VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE

AI&DS Insights

Monthly Awareness Bulletin

ISSUE 06 | February 2025

"He who conquers himself is the mightiest warrior"

Republic Day

The Artificial Intelligence and Data Science department celebrated Republic Day with patriotic fervor and enthusiasm. Faculty members came together, dressed in shades of saffron, white, and green, to honor the spirit of unity and freedom. The department was adorned with the tricolor, featuring vibrant decorations, inspiring posters, and a beautifully crafted rangoli symbolizing national pride. The celebration included a flag-hoisting ceremony, thought-provoking speeches, and a heartfelt tribute to the nation's rich heritage. The event resonated with patriotic songs and spirited discussions, fostering a deep sense of unity and respect for the country. Moments from this memorable celebration were shared on social media, receiving heartfelt appreciation and making it an inspiring occasion for all.

TOON

Faculty Article

Federated Learning – The Next Frontier in Privacy-Preserving AI

In this edition of our e-bulletin, we explore federated learning, a transformative approach to machine learning that is reshaping how we build AI systems while safeguarding privacy. As data privacy concerns grow and regulations tighten, federated learning offers a promising solution for industries looking to harness the power of AI responsibly.

What is Federated Learning?
Federated learning (FL) is a decentralized machine learning technique where models are trained across multiple devices or servers without transferring raw data to a central location. Instead, the model travels to the data, learns locally, and only shares updates with a central server. This ensures that sensitive information remains on the device, addressing critical privacy and security concerns.

How Does Federated Learning Work?

1. Initialization: A global model is created on a central server.
2. Distribution: The model is sent to participating devices (e.g., smartphones, IoT devices, or hospitals).
3. Local Training: Each device trains the model using its own data.
4. Update Sharing: Only the model updates (not the raw data) are sent back to the server.
5. Aggregation: The server combines updates to improve the global model.

This process repeats, enabling continuous learning without compromising data privacy.

Why Federated Learning Matters

1. Privacy Preservation: Keeps sensitive data on local devices, reducing the risk of breaches.
2. Regulatory Compliance: Helps organizations adhere to strict data protection laws like GDPR and HIPAA.
3. Efficiency: Leverages the computational power of edge devices, reducing the need for centralized infrastructure.
4. Personalization: Enables tailored AI experiences without sharing personal data.

Real-World Applications

- Healthcare: Hospitals collaborate to train AI models for disease diagnosis without sharing patient records.
- Finance: Banks detect fraudulent transactions using local transaction data, ensuring customer privacy.
- Smart Devices: Improves features like predictive text and voice recognition on smartphones without uploading user data.
- Autonomous Vehicles: Enables self-driving cars to learn from each other's experiences without sharing sensitive data.

Challenges and Opportunities
While federated learning is revolutionary, it faces challenges such as communication overhead, data heterogeneity, and security risks. However, ongoing research in secure multi-party computation, differential privacy, and efficient communication protocols is addressing these issues, paving the way for broader adoption.

The Future of Federated Learning
As industries increasingly prioritize privacy and security, federated learning is poised to become a cornerstone of AI development. Companies like Google, Apple, and NVIDIA are already investing heavily in this technology, signalling its potential to transform sectors ranging from healthcare to finance.

Conclusion
Federated learning represents a paradigm shift in how we approach AI, offering a way to harness the power of data while respecting privacy. As the technology matures, it has the potential to unlock new possibilities across industries, from personalized healthcare to smarter cities. In a world where data privacy is no longer optional, federated learning is not just a technical innovation—it's a necessity. The future of AI is collaborative, decentralized, and privacy-preserving. Federated learning is leading the way.

