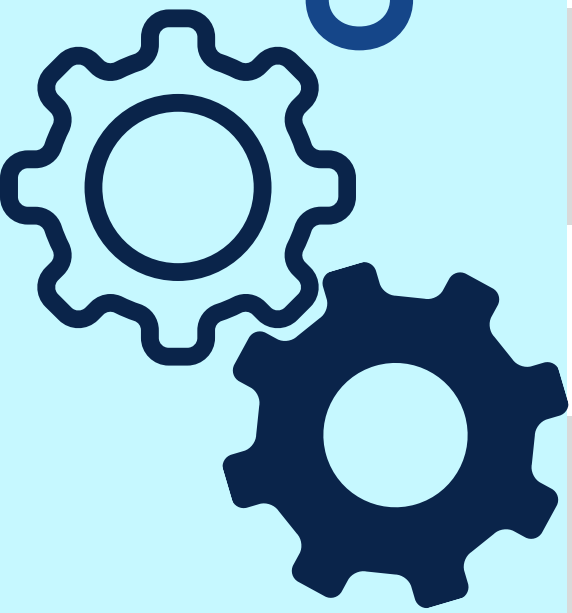
TABLE OF CONTENTS



01	COVER PAGE
02	INDEX
03	MENTORS
04	TEAM
05	VISION/MISSION
06	ACHIEVEMENTS
07	EVENTS
08	ARTICLES
09	CREDITS
10	LAST PAGE

A NOTE FROM OUR MENTORS

Our mission at CCET is not only to produce engineering graduates but to produce engineering minds.

Dr. Manpreet Singh
Principal CCET (Degree Wing)

ACM CCET provides student a great opportunity to learn scientific and practical approach of computer science.

Dr. Sunil K. Singh
Professor and HOD, CSE | Faculty Mentor

Every person should be provided with an opportunity to learn and explore the field of computer science

Dr. Sudhakar Kumar
Assistant Professor, CSE | Faculty Sponsor

Association for Computing Machinery at CCET

Research and Development

Student Speaker Program

Competitive Codong

Designing & Digital Art

Internship & Career Opportunity

ABOUT

The CCET ACM Student Chapter brings together the Association for Computing Machinery (ACM) and ACM-W, fostering a vibrant community of computing enthusiasts committed to innovation, learning, and inclusivity. Under the expert mentorship of Dr. Sunil K. Singh and Dr. Sudhakar Kumar, the chapter actively organizes technical workshops, coding competitions, hackathons, and outreach programs that encourage both skill development and collaboration. While ACM focuses on advancing computing as a science and profession, ACM-W works towards empowering and supporting women in computing, ensuring equal opportunities and representation. Together, they create a dynamic platform at CCET where students can explore emerging technologies, share knowledge, and grow as competent and responsible computing professionals.

CCET ACM STUDENT CHAPTER

Research and Development

Student Speaker Program

Competitive Codong

Designing & Digital Art

Internship & Career Opportunity

ABOUT ACM

ACM boosts up the potential and talent, supporting the overall development needs of the students to facilitate a structured path from education to employment. Our Chapter CASC focuses on all the aspects of growth and development towards computer technologies and various different elds. Overall, we at CCET ACM Student Chapter, through collaboration and engagement in a plethora of technical activities and projects, envision building a community of like-minded people who love to code, share their views, technical experiences, and have fun. We have been trying to encourage more women to join the computing eld, so we started an ACM-W Chapter to increase the morale of women. CASC launched an app which aimed at maintaining deco- rum of reading among CS members and sharing their ideas.

CCET ACM-W STUDENT CHAPTER

Research and Development

Student Speaker Program

Competitive Codong

Designing & Digital Art

Internship & Career Opportunity

ABOUT ACM-W

The CCET ACM-W was founded in October 2021 with an aim to empower women in the field of computing and increase the global visibility of women in the field of research as well as development. We provide a platform for like-minded people so that they can grow together and contribute to the com- munity in a way that shapes a better world. Our chapter was founded to encourage students, especially women, to work in the field of computing. The chapter's main goal is to create even opportunities and a positive environment for students, where they can work to develop themselves profession- ally. We at the ACM Student chapter aim to build a globally visible platform where like-minded people can collaborate and develop in their field of interest.

VISION

Chandigarh College of Engineering and Technology aims to be a center of excellence for imparting technical education and serving the society with self-motivated and highly competent technocrats.

MISSION

1. To provide high quality and value based technical education.
2. To establish a center of excellence in emerging and cutting edge technologies by encouraging research and consultancy in collaboration with industry and organizations of repute.
3. To foster a transformative learning environment for technocrats focused on inter-disciplinary knowledge; problem-solving; leadership, communication, and interpersonal skills.
4. To imbibe spirit of entrepreneurship and innovation for development of enterprising leaders for contributing to Nation progress and Humanity.

DEPARTMENT-VISION AND MISSION

VISION

To produce self-motivated and globally competent technocrats equipped with computing, innovation, and human values for ever changing world and shape them towards serving the society.

MISSION

M1. To makethe department a smart centre for learning, innovation and research, creativity, andentrepreneurship for the stakeholders (students/scholars, faculty, and staff).

M2. To inculcate a strong background in mathematical, theoretical, analytical, and practical knowledge in computer science and engineering.

M3. To promote interaction with institutions, industries and research organizations to enable them to develop as technocrats, entrepreneurs, and business leaders of the future.

