SPIT SHIELD - Advanced Cyber Security Lab

Government Research Proposal

Dr. D. D. Ambawade, Department of E&TC, SPIT Mumbai

October 2025

Contents

1 PROJECT SHIELD

SHIELD

Securing Hardware & Infrastructure through Education, Labs & Defense

SPIT SHIELD

Securing Hardware & Infrastructure through

Education, Labs & Defense

Advanced Cyber Security Research & Training Laboratory

Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology
Department of Electronics & Telecommunication Engineering

Total Budget: 4,00,00,000 (Four Crores)

Duration: 36 Months (Mid-2026 to Mid-2029)

2 Executive Summary

2.1 Project Overview

Project Name: SPIT SHIELD (Securing Hardware & Infrastructure through Education, Labs & Defense)

Institution: Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology (SPIT)

Department: Electronics & Telecommunication Engineering

Principal Investigator: Dr. D. D. Ambawade (IT Incharge & Associate Professor)

Total Budget: 4,00,00,000 (Four Crores)

Duration: 36 Months (June 2026 - May 2029)

Proposal Type: Government Research Funding Initiative

2.2 Vision Statement

To establish a **world-class, enterprise-grade Cyber Security Research and Training Laboratory** that serves as a hub for cutting-edge research, industry collaboration, and development of next-generation cybersecurity professionals capable of addressing emerging threats in Industry 4.0 and beyond.

2.3 Mission Objectives

1. **Education Excellence**: Train 500+ students annually in advanced cybersecurity domains
2. **Research Innovation**: Conduct cutting-edge research in IoT security, AI-based threat detection, and cyber-physical systems
3. **Industry Collaboration**: Partner with leading cybersecurity firms and government agencies
4. **Centre of Excellence**: Establish SPIT as a recognized cybersecurity research hub in Western India
5. **National Security**: Contribute to India's cybersecurity preparedness and digital sovereignty

2.4 Budget Summary

Category	**Allocation ( )**	**Percentage**
Infrastructure & Hardware	1,85,00,000	46.25%
Personnel (36 months)	1,08,00,000	27.00%
Software & Licensing	45,00,000	11.25%
Office & Facilities	25,00,000	6.25%
Training & Certifications	15,00,000	3.75%
Contingency & Misc.	22,00,000	5.50%
TOTAL	**4,00,00,000**	**100%**

2.5 Key Deliverables

2.5.1 Research Infrastructure

- 60+ High-performance Cyber Security Workstations
- 15+ Vulnerable Physical Systems for Penetration Testing
- Enterprise-grade Network Security Lab with IDS/IPS
- Cyber-Physical Systems (CPS) Testbed
- Industrial Control Systems (ICS) Security Lab
- IoT Security Research Platform
- AI/ML Threat Detection Infrastructure with GPU Clusters
- Digital Forensics Laboratory
- Malware Analysis & Reverse Engineering Lab
- Blockchain & Cryptocurrency Security Testbed

2.5.2 Educational Outcomes

- 20+ Specialized Course Modules
- 500+ Students trained annually
- Industry-recognized Certifications
- 50+ Research Publications (3 years)
- 100% Placement in Cybersecurity Roles

2.5.3 Research Contributions

- 10+ Government/Industry Funded Projects
- 3+ Patent Applications
- National/International Collaborations
- Open-source Security Tools Development

2.6 Strategic Importance

2.6.1 National Priority Alignment

- Supports **Digital India Initiative**
- Contributes to **National Cyber Security Policy 2023**
- Aligns with **NEP 2020** skill development goals
- Strengthens **Atmanirbhar Bharat** in cybersecurity

2.6.2 Industry Relevance

- Addresses critical skills gap (3.5M cybersecurity jobs unfilled globally)
- Industry 4.0 security requirements
- Critical infrastructure protection
- 5G/6G security research

2.6.3 Academic Excellence

- First comprehensive lab in Mumbai region
- NAAC/NBA accreditation enhancement
- International ranking improvement

- Academic-Industry partnership model

2.7 Expected Outcomes (3 Years)

2.7.1 Quantitative Targets

- **1,500+ Students** Trained
- **50+ Research Papers** Published
- **100+ Industry Collaborations**
- **500+ Professional Certifications**
- **2 Cr+ External Research Grants**

2.7.2 Qualitative Outcomes

- Establish SPIT as premier cybersecurity education hub
- Contribute to national security research
- Develop indigenous security solutions
- Create a sustainable innovation ecosystem

3 Introduction and Background

3.1 Global Cybersecurity Landscape

The digital transformation of industries, governments, and societies has created an unprecedented demand for robust cybersecurity infrastructure and skilled professionals.

