientific society with a mandate to develop skilled human resources capable of meeting the evolving needs of the electronics and IT industries. The Calicut center plays a significant role in delivering high-quality technical education and industry-oriented training programs to students, professionals, and government organizations. NIELIT Calicut offers a wide range of academic programs, including long-term diploma courses, short-term certification programs, industrial training, and internships in domains such as **VLSI design, embedded systems, FPGA development, cybersecurity, artificial intelligence, Internet of Things (IoT), and digital signal processing**. These programs are carefully designed to align with current industry standards and technological advancements. The institute emphasizes a balanced approach that integrates strong theoretical foundations with extensive hands-on practical training, enabling learners to apply classroom concepts to real-world engineering problems. In addition to training and education, NIELIT Calicut is actively involved in consultancy services, research initiatives, and collaborative projects with academic institutions, industries, and government agencies. The institute regularly conducts workshops, seminars, and faculty development programs to promote continuous learning and technological awareness. Modern laboratories equipped with advanced tools and licensed software provide an ideal environment for experimentation, design, and innovation. Through its structured curriculum, experienced faculty, and focus on practical implementation, NIELIT Calicut serves as a bridge between academic learning and industrial requirements. The internship program offered by the institute provides students with valuable exposure to professional work culture, technical problem-solving, and project-based learning. This environment played a crucial role in facilitating the successful completion of the FPGA-based project undertaken during this internship.

1.2. Objectives of the Internship

The primary objective of this internship was to gain **practical exposure to FPGA-based digital system design** and to understand how theoretical concepts learned in academic courses are applied in real-world engineering applications. The internship aimed to strengthen the intern's knowledge of **Verilog Hardware Description Language (HDL)** and its use in designing, simulating, and implementing digital systems on FPGA platforms. A key objective was to develop an understanding of **Finite State Machine (FSM)** design techniques and their importance in controlling complex digital systems.Another important objective of the internship was to learn the complete **FPGA development flow**, including RTL coding, functional simulation, synthesis, implementation, and hardware verification using industry-standard tools such as **Xilinx Vivado**. The internship also aimed to improve debugging skills by analyzing simulation waveforms, identifying logical and timing issues, and resolving hardware-related challenges during FPGA implementation. Emphasis was placed on writing structured, modular, and reusable Verilog code following good design practices.The internship further sought to apply technical knowledge to a **real-world, socially relevant problem**, resulting in the development of an **FPGA-Based Intelligent Border Intrusion Detection and Tamper Monitoring System**. This objective encouraged the intern to think beyond academic exercises and design a system with practical significance in defense and security applications. Learning to integrate features such as multi-zone detection, alert escalation, tamper detection, and arm/disarm control was an essential part of achieving this objective.In addition to technical goals, the internship aimed to enhance **professional skills**, including documentation, time management, effective communication, and systematic problem-solving. Exposure to a professional training environment helped the intern understand industry expectations, work discipline, and collaborative learning practices. Overall, the internship objectives were successfully achieved by combining technical training, hands-on project development, and continuous learning under expert guidance at NIELIT Calicut.

1.3. Scope of the Internship

The scope of this internship encompassed a comprehensive learning experience in the field of digital electronics and FPGA-based system design. It included gaining foundational and advanced knowledge of digital logic concepts, Verilog HDL coding, and FSM-based control systems. The internship provided hands-on exposure to designing and implementing digital systems that interact with real hardware inputs and outputs, such as switches and LEDs, using FPGA technology.A significant part of the internship scope involved understanding the end-to-end FPGA design workflow, starting from problem analysis and system specification to RTL design, simulation, synthesis, and on-board testing. The intern was trained to use professional tools like Xilinx Vivado for code development, functional verification, and timing analysis. Writing testbenches to verify all possible functional scenarios and ensuring reliable system behavior was also within the scope of the internship.The project work formed the core of the internship scope, focusing on the development of an Intelligent Border Intrusion Detection System. This included implementing multi-zone intrusion monitoring, priority-based zone identification, dynamic alert escalation and downgrade, time-based tamper detection, and an arm/disarm mechanism. The scope also covered optimizing the design for hardware visibility using clock division techniques and validating system performance on FPGA hardware.Beyond technical aspects, the internship scope included improving analytical thinking, debugging methodologies, and documentation skills. The intern was encouraged to maintain clear project documentation, explain design decisions, and justify system behavior during reviews and discussions. Exposure to professional training practices and structured learning at NIELIT Calicut broadened the intern’s understanding of career opportunities in VLSI , and hardware design. Overall, the internship scope was well-defined to provide both depth and breadth of knowledge, preparing the intern for future academic and professional challenges in the electronics domain.