M4. To provide a friendly environment while developing interpersonal skills to bring out technocrat's inherent talents for their all-round growth

Achievements

Recent publications from our team highlight significant advancements across various domains of Computer Science, from Deep Learning and security to intelligent systems. These contributions were published in high-impact journals, conferences, and book chapters throughout late 2024.

Journal Articles

- **Unleashing the Power of Multi-Agent Reinforcement Learning for Algorithmic Trading in the Digital Financial Frontier and Enterprise Information Systems**
  Aug 2024
  Saket Sarin, Sunil Kr Singh, Sudhakar Kumar, Varsha Arya

- **Synergistic application of neuro-fuzzy mechanisms in advanced neural networks for real-time stream data flux mitigation**
  Aug 2024
  Shivam Goyal, Sudhakar Kumar, Sunil Kr. Singh, Brij B. Gupta

Conference Papers

- **Improving Automated Text Editing and Understanding with Advanced Named Entity Recognition Techniques**
  Sep 2024
  Vanshika Chilkoti, Sudhakar Kumar, Sunil Kr. Singh, Brij B. Gupta

- **Intelligent FaultEdge: AI-Driven Fault-Tolerant Edge Framework for Smart Grid Monitoring in IoT**
  Aug 2024
  Tushar Singh, Sudhakar Kumar, Sunil Kr. Singh, Brij B. Gupta

- **Gestational Diabetes Prediction using Machine Learning for Consumer Electronics Healthcare**
  Aug 2024
  Sahil Garg, Sudhakar Kumar, Sunil Kr. Singh, Brij B. Gupta

Book Chapters

- **Detailed Evolution Process of CNN-Based Intrusion Detection in the Context of Network Security**
  Oct 2024
  Sudhakar Kumar, Sunil Kr Singh, Amanpreet Singh, Varsha Arya
- **Cyber Synergy-Unlocking the Potential Use of Biometric Systems and Multimedia Forensics in Cybercrime Investigations**
  Oct 2024
  Ruchika Thakur, Sunil Kr Singh, Sudhakar Kumar, Krishana Singla
- **Automatic parallelization for multicore architectures: Role, importance, and opportunities**
  Sep 2024
  Sunil K. Singh, Sudhakar Kumar
- **Secure and cost-effective key management scheme for the Internet of Things-supported WSN**
  Sep 2024
  Rakesh Kumar, Sunil Kr Singh, D.K. Lobiyal, Sudhakar Kumar
- **Computational intelligence in decision support: Scope and techniques**
  Sep 2024
  Sunil Kr Singh, Brij. B. Gupta, Sudhakar Kumar
- **Applying Visual Cryptography to Decrypt Data Using Human Senses**
  Jul 2024
  Dikshant Rajput, Sunil Kr Singh, Kwok Tai Chui, Sudhakar Kumar
- **Zero Knowledge Proofs and Their Applications in Cryptography: Advancements, Challenges, and Future Aspects**
  Jul 2024
  Tanish Aggarwal, Sunil Kr Singh, Arcangelo Cartiglione, Sudhakar Kumar

EVENTS

OOPS Workshop

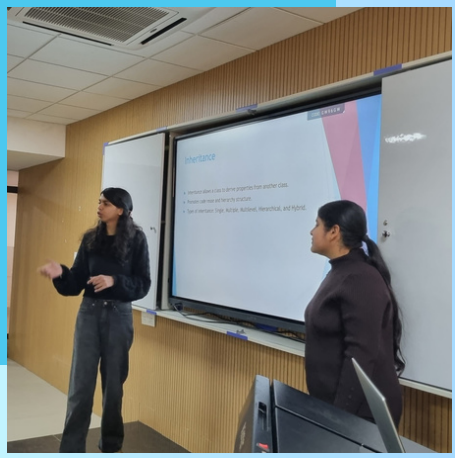
Date: 6th Feb, 2025
Number of attendees in the event: 7

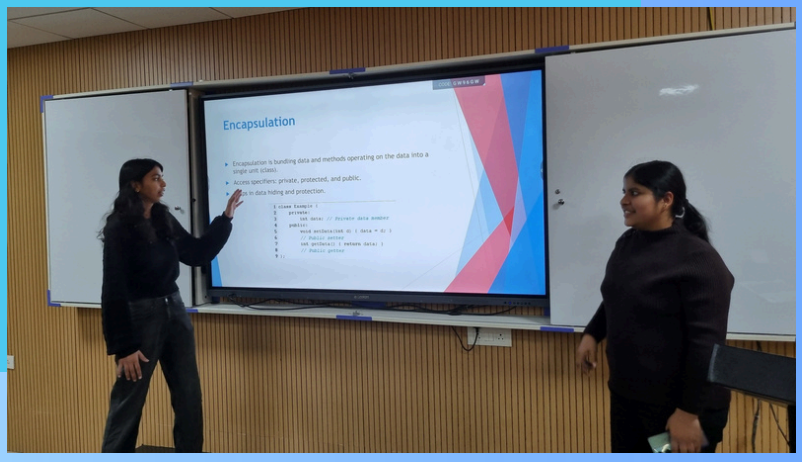
The workshop on Object-Oriented Programming (OOP) was successfully conducted, providing participants with a comprehensive understanding of key concepts such as Classes & Objects, Inheritance, Polymorphism, Encapsulation, and Abstraction. Through interactive discussions and real-world examples, attendees gained valuable insights into how OOP enhances code efficiency, scalability, and reusability.

