DECEMBER | 2025
DEPARTMENT OF INFORMATION TECHNOLOGY

Future Institute of Engineering and Management
https://www.futureeducation.in/fiem/

IT INSIGHTS

Where Information Meets Illumination...

B.Tech in Information Technology

Voice of the Department of Information Technology (FIEM)

Healing Through Code: Role of Information Technology in Music Therapy

- Preserving Therapeutic Traditions

Music therapy, rooted in centuries of cultural practice, is being revitalized through Information Technology. What was once shared in intimate settings is now safeguarded by digital archives, high fidelity recordings, and secure cloud platforms. This ensures therapeutic compositions, guided sessions, and research findings remain accessible for practitioners and patients alike.

- Enhancing Sound for Healing

Advanced signal processing and acoustic modeling allow therapists to deliver music with precision. From noise reduction to personalized soundscapes, IT ensures that therapeutic sessions maintain clarity and resonance, amplifying the calming and restorative effects of music.

- AI Driven Personalization

Artificial Intelligence is transforming music therapy by tailoring interventions to individual needs. Intelligent systems can analyze brainwave patterns, track emotional responses, and recommend therapeutic ragas or rhythms. Virtual assistants and mobile apps extend access, enabling patients to benefit from guided therapy even outside clinical environments.

- Expanding Access and Reach

Digital platforms and telehealth solutions have broken barriers of geography. Patients can now participate in remote therapy sessions, while data analytics helps institutions measure outcomes, refine techniques, and promote holistic well being across diverse populations.

Prof. Debjyoti Basu

- Immersive Healing Experiences

Virtual reality and interactive multimedia are creating immersive therapeutic environments. Patients can engage with calming visuals, guided soundscapes, and interactive exercises, blending tradition with modern engagement tools to foster deeper emotional and psychological healing.

- The Silent Enabler

Behind these innovations stands the IT Department - the silent enabler of transformation. By integrating technological expertise with therapeutic practice, IT ensures that music therapy not only adapts to the digital age but thrives as a powerful tool for healing and well being.

-Prof. Debjyoti Basu
Assistant Professor
Department of Information Technology

Agentic AI in Cybersecurity: A Technical Write-up

Agentic Artificial Intelligence (AI) represents a paradigm shift in cybersecurity, moving beyond traditional automation and reactive models towards autonomous, goal-driven systems capable of independent decision-making, planning, and action. Unlike conventional AI that often serves as a pattern recognition tool for human analysts, an Agentic AI system functions as an intelligent agent to achieve complex security objectives with minimal human intervention.

1. Technical Architecture of an AI Agent

The core of Agentic AI is an intelligent agent, which operates on a continuous loop of sensing, reasoning, acting, and learning. This architecture typically comprises several interconnected components:

- Perception Layer (Sensing): The agent continuously collects and processes data from its environment. In cybersecurity, this involves ingesting vast amounts of data from *Security Information and Event Management (SIEM) systems*, *Endpoint Detection and Response (EDR)* solutions, network traffic logs, cloud configuration audit trails, and threat intelligence feeds.

Ms. Jaita Chakraborty

This layer often utilizes Natural Language Processing (NLP) and Machine Learning (ML) models to filter noise and identify raw security signals.

- Reasoning and Planning Engine: This is the cognitive core, where the agent interprets the gathered data, formulates a strategy, and breaks down complex security goals into a sequence of executable sub-tasks.
  1. Goal Setting: Based on pre-defined security policies or dynamic threat assessment, the agent sets an objective (e.g., "Investigate and contain lateral movement on endpoint X").
  2. LLM Integration: *Large Language Models (LLMs)* are often integrated here, providing the agent with high-level reasoning, contextual understanding, and the ability to generate dynamic plans or code to achieve its goals.
  3. Decision-Making: The agent evaluates multiple potential actions using models like *Reinforcement Learning (RL)*, *probabilistic models*, or *expert system* logic to select the optimal, risk-aligned action.