3.1.1 Key Statistics

Metric	**Value**	**Source**
Global Cybersecurity Market	$173.5 Billion (2022)	Gartner
Projected Market (2028)	$266.2 Billion	Markets & Markets
Unfilled Cybersecurity Jobs	3.5 Million Globally	(ISC)^2
India Cybersecurity Jobs Gap	500,000+ Positions	NASSCOM
Average Cost of Data Breach	17.9 Crores	IBM Security Report
Cyber Attacks Growth (YoY)	38% Increase	Check Point Research

3.2 India's Cybersecurity Imperative

3.2.1 National Priority Areas

1. **Government Initiatives**
   - National Cyber Security Policy 2023
   - Digital India Mission
   - Smart Cities Project
   - UPI & Financial Digitization
2. **Industry 4.0 Security**
   - Industrial IoT (IIoT) vulnerabilities
   - Smart Manufacturing security
   - Supply chain protection
   - OT/IT convergence challenges
3. **Critical Infrastructure Protection**
   - Power sector (smart grids)
   - Transportation systems
   - Healthcare digitization
   - Banking & Finance
4. **Education & Skills Development**
   - NEP 2020 skill development goals
   - Industry-academia gap
   - Practical hands-on training deficit
   - Research & innovation ecosystem

3.3 Need Analysis

3.3.1 Current State of Cybersecurity Education in India

3.3.1.1 Challenges Identified

1. **Limited Practical Infrastructure**

   - Most institutions have only basic computer labs
   - Lack of specialized security equipment
   - No cyber-physical systems testbeds
   - Insufficient vulnerable systems for ethical hacking
2. **Theoretical Focus**
   - 80% theory vs 20% practical (industry needs reverse)
   - Limited exposure to real-world attack scenarios
   - Outdated curriculum not aligned with current threats
   - No hands-on experience with enterprise tools
3. **Resource Constraints**
   - High cost of commercial security tools
   - Lack of licensed software and platforms
   - Insufficient faculty training
   - No dedicated cybersecurity labs
4. **Industry Disconnect**
   - Graduates not job-ready
   - Lack of industry-standard certifications
   - No exposure to production environments
   - Limited internship opportunities

3.4 About SPIT

3.4.1 Institutional Profile

Bharatiya Vidya Bhavan’s Sardar Patel Institute of Technology

- **Established**: 1962
- **Type**: Autonomous Institute affiliated to University of Mumbai
- **Accreditation**: NBA Accredited Programs, NAAC ‘A’ Grade, Autonomous Status since 2020
- **Location**: Andheri (West), Mumbai - 400058

3.4.2 Key Achievements

- 60+ years of engineering education excellence
- 10,000+ successful alumni in industry
- Strong industry connections (TCS, Infosys, Accenture, Cisco, etc.)
- Active research culture with 200+ publications annually
- Modern infrastructure and facilities

4 Infrastructure Specifications

4.1 Lab Layout and Design

4.1.1 Physical Space Requirements

Total Area Required: 3,500 sq. ft. (325 sq. meters)

4.1.2 Lab-wise Distribution

Lab Name	Area (sq.ft)	Capacity	Primary Focus
Network Security Lab	500	20 students	Firewall, IDS/IPS, Network Analysis
Penetration Testing Lab	500	15 students	Ethical Hacking, Vulnerability Assessment
Digital Forensics Lab	400	12 students	Incident Response, Evidence Analysis
AI/ML Security Lab	400	15 students	Threat Detection, Adversarial ML
IoT Security Lab	350	12 students	Device Security, Firmware Analysis
CPS/ICS Security Lab	450	10 students	SCADA, Industrial Systems
Server Room & SOC	600	8 analysts	Infrastructure, Monitoring
Malware Analysis Lab	300	8 students	Reverse Engineering, Sandboxing
Conference Room	250	30 people	Meetings, Presentations
Office Space	200	6 staff	Administrative, Faculty
Storage & Utility	150	-	Equipment, Maintenance

4.2 Workstation Specifications

4.2.1 Category A: High-Performance Security Workstations (15 Units)

Purpose: Malware analysis, reverse engineering, AI/ML training, penetration testing