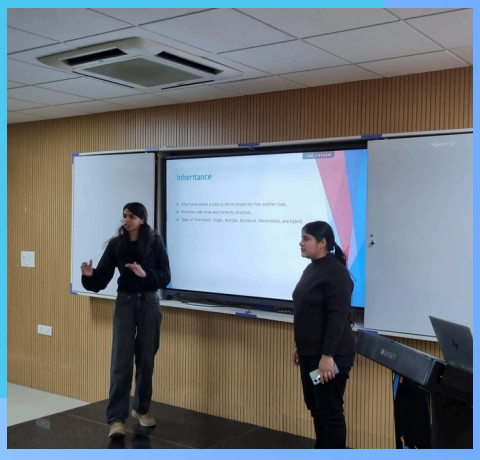
A special thanks to Vanshika Singla and Ravina Mittal for delivering an engaging and informative session, making complex concepts easy to grasp and apply. The enthusiasm and participation from the attendees made the workshop even more impactful.

We appreciate everyone who joined us and contributed to the success of this session. Stay tuned for more exciting learning opportunities in the future!

GLIMPSE FROM THE EVENT







Articles

AI in Software Development

Introduction

Artificial intelligence (AI) is reshaping software development, automating mundane tasks, improving developer productivity, and redefining workflows. From code generation tools to advanced AI agents, the field is experiencing rapid transformation. However, the integration of AI into software engineering also brings technical, ethical, and operational challenges that warrant careful consideration.

Key Research & Innovations

- **Survey-based Insights**

A quantitative study surveying 250 professionals in Saudi Arabia and Jordan showed that 68 % used AI tools (e.g. GitHub Copilot, IntelliCode) in at least one SDLC phase. About 74 % reported time reductions on routine coding tasks 62 % observed fewer post-release defects. Yet only 40 % fully trusted AI-generated recommendations, and 58 % cited skill gaps as barriers. Formal training boosted gains by ~30 %.

- **Taxonomizing AI for Engineering**

A March 2025 study frames AI not only as a code generator but as a suite of tools for tasks across problem formulation, documentation, testing, debugging, and architecture. It highlights research bottlenecks and future directions for achieving more fully automated software engineering workflows.

- **AI Safety in Practice**

A 2025 mixed-method investigation of 86 practitioners and 874 AI-related incidents revealed that many

downstream developers are aware of risks—like data leakage and bias—but lack consistent guidelines or safety policies. Practices vary widely, especially during model selection and documentation phases.

- **Ethical, Legal & IP Issues**

A peer-reviewed 2024 paper examines questions of code ownership, bias, privacy, and accountability when using AI tools such as Copilot and ChatGPT. It argues that responsible integration demands transparency, policy frameworks, and stakeholder engagement to avoid legal and ethical pitfalls.

- **Real World Productivity Gains and Limitations**

Recent industry studies draw mixed conclusions: Atlassian reports 68 % of developers save over 10 hours per week using AI, but most of their time is spent on noncoding tasks not fully addressed by current tools. Conversely, the METR study found experienced developers working in large codebases were actually slower when using AI tools like Copilot or Cursor, especially for extensions or debugging tasks.

Challenges & Considerations
Technical Challenges

- Data quality & availability: Highquality, clean software artifacts are needed to train AI tools. Noise, inconsistency, and restricted access impair model performance.
- Integration with legacy systems: Many existing workflows and systems are incompatible with new AI tools, requiring reengineering, middleware, or phased migrations.

Trust, Reliability & Explainability

Articles

- AI generated code can include hallucinated package names (“slopsquatting”) or subtle bugs–even if it looks plausible. Nearly 20 % of generated code referenced nonexistent packages, posing supply chain security risks.
- Explainability remains limited; complex models are often opaque, reducing trust and making debugging harder. In many cases, AI output must be human reviewed and interpreted.

Ethical, Legal & IP Concerns

- Who owns AIgenerated code? Legal frameworks are still evolving. Models trained on open or proprietary code may inadvertently reproduce copyrighted content.
- Bias can permeate AI recommendations if training data reflects skewed practices or perspectives. Fairness-aware audit processes are essential.

Workforce & Adoption Issues

- Developers need both domain and AI expertise, yet many lack formal training. Only organizations that invest in training see optimal results
- Resistance to change is common. Developers may fear displacement or distrust AI suggestions. Transparent communication and practical support reduce resistance.

Operational & Resource Constraints

- AI tools demand significant compute resources, hardware, and licensing, often beyond the budgets of smaller teams.
- Model drift–the gradual loss of performance over time due to changing data–requires reinforcement and retraining cycles for reliable AI performance.

Articles

Productivity Paradoxes & Strategic Risk

- While AI can accelerate new development, it may slow maintenance or refactoring of large legacy codebases. Inefficiency can emerge in complex settings.
- Zoho founder Sridhar Vembu suggests generativeAI may render large legacy systems obsolete, challenging their long-term value and requiring strategic reassessment.

Conclusion

AI is undeniably transforming software development—automating code generation, supporting testing and architecture, improving productivity, and enabling powerful new workflows. But its adoption brings profound technical, ethical, operational, and organizational challenges. Addressing these requires investment in data governance, developer training, integration planning, ethical transparency, and oversight frameworks. Rather than replacing developers, AI is becoming a potent collaborator—but only when deployed carefully and with human-in-the-loop safeguards.