- Action Layer (Execution): The agent executes the chosen actions by interacting with external security tools and infrastructure via *Application Programming Interfaces (APIs)*. Actions can include:
  1. Quarantining a host via an *EDR/Network Access Control (NAC)* tool.
  2. Blocking an IP address at a *firewall* or *Web Application Firewall (WAF)*.
  3. Initiating a password reset or *multi-factor authentication (MFA)* challenge for a compromised account.

- Memory and Learning: This layer ensures continuous improvement and context maintenance.
  1. Episodic Memory: Stores details of past incidents, investigations, and actions taken.
  2. Continual Learning: Uses feedback loops from action outcomes to refine the underlying ML models, improving the accuracy of future perceptions, reasoning, and decision-making.

A visual representation of the core architectural components of an AI agent: fig.1

2. Key Applications in Cyber Defense

Agentic AI's autonomy and speed make it uniquely suited to address the most pressing challenges in modern *Security Operations Centers (SOCs)*:

Application Area	Application Area	Application Area
Autonomous Threat Detection	Continuously monitors the attack surface (network, cloud, endpoints) for subtle anomalies, correlating events across disparate systems to identify sophisticated Advanced Persistent Threats (APTs).	Real-time, context-aware anomaly detection that goes beyond static rulesets.
Immediate Incident Response	Executes multi-step containment and remediation playbooks without human latency. The agent can auto-triage alerts, enrich data with threat intelligence, isolate affected assets, and initiate forensic data collection.	Significant reduction in *Mean Time To Detect (MTTD)* and *Mean Time To Respond (MTTR)*, minimizing attack window.
Alert Triage and Orchestration	Filters high volumes of alerts, intelligently grouping, prioritizing, and resolving false positives. It integrates with Security Orchestration, Automation, and Response (SOAR) platforms to manage complex workflows.	Dramatic reduction in alert fatigue for human analysts, allowing them to focus on high-stakes, novel threats.
Cloud Security Posture Management	Proactively scans Infrastructure-as-Code (IaC) templates and live cloud environments (*AWS, Azure, GCP*) for misconfigurations (e.g., overly permissive IAM roles, open S3 buckets) and executes immediate corrective actions.	Continuous governance and automated remediation of configuration drift and compliance violations.
Vulnerability Analysis	Automates the entire vulnerability management lifecycle, from scanning and triage to exploitability analysis and patch deployment prioritization based on real-world threat intelligence.	Faster, risk-based vulnerability management.

Illustration depicting Agentic AI in action within a cybersecurity context, highlighting its various applications:fig.2

3. Security Challenges and Mitigation Strategies

The introduction of autonomous agents creates a new attack surface and unique security risks that must be addressed through a "security-by-design" approach.

Agentic AI Risk	Description	Technical Mitigation Strategy
Prompt/Data Injection	Malicious inputs are fed to the agent (e.g., through log data or a seemingly harmless email) to manipulate its reasoning or trick it into taking unintended, harmful actions.	Strict Input Validation and Sanitization at the Perception Layer. Implement Guardrails within the LLM to restrict sensitive actions, and use Adversarial Training to improve model resilience.
Cross-Agent Task Escalation	A compromised low-privilege agent exploits the trust mechanism between agents (Multi-Agent Systems - MAS) to impersonate a higher-privilege agent and gain unauthorized access or escalate tasks.	Apply Zero Trust Principles to agent identities. Implement granular, context-aware privilege management (Least Privilege) for each agent's tool access (Action Layer).
Autonomous Policy Violation	A poorly constrained agent, in its pursuit of a goal, executes an action that violates a critical business policy (e.g., shutting down a core business system).	Mandate a "*Human-in-the-Loop" (HITL)* process for high-impact actions. Implement clear, auditable Governance and Safety Filters to enforce constraints on the Reasoning Engine.
Model Extraction/Theft	Adversaries query the agent to infer or steal the underlying proprietary LLM or specialized security model, which can then be used to craft highly effective, targeted evasion attacks.	Implement API Rate Limiting, Watermarking, and Output Obfuscation to make model inference difficult. Secure models in protected, strictly access-controlled server environments.
Untraceable Data Leakage	Autonomous data exchange between agents or external systems (e.g., for threat enrichment) inadvertently includes and exposes sensitive information (PII, confidential data) without proper audit trails.	Enforce Mandatory Logging and Auditing of all agent actions and data flows. Use Differential Privacy or data tokenization for sensitive information processed by the agent.

