Department Of CSE

Byte Quest
Issue 178

24 Oct 2025

Department Vision

To be acenter foracademicexcellence in the field of Computer Science and Engineering education to enable graduates to be ethical and competent professionals.

Department Mission

To enablestudents to develop logic and problem solving approach that will help build their careers in the innovative field of computing and provide creative solutions for the benefit of society

Faculty Coordinators Dr. Bhargavi Peddireddy(Asc. Prof.)

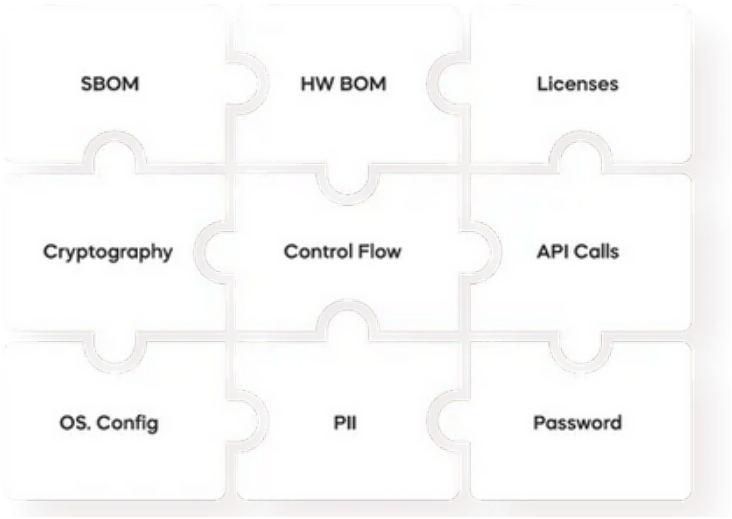
Student Coordinators: (1602-23-733-118) Sneha 1602-24-733-111, G Sathwik Reddy

Generative AI 2.0 – The Next Wave of Intelligence

A digital twin is a virtual replica of a physical system, process, or object that continuously mirrors its real-world counterpart. By integrating real-time data, simulations, and AI, digital twins enable businesses and researchers to analyze, predict, and optimize operations like never before.

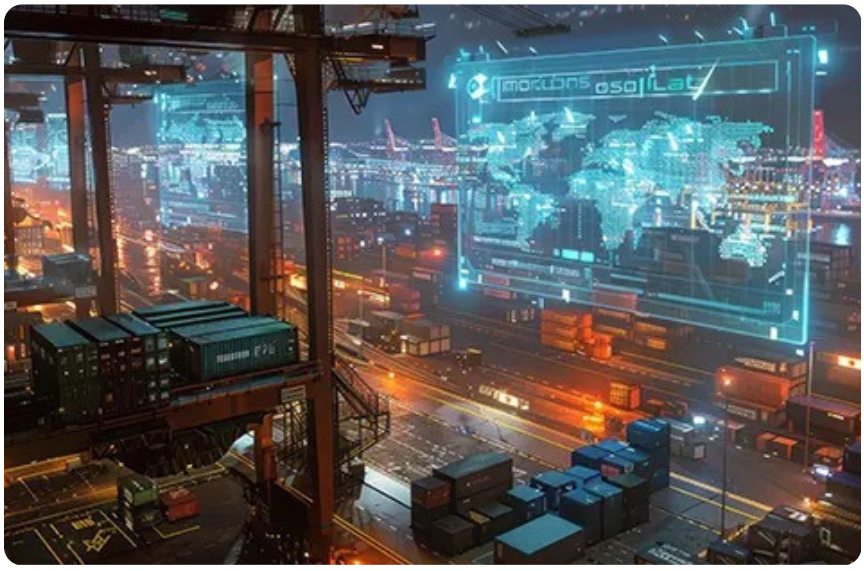
How It Works:

Real-Time Threat Simulation – Test cyberattacks safely on a virtual replica.
Continuous Monitoring – Track system health and anomalies in real time.
Predictive Security Analysis – Forecast vulnerabilities before they occur.
Incident Response Testing – Practice defense strategies without risk.
Adaptive Defense Mechanisms – Update security dynamically against new threats.



Impact Area :

Network Security – Create virtual replicas of enterprise networks to test defenses and detect vulnerabilities.
Critical Infrastructure Protection – Safeguard power grids, transportation, and healthcare systems by simulating potential attacks.
Cloud & IoT Security – Monitor and secure connected devices and cloud systems in real time.
Incident Response Training – Provide a safe environment for teams to practice handling cyberattacks.
Compliance & Risk Management – Model regulatory requirements and assess risks without disrupting real operations.



Why it Stands Out?

Cyberattacks are becoming more sophisticated, and traditional defense systems often react only after damage is done. Digital twins change this by creating a safe, virtual environment to simulate threats, predict vulnerabilities, and test responses in advance. This proactive approach reduces risks, strengthens resilience, and ensures critical systems remain secure even against evolving cyber threats.