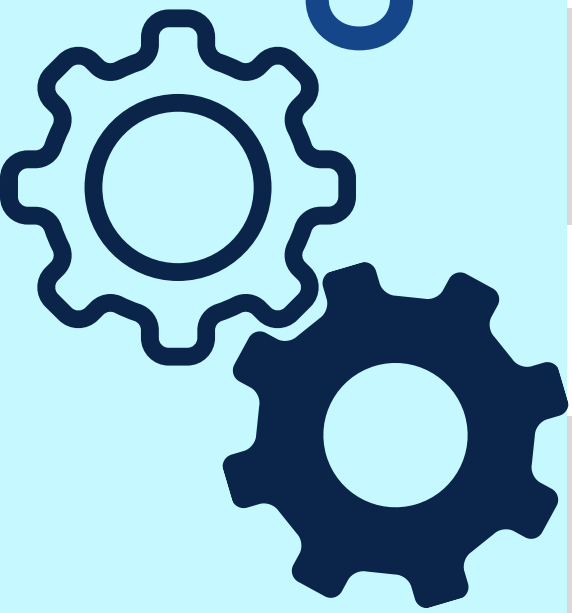
TABLE OF CONTENTS



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

- **Ensemble deep learning and EfficientNet for accurate diagnosis of diabetic retinopathy**
  Dec 2024
  Lakshay Arora, Sunil K. Singh, Sudhakar Kumar, Brij B Gupta
- **Geospectra: leveraging quantum-SAR and deep learning for enhanced geolocation in urban environments**
  Nov 2024
  Saket Sarin, Sunil K. Singh, Sudhakar Kumar, Shivam Goyal
- **Variance-driven security optimisation in industrial IoT sensors**
  Nov 2024
  Hardik Gupta, Sunil K. Singh, Sudhakar Kumar, Kwok Tai Chui

Book Chapters

- **Computational intelligence in decision support: Scope and techniques**
  Oct 2024
  Sudhakar Kumar, Sunil Kr Singh
- **Deep Learning Model for Digital Forensics Face Sketch Synthesis**
  Oct 2024
  Eshita Badwal, Sunil Kr Singh, Sudhakar Kumar, Kwok Tai Chui
- **Variance-driven security optimisation in industrial IoT sensors**
  Nov 2024
  Hardik Gupta, Sunil K. Singh, Sudhakar Kumar, Kwok Tai Chui
- **Chaotic Watermarking for Tamper Detection Enhancing Robustness and Security in Digital Multimedia**
  Oct 2024
  Harkiran Kaur, Sunil Kr Singh, Amit Chhabra, Vanshika Bhardwaj

Conference Papers

- **SentinelMet: Enhancing Metaverse Security through Deep Learning Techniques in 6G**
  Dec 2024
  Dikshant Rajput, Sunil K. Singh, Sudhakar Kumar, Brij B. Gupta
- **Advanced Evaluation of Propagation Models and Routing Protocols in Vehicular Ad-Hoc Networks**
  Nov 2024
  Anmol Jaiswal, Sunil K. Singh, Sudhakar Kumar, Kwok Tai Chui
- **Intelligent Task Offloading in IoT-Driven Digital Twin Systems via Hybrid Federated and Reinforcement Learning**
  Nov 2024
  Shivam Goyal, Sudhakar Kumar, Sunil K. Singh, Kwok Tai Chui
- **Advancing Consumer Electronics Security via Differential Privacy-based Federated Learning**
  Nov 2024
  Ayushi Manhas, Sunil Kr Singh, Sudhakar Kumar, Varsha Arya

EVENTS

DSA Bootcamp

Date: 30nd jan, 2025
Number of attendees in the event: 20

On *30th January 2025*, the CCET ACM Student Chapter began preparations for the *DSA Bootcamp*, an event designed to enhance students' understanding of *Data Structures and Algorithms (DSA)*. The organizing team planned the event meticulously, ensuring a well-structured session that would benefit both beginners and experienced coders.
The session witnessed enthusiastic participation from students eager to strengthen their problem-solving skills. The event provided in-depth knowledge on DSA concepts, equipping attendees with techniques to tackle complex programming challenges efficiently.