2. Internship Activities and Project Work

2.1 Roles and Responsibilities

PRAVIN A – Hardware Design & Core Logic Development

Responsibility	Description
Requirement Analysis	Understanding the project objectives and overall security requirements
FSM Design	Designing system states such as Safe, Alert, and High Alert with proper transitions
Verilog Coding	Developing and implementing the core Verilog HDL modules
Zone Detection Logic	Implementing single-zone and multi-zone intrusion detection logic
Tamper Detection Logic	Designing a time-based sensor tamper detection mechanism
Arm/Disarm Control	Implementing system enable and disable functionality
Debugging	Identifying and fixing logical, functional, and timing-related issues
FPGA Implementation	Synthesizing, implementing, and deploying the design on FPGA hardware

KARTHIBAN S T – Verification, Integration & Documentation

Responsibility	Description
Testbench Development	Writing comprehensive testbenches to verify all functional scenarios
Simulation & Analysis	Performing functional simulations and analyzing waveform outputs
Clock Divider Design	Implementing clock management for visible and stable hardware output
Integration	Integrating all modules into a single top-level FPGA design
Hardware Testing	Verifying LED outputs and system behavior on FPGA hardware
Result Analysis	Observing, validating, and documenting system performance
Documentation	Preparing the internship report, tables, and technical explanations
Presentation Preparation	Assisting in project presentation, demonstration, and review preparation

Collaborative Responsibilities

Activity	Contribution
System Architecture Design	Joint discussion, planning, and finalization of system design
Problem Solving	Collaborative debugging, optimization, and issue resolution
Learning & Knowledge Sharing	Mutual understanding and sharing of FPGA design concepts and design flow
Final Review	Joint validation and verification of project objectives and outcomes

2.2 Project Description / Modules Undertaken

The project titled "FPGA-Based Intelligent Border Intrusion Detection and Tamper Monitoring System" aims to design a real-time hardware security solution capable of detecting unauthorized intrusions across multiple border zones. The system continuously monitors multiple sensor inputs representing different border regions and classifies threats into different security levels such as Safe, Alert, and High Alert. A Finite State Machine (FSM) is used to control system behavior based on zone activity and tamper conditions. The project also incorporates a tamper detection mechanism to identify abnormal sensor behavior, such as sensor jamming or prolonged constant inputs. An arm/disarm control feature ensures that the system operates only when authorized, improving system reliability and security.

The project was developed using a modular approach to simplify design, testing, and future expansion. The key modules undertaken during the project include:

Zone Detection Module: Monitors multiple zone inputs and identifies active zones.

Priority Encoder Module: Determines the highest-priority active zone for indication.

FSM Controller Module: Controls system states and transitions based on inputs.

Tamper Detection Module: Detects sensor jamming using time-based logic.

Arm Control Module: Enables or disables intrusion detection.

Clock Divider Module: Slows down system clock for human-perceivable LED outputs.

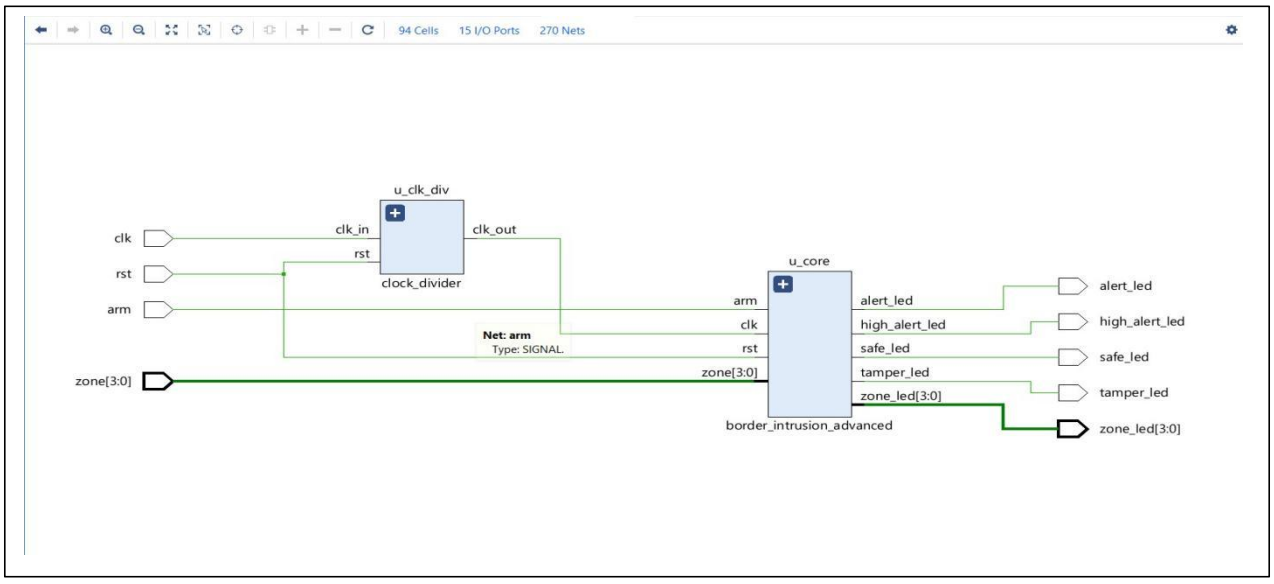
Output Display Module: Drives LEDs to indicate system status and alerts.

