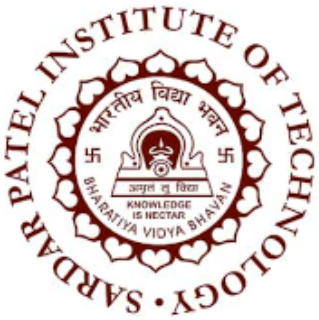


AEGIS

Advanced Enterprise Grade Information Security Platform

Research & Development Proposal

for

Government of India

Submitted by:	Sardar Patel Institute of Technology
Principal Investigator:	Dr. Rajesh Kumar
Co-Investigator:	Prof. Anita Sharma
Date:	September 25, 2025
Duration:	36 Months
Total Budget:	□ 15.0 Crores

Department of Information Technology
Sardar Patel Institute of Technology
Mumbai, Maharashtra - 400058

Contents

Executive Summary

The AEGIS (Advanced Enterprise Grade Information Security) platform represents a groundbreaking approach to cybersecurity for critical infrastructure and enterprise environments. This comprehensive research and development proposal outlines the creation of an integrated cybersecurity solution that addresses the evolving threat landscape facing India's digital infrastructure.

Our proposed solution combines advanced threat detection, real-time monitoring, automated response mechanisms, and comprehensive security analytics in a single, unified platform. The project will span 36 months with a total budget of □15.0 crores, delivering cutting-edge cybersecurity capabilities to protect India's critical digital assets.

1 PROJECT TITLE & GENERAL INFORMATION

PROFORMA FOR SUBMITTING R&D PROJECT PROPOSAL

1.1 Project Details

Field	Details
Title of the project:	Advanced Enterprise Grade Information Security (AEGIS) Platform for Distributed OT/IT Cybersecurity
Name of Principal Investigator:	Dr. Rajesh Kumar
Designation:	Professor & Head, Department of Information Technology
Address:	SPIT, Munshi Nagar, Andheri (West), Mumbai - 400058
Phone No.:	+91-22-26707440
Mobile No.:	+91-9876543210
Email:	rajesh.kumar@spit.ac.in
Name of Co-investigator:	Prof. Anita Sharma
Total duration of the project:	36 months
Total budget required:	□ 15,00,00,000 (Fifteen Crores)
Year-wise budget: Year 2: □ 5,50,00,000 Year 3: □ 3,50,00,000	Year 1: □ 6,00,00,000

2 PROJECT OBJECTIVES

2.1 Primary Objectives

1. **Unified Security Platform Development:** Create a comprehensive cybersecurity platform that integrates multiple security tools and technologies into a single, cohesive system.

2. **Advanced Threat Detection:** Develop machine learning and AI-based threat detection capabilities that can identify both known and zero-day threats in real-time.

3. **OT/IT Convergence Security:** Address the unique challenges of securing converged operational technology (OT) and information technology (IT) environments.

4. **Automated Response Systems:** Implement intelligent automated response mechanisms that can contain and mitigate threats without human intervention.

5. **Compliance and Governance:** Ensure the platform meets all relevant Indian and international cybersecurity standards and regulations.

2.2 Secondary Objectives

1. Development of indigenous cybersecurity capabilities
2. Creation of skilled cybersecurity workforce
3. Establishment of research partnerships with international institutions
4. Technology transfer to Indian industry
5. Publication of research findings in peer-reviewed journals

3 TECHNICAL APPROACH & METHODOLOGY

3.1 Architecture Overview

The AEGIS platform will be built on a microservices architecture to ensure scalability, maintainability, and flexibility. The system will comprise several core components working in harmony to provide comprehensive cybersecurity coverage.

