VIDYAVARDHINI'S COLLEGE OF ENGINEERING AND TECHNOLOGY
K.T. Marg, Vasai(W) Dist-Palghar, 401201
DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

AI&DS Newsletter
Volume 2; Issue 1; November 2024

INTELLIVERSE

Generative AI: Revolutionizing Cybersecurity to Prevent Security Breaches

What is a Security breach?

A security breach occurs when an unauthorized party gains access to a system, network, or data, bypassing security measures. This can lead to data theft, system damage, or exposure of sensitive information. Common types of security breaches include hacking, where attackers exploit system vulnerabilities; malware attacks that use viruses, ransomware, or spyware to steal or corrupt data; and phishing scams that trick users into revealing credentials. To prevent security breaches, organizations should implement strong authentication methods like multi-factor authentication (MFA), use firewalls and intrusion detection systems.

Introduction:

Generative AI represents a groundbreaking advancement in the field of artificial intelligence, distinguished by its ability to create new, synthetic content that mimics real-world data. Unlike traditional AI systems, which primarily focus on analyzing and interpreting existing data to make decisions or predictions, generative AI is designed to produce novel outputs. This capability opens up a myriad of possibilities across various industries, from art and entertainment to healthcare and cybersecurity.

At its core, generative AI leverages machine learning algorithms to learn patterns from large datasets and generate new content that resembles the original data. This process involves training models on extensive datasets, enabling them to understand and replicate the underlying structures and characteristics of the data.

Impact of Generative AI on Security Breaches

Generative AI profoundly impacts security breaches, enhancing cybersecurity measures and introducing new risks. Here are some key aspects of its impact:

- **Enhanced Threat Detection and Response:**

Generative AI can significantly improve threat detection by learning from historical security data and identifying patterns indicative of cyber threats. This proactive approach allows security systems to respond more rapidly and effectively to potential breaches, minimizing their impact, and enabling predictive defense strategies.

- **Synthetic Data for Training:**

Generative AI can create synthetic data that mimics real data without exposing sensitive information. This synthetic data can be used to train security models and algorithms, enhancing data privacy and reducing the risk of breaches, while also allowing for more robust testing environments.

- **Automation of Security Measures:**

Generative AI streamlines cybersecurity by automating routine tasks such as configuring firewalls or scanning for vulnerabilities. This automation enhances operational efficiency and reduces the likelihood of human error, which is often a significant vulnerability in cybersecurity defenses, thereby allowing security teams to focus on strategic initiatives.

GEN-AI Models

- Threat Intelligence Analysis – Google Threat Intelligence uses generative AI (Gemini AI) to analyze and summarize vast threat databases, helping security teams quickly identify emerging threats.
- Automated Risk Assessment – Secureframe's Comply AI for Risk automates security risk evaluations, providing organizations with insights into vulnerabilities and suggested remediation actions.
- Malicious Code Detection – VirusTotal Code Insight uses Google's Sec-PaLM generative AI model to analyze and summarize code behavior, identifying potential malware before it spreads.
- Phishing and Social Engineering Defense – ZeroFox's FoxGPT scans and summarizes large datasets to detect phishing attempts and impersonation threats in real time.
- Dark Web Monitoring – Flare's Threat Flow analyzes underground forums and leaked data, summarizing relevant threats for organizations to act on before they escalate.

Generative AI Tools for Avoiding Security Breaches

Generative AI has emerged as a pivotal technology in enhancing cybersecurity measures across organizations. By leveraging advanced algorithms, these tools can detect threats, assess risks, and automate incident responses with unprecedented efficiency

Generative AI is transforming cybersecurity by enhancing threat detection, risk assessment, and incident response. Tools like Secureframe's Comply AI automate risk assessments and provide remediation guidance, helping organizations address vulnerabilities efficiently. Google's Threat Intelligence, powered by the Gemini AI model, enables conversational threat analysis using extensive security data. Tenable ExposureAI offers natural language searches and attack path narratives, simplifying exposure management. SentinelOne's Purple AI enhances threat hunting with a natural language interface and behavioral analysis. VirusTotal Code Insight, leveraging Google's Sec-PaLM model, summarizes code behavior to detect malicious scripts. ZeroFox's FoxGPT accelerates intelligence analysis for phishing and account takeover threats, while Flare's Threat Flow streamlines threat intelligence with tailored, AI-generated summaries.

Departmental Activities

EVENTS

TECHX - Product Showcase

The NSDC's 'Tech X' showcase, led by Akshay Bharambe, featured student-developed AI and data science products. Exhibits like Parking Pal and Solomon CMS highlighted practical applications of machine learning and database systems.

TechBlitz

VCET's NSDC hosted "TechBlitz" on March 15th, 2024, showcasing student talent in AI-driven web development, UI/UX design, and data science. The event highlighted the intersection of technology and education within the AI and Data Science department.

Code-O- Fiesta

Code-O-Fiesta 2024 was held on 20th September at Vidyavardhini's College of Engineering and Technology, organized by the departments of Artificial Intelligence and Data Science & Computer Science Engineering (Data Science).

