CyberSentinelAI: Cybersecurity Agent for ERP Systems

PROJECT PROPOSAL PRESENTATION

Name of the Students

- Johns Jaison
- Liz Johnson
- Pranav C Pradeesh
- Sana P Anwar

Name of the Guide :

- Ms. Aiswarya Mohan

RSET

Introduction

- **Enterprise ERP systems** (like SAP, Oracle, Microsoft Dynamics) handle critical operations and are frequent targets of cyber attacks, yet traditional security methods remain reactive and insufficient.

- **CyberSentinelAI** is an AI-driven cybersecurity agent that autonomously simulates ethical hacking within ERP systems to proactively uncover vulnerabilities, misconfigurations, and suggest security improvements.

- The project aims to **minimize threat exposure**, improve real-time monitoring, and offer strategic remediation, strengthening proactive cybersecurity in enterprise environments.

RSET

Background

- **Traditional ERP cybersecurity methods** (manual testing, signature-based detection) are outdated and insufficient for the complexity and scale of modern, cloud-based ERP systems, which face threats like misconfigured APIs, unpatched modules, and insider attacks.

- **Existing tools** like vulnerability scanners and penetration testing frameworks are periodic and human-operated, creating a critical gap due to the lack of continuous, adaptive, ERP-specific monitoring and defense mechanisms.

- **CyberSentinelAI** fills this gap by integrating AI (reinforcement learning, deep learning, adversarial networks) with ethical hacking to create an intelligent, self-learning penetration testing framework tailored to ERP systems, capable of proactive, evolving threat detection and response.

Project Objectives -

List of Software functionalities:

- **ERP Integration:** Secure connectors for popular ERP systems (SAP, Odoo). Enables real-time data access, log extraction, and behavior emulation
- **Attack Simulation:** Launches controlled cyberattacks like SQLi, XSS, etc. Evaluates ERP system resilience
- **Reporting Dashboard:** Web interface to visualize attacks, logs, vulnerabilities. Enhances usability and decision-making
- **Access Control:** Role-based permissions and test boundaries. Ensures safe operations and system integrity
- **Environment Simulation:** Dockerized or virtual sandbox environments for testing. Provides safe, repeatable testing spaces

Project Objectives -

List of AI/DS Modules

Attacking Module	**Protection Module**
Reinforcement learning model (PPO/DQN) evolves to try smarter, stealthier attacks based on past results.	Trained on logs, attack patterns, and malware datasets. Uses anomaly detection (LSTM, Isolation Forest, Autoencoders) to stop or flag attacks as they happen.
Matches system behavior and logs with known CVEs, uses **CVSS scores** and **CAPEC patterns** to assess severity of attacks.	Predictive modelling: Predicts likely attack vectors based on current system usage, vulnerabilities, and attack history.
Analyzes impact of vulnerabilities and suggests security improvements or patches automatically.	Web dashboard for real-time security status, threats detected, vulnerabilities scored, and recommended fixes
Tools like Metasploit, Nmap, Nikto, and custom scripts simulate real attacks for training and testing.	Monitors ERP logs and user behavior. Flags deviations from normal patterns using ML algorithms.

Literature Survey

Title of Paper, Authors	Journal / Conference	Year	Technologies / Algorithms Used	Advantages / Features	Limitation
"Deep Learning-Enabled Big Data Analytics for Cybersecurity Threat Detection in ERP Ecosystems" Krishna Madhav Jha, Varun Bodepudi, Suneel Babu Boppana, Niharika Katnapally, Srinivasa Rao Maka, Manikanth Sakuru	Journal: Review of Contemporary Philosophy	2023	● Deep Learning ● Big Data Analytics ● Autoencoders	Combines deep learning and big data analytics to manage cybersecurity threats in an ERP ecosystem. Deep learning models can rapidly process vast amounts of data, which streamlines threat intelligence in near real-time	Big data analytics on their own are insufficient for a rapidly growing threat landscape Deep learning algorithms require significant computational resources and may overfit the training data due to their complexity.