Dr. Milind Kulkarni
Professor, (AI&DS),VIT Pune

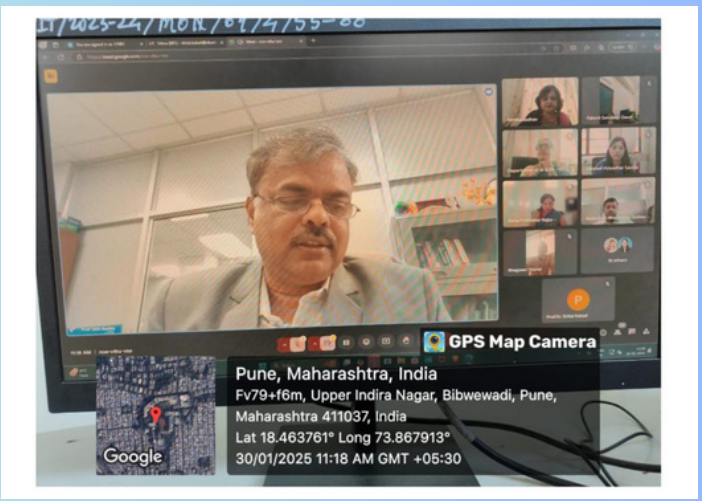
Activities

The FDP on "Academia-Industry Synergy: Leveraging Expertise for Mutual Growth" aimed to bridge the gap between academic institutions and the industry by fostering collaboration. Its primary goal was to share knowledge, align academic outcomes with industry needs, and explore innovative approaches for mutual growth, benefiting both educators and professionals while enhancing the overall quality of education and workforce readiness.

By VAISHALI RAJPUT, SURBHI KAKADE

A lecture on STELA 5.0 AI: System for Teaching, Education, Learning, and Assessment Framework was held online on 30th January 2025 from 11 am to 12:30 pm. The session was coordinated by Dr. Shital Dongre and Dr. Varsha D. Jadhav, with Dr. S. Ramanarayana Reddy, Professor & HoD at IGDTUW, as the resource person. He introduced STELA 5.0 AI, an innovative framework for teaching Python, AI, and ML. The platform integrates theory, hands-on experiments, projects, quizzes, assessments, and real-time feedback. Utilizing AI and ML APIs, it provides personalized learning experiences and supports web, iOS, and Android platforms. Dr. Mukund M Kulkarni also introduced the guest to Vishwakarma Institute of Technology. Faculty members from Vishwakarma Institute of Technology, Pune and Vishwakarma Institute of Information Technology, Pune attended the session.

By Dr. VARSHA JADHAV



An industry visit to e-Zest by Accion Labs was organized, focusing on Product Deployment. Students Aarya Pise, Gayatri Nangare, Amarsinh Nangare, and Radhika Jaju participated in the visit, gaining insights into real-world product deployment processes. The visit was guided by Faculty Members Surabhi Kakade and Neha Rajas, offering students valuable industry exposure and learning opportunities.

By SURBHI KAKADE

Activities

At BITOSA Pune event on Engineering a Digital Future - The Role of Digital and Cyber Security.

By SURBHI KAKADE

Project Demo- Silicon Stack- TY C Students on GenAI Project Development for e-Zest by Accion Labs on Jan 17th
Students
Aarya Pise
Gayatri Nangara
Radika Jaju
Amarsinh Nangare
Faculty
Surabhi Kakade
Neha Rajas

Faculty Publications

Name	Summary
Ganesh Shankar Ubale	Published Research Paper in Scopus Indexed International Conference on Innovations and Challenges in Emerging Technologies (ICICET) 2024 on 06 August 2024. Paper Title is "CarLINK: AI Driven Traffic Adviser for Automobiles "
Lokesh Sheshrao Khedekar	Paper Title: Cost-Effective Dual-Axis Joystick with Haptic Feedback for Enhanced User Interaction
Lokesh Sheshrao Khedekar	Paper Title: AgriTech: Technology Driven E-Commerce Platform for Sustainable Agricultural Development
Dr. Hrushikesh Joshi	The paper, "Advanced Techniques in Post-Quantum Cryptography for Ensuring Data Security in the Quantum Era," outlines the need for post-quantum cryptography (PQC) due to the threat posed by quantum computers to current security methods. It discusses advanced PQC techniques that ensure data security against quantum attacks.
Dr Shubham Joshi	Presented a paper titled "Necessity of Information Security in Safeguarding Smart Grid Infrastructure" at the 5th International Conference on Smart Electronics and Communication (ICOSEC 2024). The paper is published in the conference proceedings and indexed in Scopus.