SEMINARS

Expert Lecture on PowerBI

On March 1st, 2024, VCET's NSDC hosted Ms. Isha Prakash, Testriq's Data Science Head, for a Power BI expert lecture. The session focused on practical data visualization, using e-commerce examples.

NVIDIA Jetson AI Edge Device

This Seminar was held in the collaboration of EXTC department and AI & DS department. Chief Guest and the speaker was Mr. Anil Sarode. The seminar introduces participants to NVIDIA Jetson AI Edge devices. It covers the device's architecture, features, and applications, followed by live demos with DeepStream and Generative AI

INDUSRIAL VISIT

An industrial visit is a valuable learning experience that bridges theoretical knowledge with real-world applications. Visiting companies like Testriq, specializing in quality assurance and software testing, and Contentstack.

TOPPERS (A.Y. 2023-2024 EVEN SEM)

SE SEM 4

- Dnyanesh Baburao Panchal 10
- Priyanka Narendra Bhandari 9.87
- Jaffari Mohammed Ali 9.3

TE SEM 6

- Devharsh Jha 9.64
- Hemani Maurya 9.45
- Neha Singh 9.45
- Sakshi Karande 9.32

BE SEM 8

- Chetan Sakpal 9.5
- Devashree Pawar 9.27
- Prachi kadam 9.18

Placements & Higher Studies

A total of 20 students have been successfully placed through placement program.
A number of 4 students have chosen to pursue higher education, opting to further their academic and professional growth in renowned Academies.

Industry Interaction: MoU

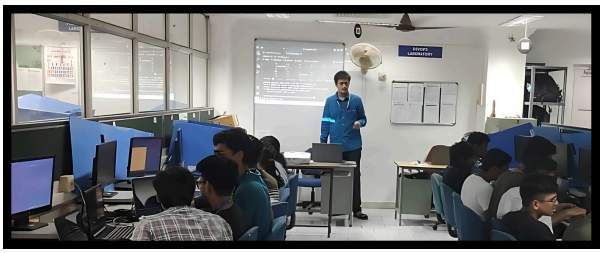
Sr. No	Organization with which the MoU was signed
1.	Fafadia Tech
2.	Prime Softech Solutions Pvt. Ltd
3.	HKI Infotech
4.	Edba Academy
5.	TESTRIQ QA Lab LLP, Mumbai
6.	Parking Pal

Student Achievements

- The team of Pritesh Verma, Varun Soni, Harshvardhan Surve, and Anum Sharif won the 1st prize in the 24-hour Hackathon 'Avalon' at Terna College of Engineering and Technology.
- They also secured the 1st prize in Code-O-Fiesta 2023, an inter-college event held at VCET.
- A team led by Shubham Jangid secured 1st position in the Business Plan Presentation held at St. John College of Engineering and Management.
- The team of Pritesh Verma, Varun Soni, Harshvardhan Surve, and Anum Sharif won the 1st prize in the NextTech Hackathon at Vasantdada Patil Pratishthan's College of Engineering.
- Chinmay Satam won the 1st prize in Solo Singing at L. R. Tiwari College of Engineering.
- A team consisting of Pritesh Verma, Varun Soni, Harshvardhan Surve, Sharib Khan, and Aryan Darade won the 1st prize at HACKSRM 5.0, a hackathon organized by SRM University, Andhra Pradesh.
- Esplanade Education Society's Niranjana Majithia College of Commerce achieved 3rd rank, with Chinmay Satam as the winner.
- Konisha Thakare and her team secured 1st place in the TechBlitz UI/UX Designing competition, an inter-college event.
- Shikha Choudhary conducted an Expert Lecture on AI & ML for the Engineering Department at Government Polytechnic Mumbai on March 22nd and 23rd, 2024, in offline mode for first and second-year diploma students.

Intra Institutional Internship on 'Data Science' from 10/06/2024 to 21/06/2024 organized by the Department of Artificial Intelligence and Data Science in coordination with IIIC, VCET and in collaboration with Codex Technologies.

Intra Institutional Internship on 'Generative AI' from 10/06/2024 to 21/06/2024 organized by the Department of Artificial Intelligence and Data Science in coordination with IIIC, VCET and in collaboration with Citius CloudServices and ContexIQ.



VCET TECHZETTE विसीईटी ज्ञानपत्र
ISSN: 2584-0886 (Online)

TechZette, hosted by Vidyavardhini's College of Engineering and Technology, is a collaborative technical blog on AI, data science, and more, featuring articles from faculty, experts, and students. You can contribute your own articles too!

Staff Incharge: Ms. Sweety Patil & Ms. Rujuta Vartak

Editors:
Ms. Ojasi Prabhu
Mr. Pradeep Rathod
Ms. Saloni Sutar
Mr. James Lewis

Technical Team:
Mr.Parth Raut
Ms. Konisha Thakare
Mr. Saurabh Vishwakarma
Mr. Soham Sawant