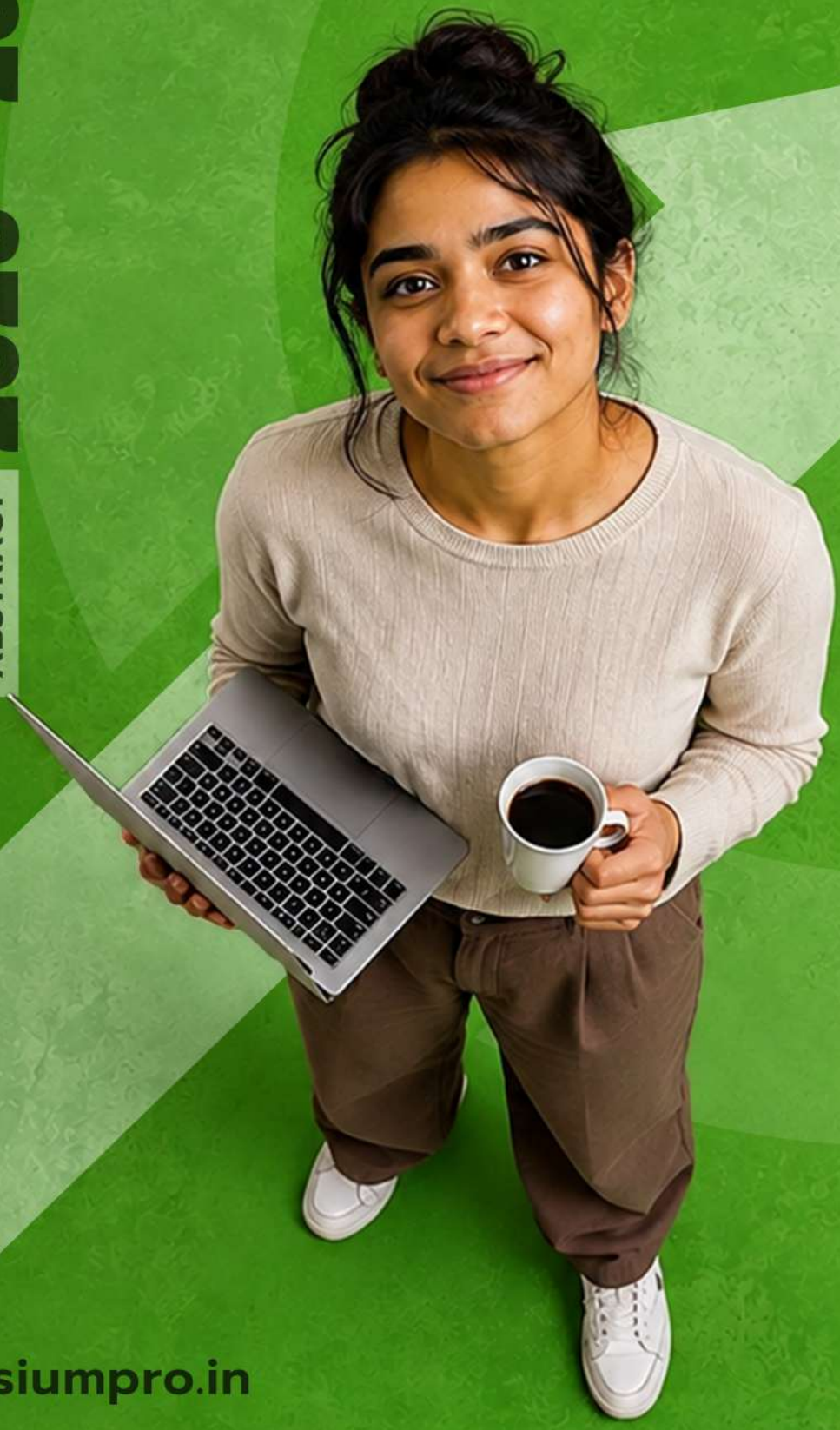
ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

CYBER SECURITY

2026 - 2027

TITLE & ABSTRACT

Advanced Academic Final Year Projects



elysiumpro.in

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Standards-Compliant Zero Trust Framework-Based Software-Defined Perimeter (SDP) for Securing Residential IoT Networks

This project develops a Zero Trust cybersecurity framework for protecting residential IoT devices from unauthorized access. Machine learning analyzes device behavior, network traffic, and authentication patterns to identify suspicious activities. A Software-Defined Perimeter controls access based on device identity, security status, and behavioral analysis. Deep learning can detect abnormal communication patterns and potential cyberattacks in real time. When a high-risk activity is detected, the system generates an alert and sends an email notification to the administrator.