Each module was individually developed, tested, and then integrated to form a complete FPGA-based intrusion detection system.

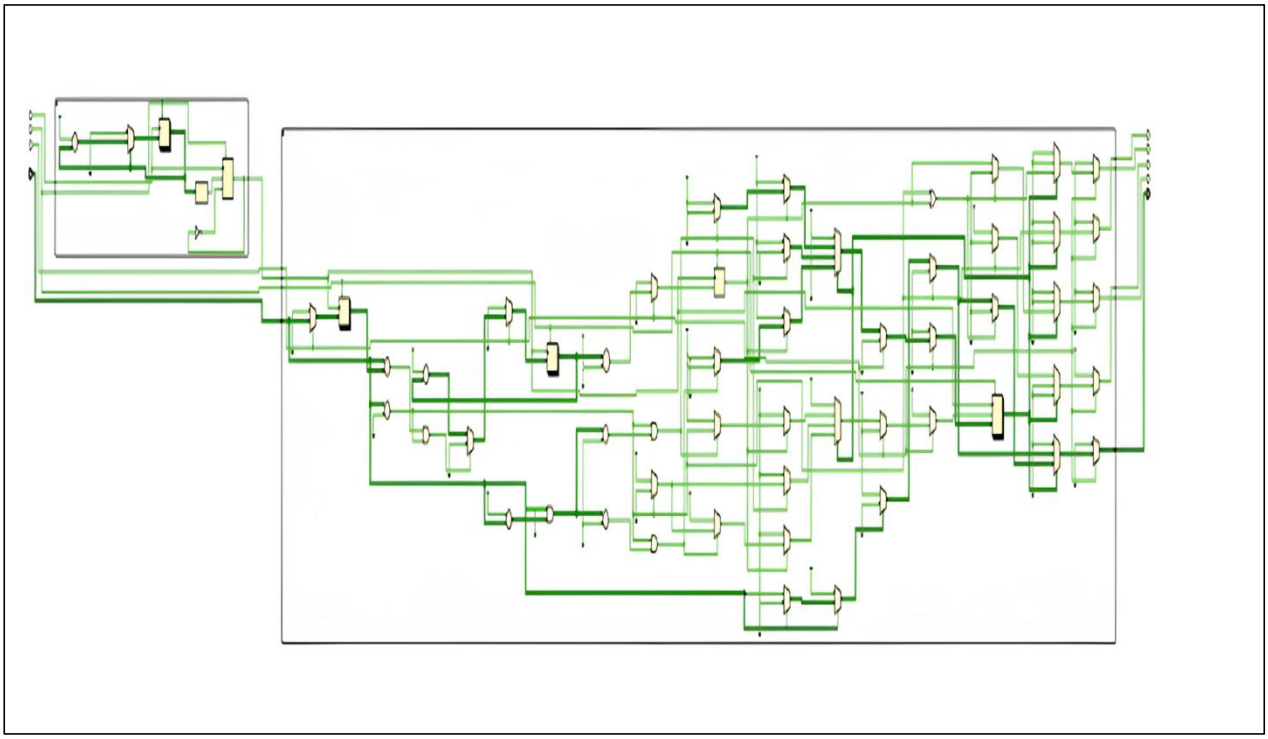
2.3 Methodology / Algorithm / System Design

The system was designed following a structured hardware design methodology using Verilog HDL and FPGA implementation techniques. Initially, the system requirements were analyzed to identify input conditions, output indications, and security states. Based on these requirements, a Finite State Machine (FSM) was designed to represent different operational modes of the system.The methodology begins with checking the arm signal. When the system is disarmed, all intrusion detection logic is disabled, and the system remains in a safe state. Once armed, the system enters the monitoring state and continuously observes zone inputs. If a single zone becomes active, the system transitions to the Alert state. If multiple zones are active simultaneously, or if a tamper condition is detected, the system escalates to the High Alert state. The system also supports dynamic escalation and downgrade of alert levels based on real-time zone activity. A priority encoding algorithm is used to identify the most critical active zone for indication. Tamper detection is implemented using a time-based counter that monitors whether a zone input remains unchanged for a predefined duration, indicating possible sensor jamming. A clock divider is used to reduce the FPGA clock frequency for visible LED indication. Finally, the design was simulated using testbenches to verify all functional scenarios before being implemented and tested on FPGA hardware.