Throughout the session, participants engaged in interactive discussions, problem-solving exercises, and hands-on coding sessions, making the learning experience highly productive. The speakers shared valuable insights, emphasizing the significance of DSA in competitive programming and technical interviews.
The event concluded with a Q&A session where students clarified their doubts and received guidance on further improving their coding skills. The bootcamp was well-received, with attendees appreciating the initiative and looking forward to similar knowledge-sharing events in the future.

GLIMPSE FROM THE EVENT

Articles

Low-Code/No-Code Platforms: Are Developers Being Replaced?

Introduction

The world of software development is changing dramatically. The emergence of Low-Code/No-Code (LCNC) platforms has made it possible for people with little to no coding knowledge to create complete applications. There is discussion about whether traditional developers are being displaced as a result of this democratization of development. Although LCNC platforms like Bubble, Mendix, and OutSystems provide accessibility and quicker development cycles, they also bring new dependencies and technical restrictions. The technological underpinnings of LCNC platforms, their capabilities, and whether they are ready to replace traditional software engineers are all covered in this article.

Rise of Low-Code/No-Code Development

While no-code platforms do away with the need for coding entirely, low-code platforms offer a visual development environment where users can create apps using drag-and-drop interfaces and predefined logic.

The following factors have contributed to the growth of LCNC platforms:

- The need for quick digitization, particularly in the wake of COVID-19.
- The global lack of qualified developers.
- The emergence of citizen developers in non-technical fields (such as human resources and marketing).

Gartner predicts that by 2025, LCNC technologies will be used in 70% of new enterprise applications, up from less than 25% in 2020 [1].

Articles

Technical Landscape: Tools like Bubble and Mendix

Numerous platforms catered to distinct audiences and application scopes have emerged within the low-code/no-code (LCNC) ecosystem. Among these, Bubble is a well-liked no-code tool that is mainly targeted at startups and small enterprises looking to quickly develop MVPs and web applications. Bubble is a no-code platform that prioritizes user-friendliness by providing a visual interface with a robust UI builder, backend workflows, and plugin integrations. These features make it possible for users with little technical knowledge to create useful applications quickly and with little coding.
Bubble does have some disadvantages, though. Performance bottlenecks may occur in complex applications, and developers face difficulties with vendor lock-in and restricted source code access, which limit the applications' long-term flexibility and portability.

Mendix, on the other hand, is a powerful low-code platform designed for enterprise-level applications. In contrast to Bubble, Mendix supports more technically complex solutions by permitting the inclusion of custom Java code. Large organizations prefer it because of its architecture, which supports scalable microservices.Mendix also offers thorough support for DevOps procedures, such as pipelines for continuous integration and continuous deployment (CI/CD). Teams can maintain high levels of software reliability and expedite deployment

thanks to these features. But there is a price for this extra sophistication: Mendix's enterprise pricing models can be unaffordable for startups or smaller businesses, and its learning curve is higher for non-technical users.

There are a number of technical distinctions between the two platforms. Bubble is appropriate for users who value simplicity over extensibility because it is a no-code platform that does not support custom code development. However, because Mendix integrates with Java, developers can add custom logic where needed. From the standpoint of target audience, Mendix is more in line with businesses and IT departments, whereas Bubble primarily serves entrepreneurs and startups. Another important distinction is scalability: Mendix supports offline access and is based on a microservices-based architecture that improves scalability, while Bubble offers limited scalability and no support for offline functionality. Bubble has limited capabilities when it comes to integrating AI and machine learning, whereas Mendix offers moderate support, particularly when combined with custom code integrations.

This contrast draws attention to the wide range of capabilities and use cases found in the LCNC environment. The intricacy of the application, the technical expertise of the development team, and the organization's long-term strategic objectives all play a significant role in the decision between platforms like Bubble and Mendix. Low-code platforms provide a more scalable and adaptable method for mission-critical enterprise applications,

while no-code tools reduce the barrier to software development.

Integration with AI and Robotics

Despite being primarily utilized for web and mobile applications, LCNC platforms are increasingly being integrated with AI/ML APIs and even robotic process automation (RPA). Business users can create bots and use AI Builder to automate tasks with tools like Microsoft Power Platform.
LCNC interfaces, such as Siemens' MindSphere and ABB's RobotStudio, are being investigated to program robotic movements or carry out data visualization without requiring extensive coding knowledge, even though traditional programming is still the norm in industrial robotics.