References

[[1] Mohammad Baqar, Balancing Innovation and Ethics in AI-Driven Software Development, Aug 2024

[2] Haoyu Gao et al., AI Safety in the Eyes of the Downstream Developer, Mar 2025

[3] Mdpi survey, AI-Driven Innovations in Software Engineering, Quantitative Analysis, 2024 / 2025

[4] Alex Gu et al., Challenges and Paths Towards AI for Software Engineering, Mar 2025

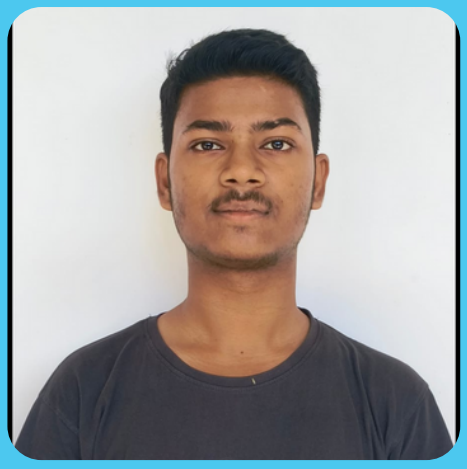
Articles

[5] Atlassian developer productivity study, 2025

[6] METR study on AI coding productivity, July 2025

[7] TechRadar article on slopsquatting risk from hallucinated packages, July 2025

[8] Commentary by Zoho's Sridhar Vembu on AI and legacy codebases, Jun 2025



Sahil Kumar

Articles

The Rise of Edge AI: Transforming Intelligent Computing at the Device Level

Introduction

Edge AI is the union between edge computing and artificial intelligence (AI) to facilitate smart processing near or at the point where data originates [4]. In conventional AI workflows, data captured by sensors, cameras, and devices is sent over the internet to distant cloud-based servers for processing and deduction. While such an approach adds latency, bandwidth utilization, privacy breach points, and reliance on smooth internet connections, Edge AI overcomes all such shortcomings by deploying AI models on devices like smartphones, smart cameras, industrial sensors, and autonomous vehicles. Local computation through such functioning facilitates speedier, more efficient, and privacy-friendly decisions. Edge AI is also expanding greatly in many industries amid the growth of Internet of Things (IoT) devices and the need for responses in real time. For self-driving cars, for instance, edge inference can help detect pedestrians or road signs in real time without reliance on the cloud. Wearable devices for the healthcare market can monitor vital signs and offer auto alerts. Such a paradigm is moving computation to decentralized intelligence, redesigning the architecture of modern systems and opening new innovation avenues.

Core Benefits of Edge AI

Having the AI on the edge is far more advantageous than cloud-based technology:

• Ultra-low latency: Edge AI processes data where it is created, thereby decreasing latency induced through data transmission. That is where such technologies as robotics, driverless vehicles, And augmented reality are introduced.
• Offline functionality: Edge-AI-equipped devices are able to function even when network connectivity, improving resilience and availability.
• Bandwidth efficiency: To process data on-premises, you must transfer over just such pertinent data or insights, conserving bandwidth.
• Greater privacy and security: Private or sensitive data can be stored on-device, decreasing vulnerability to online dangers and compliance with data protection legislations such as GDPR.
• Scalability: Edge AI spreads computational workloads across devices such that it minimizes dependence on base infrastructure whilst permitting scale-wide deployment.

Technical Challenges at the Edge

Although Edge AI has many benefits, But deploying AI on edge devices has some technical challenges [3]:
• Limited compute resources: Edge devices often have limited CPU, GPU, or memory resources compared to cloud servers. Efficient model optimization is essential.
• Power and thermal constraints: Battery-y-operated and passively cooled devices must balance performance with energy efficiency. • Hardware heterogeneity: A wide range of edge devices –from microcontrollers to embedded GPUs–requires cross-platform model compatibility and tuning.
• Network variability: Infrequent or unreliable

connectivity complicates tasks like remote updates and synchronization.
• Security concerns: Edge devices are more vulnerable to manipulations, so endpoint protection needs to be strong as well as secure model deployment.

Edge AI Hardware and Platforms

Multiple hardware and software platforms are being developed to enable efficient edge AI:

• Nvidia-jetson:Jetson is made up of Jetson Nano, Xavier, and AGX Orin offering GPUaccelerated inference for autonomous robots, drones, and embedded vision systems. • Google Coral: Edge TPU-enabled Coral devices are low-power, high-speed in-Difference in form factors appropriate for IoT and embedded applications.
• Apple Neural Engine (ANE): ntegrated into iPhones, iPads, and Macs, ANE runs Ondevice work related to ML like image recognition and speech recognition.
• Qualcomm AI Engine: Found in Snapdragon SoCs, it provides edge AI for mobile, auto- motivational motivator, and IoT applications.
• Intel Movidius and OpenVINO: These SoC and software enable AI inference on visioncentric security and industrial automation solutions.
• Xilinx Versal AI Edge: Combine adaptive compute acceleration with AI engines for deterministic real-time workloads for the automotive and aerospace markets. • Software toolkits: AWS IoT Greengrass, Microsoft Azure IoT Edge, Google Cloud IoT offer orchestration, model deployments, and lifecycle management.

Model Optimization for Edge Deployment

To meet the constraints

of edge environments, AI models undergo various optimizations:

• Quantization: educes model size and computation by converting floating-point weights, To reduce precision formats such as INT8.

• Pruning: Removes redundant weights or neurons to save on memory and accelerate [2].

• Knowledge distillation: rain small models (students) to emulate the performance of larger ones (teachers).