(i) Block diagram



(ii) Internal Schematic Circuit



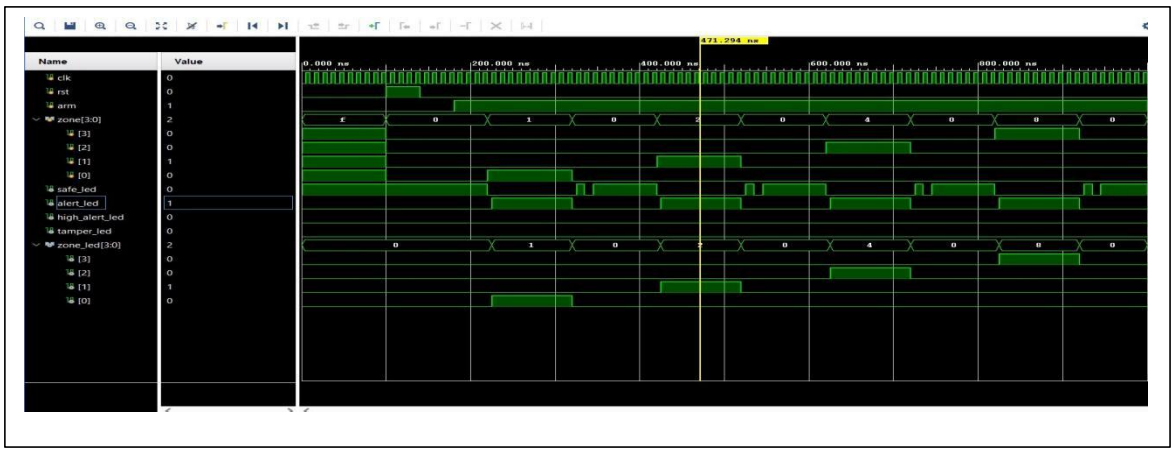
2.4 Tools and Technologies Used

The project was developed and implemented using industry-standard FPGA design tools and hardware platforms to ensure reliability and real-time performance. The primary design and simulation tool used for this project was Xilinx Vivado Design Suite, which provides an integrated environment for writing Verilog HDL code, performing functional simulation, synthesis, and hardware implementation. Vivado was used to analyze design behavior through waveform simulation, enabling effective debugging and verification of all system modules.The target hardware platform for implementation was the BASYS-3 FPGA development board, which is based on the Xilinx Artix-7 FPGA. The BASYS-3 board was selected due to its suitability for educational and prototyping purposes, availability of on-board LEDs and switches, and compatibility with Vivado tools. On-board switches were used to represent zone sensors and the arm signal, while LEDs were used to display system status such as Safe, Alert, High Alert, Tamper indication, and active zones.The project employed Verilog Hardware Description Language (HDL) for designing the digital logic and Finite State Machine (FSM) modeling techniques for system control. A clock divider was implemented to reduce the FPGA clock frequency for human-perceivable output behavior. Simulation and verification were carried out using Vivado's built-in simulator, and final hardware validation was performed by programming the BASYS-3 board.

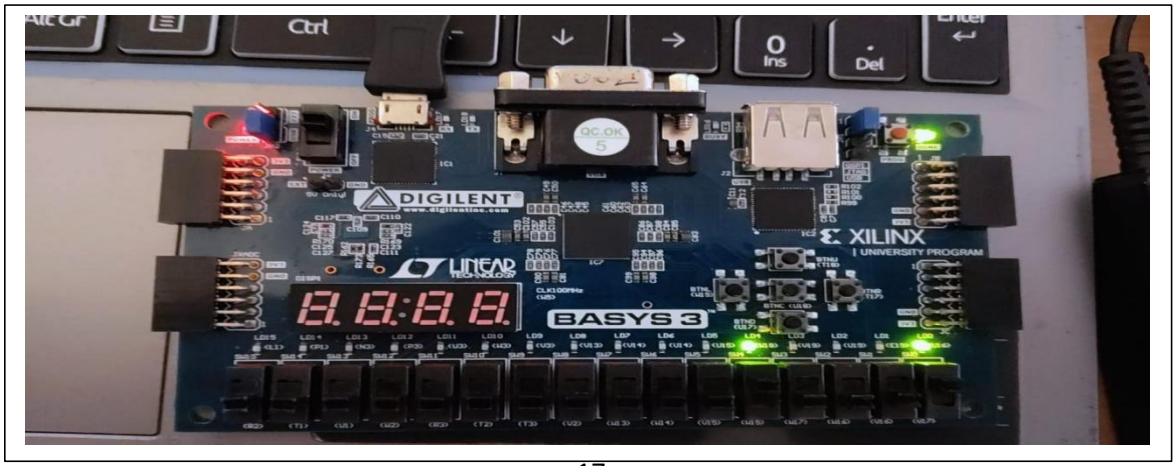
2.5 Results and Outcome Analysis

The FPGA-based border intrusion detection system was successfully designed, simulated, and implemented on the BASYS-3 FPGA board, demonstrating correct real-time operation under all tested conditions. The system accurately detected single-zone intrusions and indicated them through the Alert state, while multi-zone intrusions or tamper conditions correctly escalated the system to the High Alert state. The dynamic escalation and downgrade of alert levels functioned as intended, ensuring realistic and responsive system behavior. The arm/disarm control effectively enabled and disabled intrusion detection, confirming secure system operation. Hardware testing on the BASYS-3 board confirmed stable LED indications, clear visualization of system states, and correct mapping of inputs and outputs. Overall, the project achieved its intended objectives by successfully implementing a reliable and scalable FPGA-based security system. The outcome demonstrates the practical application of FPGA technology, FSM-based control logic, and hardware verification techniques in real-world security and surveillance systems.