Component	Specification	Unit Cost ( )
Processor	Intel Core i7-13700K / AMD Ryzen 7 7700X	32,000
RAM	32GB DDR5	15,000
GPU	NVIDIA RTX 4060 8GB	35,000
Storage (Primary)	2TB NVMe SSD	18,000
Storage (Secondary)	2TB SATA SSD	12,000
Monitor	27” QHD IPS	25,000
OS	Windows 11 Pro + Ubuntu Linux	18,000
UPS	1KVA UPS	8,000
Peripherals	Keyboard + Mouse	4,000
Assembly	-	3,000

Component	Specification	Unit Cost ( )
TOTAL PER UNIT		**2,00,000**
Total for 15 Units		**30,00,000**

4.2.2 Category B: Standard Security Workstations (25 Units)

Component	Specification	Unit Cost ( )
Processor	Intel Core i5-13400 / AMD Ryzen 5 5600	18,000
RAM	16GB DDR4	6,000
GPU	GTX 1650 4GB	15,000
Storage	1TB SSD	10,000
Monitor	24” Full HD	12,000
OS	Windows 11 Pro	18,000
UPS	600VA UPS	5,000
Peripherals	Keyboard + Mouse	3,000
Assembly	-	3,000
TOTAL PER UNIT		**1,20,000**
Total for 25 Units		**30,00,000**

4.2.3 Category C: Basic Lab Workstations (20 Units)

Component	Specification	Unit Cost ( )
Processor	Intel Core i3-13100	12,000
RAM	16GB DDR4	6,000
Storage	512GB SSD	5,000
Monitor	22” Full HD	10,000
OS	Windows 11 Pro	18,000
Peripherals & UPS	Complete set	9,000
TOTAL PER UNIT		**60,000**
Total for 20 Units		**12,00,000**

4.3 Network Infrastructure

Item	Specification	Qty	Cost ( )
Enterprise Firewall	FortiGate 100F / Sophos XG 230	2	8,00,000
Managed Core Switch	48-port Gigabit L3 with 10G uplinks	2	6,00,000
Access Switches	24-port Gigabit managed	6	3,00,000
Wireless System	Controller + 8 APs (WiFi 6)	1 set	5,00,000
IDS/IPS	Open-source on dedicated hardware	2	4,00,000

Item	Specification	Qty	Cost ( )
Network Monitoring	Packet capture & analysis tools	2	3,00,000
Cabling & Infrastructure	Cat6A cabling, patch panels, racks	1 set	6,00,000
TOTAL			**35,00,000**

4.4 Server Infrastructure

Item	Specification	Qty	Cost ( )
Hypervisor Servers	Dell R650 (Xeon Silver, 256GB RAM)	3	18,00,000
Storage Server	48TB usable RAID10	1	6,00,000
Backup Solution	NAS with 24TB capacity	1	2,50,000
Server Racks	42U racks with PDUs	2	2,50,000
KVM & Management	IP KVM switches	1	1,00,000
TOTAL			**30,00,000**

4.5 Specialized Equipment

4.5.1 GPU Cluster for AI/ML (15,00,000)

Item	Specification	Qty	Cost ( )
GPU Workstations	2x RTX 4090 per system	2	10,00,000
Storage for ML	20TB NVMe SSD array	1	3,00,000
Networking	10GbE switches for cluster	1	2,00,000

4.5.2 Cyber-Physical Systems Lab (10,00,000)

Item	Specification	Qty	Cost ( )
PLC Training Kits	Siemens/Allen-Bradley starter kits	4	4,00,000
SCADA Software	Academic licenses	2	2,00,000
HMI Panels	10” industrial touchscreens	4	2,00,000
Simulation Software	Factory I/O, MATLAB Simulink	-	2,00,000

4.5.3 Digital Forensics Lab (8,00,000)

Item	Specification	Qty	Cost ( )
Forensic Workstations	High-spec with write blockers	3	4,50,000

Item	Specification	Qty	Cost ( )
Write Blockers	USB/SATA write blockers	6	1,50,000
Mobile Forensics	Mid-tier extraction tools	1	1,50,000
Evidence Storage	Secure cabinets and bags	-	50,000

4.5.4 IoT Security Lab (5,00,000)

Item	Specification	Qty	Cost ( )
Dev Boards	Raspberry Pi, Arduino, ESP32	50	1,50,000
IoT Devices	Smart devices for testing	25	1,50,000
Analysis Tools	Logic analyzers, oscilloscopes	4	1,50,000
Wireless Tools	SDR dongles, WiFi adapters	10	50,000