Current Applications and Use Cases

These days, LCNC platforms are utilized to:

• Create internal dashboards and CRMs for startups (Bubble).

• Create enterprise-class apps for insurance and finance (Mendix, OutSystems).

• Use Microsoft Power Apps to automate form submissions and approval processes.

• Use more intelligent, interactive tools (like Airtable or Glide) in place of Excel.
One prominent example is ProRail, a Dutch railway operator that used Mendix to create a digital inspection platform, reducing development time by 60% [2].

Future Directions and Developer Roles

Although LCNC platforms provide speed and flexibility, they are not a cure-all: • Traditional development is still necessary for scalability and performance.

• Expert engineers are still needed for cybersecurity, AI/ML pipelines, and complex integrations.

• By becoming "solution architects," developers are empowering citizen developers and incorporating LCNC apps into larger ecosystems. Furthermore, in order to bridge the gap between natural language and code, LCNC tools may soon incorporate LLMs (Large Language Models) such as GPT-4 to generate application logic [3]. It's more likely that developers' responsibilities will move toward high-level problem-solving, system design, and governance rather than being replaced.

Conclusion

Software development is being revolutionized by low-code and no-code platforms. Although they speed up delivery and empower non-developers, they currently work in tandem with professional developers rather than in place of them. Their performance, control, and flexibility limitations show that competent developers are still essential, particularly for scalable, mission-critical systems. Developers should welcome LCNC as an ally—an evolving toolkit that expands their influence across technical and non-technical domains—instead of worrying about being replaced.

References

[1] Sun, X., Lin, Y., & Liu, B. (2023). Using large language models to enable low-code development. *arXiv preprint*, arXiv:2305.17157.

Articles

[2] Gartner. (2021). *Magic Quadrant for Enterprise Low-Code Application Platforms*.
[3] HCLTech. (2023). *Low-code/no-code trends beyond 2023*.
[4] Mendix. (2020). *ProRail's inspection app: A Mendix case study*.
[5] Salkever, A., & Wadhwa, V. (2020, November 17). The future of software development is no-code. *Foreign Policy*.

Shreya

Articles

The Future of Artificial Intelligence: Transforming Industries in 2025

Introduction

Artificial Intelligence (AI) continues to be a driving force in reshaping industries, from healthcare to finance, as it evolves at an unprecedented pace. In 2025, AI's advancements, particularly in generative AI, agentic AI, and ethical AI development, are setting new benchmarks for innovation and efficiency. This article explores the latest trends in AI, their impact on various sectors, and the challenges that accompany their adoption, providing insights into how AI is shaping the future of technology.

The Rise of Generative and Agentic AI

Generative AI, exemplified by large language models (LLMs) like ChatGPT, has seen remarkable growth. In 2023, Google searches for generative AI spiked by nearly 700%, reflecting its widespread adoption across industries [1]. These models have expanded from text generation to advanced capabilities in video, audio, and image processing, enabling applications like automated content creation and personalized customer experiences.

Agentic AI, a newer trend, builds upon generative AI by enabling autonomous systems that can plan, act, and learn with minimal human intervention. These agents are transforming workflows in sectors like logistics and

customer service by breaking complex tasks into manageable parts and adapting to real-time feedback [2].

Current Research (2022-2025)

Recent research and market analysis reveal several cutting-edge AI trends that have emerged between 2022 and 2025. One of the most significant developments is the explosion of generative AI. In 2023 alone, Google searches for "Generative AI" increased by over 700% [1], reflecting its mainstream adoption. Tools such as ChatGPT, Google's Gemini, and Anthropic's Claude are redefining how content is written, designed, and coded. These large language models (LLMs) are increasingly being integrated into productivity suites, customer relationship management (CRM) platforms, and educational software to enhance efficiency and personalization [1][3].

Another major advancement is the rise of agentic AI, where autonomous agents like AutoGPT, BabyAGI, and Cognition AI's Devin are capable of independently planning and executing complex, multi-step tasks [2]. These agents are now widely used in sectors like logistics, customer support, and DevOps to reduce manual intervention and boost productivity. Gartner forecasts that by 2026, more than 50% of enterprise applications will integrate agentic systems to streamline operations [2].