(i) Waveform



(ii) FPGA Board Output



3. Skills and Learning Outcomes

3.1 Technical Skills Acquired

During the internship at the National Institute of Electronics & Information Technology (NIELIT), Calicut, significant technical skills were acquired through hands-on involvement in the design and implementation of an FPGA-based border intrusion detection system. One of the major technical skills developed was proficiency in Verilog Hardware Description Language (HDL), including writing synthesizable code, modular design, and implementing combinational and sequential logic.A strong understanding of Finite State Machine (FSM) design was gained by modeling system behavior across different operational states such as Safe, Alert, and High Alert. The internship also enhanced knowledge of digital logic design concepts, including priority encoding, counters, clock division, and synchronous system design.Practical experience was gained in using the Xilinx Vivado Design Suite for simulation, synthesis, and hardware implementation. Skills in testbench development and functional verification were developed by validating all possible system scenarios through waveform analysis. The internship further improved understanding of FPGA implementation flow, including constraint assignment, bitstream generation, and programming the BASYS-3 FPGA board.Additionally, experience was gained in hardware debugging, where simulation results were correlated with real-time FPGA behavior to identify and resolve timing and logical issues. Overall, the internship significantly strengthened technical competence in FPGA-based system development, bridging the gap between theoretical digital design concepts and real-world hardware implementation.

3.2 Professional Skills Acquired

During the internship, several professional skills were developed alongside technical expertise. Effective communication skills were enhanced through regular interactions with mentors and team members, including explaining technical concepts, discussing design decisions, and presenting project progress. Teamwork and collaboration skills were strengthened by working in a team of two, sharing responsibilities, coordinating tasks, and jointly resolving design challenges.The internship also improved time management and planning skills, as project milestones had to be completed within a fixed duration. Adhering to schedules for design, simulation, testing, and documentation helped develop discipline and accountability. Problem-solving and analytical thinking were enhanced through systematic debugging, waveform analysis, and logical reasoning to resolve design and hardware implementation issues.Additionally, experience was gained in technical documentation and report writing, where structured documentation was prepared in accordance with academic and professional standards.

3.3 Personal and Career Development

The internship played a significant role in personal growth and career development by providing clarity on future career goals in the field of VLSI design, FPGA development, and embedded systems. Hands-on experience with real hardware increased confidence in applying theoretical knowledge to practical problems. The project enhanced independent learning ability and adaptability when faced with new tools and complex design challenges.Working on a defense-oriented security application fostered a sense of responsibility and motivation to contribute to technology-driven solutions with real-world impact. The internship also helped in identifying areas of interest for further specialization, such as advanced FPGA architectures, hardware security, and system optimization. Overall, the internship experience at NIELIT strengthened both technical confidence and professional readiness, laying a strong foundation for future academic pursuits and career opportunities in the electronics and semiconductor industry.

4. Challenges and Solutions

The development and implementation of the FPGA-Based Intelligent Border Intrusion Detection and Tamper Monitoring System involved multiple technical and practical challenges. These challenges were encountered during different stages of the internship, including design, simulation, verification, and hardware implementation. Addressing these challenges played a vital role in improving both technical understanding and problem-solving skills. This chapter discusses the major challenges faced during the project and the solutions and strategies adopted to overcome them.

4.1 Challenges Faced

Understanding FSM-Based System Behavior

One of the primary challenges faced during the project was understanding and correctly implementing Finite State Machine (FSM) behavior for a real-time security system. Designing state transitions that accurately reflected system requirements such as safe operation, alert escalation, and alert downgrade required careful analysis. Initially, the FSM exhibited unexpected behavior due to incomplete state transition conditions, particularly during dynamic escalation and downgrade scenarios when zone inputs changed rapidly.

Handling Clock-Related Timing Issues

Another significant challenge was managing clock timing behavior in the FPGA environment. The BASYS-3 board operates at a high clock frequency, which caused LED outputs to change too rapidly to be observed by the human eye. This made debugging and validation difficult, as state transitions occurred almost instantaneously. Additionally, understanding the effect of synchronous state updates and clock-edge-based logic introduced complexity in interpreting simulation waveforms and hardware outputs.

Simulation and Hardware Mismatch

During initial testing, differences were observed between simulation results and actual FPGA behavior. Certain outputs behaved correctly in simulation but appeared unstable or unexpected on hardware. These discrepancies were primarily due to real-world hardware factors such as switch bounce, asynchronous input behavior, and clock sampling effects, which are not always evident in ideal simulation environments.

Implementing Reliable Tamper Detection

Designing an effective tamper detection mechanism was another challenge. The requirement was to detect sensor jamming or abnormal behavior without generating false alarms. Implementing a time-based detection approach required selecting appropriate counter thresholds and ensuring that normal zone activity did not incorrectly trigger tamper alerts. Balancing sensitivity and reliability was a critical challenge.

ARM / DISARM Control Integration

Integrating the arm/disarm control into the system logic presented additional complexity. Initially, zone detection and alert generation continued even when the system was disarmed, which did not align with real-world security requirements. Ensuring that all detection logic was properly gated by the arm signal without introducing unintended state behavior required careful restructuring of the FSM and output logic.