5 Budget Breakdown

5.1 Overall Budget Allocation (4,00,00,000)

5.1.1 Detailed Hardware Breakdown (1,85,00,000)

Category	Budget ( )	Percentage
Workstations (60 units)	75,00,000	40.5%
Network Infrastructure	35,00,000	18.9%
Server Infrastructure	30,00,000	16.2%
GPU Cluster for AI/ML	15,00,000	8.1%
CPS Lab Equipment	10,00,000	5.4%
Digital Forensics	8,00,000	4.3%
IoT Lab Equipment	5,00,000	2.7%
Vulnerable Machines	3,00,000	1.6%
Displays & Monitors	4,00,000	2.2%
TOTAL	**1,85,00,000**	**100%**

5.2 Software & Licensing Budget (45,00,000)

Category	Software/Platform	Cost (3 years)
Operating Systems	Windows, Linux, Server licenses	18,80,000
Security Tools	Burp Suite Pro, Metasploit Pro, Nessus	18,75,000
Forensics	EnCase, X-Ways, Autopsy	20,00,000
Malware Analysis	IDA Pro, Ghidra (open-source)	12,50,000
SIEM & SOC	Splunk, ELK Stack	9,00,000
Virtualization	VMware vSphere, Proxmox	6,00,000
Cloud Platforms	AWS/Azure Education Credits	5,00,000
Training Platforms	Hack The Box, TryHackMe	6,75,000
Development	GitHub, JetBrains	5,70,000
AI/ML Tools	NVIDIA AI Enterprise	6,00,000
Contingency	Updates, new tools	5,00,000
TOTAL		**1,13,50,000**
Optimized (Academic Pricing)		**45,00,000**

Note: 60-70% academic discounts applied. Open-source alternatives prioritized.

5.3 Personnel Budget (1,08,00,000 for 36 months)

Position	Qty	Monthly ( )	36 Months ( )
Lab Director (50% allocation)	1	75,000	27,00,000
Sr. Research Associate 1	1	80,000	28,80,000
Sr. Research Associate 2 (30M)	1	80,000	24,00,000

Position	Qty	Monthly ( )	36 Months ( )
System Administrator	1	60,000	21,60,000
Lab Technician 1	1	40,000	14,40,000
Lab Technician 2 (24M)	1	40,000	9,60,000
Administrative Assistant	1	35,000	12,60,000
TOTAL	**7**		**1,38,00,000**
Optimized			**1,08,00,000**

5.4 Office & Facilities Budget (25,00,000)

Category	Item/Work	Cost ( )
Civil Work	False ceiling, electrical, flooring	20,00,000
HVAC	Precision AC, Split ACs	7,00,000
Power Backup	Generator, UPS Systems	14,00,000
Safety	Fire suppression, extinguishers	3,60,000
Access Control	Biometric, CCTV	4,40,000
Furniture	Desks, chairs, cabinets	15,00,000
Signage	Lab signage and branding	1,00,000
TOTAL		**65,00,000**
Optimized		**25,00,000**

5.5 Training & Certification Budget (15,00,000)

Purpose	Details	Cost ( )
Faculty Training	CEH, OSCP, CISSP for 5 faculty	5,00,000
Industry Workshops	Guest lectures, workshops	3,00,000
Conference Attendance	International & national	4,00,000
Student Certifications	Subsidized for top performers	2,00,000
Online Learning	Coursera, Udemy subscriptions	1,00,000
TOTAL		**15,00,000**

5.6 Contingency & Miscellaneous (22,00,000)

Category	Purpose	Allocation ( )
Equipment Repair	Annual maintenance	5,00,000
Software Updates	Annual renewals	4,00,000
Consumables	Cables, peripherals	2,00,000
Travel	Industry visits	3,00,000
Publications	Paper fees	2,00,000
Marketing	Promotional materials	1,00,000
Utilities	Electricity, internet	3,00,000
Contingency Buffer	Unforeseen expenses	2,00,000
TOTAL		**22,00,000**

Category	Purpose	Allocation ( )

6 Personnel Requirements

6.1 Organizational Structure

6.1.1 Team Composition

Total Team: 7 core members + 4-6 student assistants

1. **Lab Director** (50% allocation) - Dr. D. D. Ambawade
2. **Senior Research Associate 1** - Network Security & Penetration Testing
3. **Senior Research Associate 2** - AI/ML & IoT Security
4. **System Administrator** - Infrastructure Management
5. **Lab Technician 1** - Network & Pentesting Labs
6. **Lab Technician 2** - AI/ML & IoT Labs
7. **Administrative Assistant** - Operations Support

6.2 Detailed Role Descriptions

6.2.1 1. Lab Director (27,00,000 / 36 months)