Exploiting Kubernetes' Image Pull Implementation to Deny Node Availability

This project focuses on detecting and preventing resource-exhaustion attacks targeting Kubernetes container environments. Machine learning models analyze container image requests, node utilization, network traffic, and resource consumption patterns. Deep learning techniques identify abnormal image-pulling behavior that may indicate an availability attack. The monitoring system continuously evaluates Kubernetes nodes and detects unusual resource usage. When suspicious activity is identified, administrators receive real-time alerts and email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

KAIR: Knowledge-Aware Iterative Retrieval for Multiagent Systems

This project develops a secure multi-agent information retrieval system using knowledge-aware machine learning techniques. AI models analyze agent requests, retrieved information, and communication behavior to identify potentially unsafe or abnormal interactions. Deep learning can be used to detect malicious instructions, unauthorized information retrieval, and suspicious agent behavior. Security policies are applied to control communication between multiple agents. Detected security violations can trigger real-time dashboard alerts and email notifications.

Privacy-Preserving Against Gradients Leakage Attacks via Joint Differential Privacy in Federated Learning

This project develops a privacy-preserving federated learning framework to protect sensitive training information from gradient leakage attacks. Machine learning models are trained collaboratively without directly sharing raw user data. Differential privacy mechanisms protect model updates before they are transmitted to the central aggregation system. Deep learning models can be monitored for unusual gradient patterns indicating potential privacy attacks. When suspicious training behavior is detected, the system generates security alerts and sends email notifications to the administrator.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Architectural Strategies for Automotive Predictive Maintenance: Balancing System Efficiency and Security Through Advanced Risk Analysis

This project combines predictive maintenance with cybersecurity monitoring for connected automotive systems. Machine learning analyzes vehicle sensor data to predict component failures and maintenance requirements. Deep learning models simultaneously analyze CAN or network traffic to identify potential cyberattacks. A risk analysis module combines maintenance and security information to determine the overall vehicle risk level. Critical anomalies can trigger real-time warnings and automated email notifications for maintenance or security teams.

N-k Security Assessment With Quantum Annealing

This project develops an intelligent security assessment framework for analyzing multiple simultaneous failures or cyberattack scenarios in complex infrastructure. Machine learning techniques evaluate system vulnerabilities, dependencies, and potential attack combinations. Optimization methods inspired by quantum annealing identify high-risk combinations requiring immediate attention. Deep learning can support prediction of security-impact patterns from historical incident data. When critical security conditions are identified, the system provides dashboard alerts and sends email notifications to responsible personnel.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

QATNet: A Lightweight Quantum–Classical Tabular Network for Low-Latency Intrusion Detection

QATNet is a lightweight intrusion detection framework designed for rapid cybersecurity analysis of network traffic. A hybrid quantum-classical or simulated quantum-classical model can classify network records into normal and malicious categories. Machine learning preprocessing and feature selection reduce computational requirements for real-time detection. Deep learning components improve identification of complex attack patterns in tabular security data. Detected attacks are recorded immediately and critical incidents trigger automated email notifications.

SAFE-ADVENT: Privacy-Preserving and Resilient Distributed Federated Learning for DDoS Attacks Detection in 5G-V2X Networks

This project develops a privacy-preserving federated learning system for detecting DDoS attacks in 5G vehicle-to-everything networks. Distributed devices train deep learning intrusion detection models without sharing raw network traffic. Privacy mechanisms protect sensitive vehicle and communication information during model aggregation. The system continuously analyzes traffic behavior to identify abnormal attack patterns. When a DDoS attack is detected, the system generates a real-time security alert and sends an email notification to the network administrator.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Minos: Bringing Accountability and Traceability to Attribute-Based Keyword Search

This project develops a secure multi-agent collaboration framework that uses AI to coordinate communication between autonomous agents. Machine learning models evaluate agent behavior, communication patterns, and contextual information to identify suspicious interactions. Deep learning can classify anomalous communication sequences and potential malicious agent behavior. A leader-driven coordination mechanism controls task assignment and information exchange. Detected security anomalies are recorded and administrators receive email notifications for critical events.