• Edge-specific architectures: Compact models like MobileNet, Tiny-YOLO, and EfficientNet are optimized for hardware-limited devices.

• On-device compilation: There are libraries like TensorFlow Lite, PyTorch Mobile, and TVM available to compile models as well as optimize them for specific hardware targets.

Edge AI Applications in Everyday Life

Edge AI is stimulating innovation in all industries:

• Autonomous vehicles: Vehicles utilize on-board AI to see objects, understand traffic lights, And sail safely in real time.

• Intelligent surveillance:Cameras perform motion detection, facial recognition, anomaly locally-oriented detection for reducing storage and response time.

• Wearables and healthcare: Wearables like smartwatch monitor heart rate, oxygen level, and sleep patterns and inform people about anomalies.

• Industrial automation: Edge AI is deployed by plants for quality testing, predictive maintefinance, and safety monitoring.

• Customer and retail experience: Edge-based vision is employed by retail stores for foot traffic monitoring, stock

on shelves examination, and customized advertising.
• Smart homes and cities: From smart lights to traffic management to voice assistants, edge AI powers responsive and context-aware environments.

Future Trends and Outlook

Edge AI is expanding exponentially with the main trends shaping its direction [1]:
• Federated learning: Distributed model learning on devices facilitates privacy and Personalization by decentralizing data pooling [5].
• 5G integration: Multi-gigabit low-latency networks like 5G are also complementary to edge AI, especially for AR/VR and remote diagnostics.
• Sensor-level AI: Sensor-level AI is enabled by ultra-low-power microcontroller-level AI through TinyML applications such as wearables and environmental monitoring.
• Device orchestration using AI: Distributed edgeintelligence manages swarms of Smart devices for manufacturing and logistics.
• Energy-aware AI: Research into energy-efficient algorithms and neuromorphic computing facilitates sustainable edge deployments

Conclusion

Edge AI is a paradigm-shifting method for designing and deploying smart systems. By moving inference closer to data generation points, it creates new insights in responsiveness, scalability, and privacy preservation. While there are challenges in hardware limitations, standardization, and security, the ecosystem is quickly emerging through developments in model optimization, hardware acceleration, and distributed learning. As the nature of computation becomes further

decentralized, Edge AI is becoming one of the foundations for next-generation AI-based infrastructure.

References

[1] Sukhpal Singh Gill, Muhammed Golec, Jianmin Hu, Minxian Xu, Junhui Du, Huaming Wu, Guneet Kaur Walia, Subramaniam Subramanian Murugesan, Babar Ali, Mohit Kumar, et al. Edge ai: A taxonomy, systematic review and future directions. Cluster Computing, 28(1):18, 2025.

[2] En Li, Liekang Zeng, Zhi Zhou, and Xu Chen. Edge ai: On-demand accelerating deep neural network inference via edge computing. IEEE transactions on wireless communications, 19(1):447-457, 2019.

[3] Tobias Meuser, Lauri Loven, Monowar Bhuyan, Shishir G Patil, Schahram Dustdar, Atakan ´ Aral,

[3] Tobias Meuser, Lauri Loven, Monowar Bhuyan, Shishir G Patil, Schahram Dustdar, Atakan ´ Aral, Suzan Bayhan, Christian Becker, Eyal De Lara, Aaron Yi Ding, et al. Revisiting edge ai: Opportunities and challenges. IEEE Internet Computing, 28(4):49-59, 2024.

[4] Raghubir Singh and Sukhpal Singh Gill. Edge ai: a survey. Internet of Things and CyberPhysical Systems, 3:71-92, 2023.

[5] Xiaofei Wang, Yiwen Han, Chenyang Wang, Qiyang Zhao, Xu Chen, and Min Chen. Inedge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. Ieee Network, 33(5):156-165, 2019.

Articles

Ritika Kalia

Computer Vision and Robotics Integration

Abstract

The fusion of computer vision and robotics is revolutionizing how machines perceive, interpret, and interact with the real world. By endowing robots with sight, we empower them with contextual understanding and adaptability, paving the way for advanced automation in fields as diverse as manufacturing, healthcare, logistics, and agriculture. This article explores the enabling technologies, practical applications, ongoing challenges, and future potential of computer vision-powered robotics, highlighting not only technical achievements but also societal impacts.

Introduction

Computer vision centers on giving machines the ability to extract meaningful information from visual data, mirroring human sight. When integrated with robotics—the engineering of autonomous or semi-autonomous machines—we create intelligent agents capable of perceiving their surroundings, making informed decisions, and acting accordingly. With advances in deep learning, sensor hardware, and real-time inference, this convergence is at the forefront of technological progress.

Robots now routinely scan factory floors for quality assurance, navigate dynamic hospital corridors, and delicately pick fruits in orchards guided by computer vision algorithms. This capability represents a significant shift from rigid, pre-programmed

machines to adaptable, perceptive agents able to cope with unstructured environments and varied tasks. Ultimately, the integration empowers robots to augment human capabilities, operate in hazardous areas, and improve productivity across domains.