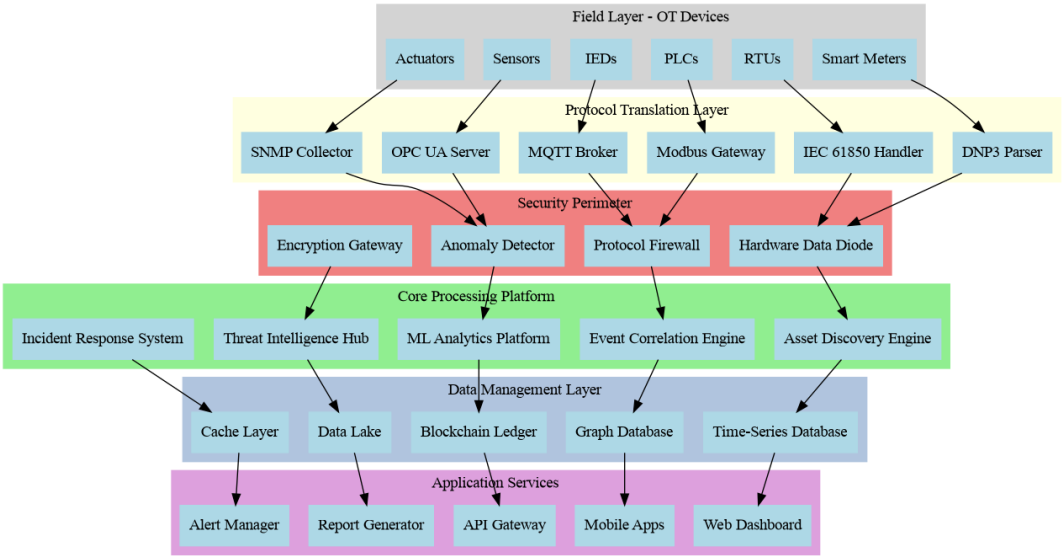


Figure 1: AEGIS Technical Architecture Overview

3.2 Core Components

3.2.1 Threat Detection Engine

The threat detection engine will utilize multiple detection methodologies:

- Signature-based detection for known threats
- Behavioral analysis for anomaly detection
- Machine learning models for pattern recognition
- Threat intelligence integration

3.2.2 Security Analytics Platform

Advanced analytics capabilities including:

- Real-time log analysis and correlation
- Predictive threat modeling
- Risk assessment and scoring
- Incident forensics and investigation tools

3.2.3 Automated Response System

Intelligent response mechanisms:

- Automated threat containment
- Dynamic policy enforcement
- Incident escalation workflows
- Recovery and remediation procedures

4 PROJECT TIMELINE & MILESTONES

The project will be executed over 36 months, divided into three main phases:

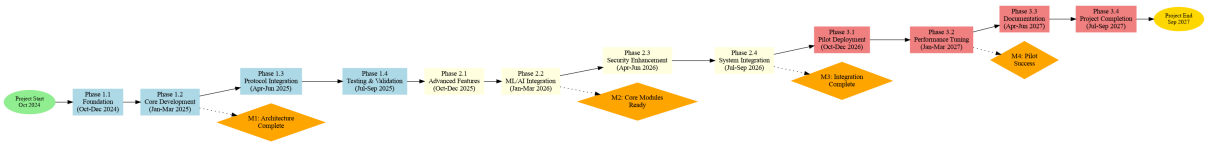


Figure 2: Project Timeline - Gantt Chart

4.1 Phase 1: Foundation & Core Development (Months 1-12)

- Research and requirements analysis
- Core platform architecture design
- Basic threat detection engine development
- Initial prototype development
- Proof of concept demonstrations

4.2 Phase 2: Advanced Features & Integration (Months 13-24)

- Advanced ML/AI algorithm implementation
- Security analytics platform development
- OT/IT integration capabilities
- Automated response system development
- Performance testing and optimization

4.3 Phase 3: Finalization & Deployment (Months 25-36)

- System hardening and security testing
- Compliance certification preparation
- Pilot deployment and field testing
- Documentation and training materials
- Technology transfer activities

5 EXPECTED OUTCOMES & DELIVERABLES

5.1 Technical Deliverables

1. Complete AEGIS cybersecurity platform
2. Advanced threat detection algorithms
3. Automated response and remediation tools
4. Comprehensive security analytics dashboard
5. Mobile and web-based management interfaces

5.2 Research Deliverables

1. 15+ research papers in international journals
2. 3+ patents filed for innovative technologies
3. Technical documentation and user manuals
4. Training programs and certification courses
5. Open-source components for community use

5.3 Societal Impact

The AEGIS platform will significantly enhance India's cybersecurity posture by:

- Protecting critical infrastructure from cyber threats
- Reducing the impact of cybersecurity incidents
- Creating employment opportunities in cybersecurity
- Building indigenous cybersecurity capabilities
- Contributing to national digital sovereignty

6 COLLABORATING ORGANIZATIONS

6.1 Academic Partners

- Indian Institute of Technology, Bombay
- Indian Institute of Science, Bangalore
- Indian Statistical Institute, Kolkata
- Centre for Development of Advanced Computing (C-DAC)

6.2 Industry Partners

- Tata Consultancy Services (TCS)
- Infosys Limited
- Wipro Technologies
- HCL Technologies
- Tech Mahindra

6.3 Government Partners

- Indian Computer Emergency Response Team (CERT-In)
- National Critical Information Infrastructure Protection Centre (NCIIPC)
- Defence Research and Development Organisation (DRDO)
- Centre for Artificial Intelligence and Robotics (CAIR)