Debugging and Verification Complexity

As the project involved multiple interacting modules, debugging issues across the system became increasingly complex. Identifying whether errors originated from the FSM, zone detection logic, tamper logic, or clock divider required systematic analysis. Developing comprehensive testbenches to verify all possible operational scenarios was time-consuming but necessary.

4.2 Solutions and Strategies Adopted

Structured FSM Design and Refinement

To address FSM-related challenges, a systematic approach was adopted by clearly defining each state and its corresponding transition conditions. State transition diagrams were reviewed and refined to include all possible scenarios, including escalation and downgrade between alert levels. Incremental testing was performed by simulating each state independently before full system integration, which significantly improved FSM reliability.

Clock Divider Implementation

To overcome timing and visibility issues, a clock divider was implemented to reduce the effective operating frequency of the system. This allowed LED outputs to remain stable and visible for human observation. The use of a slower clock also simplified debugging by making state transitions easier to track during both simulation and hardware testing.

Bridging Simulation and Hardware Behavior

To minimize discrepancies between simulation and hardware behavior, careful attention was given to synchronizing inputs and handling real-world hardware effects. Switch inputs were treated as asynchronous signals, and their behavior was analyzed over multiple clock cycles. Extended simulation runs and waveform analysis were used to understand timing relationships, enabling effective correlation between simulation and FPGA outputs.

Optimized Tamper Detection Strategy

The tamper detection logic was improved by implementing a time-based counter mechanism that monitored stable zone patterns over consecutive clock cycles. Threshold values were carefully chosen to ensure reliable detection of sensor jamming while avoiding false positives caused by brief or normal input variations. Reset conditions were also incorporated to ensure tamper alerts cleared appropriately when conditions normalized.

ARM Gating of FSM and Outputs

To ensure correct system behavior, the arm signal was integrated as a gating mechanism across both FSM transitions and output logic. When the system was disarmed, the FSM was forced into a safe state and all intrusion detection logic was disabled. This approach ensured predictable system behavior and improved overall system reliability and security compliance.

Comprehensive Testbench Development

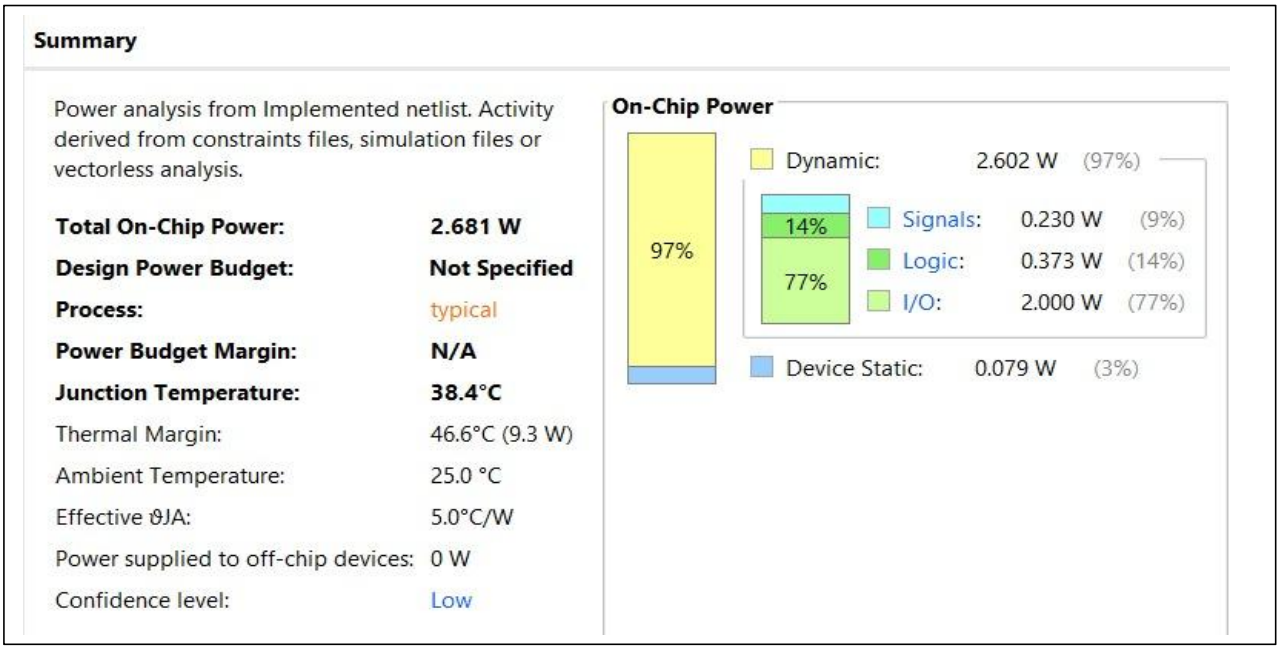
To manage debugging complexity, a comprehensive and exhaustive testbench was developed to validate all functional scenarios, including single-zone intrusion, multi-zone attacks, alert escalation and downgrade, tamper detection, reset behavior, and arm/disarm functionality. Systematic verification helped identify corner cases and ensured robust performance before hardware deployment.