The field has also seen progress in multimodal AI, where models can process and generate content across multiple data types—including text,images, audio and video - within as single

unified framework. Technologies such as OpenAI's GPT-4o and Google's Gemini exemplify this shift, offering real-time vision, audio, and language understanding in a seamless user experience [4].

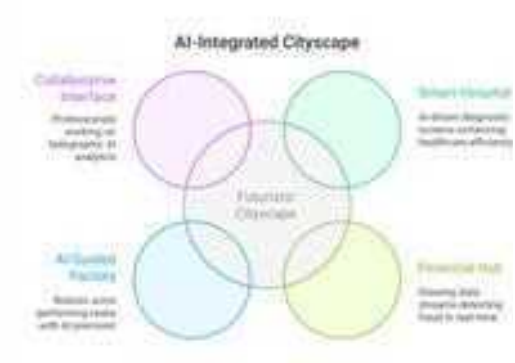
Finally, the democratization of AI has been accelerated by the release of powerful open-source models like LLaMA, Mistral, and Falcon. These tools are enabling smaller organizations, startups, and academic researchers to access high-performance AI capabilities without the need for massive infrastructure or financial investment [5]. This growing accessibility is leveling the playing field and fostering innovation across diverse sectors worldwide.

AI in Industry Applications

AI's transformative potential is evident across multiple sectors:

·Healthcare: AI-powered diagnostic tools can now analyze medical images with greater accuracy than human experts, significantly improving patient outcomes [3].

- Finance: AI is revolutionizing fraud detection, automating trading strategies, and improving risk analysis. Around 73% of U.S. companies are leveraging AI for at least one business function [4].
- Retail: Businesses use AI-driven recommendation engines to enhance user engagement and customer satisfaction [5].Manufacturing: Predictive maintenance systems powered by AI are reducing machinery downtime by up to 30%, cutting costs and enhancing productivity [6].



Ethical AI and Governance

- As AI adoption grows, so do concerns about its ethical implications. Biased algorithms can lead to discriminatory outcomes, particularly in hiring, lending, and policing. To address this, developers are emphasizing diverse training data and explainable AI (XAI) models to improve transparency [7].

- Moreover, AI governance platforms are emerging to monitor AI systems and ensure they comply with ethical and legal standards [2].

However, the global nature of AI development means that regulatory consistency remains elusive, with significant variation in rules across countries and regions.

Challenges and Limitations

Despite its promise, AI is not without limitations:

- Privacy Concerns: AI systems often rely on sensitive personal data, raising issues around consent and misuse.
- Intellectual Property: AI-generated content blurs the lines of authorship and copyright, challenging existing IP frameworks.
- AI Hallucinations: Generative models can produce inaccurate or fabricated information, which can be harmful in critical domains like healthcare or law.
- Energy Consumption: Training large models consumes enormous

- amounts of energy, raising sustainability concerns [8].
- Talent Shortage: The demand for AI professionals continues to outpace supply, leaving gaps in expertise that hinder implementation [9].

Addressing these issues will require robust policy-making, continued investment in AI education, and sustainable AI development practices.

The Road Ahead

- Looking forward, AI will increasingly be integrated with other cutting-edge technologies:
- Edge AI: Processing data locally (on-device) instead of in the cloud will reduce latency and bandwidth usage. The edge AI market is expected to reach $15.7 billion by the end of 2025 [10].
- Quantum Computing: Though still in early stages, quantum computing promises to significantly accelerate AI computation, revolutionizing sectors like cryptography, materials science, and drug discovery [11].To ensure AI's impact is both transformative and equitable, it must be accompanied by strong ethical frameworks, cross-border cooperation, and sustainable innovations.

Conclusion

In 2025, AI is at the forefront of digital transformation. From improving diagnostic accuracy to enhancing supply chain efficiency, its impact spans all sectors. While challenges such as ethical concerns and the talent gap remain, the integration of AI with other technologies like edge and quantum computing, along with responsible governance,

will help harness its full potential. The future belongs to those whoadapt, innovate, and use AI not just as a tool—but as a partner in progress.

References

[1] McKinsey & Company, McKinsey Technology Trends Outlook 2024, 2024.

[2] Gartner, Top 10 Strategic Technology Trends for 2025, Gartner Research, 2024.

[3] BNMIT, "Top 10 Emerging Trends in Computer Science Engineering," BNMIT, 2023.