COSMIC: Leader-Driven Context-Oriented Collaboration Between Agents

This project develops a secure multi-agent collaboration framework that uses AI to coordinate communication between autonomous agents. Machine learning models evaluate agent behavior, communication patterns, and contextual information to identify suspicious interactions. Deep learning can classify anomalous communication sequences and potential malicious agent behavior. A leader-driven coordination mechanism controls task assignment and information exchange. Detected security anomalies are recorded and administrators receive email notifications for critical events.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Optimal Partitioning of Square Computational Domains for Parallel Computing on Hybrid Servers With Heterogeneous Processors and Heterogeneous Communication Links

This project develops an intelligent resource allocation framework for secure parallel computing environments. Machine learning predicts workload requirements, processor availability, communication delays, and resource utilization. Deep learning can optimize computational task partitioning based on historical execution patterns. The system monitors resource behavior to identify abnormal workloads or possible resource-based attacks. If suspicious resource utilization or unexpected execution behavior occurs, administrators can receive real-time alerts and email notifications.

Analysis of the Influence of CT Imaging Conditions on the CT Image Features of Pulmonary Nodule Phantoms

This project applies a Transformer and convolution-based deep learning framework for recognizing subtle facial expressions from security camera or authentication data. The system extracts spatial and temporal features from facial images to identify microexpressions associated with suspicious behavior. Machine learning classification can support behavioral security assessment and identity verification. The framework can be integrated with access-control systems for real-time monitoring. Suspicious facial behavior or authentication anomalies can trigger security alerts and email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

DaV3is: Data Flow-Based Vulnerability Verification Through Visualization

This project develops a cybersecurity vulnerability analysis system based on application data-flow visualization. Machine learning models analyze source-code flows, dependencies, and execution patterns to identify potential vulnerabilities. Deep learning can classify vulnerable data-flow patterns and prioritize high-risk security issues. Visualization dashboards help security analysts understand the location and impact of detected vulnerabilities. Critical vulnerabilities can automatically generate alerts and email notifications for security teams.

Securing Networked Discrete Event Systems for Diagnosability Under Attacks

This project develops an intelligent security monitoring system for networked discrete event systems. Machine learning analyzes system events and communication sequences to detect abnormal or malicious behavior. Deep learning models can learn complex attack patterns and distinguish normal system transitions from compromised states. The system maintains security logs and evaluates the diagnosability of potential attacks. When a critical attack is identified, an alert is generated and an email notification is sent to the administrator.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Strategic Decision-Making in Uncertain Turn-Based Security Games

This project develops an AI-based cybersecurity decision-support system using strategic security game models. Machine learning analyzes historical attack and defense patterns to estimate potential attacker behavior. Deep reinforcement learning can determine suitable defensive actions under uncertain security conditions. The system evaluates multiple possible attack scenarios and recommends appropriate mitigation strategies. Critical threats can trigger immediate dashboard alerts and automated email notifications.

Accurate and Energy-Efficient Detection of Cyberattacks Against Non-Linear AGC Systems

This project develops a machine learning-based intrusion detection system for automatic generation control environments. Network and control-system measurements are analyzed to identify abnormal behavior and cyberattack patterns. Deep learning models classify different attack types while maintaining efficient computational performance. Energy-aware processing helps reduce the resource requirements of continuous monitoring. When a critical attack is detected, the system generates an alert and sends an email notification to the control administrator.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Game-Theoretic Analysis of Multi-Source Information Freshness Under False Data Injection

This project develops a cybersecurity framework for detecting false data injection attacks in multi-source information systems. Machine learning analyzes data freshness, consistency, and source behavior to identify suspicious information. Deep learning models can detect complex temporal patterns associated with manipulated data. Game-theoretic techniques help determine suitable defensive strategies against intelligent attackers. Detected false-data incidents are logged and critical events trigger email notifications.

Perfect Privacy for Discriminator-Based Byzantine-Resilient Federated Learning

This project develops a privacy-preserving federated learning system capable of detecting malicious participants during collaborative model training. Machine learning models analyze client updates to identify abnormal or Byzantine behavior. Deep learning enables secure distributed model training while privacy mechanisms reduce exposure of sensitive information. A discriminator-based mechanism separates trustworthy and suspicious model updates. Malicious participation is logged and administrators can receive automated email alerts for security incidents.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Design of Physical Layer Challenge Response Authentication With RIS and Multiple-Antenna Devices

This project develops a machine learning-based authentication mechanism for wireless communication systems. Physical-layer signal characteristics are collected from multiple antennas and reconfigurable intelligent surfaces to identify legitimate devices. Deep learning models learn unique signal patterns and distinguish authorized devices from potential impersonators. Challenge-response mechanisms provide an additional layer of authentication security. Failed authentication attempts or suspicious signal behavior can trigger real-time alerts and email notifications.