Faculty Publications

Name	Summary
Lokesh Sheshrao Khedekar	A BLOCKCHAIN BASED JUDICIAL PETITION FILING SYSTEM
Lokesh Sheshrao Khedekar	A BUS MANAGEMENT AND CROWD CONTROL SYSTEM
Lokesh Sheshrao Khedekar	A GESTURE-BASED VOLUME CONTROL SYSTEM USING COMPUTER VISION AND AUDIO PROCESSING
Vaishali Vidyadhar Savale	The Spybot is an advanced, real-time surveillance system with 180-degree vision using an ESP32-CAM module. It employs YOLO and OpenCV for efficient object detection. The wireless Intel Seeker variant is versatile for security, military, and disaster response in diverse environments.
Dr. Varsha D. Jadhav	Presented a Scopus-indexed paper titled "Key Safe Algorithms for Blockchain Technologies" at the 2024 ICCUBEA conference. It compares Shamir's Secret Sharing Scheme, Blakley's Scheme, and the Asmuth-Bloom Scheme for group key management in blockchain, finding Shamir's scheme the fastest and all three robust against attacks.

Topic of the Month
Advances in Non Linear Variational Inequatities

TThe paper **"Early Prediction of Alzheimer Disease and Multiclass Classifier System"** focuses on utilizing machine learning techniques to improve the early detection and classification of Alzheimer's disease (AD). It highlights the significance of early diagnosis in managing and potentially slowing the progression of AD.

Key Points of the Paper:

1. **Introduction to Alzheimer's Disease (AD)**
- Alzheimer's disease is a progressive neurodegenerative disorder that primarily affects memory, cognition, and daily functioning.
- Early detection is crucial to manage symptoms and delay progression through therapeutic interventions.

2. Challenges in Early Diagnosis
- Traditional diagnostic methods rely on clinical symptoms, neuroimaging, and cognitive assessments, but these are often detected in later stages.
- Lack of reliable early detection techniques leads to delayed interventions.

3. Machine Learning for Early Prediction
- The study introduces a multiclass classification system to categorise different stages of AD, potentially including:

- Normal (Healthy)

- Mild Cognitive Impairment (MCI)

- Early-stage Alzheimer's

- Advanced-stage Alzheimer's

- Machine learning models are trained on datasets containing patient records, cognitive test scores, and medical imaging data (MRI, PET scans, etc.).

4. Multiclass Classifier System
- The system employs **various classification algorithms** such as:

- Support Vector Machines (SVM)

- Random Forest

- Deep Learning models (e.g., Convolutional Neural Networks - CNNs)

These models analyze complex patterns in brain imaging and patient data to make accurate predictions.

5. Dataset and Feature Selection
- Features such as brain atrophy, hippocampal volume, amyloid plaque deposits, and cognitive test results are considered.
- The study likely uses publicly available datasets like ADNI (Alzheimer's Disease Neuroimaging Initiative) to train and validate models.

6. Performance Metrics and Results
- The classifiers are evaluated using metrics such as:

- Accuracy

- Sensitivity & Specificity

- Precision-Recall

- F1-score

The study compares the effectiveness of different models in distinguishing between AD stages.

7. Implications and Future Scope
- The findings suggest that machine learning can significantly enhance early diagnosis.
- Further improvements could involve **integrating genetic data, lifestyle factors, and real-time monitoring** using wearable devices.
- AI-based clinical tools could assist doctors in making faster and more accurate diagnoses.

Reference:
https://drive.google.com/open?id=1sVONIsT_hB_EAp-06gJVXdGNQkewe7ou

Jainivas Anandhan
TY AIDS - B

Dr Minal Barhate

Prof. Lokesh Khedekar

Ishika Golecha
SY AIDS-A

Gaurang Gulhane
SY AIDS-A

Utkarsha Dhawle
SY AIDS-A

Janhavi Deo
SY AIDS-A