CLOUD SECURITY & DIGITAL FORENSICS

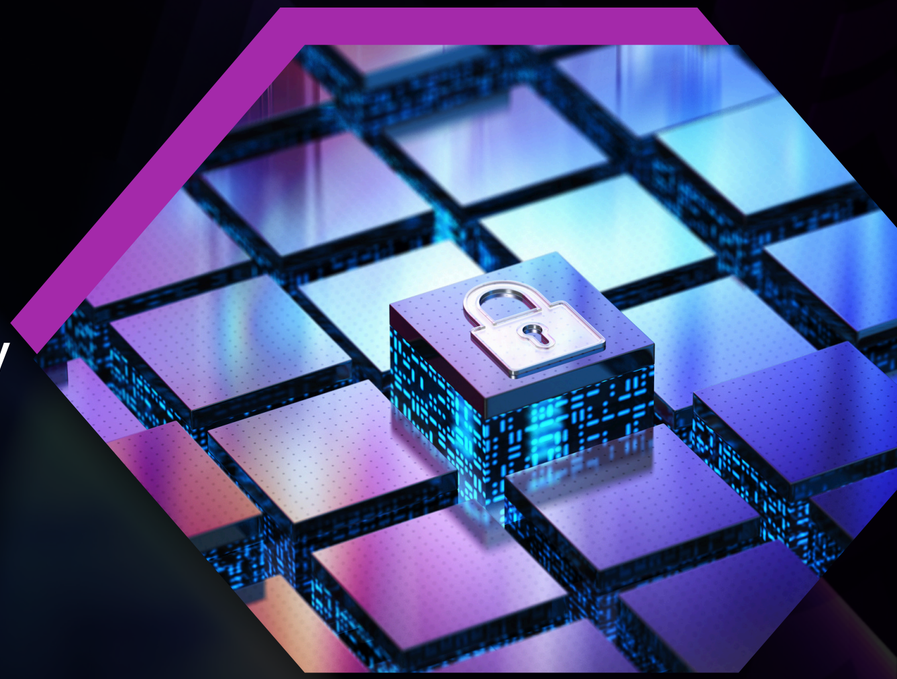
SECURING THE FUTURE OF DIGITAL INFRASTRUCTURE

Becky Passmore, Assistant Professor
Dr. Sandra Leiterman, Director of Cybersecurity Education and Outreach

University of Arkansas at Little Rock

WHY THIS MATTERS NOW

- 94% of enterprises use cloud services
- 450,000 unfilled cybersecurity jobs nationally
- 45% of data breaches are cloud-based



THE BIG PICTURE CHALLENGE

Traditional Approach

Physical Servers, controlled networks, predictable environments. Security tools are designed for the things you can touch and control

Cloud Reality

Virtual everything, distributed globally, shared infrastructure. Security must work across environments not directly controlled.

CLOUD SECURITY ESSENTIALS

MULTI- CLOUD REALITY

An average enterprise uses 5 + cloud providers. Each has different security tools, policies and interfaces.

SHARED RESPONSIBILITY

Cloud providers secure the infrastructure. While organizations secure data, applications, configurations and users.

VISIBILITY CHALLENGE

Traditional network monitoring does not work for cloud. New approaches to see across the could boundaries are needed.

REAL- WORLD CHALLENGE

Multi-Cloud Data Breach Scenario

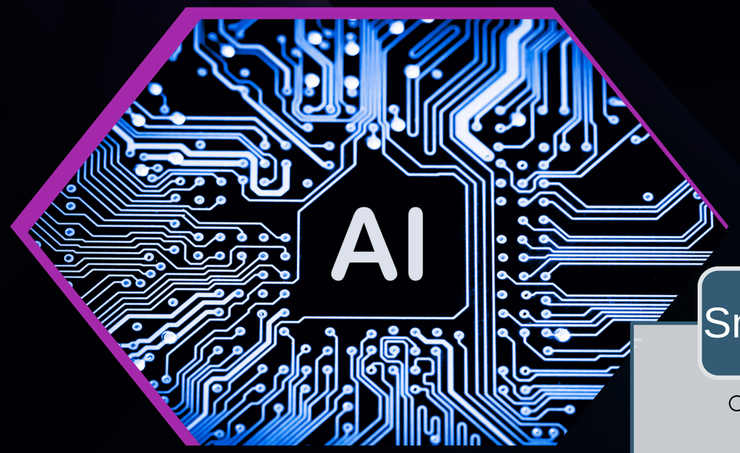
The Situation: A company using AWS, Azure, Google Cloud discovers unusual data access patterns.

The Problem: Logs are scattered across three different systems, each with different formats and retention periods.

Traditional Response: This would take weeks to correlate data manually.

Modern Solution: AI-powered tools can analyze all three environments simultaneously and identify the attack path in hours, not weeks

AI-POWERED SECURITY



Artificial Intelligence is not just a **“buzzword”** – it’s solving real cloud security problems

Smart Detection

- AI can spot unusual patterns and behaviors that humans might miss, catching threats faster.

Automated Response

- When threats are detected, AI can automatically contain them and start the investigation.

Predictive Security

- Machine learning models predict where attacks are likely to occur next.

AI SUCCESS STORY

After AI: False positives reduced by 85%, analysts focus on real threats, response time improved from hours to minutes.

Before AI: Security analysts spent 80% of their time on false alarms, investigating thousands of alerts daily

CLOUD FORENSICS

When security incidents happen, we need new ways to investigate

Digital Evidence: Logs, snapshots, and metadata become primary sources of evidence

Rapid Response: Cloud environments change quickly, so evidence must be preserved fast.

Key difference: In traditional IT, evidence was on physical servers you could touch. In the cloud, evidence is scattered across virtual environments, logs, and multiple data centers.

CLOUD INVESTIGATION REALITY

Evidence

Logs, API calls, metadata, configuration snapshots – all digital, all distributed across multiple systems.

Timeline

Cloud environments change constantly. Evidence must be preserved immediately, or it is lost, possibly forever.

Analysis

New tools automatically correlate evidence across cloud providers to reconstruct what happened.

THE EDUCATION CHALLENGE

65% of cybersecurity professionals say they lack cloud security skills

Industry Reality

- Companies desperately need professionals who understand cloud architecture, security and forensics.

Academic Gap

- Most cybersecurity programs still teach traditional network security, not cloud-native approaches.

The Solution

- Hands-on programs that combine cloud technology with real security scenarios.

ACADEMIC PROGRAM FRAMEWORK

A practical 16-week course structure that institutions can adapt

Weeks 1-4

Cloud Fundamentals & Multi-Cloud Security

Weeks 5-8

AI Security Tools & Threat Detection

Weeks 9-12

Digital Forensics & Investigation Methods

Weeks 13-16

Hands-on Labs & Real-World Scenarios

Key Features: Students work with actual cloud environments and investigate simulated security incidents.

THE PATH FORWARD

For IT Leaders

- Start planning AI-enhanced security strategies. The tools exist – implementation and communication are the challenges

For Educators

- Develop practical cloud security programs and curriculum that prepare students for real challenges.

For Everyone

- The future of digital security depends on bridging the gap between evolving technology and human expertise


****
QUESTIONS