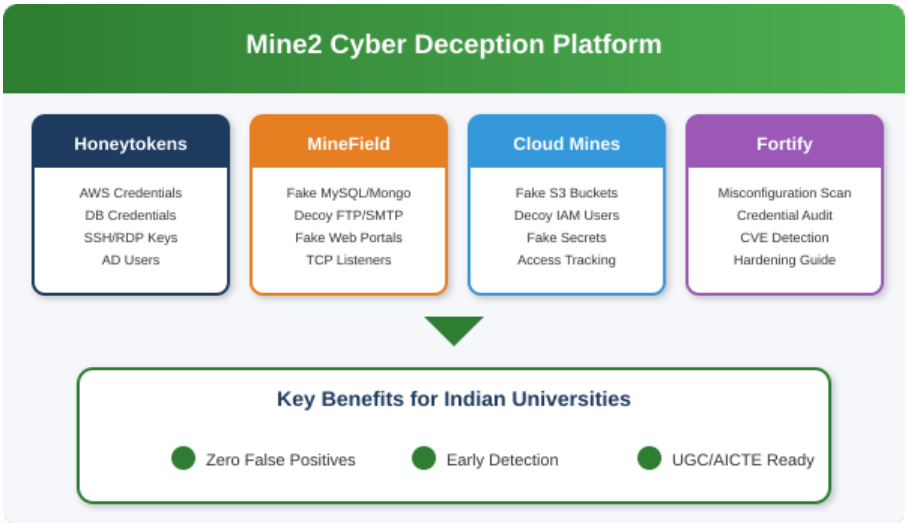
SECURING INDIAN HIGHER EDUCATION

Cyber Deception Strategies for Universities and Colleges

A Mine2 Industry Whitepaper



UGC & AICTE Compliant | CERT-In Ready | DPDP Act 2023 Aligned

www.mine2.io | info@mine2.io

Executive Summary

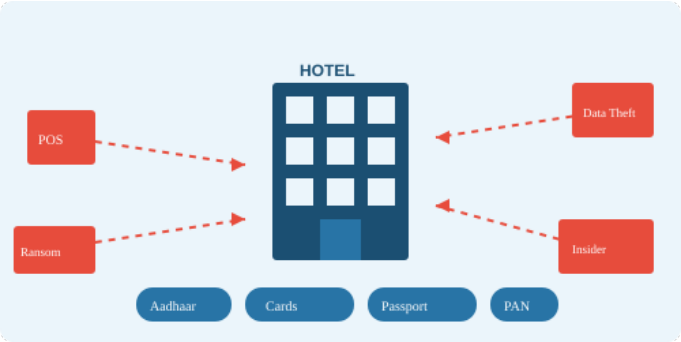
Indian higher education institutions face unprecedented cybersecurity challenges. Universities manage vast networks serving lakhs of students while protecting sensitive data including Aadhaar details, research IP, and financial records. The open nature of academic environments creates vulnerabilities that traditional defenses struggle to address.

Mine2's cyber deception platform deploys intelligent traps throughout your infrastructure that detect attackers who bypass perimeter defenses. By placing honeytokens, decoy systems, and deceptive resources across your environment, Mine2 provides early warning of breaches with near-zero false positives.

The Challenge

According to CERT-In, the education sector ranks among India's top targets for ransomware and data breaches. Contributing factors include:

- **Open Networks:** Thousands of devices across multiple campuses
- **High-Value Data:** Aadhaar, research IP, financial records, exam data
- **Budget Constraints:** Protecting assets worth crores with limited resources
- **Diverse Users:** Varying security awareness across students, faculty, and staff



Why Traditional Security Falls Short

- **Perimeter-focused:** Assumes attackers are outside; fails against compromised credentials
- **Signature-based:** Misses zero-day exploits and sophisticated APTs
- **Alert fatigue:** Thousands of false positives overwhelm small teams
- **Late detection:** Average dwell time exceeds 200 days

Mine2 Cyber Deception Platform

Honeytokens

Digital tripwires that alert when accessed: AWS/DB credentials, SSH/RDP keys, VPN configs, decoy documents (Student_Aadhaar_Data.xlsx), and AD user accounts.

MineField

Decoy network services: fake MySQL/MongoDB, FTP/SMTP servers, web portals, and IoT/CCTV interfaces. Any connection triggers immediate alerts.

Cloud Mines

AWS deception: automated discovery, intelligent suggestions, and deployment of fake S3 buckets, IAM users, and secrets with access tracking.

Fortify

Proactive hardening: misconfiguration detection, credential audits, CVE scanning, and prioritized remediation guidance.