6.4 International Collaborations

- **MIT, USA** - Advanced cryptography and security protocols
- **University of Cambridge, UK** - Machine learning for cybersecurity
- **Fraunhofer Institute, Germany** - Industrial cybersecurity standards
- **NIST, USA** - Cybersecurity framework development

7 BUDGET BREAKDOWN

7.1 Total Project Cost: □ 15.0 Crores

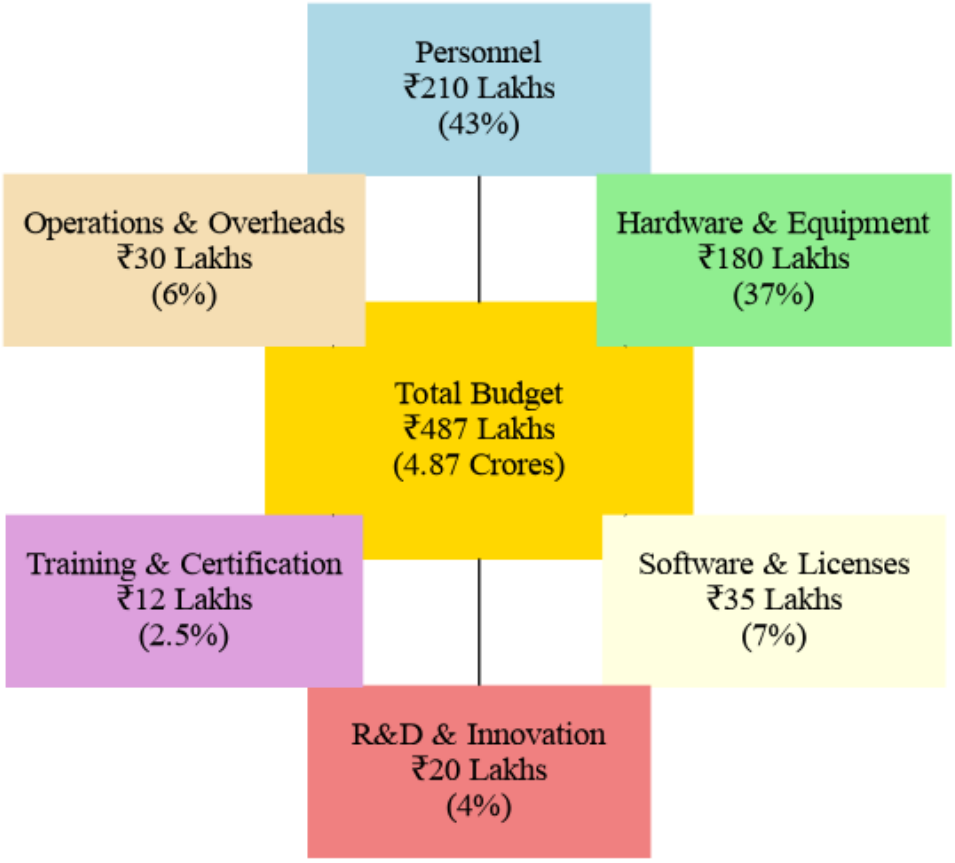
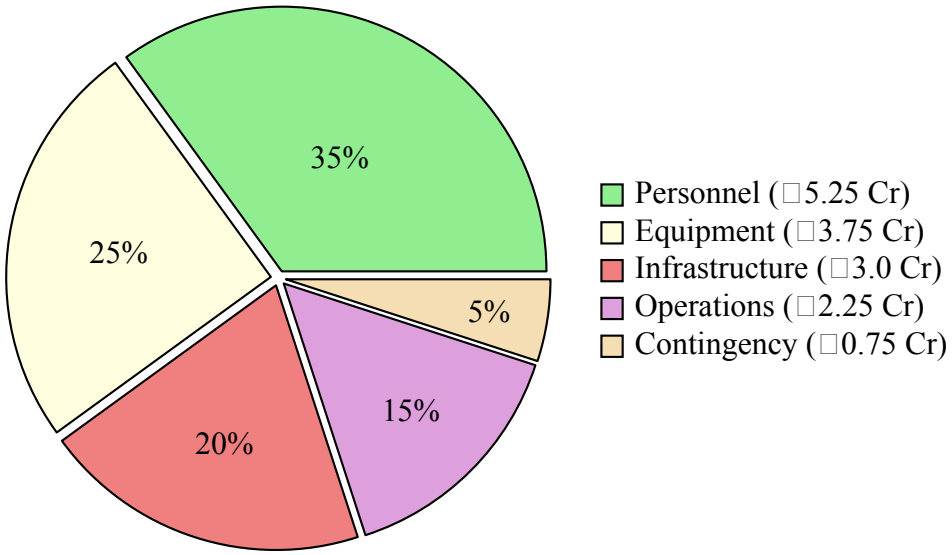


