A Meta-Analysis of the Effectiveness of Deep Learning Algorithms, Generative AI, and Agentic AI in Forecasting School Cyberattacks

Authors: Thushan Amarasinghege, Kalpdrum Passi

Presenter: Thushan Amarasinghege, Laurentian University

Email: tamarasinghege@laurentian.ca

Laurentian University
Université Laurentienne

IARIA

Thushan Amarasinghege: Biography

- Thushan Amarasinghege is a PhD researcher in Engineering Science at Laurentian University, specializing in the intersection of Artificial Intelligence and Cybersecurity.
- With over 11 years of experience in ICT education and academic leadership, he has authored numerous studies on deep learning, generative AI, and quantum computing applications.
- His recent work focuses on developing predictive models for cyberattack forecasting and mitigating the challenges of AI integration in educational environments.
- He is a Graduate Teaching Assistant for Mechatronics and holds advanced degrees in Software Technology and Information Technology.

LaurentianUniversity
UniversitéLaurentienne

IARIA

Research Interests & Current Projects

Research Interests

- **Predictive Cybersecurity:** Leveraging Deep Learning, Agentic AI, and Bayesian modeling for forecasting network vulnerabilities and school cyberattacks.
- **AI in Pedagogy:** Exploring the challenges and mitigation strategies of integrating Large Language Models and Generative AI into Engineering and K-12 curricula.
- **Future Computing Paradigms:** Investigating the practical applications of Quantum, DNA, and Silicon-based cognitive systems in scientific computing.
- **Formal Methods:** Semantic foundations for software engineering and lightweight formal methods for programming integrity.

LaurentianUniversity
UniversitéLaurentienne

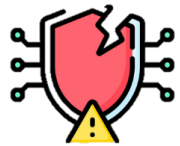
IARIA

Research Interests & Current Projects cont…

Current Projects

- **Meta-Analysis of Agentic AI:** Evaluating the effectiveness of autonomous AI agents in real-time threat detection and forecasting.
- **HPC Data Handling:** Improving data throughput and integrity for distributed scientific computing in High-Performance Computing environments.
- **Fusion Engineering & XR:** Enhancing engineering simulations through Digital Twins and Augmented Reality (AR/VR) integration.

Introduction & Problem Statement



The Problem

- Educational institutions face critical operational issues in cybersecurity due to heterogeneous user populations and limited security resources

Current Threats

- Frequent ransomware campaigns, credential theft, and data exfiltration misuse existing behavioral and infrastructure patterns.

Laurentian University
Université Laurentienne

IARIA

The Need

- Transitioning from reactive measures to predictive and adaptive security mechanisms.

Objective

- Systematic meta-analysis of studies from 2015 to 2025 evaluating AI-based security for school networks.

AI Paradigms in Cybersecurity

Laurentian University
Université Laurentienne

Deep Learning (DL):

- Utilizes CNNs, RNNs, and Transformers to identify known attack signs and abnormal traffic.

Strength

- Excellent pattern recognition in high-dimensional data.

Limitation

- Requires massive labeled datasets and lacks interpretability in dynamic environments.

Agentic AI

- Composed of autonomous software agents capable of reasoning and executing defensive actions.

Strength

- Continuous decision-making and independent operations.

Context

- Ideal for rapidly changing threat landscapes.

Methodology & Statistical Model

Laurentian University
Université Laurentienne

IARIA

Data Sources

- Academic databases (IEEE Xplore, ACM, Scopus) for peer-reviewed studies (2015–2025).

Statistical Approach

- A **Random-Effects Model** was utilized to account for differences in study populations, datasets, and network setups.