Enabling Technologies

A range of cutting-edge technologies has propelled computer vision and robotics into new realms:

- Deep Learning Models: The advent of convolutional neural networks (CNNs) and vision Transformers has significantly improved object detection, segmentation, and scene comprehension in machines . These architectures enable robots to distinguish objects in complex environments with human-like accuracy. For example, CNNs allow robotic manipulators to recognize and differentiate tools or parts in manufacturing lines, adapting to new shapes and textures without explicit programming.
- 3D Perception and Sensor Fusion: Robots benefit enormously from combining multiple sensing modalities. LIDAR sensors create precise depth maps of environments
- enabling robots to navigate and avoid obstacles in three dimensions . Stereo cameras and RGB-D sensors further complement these data streams, enriching spatial awareness. Integrating visual input with inertial measurement units (IMUs) and tactile feedback leads to a more holistic perception, necessary for complex tasks such as dynamic balancing or object manipulation.

- Edge Computing and Real-Time Inference: Middleware and embedded accelerators allow robots to perform sophisticated vision processing locally, reducing dependence on cloud connectivity . This autonomy is crucial in latency-sensitive environments such as autonomous vehicles or surgical robots, where split-second decisions are vital. Innovations in hardware like NVIDIA Jetson and Google Coral have made it feasible to deploy deep vision networks efficiently on compact robotics platforms
- .Simultaneous Localization and Mapping (SLAM): SLAM algorithms utilize visual data combined with odometry and inertial sensors to build real-time maps of unknown environments while estimating the robot's location within. Vision-based SLAM variants, such as ORB-SLAM, employ feature detection methods and bundle adjustment optimizations to navigate complex indoor and outdoor spaces reliably .

Applications Across Industries

Computer vision-enhanced robots are changing the landscape of multiple sectors, driving efficiency and enabling new capabilities:

- Manufacturing: Vision-guided robots now inspect complex assemblies for minute defects invisible to human inspectors, using high-resolution cameras and AI models trained on diverse datasets. Robots also participate in assembly lines where rapid identification and positioning of parts are required, enhancing throughput and reducing errors. Collaborative robots (cobots) equipped with

Articles

- vision sensors share workspaces safely with human operators, increasing flexibility and productivity .
- Healthcare: Vision-powered robots assist surgeons with enhanced precision in minimally invasive surgeries, utilizing real-time imaging to adaptively guide instruments. Patient monitoring robots analyze facial expressions and body language to detect pain or distress, providing timely alerts to medical staff. Automated lab systems identify and sort samples with reduced contamination risks, streamlining clinical workflows .
- Logistics and Warehousing: Automated guided vehicles (AGVs) and drones use vision systems for aisle navigation, package identification, and stock management. Advanced AI enables recognition of thousands of SKU types under varying lighting, supporting rapid order.
- fulfillment and reducing human errors. The Amazon robotics warehouses exemplify high-scale deployment of vision-enabled robotic fleets .
- Agriculture: Vision-based robotics systems are revolutionizing traditional farming. Robots autonomously navigate fields, distinguishing ripe fruits from foliage, assessing plant health, and precisely targeting herbicide applications. These functions optimize yield, reduce chemical use, and alleviate labor shortages while enabling data-driven farm management.

Human-Robot Collaboration

Vision-driven collaborative robots-often referred to as cobots-bring human-robot

interaction to an unprecedented level. Through advanced vision algorithms, these machines can recognize human gestures, body poses, and even facial expressions, enabling natural and intuitive communication channels . Cobots dynamically adjust their motions to avoid collisions, yielding a safer industrial environment. For example, in automotive assembly lines, cobots interpret workers' hand signals to execute complementary movements, increasing efficiency without requiring costly fencing or extensive reprogramming. Beyond factories, assistive robots in homes leverage vision-based recognition to understand user intent—opening doors, offering objects, or providing companionship—enhancing accessibility for people with disabilities or the elderly.

Challenges

Although the prospects are bright, several significant hurdles remain for the seamless integration of computer vision in robotics:

- Robustness in Diverse Environments: Unlike controlled lab scenarios, real-world environments are full of unpredictability—lighting variations, occlusions, clutter, and dynamic obstacles can all challenge vision-based systems. For instance, shadows or glare might cause misclassification, while rain or dust can degrade sensor inputs. Researchers continue to explore adaptive models and multi-sensor redundancy methods to increase system resilience .
- Real-Time Processing Trade-offs: Achieving the necessary speed for

perception-driven tasks-such as obstacle avoidance or human-robot collaboration-requires balancing model accuracy with computational efficiency. High-fidelity models tend to be resource-intensive, while lightweight models may sacrifice precision. Engineering constraints on power, weight, and cooling further limit onboard compute capabilities, leading to continuous innovation in model compression, quantization, and hardware acceleration

- Generalization and Transfer Learning: Vision models often struggle with objects or scenarios not encountered during training. For robotics operating in diverse, dynamic settings, the ability to learn new concepts incrementally or transfer knowledge between tasks is critical. Current research investigates meta-learning techniques and continual learning frameworks to enablerobots to adapt rapidly without exhaustive retraining .

Ethical and Societal Implications: As robots become increasingly autonomous, concerns about transparency, accountability, and societal impact rise. Ensuring decisions made by vision-based robots are interpretable and aligned with human values is essential to build trust and acceptance. Privacy concerns arise as robots collect large amounts of visual data in public or private spaces. Moreover, automation's impact on workforce displacement calls for thoughtful policy and ethical frameworks .