[4] SaM Solutions, "The Latest 15 Information Technology Trends in 2025," SaM Solutions, 2025.

[5] Softlabs Group, "20 Latest Trends in Information Technology," Softlabs Group, 2024.

[6] Technical Education Post, "Emerging Trends in Computer Engineering," Technical Education Post, 2024.

[7] Jobin, A., Ienca, M., and Vayena, E., "The global landscape of AI ethics guidelines," Nature Machine Intelligence, vol. 1, no. 9, pp. 389–399, 2019.

[8] Patterson, D., et al., "Carbon Emissions and Large Neural Network Training," arXiv preprint arXiv:2104.10350, 2021.

[9] EIMT, "Future of Computer Science: Trends You Need to Know in 2025," EIMT, 2025.

[10] GeeksforGeeks, "Top 25 New Technology Trends in 2025," GeeksforGeeks, 2025.

[11] Preskill, J., "Quantum computing in the NISQ era and beyond," Quantum, vol. 2, p. 79, 2018.

Ravina Mittal

Articles

Cognitive Architectures in Modern AI Systems: A Technical Overview

INTRODUCTION

Cognitive architectures are formal models of the invariant structures underlying intelligent behavior. They integrate components for memory, reasoning, learning, perception, and motor control into unified frameworks. The concept stems from early efforts in artificial intelligence (AI) and cognitive science, aiming to simulate human cognition in machines. In contrast to domain-specific algorithms, cognitive architectures serve as general-purpose infrastructures for building intelligent agents.

Historically, the early wave in the 1950s and 1960s consisted of symbolic rule-based systems such as GPS and EPAM, using structured problem solving and logical reasoning.These further evolved in more advanced architectures such as ACT (1973) and Soar (1987), incorporating learning theories, hierarchies for the purpose of memory, as well as goal-directed action. As neuroscience and psychology matured, cognitive architectures increasingly mirrored cognitive models grounded in empirical human studies.

Today, with growing demand for explainable and general AI, cognitive architectures are regaining relevance. Their explicit design, modularity, and transparency offer a principled alternative to opaque, end-to-end neural networks.Furthermore, hybrid approaches that embed large language models (LLMs) and neural networks into symbolic cognitive frameworks are emerging as

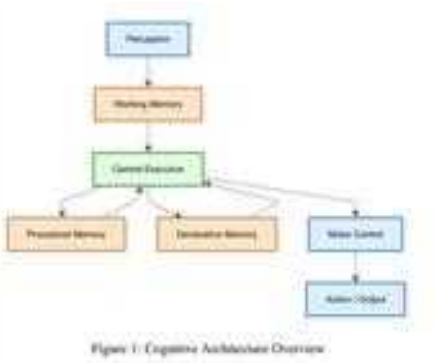
promising directions for artificial general intelligence (AGI).

The Rise of Cognitive Architectures

Cognitive architectures specify the fixed structures of cognition, including memory types, reasoning procedures, and control mechanisms. They differ from task-specific models by offering a reusable infrastructure for multiple domains. Most architectures consist of modules such as perception, action, working memory, declarative and procedural knowledge bases, and a central executive for coordination Figure 1. Architectures are broadly classified into three paradigms:

- Symbolic: These include Systems like Soar and ACT-R which represent knowledge using explicit symbols and rules, enabling high-level reasoning and interpretability.
- Connectionist: Inspired by neural networks, these models (e.g., Leabra, ART) emphasize learning and generalization through distributed representations.
- Hybrid: Architectures like CLARION and Sigma attempt to combine the strengths of symbolic reasoning with subsymbolic learning for flexibility and robustness.

• Hybrid: Architectures like CLARION and Sigma attempt to combine the strengths of symbolic reasoning with subsymbolic learning for flexibility and robustness.



Symbolic architectures are grounded in cognitive psychology and human experiments. ACTR, for instance, is extensively used to model human reaction times, memory retrieval, and learning curves. Soar, on the other hand, offers a general problem-solving framework based on production rules and goal hierarchies. Hybrid models seek to address the limitations of each paradigm by enabling, for instance, neural perception to feed into symbolic decision-making.