Role: Overall lab management, research leadership

Qualifications: Ph.D. in Cybersecurity/related field, 10+ years experience

Key Responsibilities: - Strategic planning and vision - Research project oversight - Industry liaison and fundraising - Faculty coordination - Publication and IP management

KPIs: - 5+ research publications per year - 50L+ external funding secured annually - 3+ industry partnerships established - 100+ students trained per year

6.2.2 2. Senior Research Associate 1 (28,80,000)

Role: Network Security & Penetration Testing specialist

Primary Areas: Network Security Lab, Penetration Testing Lab

Responsibilities: - Conduct research in network security - Publish papers in reputed journals - Guide M.Tech/B.Tech projects - Configure firewalls, IDS/IPS - Develop lab exercises - Lead industry-sponsored projects

Expected Deliverables (Per Year): - 3+ research papers - 2+ specialized courses - 2+ industry projects - CTF team coaching

6.2.3 3. Senior Research Associate 2 (24,00,000)

Role: AI/ML Security & IoT Security specialist

Primary Areas: AI/ML Security Lab, IoT Security Lab, CPS Lab

Responsibilities: - AI/ML security research - IoT vulnerability analysis - GPU cluster management - IoT testbed setup - Security tool development - ML model hardening

Expected Deliverables (Per Year): - 3+ research papers - 2+ funded research projects - 1+ open-source security tool - 2+ conference presentations

6.2.4 4. System Administrator (21,60,000)

Role: IT infrastructure management

Responsibilities: - Server management (physical & virtual) - Security patching and updates - Backup and disaster recovery - User account management - Performance monitoring - Network infrastructure support

Tools Proficiency Required: - Linux (RHEL/Ubuntu/CentOS) - Windows Server 2019/2022 - VMware vSphere / Proxmox - Ansible / Puppet - Nagios / Zabbix

6.2.5 5. Lab Technicians (14,40,000 + 9,60,000)

Technician 1 - Network & Pentesting Focus **Technician 2** - AI/ML & IoT Focus

Responsibilities: - Daily lab setup and maintenance - Student assistance during sessions - Equipment troubleshooting - Inventory management - Lab manual creation - Safety protocol enforcement

6.2.6 6. Administrative Assistant (12,60,000)

Role: Administrative and coordination support

Responsibilities: - Meeting scheduling and coordination - Documentation and reporting - Visitor management - Procurement support - Event organization

7 Implementation Timeline

7.1 36-Month Master Timeline

7.1.1 Phase 1: Planning and Preparation (Months 1-4)

June-September 2026

- Project kickoff meeting and charter
- Detailed lab design (floor plan, 3D models)
- Equipment specifications finalization
- Software requirements gathering
- Budget allocation and approval
- Tender document preparation
- Vendor presentations & evaluation
- Vendor selection & PO issuance

Key Deliverables: - Detailed Project Report (DPR) - Lab Design (Architecture + Layout) - Equipment Specifications - Vendor Selection Complete - Contracts Signed

7.1.2 Phase 2: Infrastructure Development (Months 3-9)

August 2026 - February 2027

- Civil Work (false ceiling, flooring, partitions)
- Electrical work (wiring, panels, lighting)
- HVAC installation (ACs, ventilation)
- Power backup (Generator, UPS)
- Fire safety systems
- Access control & CCTV
- Network cabling (Cat6A, fiber)
- Furniture installation
- Server rack setup
- Final inspections & safety clearance

Milestone: Infrastructure 100% complete by February 2027

7.1.3 Phase 3: Equipment Procurement & Installation (Months 5-12)

October 2026 - May 2027

Batch 1: October-December 2026 (1,00,00,000) - 30 workstations (Tier 1 & 2) - 3 hypervisor servers, 1 storage server - Firewalls, switches, APs - 60 monitors, peripherals

Batch 2: January-March 2027 (50,00,000) - 30 workstations (Tier 2 & 3) - Forensics, IoT, CPS equipment - 2 GPU workstations

Batch 3: Year 2 (25,00,000) - Vulnerable machines - Additional IoT devices - Expansion hardware

Milestone: 80% equipment operational by March 2027

7.1.4 Phase 4: Software Licensing & Configuration (Months 6-12)

November 2026 - May 2027

- Operating Systems deployment
- VMware vSphere setup
- Security Tools (Burp Suite, Metasploit, Nessus)
- Forensics Tools (EnCase, X-Ways)
- SIEM & Monitoring (Splunk, ELK Stack)
- Development Tools (GitHub, JetBrains)
- Training Platforms (HTB, TryHackMe)
- Cloud Platforms (AWS/Azure accounts)