Documentation and Iterative Improvement

Throughout the internship, detailed documentation was maintained to record design decisions, observed issues, and corresponding solutions. Regular review sessions with mentors helped refine design choices and adopt best practices. An iterative development approach allowed continuous improvement of the system based on testing feedback.

Utilization Report:

- **Resource Usage:** Total counts and percentages of used Look-Up Tables (LUTs), Flip-Flops (FFs), BRAMs, and DSP slices.
- **Hierarchy Breakdown:** Detailed resource usage for specific modules in your design.
- Timing Summary Report:
- **Worst Negative Slack (WNS):** The most critical metric for setup timing. A positive value means the design meets its timing requirements.
- **Worst Hold Slack (WHS):** Metric for hold timing to ensure data remains stable at registers.
- **Critical Paths:** Identification of the longest delay paths between sequential cells or ports.



Total On-Chip Power: Estimated power consumption (Watts), divided into static (leakage) and dynamic (switching) power.

Thermal Margin: Temperature estimates to ensure the device remains within safe operating limits.

Name	Slice LUTs (20800)	Slice Registers (41600)	Slice (8150)	LUT as Logic (20800)	Bonded IOB (106)	BUFGCTRL (32)
N top_border_intrusion_fpga	38	38	19	38	15	1

5. Conclusion and Future Scope

5.1 Conclusion

The internship project entitled “FPGA-Based Intelligent Border Intrusion Detection and Tamper Monitoring System” was successfully designed, implemented, and validated during the internship at the National Institute of Electronics & Information Technology (NIELIT), Calicut. The primary objective of the project was to develop a reliable, real-time hardware-based security system capable of detecting unauthorized intrusions across multiple border zones while also identifying potential sensor tampering. This objective was achieved by effectively applying digital system design concepts using Verilog HDL and deploying the system on the BASYS-3 FPGA board.The system architecture was based on a Finite State Machine (FSM) approach, which enabled structured and predictable system behavior. Different operational states such as Safe, Alert, and High Alert were clearly defined, and smooth state transitions were achieved based on real-time zone inputs and tamper conditions. The implementation of dynamic alert escalation and downgrade ensured realistic system behavior, closely reflecting real-world security requirements. The inclusion of an arm/disarm control mechanism further enhanced system safety by allowing intrusion detection to operate only when authorized.Comprehensive simulation was carried out using the Xilinx Vivado Design Suite, where all functional scenarios were thoroughly verified using a detailed testbench. Hardware implementation on the BASYS-3sYS-3 board confirmed stable operation, clear LED indications, and correct mapping of inputs and outputs. Practical challenges such as clock timing issues, FSM synchronization, and hardware debugging were successfully addressed during the development process.Overall, the project successfully met all its intended objectives and provided valuable hands-on experience in FPGA-based system design, FSM modeling, hardware verification, and real-time debugging. The internship significantly strengthened both technical and professional skills, bridging the gap between theoretical learning and practical implementation in the field of digital electronics and VLSI design.

5.2 Future Scope

Although the current system fulfills its design objectives, there is considerable scope for further enhancement and expansion to make it more suitable for real-world deployment. One major future improvement involves integrating wireless communication modules such as GSM, LoRa, or Wi-Fi to enable remote alert notifications and centralized monitoring. This would allow security personnel to receive real-time intrusion alerts without being physically present at the monitored location.The system can also be expanded by incorporating advanced sensor technologies and IoT-based sensor networks to cover larger border areas. Integration with camera modules and image-processing techniques can provide visual confirmation of intrusion events, thereby increasing system reliability. Additionally, intrusion data can be logged and stored for further analysis and reporting.Another promising area of enhancement is the application of Artificial Intelligence (AI) and Machine Learning (ML) algorithms to analyze intrusion patterns and differentiate between genuine threats and false alarms. This would significantly improve system intelligence and decision-making capabilities. Power optimization and migration to higher-capacity FPGA platforms or ASIC implementation can further enhance performance and energy efficiency.

With these advancements, the system can evolve into a comprehensive and intelligent border surveillance solution suitable for defense installations, restricted areas, and high-security environments, offering significant potential for real-world application and further research.

Appendices

Appendix A: **Supporting Materials and Project Documentation**

This appendix section provides supplementary information that supports the understanding, implementation, and verification of the FPGA-Based Intelligent Border Intrusion Detection and Tamper Monitoring System. The materials included in this section offer detailed insight into the system architecture, design methodology, and experimental validation that could not be fully presented in the main chapters.

The appendix includes the system block diagram, illustrating the interconnection between major modules such as zone detection logic, priority encoder, FSM controller, tamper detection unit, arm control logic, clock divider, and output display module. This diagram helps visualize data flow and control flow within the system. Additionally, the Finite State Machine (FSM) state diagram is included to clearly represent system states and state transitions based on zone activity and tamper conditions.