Literature Survey

Title of Paper, Authors	Journal / Conference	Year	Technologies / Algorithms Used	Advantages / Features	Limitation
“AI-Powered Big Data and ERP Systems for Autonomous Detection of Cybersecurity Vulnerabilities” Srinivasa Rao Maka, Krishna Madhav Jha, Purna Chandra Rao Chinta, Chethan Sriharsha Moore, Niharika Katnapally, Gangadhar Sadaram	Journal: Nanotechnology Perceptions Vol. 19 No. S1 (2023)	2023	● Artificial Intelligence (AI) ● Big Data ● Deep Learning	-Integrates AI and Big Data with ERP for real-time, autonomous detection of cybersecurity vulnerabilities. - Improves threat response time and accuracy. - Enables predictive analytics and proactive defense mechanisms.	- Requires high computational resources. - Risks of AI bias and ethical concerns. - Data privacy and compliance challenges. - Complex integration in legacy ERP systems..

Literature Survey

Title of Paper, Authors	Journal / Conference	Year	Technologies / Algorithms Used	Advantages / Features	Limitation
“Cybersecurity Anomaly Detection in Adversarial Environments” David A. Bierbrauer Will Kritzer Alexander Chang Nathaniel D Bastian	AAAI Fall Symposium Series 2021 (FSS-21) Washington DC USA	2021	● Isolation Forest ● Local Outlier Factor ● MIDAS ● Logistic Regression ● LDA ● Stacking Ensemble Model	-High Detextion Accuracy in adverserial conditions - Robustness against evasion attacks through adversarial training - Real-World-Relevance: Designed for IoBT	-Unsupervised methods underperformed -MIDAS only useable on certain protocols -No integration of graph-based approaches into ensemble

Literature Survey

Title of Paper, Authors	Journal / Conference	Year	Technologies / Algorithms Used	Advantages / Features	Limitation
“Automating Cyber Threat Response Using Agentic AI and Reinforcement Learning Techniques” Srinivasa Rao Maka1 Suneel Babu Boppana, Gangadhar Sadaram, Niharika Katnapally, Laxmana Murthy Karaka, Manikanth Sakuru	J. Electrical Systems 17-4 (2021): 138-148	2021	-Reinforcement learning -Gradient Boosting -Clustering -ERP Systems -Distributed systems -Big Data	-Real time and autonomous cyber threat detection -Adaptive decision making -Faster response to threats –Scalable with cloud and big data	-High computational cost for small setups -Bias in AI decision making -Data privacy and ethical concerns -Requires large and quality datasets

Product survey

Product	Key Features	Pros	Cons
Darktrace Enterprise Immune System	● Self learning AI Detects novel threats ● Anomaly detection in ERP system	● Autonomous response ● ERP specific monitoring modules ● Easy integration	● Expensive ● Can generate false positive ● complex setup

RSET

Product survey

Product	Key Features	Pros	Cons
Splunk Enterprise Security (with ML Toolkit)	● Anomaly detection using ML ● ERP data ingestion ● Custom alerts	● Scalable ● Excellent log management ● Community-driven ML tools	● Requires expertise to fine-tune ML models ● Licensing costs can be high

Product survey

Product	Key Features	Pros	Cons
SAP Enterprise Threat Detection (SAP ETD)	● Tailored for SAP ERP ● Real-time threat analysis ● Behavioral profiling	● Deep SAP integration ● Real-time alerts for SAP ● ERP-specific attacks	● Limited to SAP ERP ● High cost ● Less flexible for non-SAP integration

Methodology for Software Services

○ **Software Services**

- Requirement Analysis:
  - Study SAP/ERP security docs
- Solution Proposal:
  - Use OWASP ASVS (Application Security Verification Standard)
- Deployment Approach:
  - 2-week sprints, Jira for fast tracking.

Methodology for AI/DS Services

○ **AI/DS Modules**

- Selection Criteria:
  - Peer-reviewed papers from IEEE and Google Scholar
  - Focus on recent advancements in cybersecurity threat detection

- Process:
  - Extract performance metrics
  - Compare model architectures
  - Review datasets and feature engineering techniques used

- Data Source:
  - Static Sources - CICIDS2017, NSL-KDD, CVE JSON, ExploitDB
  - Live Sources - ERPnext, Odoo