Future Scope

Looking ahead, the union of computer vision and robotics promises even broader societal benefits

and technological leaps:

- Adaptive Learning and Autonomy: Future robots will increasingly leverage continual learning to teach themselves new tasks and adapt to novel environments on-the-fly. This evolution will enable robots to operate with minimal supervision even in highly unstructured or hazardous settings such as disaster zones or deep-sea exploration.
- Explainable and Trustworthy AI: Efforts to develop explainable AI (XAI) for vision systems will provide insights into robots' decision-making processes, fostering user trust and facilitating debugging or certification procedures. Transparent perception models may also aid in ethical deployment and compliance with regulatory bodies
- Advanced 3D and Multimodal Perception: Emerging sensors capable of capturing hyperspectral data, thermal signatures, or even chemical compositions alongside visual data will make robotic perception far richer and more nuanced.

Multimodal fusion techniques will empower robots to build comprehensive situational awareness.

- Affordable and Democratized Robotics: The falling cost of sensors, processing hardware, and open-source vision models will expand access beyond large companies to startups, academia, and hobbyists. This democratization will accelerate innovation and diversify applications, including personalized robots for homes and small businesses.

- Societal Integration and Collaboration: Vision-enabled robots will become ubiquitous partners in everyday life—from assisting in education to seniors' care and urban infrastructure maintenance—facilitating more inclusive, safe, and efficient human environments.

Conclusion

The integration of computer vision and robotics is actively reshaping our world, offering smarter, more perceptive machines capable of navigating and acting within complex, dynamic environments. While challenges in robustness, compute efficiency, and ethics remain, relentless innovation and interdisciplinary collaboration signal a future where robots not only see but understand and enrich our lives in profound ways.

References

[1] S. Levine, P. Pastor, A. Krizhevsky, J. Ibarz, and D. Quillen, Learning Hand-Eye Coordination for Robotic Grasping with Large-Scale Data Collection, The International Journal of Robotics Research, vol. 37, no. 4-5, pp. 421-436, April 2018.

[2] Y. LeCun, Y. Bengio, and G. Hinton, Deep Learning, Nature, vol. 521, no. 7553, pp. 436-444, May 2015.

[3] X. Chen, S. Ma, J. Wan, B. Li, and T. Xia, A Survey on Computer Vision for Assistive Robotics, ACM Computing Surveys, vol. 55, no. 3, pp. 1-34, 2023.

[4] S. Thrun, W. Burgard, and D. Fox, Probabilistic Robotics, MIT Press, 2005.

[5] S. Hsia and M. J. Mataric, Ethics in Robotics and AI:

Articles

Considerations for
Developers and Users,
Communications of the ACM,
vol. 64, no. 8, pp. 28–31,
August 2021.

Maanit Khatkar

Articles

Cybersecurity in the Age of Deepfakes and Generative AI

Introduction

Deepfakes and the production of synthetic content are two examples of how generative AI technologies have changed the media creation landscape in recent years. Hyper-realistic but artificially produced images, videos, or audio clips produced with sophisticated machine learning models like Generative Adversarial Networks (GANs) are known as "deepfakes." Such inventions have enormous creative and business potential, but they have also become serious cybersecurity risks. Deepfakes create new problems for safeguarding digital identities and information integrity, ranging from identity theft and political disinformation campaigns to financial fraud and corporate espionage. The technological environment, current applications, research avenues, and defense strategies that attempt to counter these new threats are all thoroughly covered in this article.

The Rise of Generative AI and Deepfakes

Over the past ten years, generative AI has advanced quickly, largely due to deep neural networks and extensive training datasets.Since their initial introduction by Ian Goodfellow in 2014, GANs have emerged as a key tool for producing realistic-looking synthetic media. Additional methods have improved generative capabilities, including Transformer-based models and Variational Autoencoders (VAEs).Deepfak applications first appeared in digital art and entertainment, but they have since spread to more alarming fields. Because they can mimic voices and appearances quite well, they are now frequently employed in phishing attacks, impersonation schemes, and disinformation campaigns.The paradigm for cybersecurity has changed as a result of these developments. These days, traditional security systems that were created to identify code-based malware or stop network intrusions are being extended to identify and protect against AI-generated visual

Articles

Advancements in Detection Algorithms and Defensive Mechanisms

In response, the cybersecurity community has developed a number of technical countermeasures aimed at identifying and thwarting deepfakes.

Detection algorithms examine minute artifacts in photos or videos that reveal their artificial origin. These algorithms are frequently based on deep learning architectures. Unnatural facial expressions, irregular blinking patterns, frame transition issues, and audio-visual inconsistencies are a few examples. Convolutional neural networks (CNNs) are used in one well-liked technique to identify subtle pixel-level irregularities that are hard for human observers to notice.Recurrent neural networks (RNNs) have also been investigated for the detection of lip synchronization and synthesized speech inconsistencies.

Analyzing frequency-domain characteristics, such as irregularities in the audio spectrograms of produced voices, is the foundation of another intriguing strategy. Cryptographic signatures and watermarking have been suggested as ways to verify the legitimacy of digital content beyond detection. Content provenance tracking and other blockchain-based solutions guarantee that any alteration to media files is documented and verifiable. Because of these advancements, digital content has an unchangeable chain of custody, making tampering traceable and, ideally, avoidable.

Integration of Generative AI in Cybersecurity Infrastructure

Generative AI is also being used for defense, despite the difficulties. In order to stress-test systems and find vulnerabilities, cybersecurity experts are simulating attacks in controlled environments using generative models. Additionally, models that can predict and adjust to novel

deepfake techniques are trained using adversarial machine learning techniques.Real-time deepfake detection systems that can be integrated into social media and video conferencing platforms are another area of emerging research.By warning users when manipulated media is found, these systems hope to increase the level of trust and legitimacy in online interactions Programs for media literacy and public awareness are equally crucial in preparing people to spot dubious content.