Weighted Mean Accuracy Formula

- Ensures studies with larger sample sizes have a proportional impact on results.

$$\bar{x} = \frac{\sum_{i=1}^{n} \omega_i x_i}{\sum_{i=1}^{n} \omega_i}$$

Performance Comparison (Results)

AI Paradigm	Mean Accuracy	Mean Precision	Key Strength
Deep Learning	87%	84%	Pattern Recognition
Generative AI	78%	N/A	Data Summarization & Synthetic Data
Agentic AI	**92%**	**92%**	**Autonomous Adaptation**

Performance Comparison (Results)

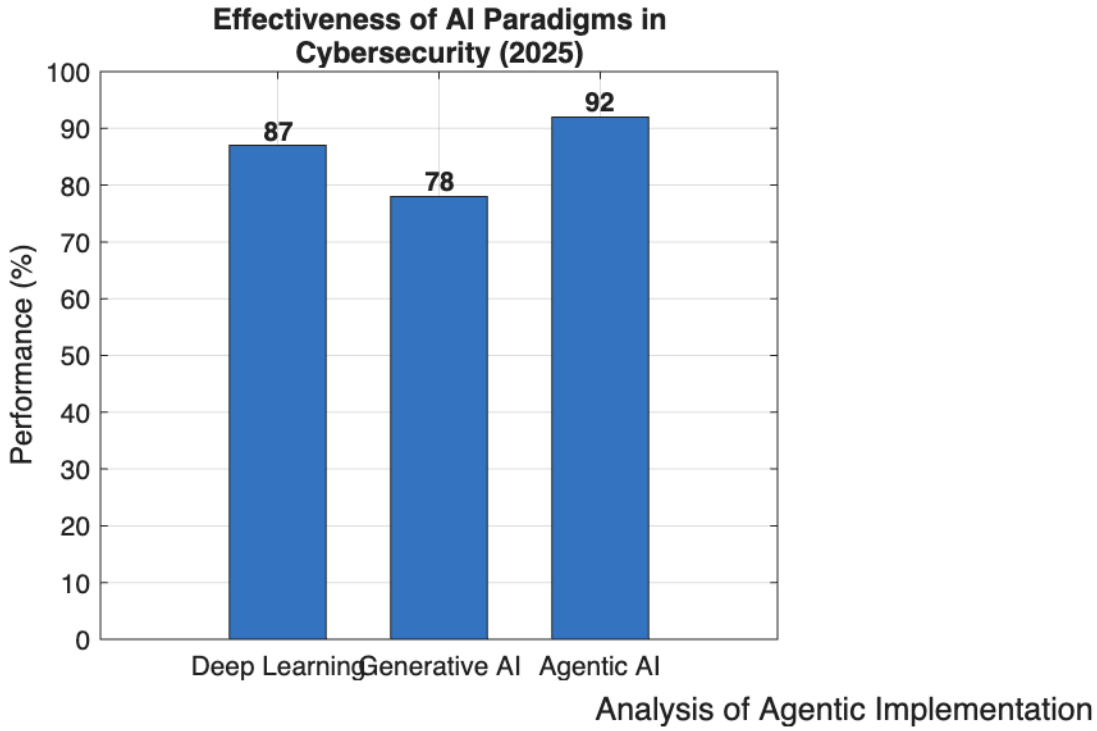


Fig. 2. Comparative Effectiveness of AI Paradigms in Cybersecurity (2025).

Observation

- Agentic AI outperforms other paradigms in accuracy and precision for contextual decision-making.

Impact on Mean Time to Respond (MTTR)

Laurentian University
Université Laurentienne

Baseline (Before Agentic AI):

- Average response time of **80 minutes**

Post-Implementation (Late 2025):

- Average response time dropped to **40–60 minutes** on a normalized scale.

Impact on Mean Time to Respond (MTTR)