Regulatory Compliance

UGC Expectations

Universities must demonstrate active controls, not just policies. UGC recognises universities are frequent ransomware targets and expects preparedness even without deep technical expertise. Mine2 provides demonstrable, working security mechanisms with low technical overhead.

AICTE Requirements

- Monitor systems for unauthorized access, misuse, and anomalies
- Safeguard PII, academic records, payroll, and examination data
- Prevent misuse of access by students, interns, or staff
- Mechanisms for early detection and incident response

Mine2 addresses all four requirements with honeytokens, decoys, and AD Mines that detect both external attackers and insider threats.

DPDP Act 2023

Section 12 – Data Principal Rights: Students and staff have rights to Access, Correction, and Erasure of their personal data. Universities must:

- **Track breaches** affecting personal data for mandatory notifications
- **Demonstrate protective controls** as 'reasonable security safeguards'

Mine2's detailed forensics enable breach tracking and comprehensive audit trails demonstrate proactive data protection measures to regulators.

CERT-In Rules

Mandatory incident reporting within 6 hours. Mine2's immediate alerts and detailed forensic data enable rapid detection, classification, and compliant reporting.

Key Use Cases

1. Student Information Systems

Threat: SIS/ERP systems with Aadhaar, bank details, scholarships. **Solution:** DB honeytokens, decoy exports (Student_Aadhaar_Export.xlsx), fake backup databases via MineField.

2. Shared AD Environment

Threat: Federated AD across university and affiliated colleges—one compromise exposes all. **Solution:** AD Mine honeytokens (fake Domain Admins, service accounts) detect credential harvesting, Kerberoasting, and privilege escalation across the entire federation.

3. CCTV & Biometric Systems

Threat: IoT devices with default credentials; attackers disable surveillance or manipulate attendance. **Solution:** MineField decoys emulating DVR/NVR interfaces and RTSP streams; Fortify scans for default passwords and vulnerable firmware.

4. Result & Grade Tampering

Threat: External/insider attacks on examination systems threaten academic integrity. **Solution:** DB honeytokens around result databases, decoy files (Final_Results.xlsx, Question_Paper_Bank.docx), fake exam portals, and examination-privileged honeytoken accounts.

5. Research Computing

Threat: Nation-state actors targeting DST/DRDO/ISRO-funded research IP. **Solution:** AWS/SSH honeytokens in HPC clusters, Cloud Mines with fake research S3 buckets, honeytoken documents in shared directories.

6. Ransomware Early Warning

Threat: Attackers spend weeks in reconnaissance before deploying ransomware. **Solution:** Honeytokens and MineField detect reconnaissance phase; strategic placement in backup directories detects backup destruction attempts.

7. Financial Operations

Threat: BEC, UPI fraud targeting fee collection and salary disbursement. **Solution:** Honeytokens for ERP systems, decoy NEFT/RTGS documents, fake finance admin accounts.

Key Benefits

- **Near-Zero False Positives:** Any honeytoken access = confirmed threat
- **Early Detection:** Catch attackers in reconnaissance, not after damage
- **Low Overhead:** No signatures, minimal tuning, no production impact
- **Compliance Ready:** Supports UGC, AICTE, CERT-In, DPDP Act requirements
- **Insider Threat Detection:** Same protection against external attackers and malicious insiders

Real-World Scenario

Day 1: Faculty falls for UGC grant phishing email. Attackers access workstation remotely.

Hours later: Attackers enumerate AD, discover 'IT Admin credentials' file on shared drive—a Mine2 honeytoken.

Immediate alert: Security team receives SMS/email with full context: source IP, user, file, timestamp.

Response: Workstation isolated, credentials reset, attackers expelled—all within hours, before accessing student data or exam systems.

Outcome: Avoided potential ₹5-10 Cr breach costs, DPDP notifications, and reputational damage. CERT-In reporting completed within mandate.

Getting Started

1. **Assessment:** Map critical assets and attack paths
2. **Planning:** Strategic placement of deception resources
3. **Deployment:** Days, not months—zero production impact
4. **Integration:** SIEM integration and team training
5. **Optimization:** Continuous coverage as environment evolves

Conclusion

Indian higher education faces sophisticated threats with limited resources. Traditional security leaves gaps that attackers exploit. Mine2's cyber deception provides a force multiplier—detecting threats early with near-zero false positives while supporting UGC, AICTE, CERT-In, and DPDP Act compliance.

The question is not whether your institution will face attacks—it's whether you'll detect them before significant damage occurs. Mine2 ensures you will.

Contact Mine2 Today

www.mine2.io | info@mine2.io