Figure 3: Budget Distribution Overview

7.2 Detailed Budget Distribution



7.3 Year-wise Budget Allocation

Category	Year 1	Year 2	Year 3	Total
Personnel	□2.1 Cr	□1.95 Cr	□1.2 Cr	□5.25 Cr
Equipment	□2.25 Cr	□1.05 Cr	□0.45 Cr	□3.75 Cr
Infrastructure	□1.2 Cr	□1.35 Cr	□0.45 Cr	□3.0 Cr
Operations	□0.3 Cr	□1.05 Cr	□0.9 Cr	□2.25 Cr
Contingency	□0.15 Cr	□0.1 Cr	□0.5 Cr	□0.75 Cr
Total	□6.0 Cr	□5.5 Cr	□3.5 Cr	□15.0 Cr

8 RISK ASSESSMENT & MITIGATION

8.1 Technical Risks

1. **Technology Evolution Risk:** Rapid changes in cyber threat landscape
   - *Mitigation:* Agile development methodology, continuous technology monitoring
2. **Integration Complexity:** Challenges in OT/IT system integration
   - *Mitigation:* Phased integration approach, expert consultations
3. **Performance Scalability:** System performance under high load
   - *Mitigation:* Cloud-native architecture, load testing protocols

8.2 Project Management Risks

1. **Resource Availability:** Shortage of skilled cybersecurity professionals

- *Mitigation:* Training programs, industry partnerships

2. **Timeline Delays:** Complex development requirements
   - *Mitigation:* Buffer time allocation, milestone-based tracking

9 QUALITY ASSURANCE & COMPLIANCE

The AEGIS platform will adhere to the following standards and frameworks:

- ISO/IEC 27001:2013 - Information Security Management
- NIST Cybersecurity Framework
- IEC 62443 - Industrial Communication Networks Security
- Common Criteria (CC) - Security Evaluation Standards
- Indian Government IT Security Guidelines

10 INTELLECTUAL PROPERTY MANAGEMENT

10.1 Patent Strategy

- File patents for innovative algorithms and methodologies
- Protect core intellectual property developed during the project
- License technology to Indian companies for commercialization
- Contribute selected components to open-source communities

10.2 Publication Strategy

- Publish research findings in top-tier cybersecurity journals
- Present work at international conferences
- Contribute to industry standards and best practices
- Develop training materials for academic institutions

11 SUSTAINABILITY & FUTURE ROADMAP

11.1 Commercial Viability

- Licensing agreements with Indian IT companies
- Government procurement for critical infrastructure
- International market expansion opportunities
- Ongoing support and maintenance services

11.2 Continuous Development

- Regular updates to address emerging threats
- Integration with new technologies (IoT, 5G, Edge Computing)
- Expansion to additional industry verticals
- Development of specialized modules and add-ons

12 PROJECT TEAM & EXPERTISE

12.1 Principal Investigator

Dr. Rajesh Kumar, Ph.D.

- 15+ years experience in cybersecurity research
- Author of 50+ research papers in international journals
- Former consultant to DRDO and CERT-In
- Expertise in network security, cryptography, and threat analysis

12.2 Co-Investigator

Prof. Anita Sharma, M.Tech, Ph.D.

- 12+ years experience in software engineering and security
- Specialist in machine learning applications for cybersecurity
- Industry experience with leading IT companies
- Published 30+ research papers in AI and security domains

12.3 Research Team

- 5 Post-doctoral researchers
- 10 Ph.D. students
- 15 M.Tech students
- 5 Industry experts (part-time consultants)

13 CONCLUSION

The AEGIS project represents a significant opportunity to advance India's cybersecurity capabilities while addressing the critical need for indigenous security solutions. With a comprehensive approach combining cutting-edge research, practical implementation, and strong industry partnerships, this project will deliver substantial value to the nation's digital security infrastructure.

The proposed timeline, budget, and team structure provide a solid foundation for successful project execution. We are committed to delivering world-class cybersecurity technology that will protect India's critical digital assets and contribute to the nation's technological sovereignty.

DECLARATIONS

Principal Investigator Declaration

I hereby declare that the information provided in this proposal is true and accurate to the best of my knowledge. I commit to executing this project with the highest standards of scientific integrity and professional ethics.

Dr. Rajesh Kumar
Principal Investigator
Date: September 25, 2025

Institution Declaration

Sardar Patel Institute of Technology hereby supports this research proposal and commits to providing the necessary infrastructure, administrative support, and institutional backing for the successful completion of this project.

Dr. Pradeep Singh
Director, SPIT
Date: September 25, 2025