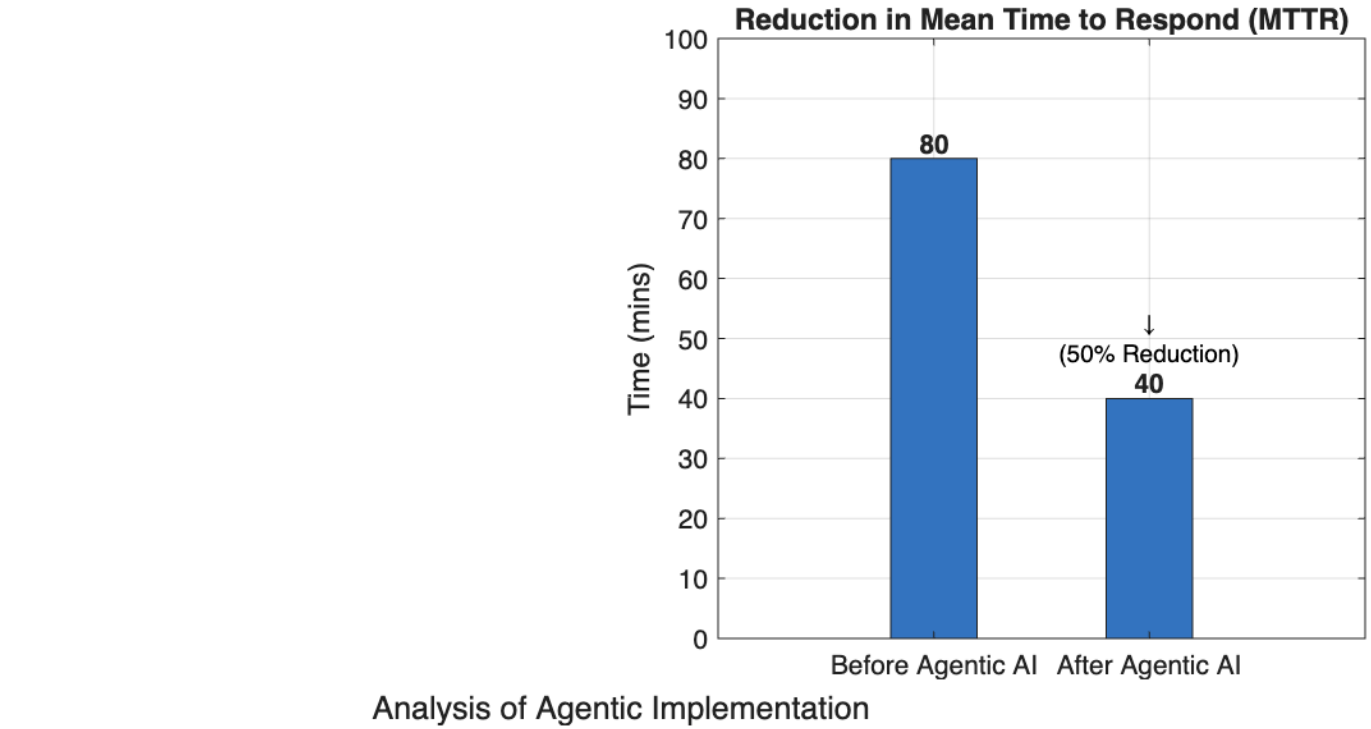


Fig. 1. Comparative reduction in Mean Time to Respond (MTTR) before and after Agentic AI implementation

Key Finding

- A **50% reduction** in MTTR (Optimistic Estimate) allows security teams to address threats twice as fast.

Benefit

- Reducing the "window of opportunity" for attackers immediately after threat detection.