AmbShield: Enhancing Physical Layer Security With Ambient Backscatter Devices Against Eavesdroppers

This project develops an AI-assisted physical-layer security framework for detecting potential eavesdropping activities. Machine learning models analyze wireless signal characteristics, communication behavior, and channel variations. Deep learning can identify abnormal signal patterns associated with unauthorized listeners or communication interference. Ambient backscatter devices are used to support secure low-power communication. When suspicious wireless behavior is detected, the system generates a security alert and sends an email notification.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Distributed Resilient State Estimation and Control With Strategically Implemented Security Measures

This project develops a secure distributed monitoring system for networked control environments. Machine learning analyzes sensor measurements and system states to identify abnormal or manipulated information. Deep learning models can detect false-data injection, sensor anomalies, and coordinated cyberattacks. Security mechanisms are applied to maintain reliable state estimation and control decisions during attacks. Critical anomalies are reported through real-time dashboards and automated email notifications.

From Simulation to Production: Few-Shot Learning for ID Card Presentation Attack Detection

This project develops a biometric security system for detecting presentation attacks during digital identity verification. Few-shot deep learning enables the model to recognize spoofing attempts using limited training samples. Image processing and feature extraction identify fake ID cards, manipulated images, or presentation attacks. The system performs real-time verification and assigns a security risk score to each authentication attempt. Suspicious or failed verification attempts can generate immediate alerts and email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Advancing Biometric Authentication With Dual-Threshold Multi-Modal Systems and Geometric Programming for Enhanced

This project develops a multi-modal biometric authentication system combining different biometric characteristics for improved security. Machine learning models extract and compare biometric features from sources such as face, fingerprint, or voice. Deep learning improves feature representation and recognition accuracy under different conditions. Dual-threshold verification provides flexible decisions between genuine and suspicious authentication attempts. Repeated failures or high-risk attempts can trigger security alerts and email notifications.

A Verifiable Federated Learning Mechanism for Digital Museum Collection Based on Homomorphic Proxy Re-Authentication

This project develops a privacy-preserving federated learning framework for protecting digital museum collections and related user information. Deep learning models can be trained collaboratively while sensitive data remains within individual institutions. Homomorphic and proxy re-authentication mechanisms protect data and model communication during collaboration. Machine learning analyzes access behavior to identify unauthorized or suspicious activities. Security violations can be recorded and administrators receive automated email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

ACHILLES: A Machine Learning Framework for Explainable and Generalized Automotive Intrusion Detection System

ACHILLES is an intelligent automotive intrusion detection framework designed to detect cyberattacks in connected vehicle networks. Machine learning models analyze CAN bus messages and network traffic to classify normal and malicious activities. Deep learning improves detection of complex and previously unseen attack patterns. Explainable AI techniques provide reasons behind detected security decisions. When a high-risk automotive attack is identified, the system generates a real-time alert and sends an email notification.

A Robust Hybrid Multicriteria Decision-Making Approach to Barriers of AI Adoption in Air Cargo

This project develops an intelligent cybersecurity and risk assessment framework for AI adoption in air cargo environments. Machine learning analyzes operational, technical, security, and organizational factors influencing AI deployment. Deep learning can identify complex relationships between cybersecurity risks and operational dependencies. A multicriteria decision-making mechanism prioritizes critical risks and recommends suitable mitigation strategies. High-priority security risks can generate automated alerts and email notifications for responsible teams.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Automating 5G Traffic Generation With Virtual UEs: A Scalable Network Testing Infrastructure

This project develops a cybersecurity testing platform that generates realistic 5G network traffic using virtual user equipment. Machine learning analyzes generated traffic to identify abnormal patterns and evaluate intrusion detection performance. Deep learning models can be trained using simulated attack and normal traffic scenarios. The platform supports scalable testing of DDoS, scanning, flooding, and other network attacks. Detected threats can be displayed in real time and critical events can trigger email notifications.