Current Applications and Research (2022–2024)

In the battle against deepfake threats, a number of groundbreaking studies and tools have surfaced between 2022 and 2024. methods [4]. For example, the basis for assessing the effects of deepfakes on facial recognition systems was established by Korshunov and Marcel's (2018) work [1]. A thorough review of media forensics methods for deepfake detection was given by Verdoliva (2020) [2]. In a similar vein, Matern et al. (2019) made significant contributions to the field by concentrating on the visual artifacts specific to synthetic faces [3].

Insights into the offensive and defensive uses of generative AI were provided by a thorough survey conducted by Mirsky and Lee (2021), which listed the entire range of creation and detectionAgarwal et al. (2019) conducted additional research on practical defenses against deepfake misuse that targets public figures, offering tools and protocols to maintain the integrity of digital identities [5].
The cybersecurity community has a number of important priorities going forward. First, as generative models become more complex, detection systems must also advance in tandem. Speed, scalability, and adaptability must be given top priority in cybersecurity tools as real-time deepfake generation becomes more widely available. Distributing detection capabilities across networks without compromising performance may be made possible by edge AI and federated learning techniques. Second, laws need to keep up with the latest developments in technology

Legislation to punish the malicious use of synthetic media is starting to be proposed by governments and regulatory agencies.**It is still** difficult to strike a balance between maintaining freedom of expressionand guaranteeing enforceability.Lastly, cooperation across disciplines is crucial. To create strong standards and moral principles for AI-generated content, technologists, ethicists, legal professionals, and legislators must collaborate. Society can maximize the advantages of generative AI while lowering its risks by establishing a coherent ecosystem.

Conclusion

The capabilities and threats of contemporary cybersecurity have been redefined by deepfakes and generative AI. The necessity for proactive, astute, and moral defenses increases as malevolent actors use these technologies for deceit and disruption. The cybersecurity community can create robust frameworks to combat the changing threats posed by synthetic media by means of ongoing research, technological advancement, and cross-sector cooperation.

In the era of deepfakes, cybersecurity's future rests not only on technological alertness but also on public awareness and legal responsibility.

References

[1] Korshunov, P., & Marcel, S. (2018). Deepfakes: A New Threat to Face Recognition? Assessment and Detection. arXiv preprint arXiv:1812.08685.

[2] Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910-932.

[3] Matern, F., Riess, C., & Stamminger, M. (2019). Exploiting visual artifacts to expose deepfakes and face manipulations. In 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW) (pp. 83-92). IEEE

[4] Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys (CSUR), 54(1), 1-41.

Articles

[5] Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2019). Protecting world leaders against deep fakes. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 38-45).

Shreya

CREDITS

Editorial Mentor Board

Dr. Sunil K. Singh
(Mentor)
Professor and HoD
Department of CSE

Dr. Sudhakar Kumar
(co-mentor)
Professor
Department of CSE

Sahil Garg
CASC Student Chairperson
(2024-2025)

Ayushi
CASC-W Student Chairperson
(2024-2025)

Jaiveer Singh
CASC Student Chairperson
(2025-2026)

Ritika Kalia
CASC-W Student Chairperson
(2025-2026)

Lead Editors

Eshmeet Singh Bhachu
CSE 2023

Vanshika Singla
CSE 2023

Content Editors

Bhavya
CSE 2023

Aanshi Bansal
CSE 2023

Feature Editors

Khushi
CSE 2023

Shreya
CSE 2023

Aarushi
CSE 2023

CASC Board

Jaiveer Singh
Chairperson

Satvik Pathak
Vice-Chairperson

Sanatan
Secretary

Shivam Vats
Membership Chair

Dhruv Bali
Treasurer

Rohan
Webmaster

Saksham
Design Head

Kritin
External Member Head

Vanshika Singla
Editorial Head

Sahil Kumar
Social Media Manager

Maanit
PR Head

Aditya
Event Manager

Japjot
Domain Director(Web & DevOps)

Hitesh
Domain Director
(Competitive Programming)

Anshul
Domain Director
(Android)

Jasvir
Marketing Head

Jasjeet
Domain Director
(AI & Ml)

CASC-W Board

Ritika Kalia
Chairperson

Samriti Sharma
Vice-Chairperson

Simar Atwal
Secretary

Mehak Negi
Membership Chair

Khushi
Treasurer

Bhavya
Webmaster

Eshmeet Singh Bachu
Design Head

Ravina Mittal
Executive Member Head

Aanshi Bansal
Editorial Head

Bhumika Bijlwan
Social Media Manager

Harshita
PR Head

Sargun
Event Manager

Shreya
Domain Director(Web & DevOps)

Hitesh
Domain Director
(Competitive Programming)

Anshul
Domain Director
(Android)

Anshika Goyal
Marketing Head

Jasjeet
Domain Director
(AI & Ml)

"Scientists explore the mysteries of what exists, while engineers bring to life what once only existed in dreams."

acmccet@gmail.com

/acmccet

http://ccet.acm.org/

CCET ACM Student chapter /acmccet /acmccet ccet-acm-student-chapterZ

CCET Details
Department of CSE
CCET, Degree Wing
Sector - 26, Chandigarh

Contact Us
For general submissions and feedback, contact us.
Website: www.ccet.ac.in

acm CCET STUDENT CHAPTER ccet.acm.org

Chandigarh College of Engg. & Tech. CCET