Aggregated performance comparison

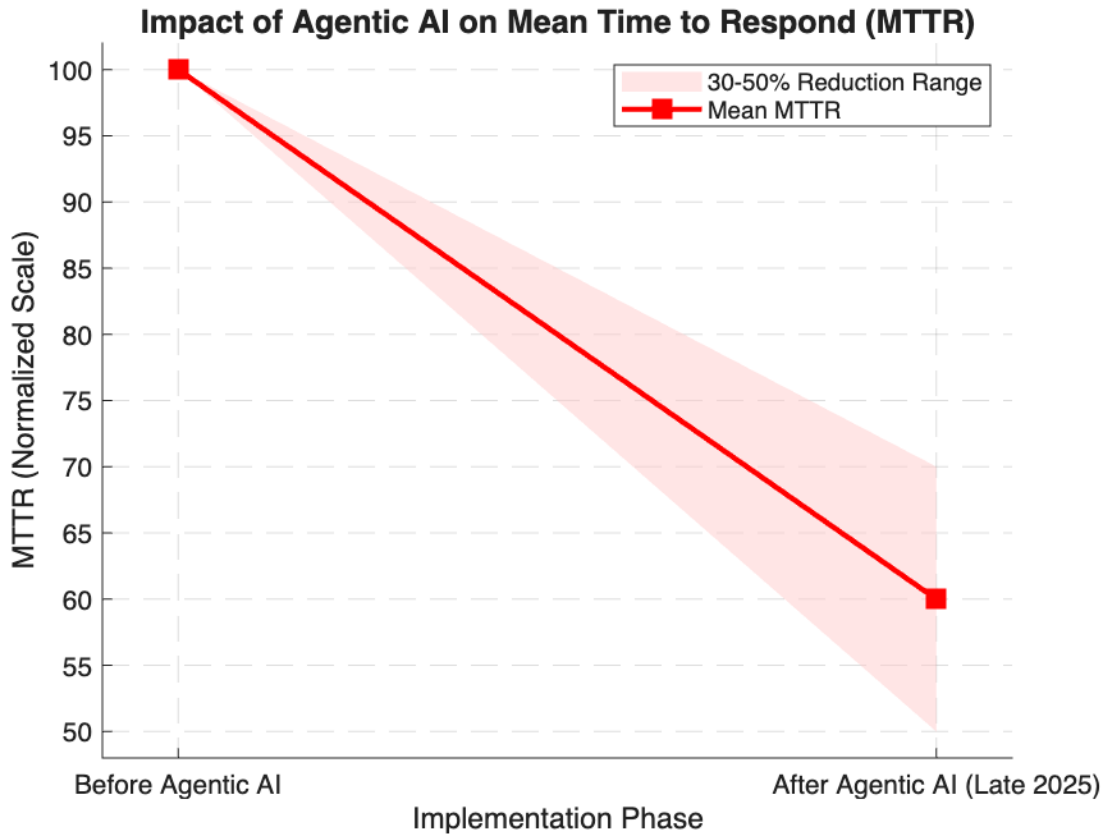


Fig. 3. Aggregated performance comparison

Proposed Four-Stage Pipeline

- **Data Input:** Raw school network traffic (logins, web activity, cloud access).
- **Deep Learning:** Identifying "Normal Behavioral Patterns" within the network.
- **Generative AI:** Anomaly detection and creating synthetic "fake" attacks to train the system for zero-day threats.
- **Agentic AI:** Autonomous Response (e.g., isolating a server or blocking a user) without waiting for human intervention.

Proposed Four-Stage Pipeline

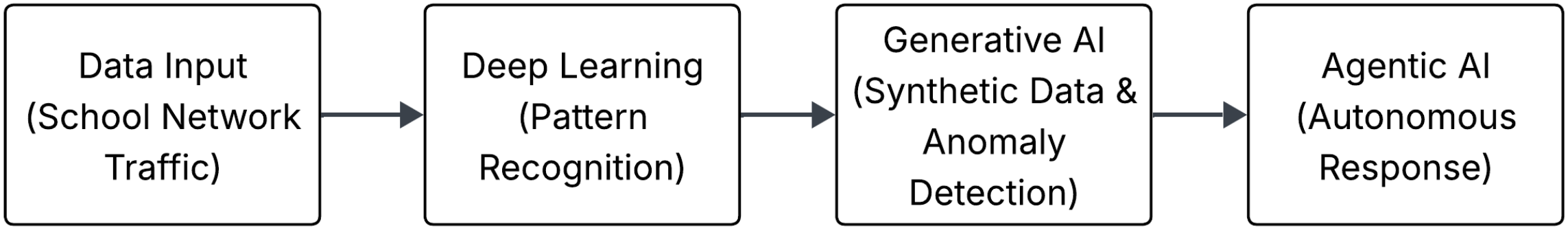


Fig. 4. The Evolution of Cybersecurity

Conclusion & Future Directions

- **Conclusion:** Combining Deep Learning's pattern recognition with Agentic AI's autonomous decision-making significantly enhances cybersecurity resilience.
- **Critical Challenge: Governance Complexity**—the need for human-in-the-loop safeguards to prevent accidental system shutdowns.

Future Work:

- * **Federated AI** for enhanced data privacy.
- Longitudinal evaluations in live school environments.
- Formal ethical and accountability frameworks for autonomous agents.

Video Link

https://youtu.be/f-E2QrsFvT4

Laurentian University
Université Laurentienne

IARIA