Classical Architectures

Soar

Soar represents cognition as a search through problem spaces using production rules. It operates via a decision cycle that involves proposing, selecting, and applying operators to achieve goals [3]. When impasses occur, Soar generates subgoals to resolve them, facilitating learning through a mechanism known as chunking, which c onsolidates new rules from experience. The architecture supports multiple memory types: procedural (rules), semantic (facts), and episodic (experience snapshots). Reinforcement learning enables it to refine decision-making over time.

Soar has been applied to cognitive robotics, military simulations, and intelligent tutoring systems

ACT-R

ACT-R (Adaptive Control of Thought-Rational) divides cognition into modular subsystems, each with a buffer that interfaces with working memory [1]. It distinguishes between declarative memory (facts) and procedural memory (rules), with production rules triggered based on the contents of these buffers

Sub-symbolic mechanisms determine activation levels of memory chunks, enabling ACTR

to simulate phenomena such as forgetting, priming, and decision latency. The architecture closely mirrors findings from experimental psychology, and has been used to model human performance in language processing, driving, and arithmetic tasks.

CLARION

CLARION (Connectionist Learning with Adaptive Rule Induction ONline) is a dual-process architecture combining implicit (neural) and explicit (symbolic) components [6]. The bottom level learns through reinforcement and error-driven adaptation, while the top level extracts and refines symbolic rules. This duality enables CLARION to model human skill acquisition and metacognition. Its architecture supports both reactive and reflective behavior, making it suitable for complex learning tasks like navigation, decision-making under uncertainty, and transfer learning

Sigma

Sigma introduces a factor graph-based approach to unify various cognitive processes [4]. It encodes reasoning, learning, and perception as probabilistic inference over graphical models, allowing for both symbolic and statistical computation within the same framework. Sigma is particularly notable for supporting mixed discrete-continuous representations, making it suitable for applications that involve uncertainty, such as dialogue systems or robotic navigation.

Architecture	Paradigm	Key Features
Soar	Symbolic	Production rules, chunking
ACT-R	Symbolic	Modular buffers, subsymbolic activations
CLARION	Hybrid	Dual-process (implicit+explicit)
Sigma	Hybrid	Probabilistic inference via factor graphs

Architecture	Applications
Soar	Military sims, tutors
ACT-R	Human modeling
CLARION	Skill acquisition
Sigma	Dialogue, robotics

Tables : Comparison of major cognitive architectures

Modern Integrations and Research (2022–2024)

Recent research integrates classical cognitive architectures with machine learning, especially LLMs and deep perception models Figure 2. Sumers et al. [5] proposed CoALA, a conceptual framework embedding LLMs as semantic processors within cognitive systems. LLMs are used for analogical reasoning, context retrieval, and theory-of-mind modeling, while symbolic modules handle structured planning and decision control.

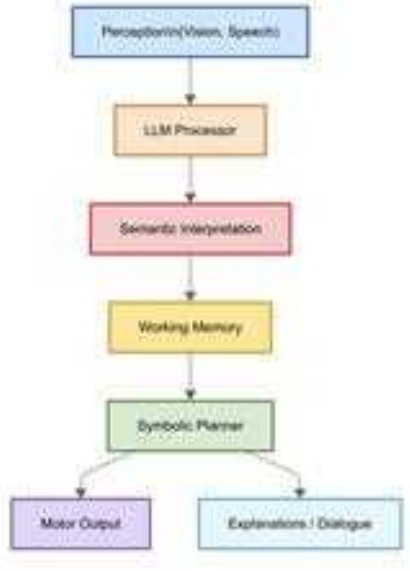


Figure 2: Modern cognitive system integrating LLMs with symbolic planners and perceptual modules.

In robotics, ACT-R/E extends ACT-R for embodied cognition [7], integrating perceptualmotor loops with cognitive control. Robots use visual inputs to populate working memory, enabling real-time interaction and adaptive learning.

OpenCog Hyperon exemplifies neuro-symbolic AGI efforts [2]. It integrates atomspace (a probabilistic knowledge graph), attention allocation, and program evolution in a distributed architecture. Hyperon supports self-modifying behavior and meta-reasoning, making it a candidate for general-purpose cognitive agents.

Other recent applications include cognitive tutoring systems, virtual assistants, and interactive narratives, where explainable and adaptive reasoning is essential.