Simulation results obtained using the Xilinx Vivado Design Suite are also presented in this section. Selected simulation waveforms demonstrate correct behavior of the system under different scenarios such as single-zone intrusion, multi-zone intrusion, alert escalation and downgrade, tamper detection, and reset operation. These waveforms validate the functional correctness of the design prior to hardware implementation.

The appendix further includes FPGA implementation details, such as pin assignment information for the BASYS-3 FPGA board, mapping of switches to zone inputs and LEDs to system outputs, and brief descriptions of the testbench structure used for verification. Together, these materials provide comprehensive technical reference information and serve as supporting evidence for the successful completion of the project.

Appendix B: Top-Level Module Code

The following Verilog code represents the **Top-Level FPGA Integration Module**, responsible for connecting the clock divider and border intrusion detection core.

```
`timescale 1ns / 1ps

module top_border_intrusion_fpga (
    input  wire       clk,
    input  wire       rst,
    input  wire       arm,
    input  wire [3:0] zone,
    output wire       safe_led,
    output wire       alert_led,
    output wire       high_alert_led,
    output wire       tamper_led,
    output wire [3:0] zone_led
);
wire slow_clk;


clock_divider u_clk_div (
    .clk_in (clk),
    .rst    (rst),
    .clk_out(slow_clk)
);
```

```
border_intrusion_advanced u_core (
    .clk          (slow_clk),
    .rst          (rst),
    .arm          (arm),
    .zone         (zone),
    .safe_led     (safe_led),
    .alert_led    (alert_led),
    .high_alert_led (high_alert_led),
    .tamper_led   (tamper_led),
    .zone_led     (zone_led)
);

endmodule
```

Appendix C: GitHub Repository

The complete source code, including Verilog HDL modules, testbench files, and project documentation for the FPGA-Based Intelligent Border Intrusion Detection and Tamper Monitoring System, is available at the following

GitHub Repository Link: https://github.com/pravin2007-ctrl/border_intrusion_system

Appendix D: Basys-3 FPGA Board Reference Manual

The hardware implementation and pin configurations used in this project are based on the official Basys-3 FPGA Board Reference Manual provided by Digilent Inc. The document contains detailed information about the FPGA architecture, onboard peripherals, pin mappings, and electrical specifications.

Reference Manual:https://digilent.com/reference/programmable-logic/basys-3/reference-manual

Appendix E: List of Acronyms and Abbreviations

Acronym	Description
FPGA	Field Programmable Gate Array
FSM	Finite State Machine
HDL	Hardware Description Language
LED	Light Emitting Diode
VLSI	Very Large Scale Integration

REFERENCES

- National Institute of Electronics & Information Technology (NIELIT). Official Website and Training Materials. https://www.nielit.gov.in
- Xilinx Inc. Vivado Design Suite User Guide. https://www.xilinx.com/support/documentation-navigation/design-hubs/dh0002-vivado-design-hub.html
- Samir Palnitkar, Verilog HDL: A Guide to Digital Design and Synthesis, Pearson Education. https://archive.org/details/veriloghdlguidet00paln
- Morris Mano and Michael D. Ciletti, Digital Design, Pearson Education. https://studylib.net/doc/27837502/digital-design-with-an-introduction-to-the-verilog-hdl
- BASYS-3 FPGA Board Reference Manual, Digilent Inc. https://digilent.com/reference/programmable-logic/basys-3/reference-manual
- Online technical articles and tutorials related to FPGA design and FSM implementation. https://www.fpga4student.com
- IEEE journals and conference papers related to digital system design and hardware security concepts. https://ieeexplore.ieee.org

PROJECT TITLE	**FPGA-BASED BORDER INTRUSION DETECTION SYSTEM**	
PROGRAM	**NIELIT INTERNSHIP PROGRAM**	
PROJECT BATCH NUMBER	**2**	
BATCH MEMBERS	**KARTHIBAN S T**	**722824106067**
	PRAVIN A	**722824106121**
NAME OF THE SUPERVISOR	**NANDITHA N VARMA**	
NAME OF THE SDG GOALS MAPPED	• **Peace, Justice and Strong Institutions** • **Industry, Innovation and Infrastructure**	
MENTION THE SDG GOALS NUMBER	• **SDG 9 – Industry, Innovation and Infrastructure** • **SDG 16 – Peace, Justice and Strong Institutions**	
NAME OF THE TRL LEVEL	**Technology Demonstration**	
MENTION THE TRL LEVEL	**TRL – 5** *(Technology validated in a relevant environment through FPGA implementation and testing)*	

Program Outcomes											**Program Specific Outcomes**		
PO1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PSO 1**	**PSO 2**	**PSO 3**
✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Signature of the Mentor

VENUE AND EXPENDITURE STATEMENT FOR THE PROJECT WORK

Laboratory details where the project is carried out	**NIELIT**
Software / Hardware details	**XILINX VIVADO SOFTWARE (2025.2), BASYS-3 FPGA**

Signature of the student

(PRAVIN A)

Signature of the Mentor

(NANDITHA N VARMA)