Milestone: All software licensed and configured by May 2027

7.1.5 Phase 5: Personnel Recruitment & Training (Months 1-36)

June 2026 - May 2029

Recruitment Timeline: - Job postings: June 2026 - Screening & Interviews: July-August 2026 - Offer & Onboarding: September 2026

Training Schedule: - Q4 2026: Infrastructure familiarization - Q1 2027: Tool-specific training - Q2 2027: Certifications (CEH, OSCP) - Q3 2027+: Advanced topics, continuous learning

7.1.6 Phase 6: Pilot & Launch (Months 10-15)

March-August 2027

Month 10-11: Pilot Testing - Internal testing with faculty (5 members) - Student pilot batch (20 volunteers) - Feedback collection & fixes - External expert review

Success Criteria: - All labs functional - 90%+ user satisfaction - No critical issues

Month 12-13: Soft Launch - Limited student batches (50-100) - Selected courses only - Intensive monitoring

Month 14-15: Full Launch - Open to all eligible students - Full course catalog - Industry events - Press release

Milestone: Full operations by August 2027

7.1.7 Phase 7: Operations & Research (Months 14-36)

August 2027 - May 2029

Research Activities: - Research proposal development - Ethics approval - Active research projects - Conference paper submissions - Journal article submissions - Patent applications - Grant applications - Industry projects

Industry Collaboration: - Q3 2027: MoU signing (3-5 companies) - Q4 2027: First industry project - Q1 2028: Internship placements (20+ students) - Q2 2028+: Joint research projects

7.2 Key Milestones

7.2.1 Year 1 Milestones (2026-2027)

Month	Milestone	Success Criteria
M2	DPR Approved	Budget & specs finalized
M4	Vendors Selected	Contracts signed
M6	Civil Work 50%	Infrastructure progressing
M9	Infrastructure Complete	Safety clearance obtained
M10	Equipment 50% Installed	Core labs functional
M12	Pilot Launch	20+ users trained

7.2.2 Year 2 Milestones (2027-2028)

Month	Milestone	Success Criteria
M14	Full Operations	100+ active users
M18	First Research Output	3+ papers submitted
M20	Industry Partnership	2+ active collaborations
M24	Capacity at 80%	300+ students trained

7.2.3 Year 3 Milestones (2028-2029)

Month	Milestone	Success Criteria
M30	25+ Publications	Journal/conference papers
M33	External Funding	50L+ grants secured
M36	Centre of Excellence	National recognition

8 Research Objectives

8.1 Research Focus Areas

8.1.1 1. AI/ML Security Research

Primary Objectives: - Develop robust defenses against adversarial ML attacks - Create frameworks for secure AI model deployment - Design AI-powered intrusion detection systems - Investigate privacy-preserving ML techniques

Proposed Projects: - Adversarial ML Defense Framework (18 months, 15L) - AI-based Network Intrusion Detection (24 months, 20L) - Privacy-Preserving Federated Learning (18 months, 12L) - Explainable AI for Security Analytics (12 months, 8L)

Expected Deliverables: - 10+ research papers in top-tier conferences - 2+ open-source AI security tools - 1+ patent application - 3+ Ph.D. theses

8.1.2 2. IoT and Embedded Systems Security

Primary Objectives: - Identify and mitigate vulnerabilities in IoT firmware - Develop secure-by-design IoT architectures - Create automated firmware analysis tools - Investigate hardware-level security mechanisms

Proposed Projects: - Automated IoT Firmware Analysis Platform (24 months, 18L) - Secure Smart Home Architecture (18 months, 12L) - Hardware Root of Trust for IoT (24 months, 20L) - IoT Botnet Detection & Mitigation (18 months, 10L)

Expected Deliverables: - 8+ research papers - Automated firmware analysis tool - Secure IoT reference architecture - 2+ patent applications

8.1.3 3. Cyber-Physical Systems (CPS) and ICS Security

Primary Objectives: - Analyze security vulnerabilities in industrial control systems - Develop intrusion detection for SCADA environments - Create testbeds for smart grid security research - Investigate resilience mechanisms

Proposed Projects: - ICS Intrusion Detection System (24 months, 25L) - Smart Grid Security Testbed (36 months, 35L) - Secure Industrial Protocol Gateway (18 months, 15L) - OT Network Security Framework (12 months, 8L)

Expected Deliverables: - 10+ research papers - Fully functional ICS security testbed - ICS-IDS system (commercializable) - 3+ industry collaborations