Image illustrating the security risks and corresponding mitigation strategies for Agentic AI in cybersecurity:fig.3

Fig:1

Fig:2

Fig:3

National-Level Dance Achievement

Fig.: Glimpses of Srija's performance and the certificate received

A *first-year* student, ***Srija Chowdhury***, showcased her talent at the prestigious ***Bharat Sanskriti Utsab 2025***, a *national-level cultural festival* honoring the richness of Indian art and culture. Competing in the *Folk Group Dance category (Gandharva)*, Srija delivered a vibrant, well-coordinated, and expressive performance, helping her team secure an impressive **3rd place**. Held at the Calcutta Blind School, Kolkata, the competition featured several highly talented groups from across the country, making this achievement a remarkable addition to the institution's cultural accolades.

Cultural Achievement at Umang 2025

Ms. Esha Dalal, a *2nd-year* IT student, won the *Solo Classical Dance competition at* ***Umang 2025***, The Bhawanipur Education Society's annual cultural fest. She emerged as the **winner** by captivating the audience and judges with a self-choreographed Odissi performance set to her own musical composition, highlighting the beauty of traditional instruments and demonstrating both creative expression and technical mastery. Her performance featured reciting the taal while dancing, an engaging jugalbandi, and intricate sequences, reflecting her exceptional skill and dedication. Competing against over 25 participants from reputed colleges across Kolkata, her victory is a testament to her hard work & talent.

Fig.: Glimpses of Ms. Esha Dalal's winning performance at Umang 2025

Stellar Performance by 3rd Year IT Students in NPTEL

Fig.: Topper certificate awarded by NPTEL to Tathagata Das

The Department proudly celebrates the exceptional achievement of **Tathagata Das**, a *3rd Year* IT student, who emerged as the **Topper** of the ***NPTEL*** *Online Certification Examination* - **Programming in Java** with an outstanding ***95%*** score. He was awarded the ***Gold certification*** *and secured a prestigious position among the* ***Top 5% performers nationwide***, reflecting his academic excellence, disciplined preparation, and advanced technical proficiency. This remarkable accomplishment brings great honour to the department and stands as a benchmark of excellence for his peers.

In addition to this distinguished success, several other 3rd Year IT students demonstrated commendable academic merit across various certification categories. In the **Gold category**, *Madhumita Saha (94%), Soham Pal (94%), Madhurima Dutta (92.27%), Priyanshu Kanji (91%), Soham Roy Chowdhury (91%) and Arnab Paul (90%)* showcased exemplary performance, reflecting strong conceptual clarity and consistent dedication. Achieving the **Silver Elite category**, *Titli Roy (85%) and Sahina Khatun (84%)* displayed commendable academic consistency and a solid grasp of core concepts, while *Niharika Das (66%) and Sayan Das (62%)*, who earned the **Elite category**, exhibited perseverance and sound foundational understanding. Collectively, these achievements underscore the department's commitment to academic excellence and the students' dedication to continuous learning, and we extend our heartfelt congratulations to all achievers on their well-deserved success.

Participation in National Art Fest 2025

Ms. Madhurima Dutta, a *3rd year* IT student, participated in the *National Art Contest* under ***The Indian Art Fest, 2025***, where her artwork was showcased and appreciated at the national level. She received a Certificate of Appreciation for her creative contribution, encouraging and highlighting young artistic talent across the country.This achievement reflects her continued dedication to the arts and creative expression.

Fig.: Certificate of Appreciation awarded to Madhurima Dutta

Thanks for Reading...

NEWSLETTER OF INFORMATION TECHNOLOGY

EDITORIAL BOARD MEMBERS

Snehan Bala
(2024-2028)

Madhurima Dutta
(2023-2027)

Sahina khatun
(2023-2027)

ADVISORY BOARD MEMBER

Prof. Ishani Das

Connecting You to the Department of Information Technology

For Queries and Support, Reach Out to Us :
ishani.das@teamfuture.in