Methodology for AI/DS Services

MODULE NAME	PURPOSE
ERP Integration	Connects and gathers data from ERP Systems
Attack Simulation	Simulates cyberattacks on ERP APIs & endpoints
Learning & Adaptation	Learns from outcomes, improves over time
Vulnerability Analysis	Detects, ranks, and matches known vulnerabilities
Monitoring & Logging	Centralizes and preprocesses logs
Reporting & Dashboard	User Interface for insights and recommendations
Accesl & Config	Security, user roles, sandbox boundaries
Sandbox Simulation	Safe ERP testing environment
Feedback & Patching	Recommends fixed, tacks remediation

Development of Software Services

Component	**Technologies**
Backend	Python(FastAPI),Node.js
ERP Integration	Odoo JSON-RPC API, odoorpc python library
Database	PostgreSQL(structured), MongoDB(logs)
DevOPS	Docker,Kubernetes,GitHub Actions

Development of AI/DS Modules

Function	Technologies
Anomaly Detection & Custom RL Models	PyTorch
Reinforcement Learning for Attack Simulation	StableBaselines3
Scalable Anomaly Detection & Predictive Modelling, NLP	TensorFlow

RSET

Integration

Function	**Technologies**
API Gateway	Kong
Auth	OAuth 2.0

Software functionalities

Strategies:

- Unit testing:
  - Test Individual Components in Isolation:
    1. ERP components
    2. Log Parser
    3. Dashboard

- Integration testing:
  - Test interactions between modules:
    1. Attack → ERP → Log Collector → Protection AI
    2. AI Output → Feedback → Dashboard
    3. Validate data consistency, time delays, and error handling

AI/DS Modules

Strategies:

- Accuracy, precision, recall on test datasets
- Time-based validation (especially for anomaly detection)
- Confusion matrices, ROC curves

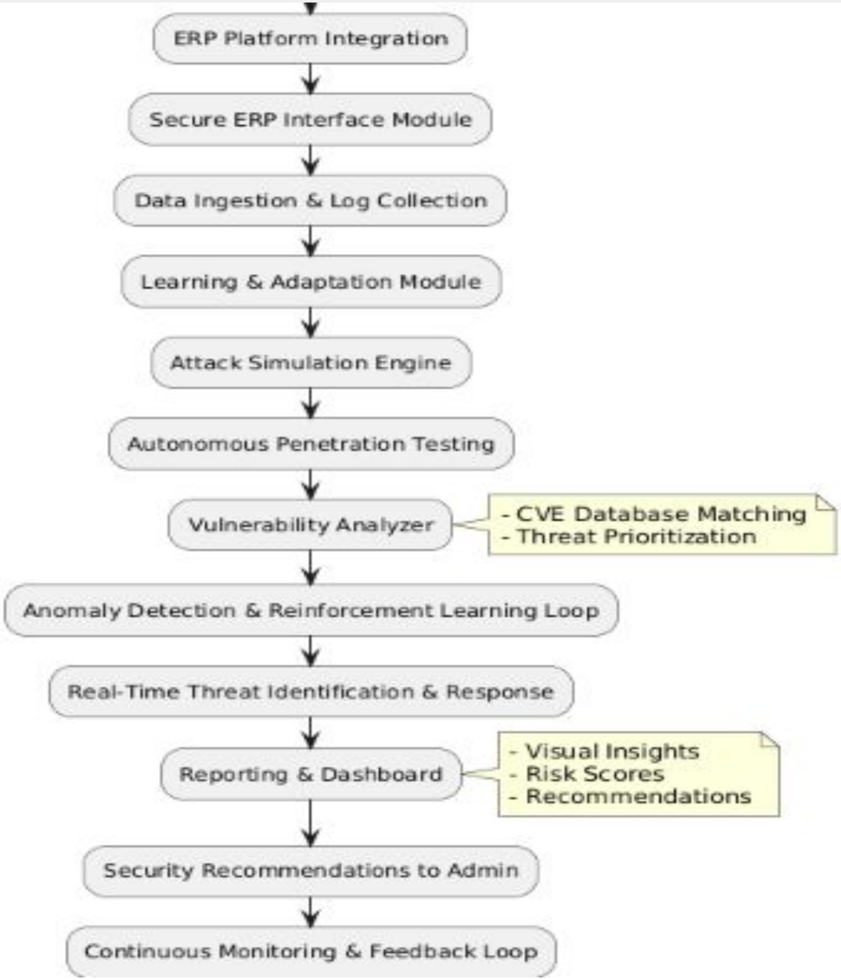
Integration

Strategies:

1. System-level black-box testing:
   - Test the system as a whole (ERP + AI modules) without accessing internal code

2. Sandbox testing:
   - Full workflow testing in isolated environment
   - Allows testing real attacks safely without affecting real ERP data

Deployment Plan


ERP Platform Integration
Secure ERP Interface Module
Data Ingestion & Log Collection
Learning & Adaptation Module
Attack Simulation Engine
Autonomous Penetration Testing
Vulnerability Analyzer
- CVE Database Matching
- Threat Prioritization
Anomaly Detection & Reinforcement Learning Loop
Real-Time Threat Identification & Response
Reporting & Dashboard
- Visual Insights
- Risk Scores
- Recommendations
Security Recommendations to Admin
Continuous Monitoring & Feedback Loop

Deployment Plan

- **ERP System:**
    - Source of business data and logs (eg: SAP, Odoo)
    - Feeds into the AI system.
- **AI Core:**
    - The central brain that learns, analyzes, and coordinates.
    - Controls attack simulations, analyzes vulnerabilities, and learns from results.
- **Attack Simulation:**
    - Performs ethical hacking (e.g.SQL injection, brute-force)
    - Sends results to the Sandbox.
- **Sandbox Environment:**
    - A safe test setup to perform attacks without harming real ERP systems.

Deployment Plan

- **Monitoring and Logging:**
  - Collects and stores ERP and attack logs for analysis.
- **Reporting and Dashboard:**
  - Displays insights, risk scores, and recommendations for users.
- **Vulnerability Analysis:**
  - Matches findings against known CVEs and ranks severity.
- **Access Control and Configuration:**
  - Manages user permissions, test boundaries, and system setup.

Plan for Documentation and Version Control

Documentation Plan

- **README.md** – Project intro, setup, and usage guide

Version Control Plan

- **Git + GitHub/GitLab** for code tracking and collaboration

Timeline

SI.No Week	Deliverable
1 Week 1-4	Finalizing Project Domain, project, and scope
2 Week 5-6	Project Proposal Submission and Presentation
3 Week 7-9	Requirement Analysis of Software and Literature Survey of AI&DS modules, submission of report and presentation
4 Week 10-12	Project Design, Submission of Report, Design Presentation
5 Week 13-14	First Level Code Review

Conclusion

- CyberSentinelAI is an AI-driven security agent designed to protect ERP systems by simulating ethical hacking, learning from attack outcomes, and identifying vulnerabilities.

- Using reinforcement learning and anomaly detection, it continuously improves its threat detection capabilities.

- Its modular microservices architecture allows easy deployment and integration with ERP platforms. By automating penetration testing and real-time analysis, the system reduces manual effort and enhances ERP security

- This project offers a scalable solution for proactive threat detection and contributes to research in intelligent cybersecurity systems.

References

- K. M. Jha, V. Bodepudi, S. B. Boppana, N. Katnapally, S. R. Maka, and M. Sakuru, “Deep Learning-Enabled Big Data Analytics for Cybersecurity Threat Detection in ERP Ecosystems,” *Review of Contemporary Philosophy*, vol. 22, no. 1, pp. 6193–6209, Dec. 2023.

- S. R. Maka, S. B. Boppana, G. Sadaram, N. Katnapally, L. M. Karaka, and M. Sakuru, “Automating Cyber Threat Response Using Agentic AI and Reinforcement Learning Techniques,” *Journal of Electrical Systems*, vol. 17, no. 4, pp. 138–148, 2021.

- C. Moore, “AI-Powered Big Data and ERP Systems for Autonomous Detection of Cybersecurity Vulnerabilities,” *Nanotechnology Perceptions*, vol. 19, no. S1, pp. 46–64, Dec. 2023, posted Jan. 28, 2025. Available: *SSRN* (abstract ID 5114902)

- D. A. Bierbrauer, A. Chang, W. Kritzer, and N. D. Bastian, “Cybersecurity Anomaly Detection in Adversarial Environments,” *arXiv preprint arXiv:2105.06742*, 2021.

RSET

Thank you