8.1.4 4. Network Security and Next-Gen Technologies

Primary Objectives: - Investigate security challenges in 5G/6G networks - Develop zero-trust network architectures - Create advanced APT detection mechanisms - Research SDN/NFV security

Proposed Projects: - 5G Security Framework (24 months, 20L) - Zero-Trust Implementation Guide (12 months, 8L) - APT Detection using Graph Analytics (18 months, 12L) - SDN Security Orchestration (18 months, 10L)

8.1.5 5. Blockchain and Cryptocurrency Security

Primary Objectives: - Audit and analyze smart contract vulnerabilities - Investigate DeFi security challenges - Develop cryptocurrency forensics techniques - Research consensus mechanism security

Proposed Projects: - Automated Smart Contract Auditor (18 months, 15L) - DeFi Security Analysis Framework (18 months, 12L) - Cryptocurrency Forensics Tool (24 months, 18L) - Blockchain Consensus Security (12 months, 8L)

8.1.6 6. Cloud and Container Security

Proposed Projects: - Container Security Scanner (12 months, 10L) - Multi-Cloud Security Framework (18 months, 15L) - Serverless Security Analysis (12 months, 8L) - DevSecOps Automation Pipeline (18 months, 12L)

8.1.7 7. Digital Forensics and Incident Response

Proposed Projects: - Advanced Mobile Forensics Framework (18 months, 15L) - Cloud Forensics Toolkit (24 months, 20L) - Memory Forensics for Malware Analysis (12 months, 8L) - Anti-Forensics Detection Techniques (12 months, 6L)

8.2 Research Output Targets (3 Years)

8.2.1 Publication Targets

Target Venues:

Top-Tier Conferences (Tier 1): - USENIX Security Symposium - IEEE S&P (Oakland) - ACM CCS - NDSS - CRYPTO/EUROCRYPT

Quality Conferences (Tier 2): - ACSAC, AsiaCCS, RAID, ESORICS - IoTDI, IoT S&P - ICICS, DIMVA

Journals: - IEEE TIFS, IEEE TDSC - ACM TOPS - Computers & Security - Journal of Cybersecurity

8.2.2 Patents and IP

Year	Patent Applications	Open-Source Tools	Industry Transfers
Year 1	1	2	0
Year 2	2	3	1
Year 3	2	2	2
Total	**5**	**7**	**3**

8.3 Research Funding Strategy

8.3.1 External Funding Targets

Funding Source	Year 1	Year 2	Year 3	Total
DST/DBT/SERB	10L	20L	30L	60L
AICTE/UGC	5L	10L	10L	25L
Industry Sponsored	5L	15L	30L	50L
International Grants	-	10L	15L	25L
TOTAL	**20L**	**55L**	**85L**	**1.6 Cr**

8.4 Industry and Academic Collaborations

8.4.1 Target Industry Partners

- **Product Vendors**: Cisco, Palo Alto, Fortinet, Check Point
- **Service Providers**: TCS, Wipro, Infosys, Accenture
- **Cybersecurity Startups**: Sequretek, Lucideus, CloudSEK
- **Cloud Providers**: AWS, Azure, GCP
- **Financial Sector**: Banks, FinTech companies

8.4.2 Academic Collaborations

- IIT Bombay - AI/ML Security
- IIIT Hyderabad - Network Security
- C-DAC - CPS Security
- International Universities - Joint publications

9 Expected Impact and Benefits

9.1 Quantitative Impact (3 Years)

- **1,500+ Students** trained in advanced cybersecurity
- **50+ Research Papers** published in top-tier venues
- **100+ Industry Collaborations** established
- **500+ Professional Certifications** awarded
- **2 Cr+ External Research Grants** secured
- **3+ Patents** filed
- **7+ Open-source Tools** developed

9.2 Qualitative Impact

9.2.1 For Students

- Hands-on experience with enterprise-grade tools
- Industry-recognized certifications
- Enhanced employability (100% placement target)
- Research opportunities (M.Tech/Ph.D.)
- Exposure to real-world security challenges

9.2.2 For Faculty

- Access to cutting-edge research infrastructure
- Opportunities for publications and patents
- Industry collaboration and consultancy
- Professional development and certifications
- National/international recognition

9.2.3 For Institution (SPIT)

- First comprehensive cybersecurity lab in region
- Enhanced NAAC/NBA ratings
- Improved national/international rankings
- Increased research funding
- Stronger industry partnerships
- Alumni network strengthening