Resilient Networked Control Systems Subject to Cyber Threats: A Data Encryption and Cloud Computing-Based Model Predictive Control Approach

This project develops a secure cloud-assisted control system for protecting networked control environments against cyber threats. Machine learning analyzes sensor and communication data to identify anomalies and potential attacks. Deep learning can classify cyberattack patterns and support predictive threat detection. Encryption protects sensitive control information during transmission and cloud processing. Critical security incidents are logged and administrators receive real-time email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Standardized Digital Twin Framework for Modeling, Monitoring, and Detection of Cyber–Physical Threats in Photovoltaic Plant Sensors

This project develops a digital twin-based cybersecurity monitoring framework for photovoltaic plants. Real-time sensor information is synchronized with a digital representation of the physical energy system. Machine learning analyzes sensor behavior to detect abnormal readings, equipment faults, and cyberattacks. Deep learning models identify complex deviations between physical measurements and digital twin predictions. When a cyber-physical anomaly is detected, the system generates alerts and sends email notifications to plant operators.

Attacks and Detections in Recommender Systems: A Comprehensive Analysis for Models, Progresses, and Trends

This project develops an AI-based security framework for detecting attacks against recommendation systems. Machine learning analyzes user ratings, interaction patterns, and recommendation behavior to identify suspicious manipulation. Deep learning models can detect complex poisoning, shilling, and profile-based attacks. The system assigns risk scores to suspicious users and evaluates the potential impact on recommendations. Detected attacks can be displayed through a security dashboard with automated email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

A Deep Reinforcement Learning Approach to Time Delay Differential Game Deception Resource Deployment

This project develops a deep reinforcement learning framework for intelligent cybersecurity defense and deception. The system models attackers and defenders as strategic players operating under uncertain time delays. Deep reinforcement learning learns optimal deception and defense resource allocation strategies from simulated attack scenarios. Machine learning evaluates attack behavior and dynamically adjusts defensive actions. High-risk attack situations can trigger immediate alerts and email notifications to security administrators.

Forseti: A Decentralized Permission Transfer Framework for IoT Leasing

This project develops a secure decentralized permission management system for leased IoT devices. Machine learning analyzes device behavior and access patterns to identify unauthorized permission usage. Deep learning can detect abnormal device interactions and suspicious access sequences. Decentralized authorization mechanisms control the transfer and revocation of IoT permissions between users. Unauthorized access attempts generate security alerts and automated email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Standards-Compliant Zero Trust Framework-Based Software-Defined Perimeter (SDP) for Securing Residential IoT Networks

This project implements a Zero Trust security architecture for protecting smart home and residential IoT environments. Machine learning continuously analyzes network traffic, device behavior, and authentication patterns to detect abnormal activities. Deep learning models identify sophisticated attacks such as botnet behavior, unauthorized access, and unusual communication. Access is dynamically controlled according to device trust and security status. Detected threats are logged and immediate email notifications are sent to the administrator.

Variational GAN-Enhanced Causal Effect Inference for Interpretable Learning in Heterogeneous IoT Systems

This project develops an AI-driven security analysis framework for heterogeneous IoT environments. Variational GAN techniques can generate representative data for improving learning when real security datasets are limited. Machine learning and causal inference techniques analyze relationships between device behavior, network events, and security outcomes. Deep learning models identify abnormal patterns and provide interpretable security insights. High-risk IoT activities can generate real-time alerts and automated email notifications.

CYBERSECURITY

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

Adaptive NetFlow IIoT Intrusion Detection With Deep Transfer Learning, Genetic Optimization, and Ensemble Methods for Network Management

This project develops an adaptive intrusion detection system for Industrial IoT networks using NetFlow traffic information. Deep transfer learning enables the model to recognize cyberattack patterns while reducing the need for extensive training data. Genetic optimization selects important network features, while ensemble learning improves classification accuracy. The system continuously monitors industrial traffic and detects attacks such as scanning, DoS, and abnormal communication. Detected threats are displayed on a monitoring dashboard and critical incidents automatically trigger email notifications.

ELYSIUMPRO
INSPIRING THE LEADING EDGE TECHNOLOGIES

ELYSIUM PRO

38K+ New Projects

85+ Expert Staffs

18+ Global Awards

2.8L+ Customer Satisfied | **27+** Specialized Domains | **112+** Campus Tie-ups | **24/7** Support Center | **57+** Countries Covered | **3200+** Journal Access

99447 93398

info@elysiumpro.in

elysiumpro.in

229, First Floor, A Block,
Elysium Campus,
Church Rd, Anna Nagar,
Madurai, Tamil Nadu -
625020.

Delivery Centres

Chennai | Coimbatore | Tirunelveli | Vellore | Trichy | Erode