9.2.4 For Industry

- Access to skilled cybersecurity professionals
- Collaborative research opportunities
- Technology transfer and innovation
- Internship and recruitment pipeline
- Joint projects and consultancy

9.2.5 For Nation

- Contribution to Digital India Mission
- Support for National Cyber Security Policy

- Strengthening critical infrastructure security
- Development of indigenous security solutions
- Reduction in cybersecurity skills gap
- Enhanced national cyber defense capabilities

9.3 Sustainability Plan

9.3.1 Revenue Generation (Post Year 3)

1. **Training Programs** (50L/year)
   - Industry certifications
   - Executive education
   - Workshop and seminars
2. **Consultancy Services** (30L/year)
   - Security audits
   - Penetration testing
   - VAPT services
3. **Research Projects** (1 Cr/year)
   - Industry-sponsored projects
   - Government grants
   - International collaborations
4. **Tool Licensing** (20L/year)
   - Commercial licensing of developed tools
   - Technology transfer

Total Projected Revenue: 2 Cr+/year (post year 3)

10 Risk Management

10.1 Potential Risks and Mitigation

Risk	Probability	Impact	Mitigation Strategy
Vendor Delays	High	Medium	Multiple vendor options, penalty clauses in contracts
Budget Overruns	Medium	High	10% contingency fund, phased procurement approach
Personnel Attrition	Low	Medium	Competitive salaries, growth opportunities, retention bonuses
Equipment Failure	Medium	Low	Extended warranty, AMC contracts, spare parts inventory
Software Licensing Issues	Low	Medium	Perpetual licenses where possible, open-source alternatives
Low Student Enrollment	Low	High	Strong marketing, industry partnerships, quality assurance
Research Output Below Target	Medium	Medium	Regular monitoring, external collaborations, incentives
External Funding Gap	Medium	High	Diverse funding sources, early grant applications, industry projects

10.2 Quality Assurance

10.2.1 Lab Operations

- Standard Operating Procedures (SOPs)
- Regular equipment maintenance
- Software updates and patch management
- Security audits
- User feedback mechanisms

10.2.2 Education Programs

- Curriculum aligned with industry standards
- Regular course reviews and updates
- Student feedback and assessment
- Industry advisory board input
- Guest lectures from experts

10.2.3 Research Activities

- Ethics committee oversight

- Peer review process
- Regular progress reviews
- Collaboration with leading institutions
- Quality publication targets

11 Conclusion

11.1 Summary

The **SPIT SHIELD (Securing Hardware & Infrastructure through Education, Labs & Defense)** project represents a strategic investment in India's cybersecurity infrastructure and human capital development. With a comprehensive budget of 4 Crores over 36 months, this initiative will:

1. **Establish a world-class cybersecurity research and training laboratory** with 10 specialized labs covering all aspects of modern cybersecurity
2. **Train 1,500+ students** in advanced cybersecurity domains with hands-on experience using enterprise-grade tools and technologies
3. **Produce 50+ high-quality research publications** in top-tier conferences and journals, contributing to the global body of cybersecurity knowledge
4. **Secure 2 Cr+ in external research funding** through government grants, industry partnerships, and international collaborations
5. **File 3+ patents** and develop 7+ open-source security tools, creating tangible intellectual property and community contributions
6. **Establish 100+ industry partnerships**, creating a sustainable ecosystem for research, training, and technology transfer
7. **Position SPIT as a Centre of Excellence** in cybersecurity education and research, recognized nationally and internationally

11.2 Strategic Value

This project aligns perfectly with: - **National priorities**: Digital India, National Cyber Security Policy 2023, NEP 2020 - **Industry needs**: Addressing the critical cybersecurity skills gap - **Academic excellence**: Enhancing SPIT's research profile and rankings - **Societal benefit**: Contributing to India's digital security and sovereignty

11.3 Call to Action

We respectfully request the funding agency to approve this proposal and support SPIT in establishing this critical infrastructure for cybersecurity education and research. The SHIELD project will serve as a model for other institutions and contribute significantly to India's cybersecurity ecosystem.

11.4 Contact Information

Principal Investigator
Dr. D. D. Ambawade
Associate Professor & IT Incharge
Department of Electronics & Telecommunication
SPIT, Andheri (West), Mumbai - 400058

Institution
Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Website: https://www.spit.ac.in

SPIT SHIELD

Securing Tomorrow's Digital Infrastructure

"Building the next generation of cybersecurity professionals and contributing to India's digital sovereignty"

Proposal Version: 1.0
Date: October 2025
Classification: For Official Use
Status: Submitted for Approval