Challenges and Considerations

- **Knowledge engineering:** Designing domain-specific rules and cognitive modules is labor-intensive. While some learning mechanisms exist, most architectures still depend on hand-coded knowledge bases, limiting scalability in open-world environments.
- **Memory modeling:** Balancing procedural, episodic, and semantic memory requires careful design. For instance, simulating long-term episodic memory demands realistic temporal decay and contextual tagging, which are difficult to implement efficiently. Moreover, integrating these systems into coherent behavior remains a challenge.
- **Representation:** Translating sensory data (images, audio) into symbolic structures for reasoning is an ongoing bottleneck. Hybrid systems often require engineered pipelines to convert neural outputs into symbolic forms, which can introduce fragility. Representation learning that bridges perception and logic is an active area of research.
- **Scalability**: As environments become more complex and interactive, cognitive architectures face computational bottlenecks. Decision cycles grow longer, memory stores expand, and rule-matching slows down. Efficient indexing, parallelization, and hardware acceleration are needed to scale these systems.
- **Benchmarking**: Evaluating general cognition lacks consensus. Most benchmarks test isolated capabilities like memory span or logical inference but fail to assess generality, transfer, or embodied learning. Shared testbeds such as the Cognitive Decathlon are being explored, but broader adoption is needed.

Future Directions

- **Neuro-symbolic** integration: Blending neural networks with rule-based logic can provide both adaptability and transparency. Architectures that support neural-symbolic feedback loops will be critical for robust general intelligence.
- **LLM-augmented reasoning:** Embedding LLMs into symbolic frameworks allows systems to tap into vast pretrained knowledge while maintaining structured control. This opens up new capabilities such as narrative reasoning, social inference, and commonsense planning.
- **Unified memory systems:** Future architectures must emulate cognitive phenomena like memory consolidation, interference, and prioritization. Drawing from neuroscience, systems may use sleep-inspired offline replay or synaptic plasticity analogs.
- **Embodied cognition:** As AI systems interact physically with their environments, cognition must integrate with perception and motor control. Architectures should accommodate real-time, sensorimotor feedback for navigation, manipulation, and social interaction.
- **Standardized evaluation:** Shared cognitive benchmarks across language, vision, motor, 5 and social domains are needed. PsychBench and the Cognitive Decathlon aim to offer such coverage.
- **Explainability and trust:** As cognitive architectures offer introspection capabilities, future research should emphasize how agents can communicate their reasoning steps to human users, improving collaboration and trust.

Conclusion

Cognitive architectures offer principled frameworks for general intelligence, rooted in decades of interdisciplinary research. From classical symbolic models like Soar and ACT-R to modern neuro-symbolic systems like OpenCog Hyperon and CoALA, they embody a modular, interpretable alternative to black-box AI. As demands for robust, transparent, and adaptive agents grow, cognitive architectures are poised to play a central role in next-generation AI systems.

References

[1] John R Anderson, Daniel Bothell, Michael D Byrne, Scott Douglass, Christian Lebiere, and Yulin Qin. An integrated theory of the mind. Psychological review, 111(4):1036, 2004.

[2] Ben Goertzel, Vitaly Bogdanov, Michael Duncan, Deborah Duong, Zarathustra Goertzel, Jan Horlings, Matthew Ikle, Lucius Greg Meredith, Alexey Potapov, Andre'Luiz de Senna, et al. Opencog hyperon: A framework for agi at the human level and beyond. arXiv preprint arXiv:2310.18318, 2023.

[3] John Edwin Laird, Keegan R Kinkade, Shiwali Mohan, and Joseph Z Xu. Cognitive robotics using the soar cognitive architecture. In CogRob@ AAAI, 2012.

4] Paul S Rosenbloom. The sigma cognitive architecture and system. AISB Quarterly, 136:4- 13, 2013.

[5] Theodore Sumers, Shunyu Yao, Karthik Narasimhan, and Thomas Griffiths. Cognitive architectures for language agents. Transactions on Machine Learning Research, 2023.

[6] Ron Sun, Edward Merrill, and Todd Peterson. From implicit skills to explicit knowledge: A bottom-up model of skill learning. Cognitive science, 25(2):203-244, 2001.

[7] J Gregory Trafton, Laura M Hiatt, Anthony M Harrison, Franklin P Tamborello, Sangeet S Khemlani, and Alan C Schultz. Act-r/e: An embodied cognitive architecture for humanrobot interaction. Journal of Human-Robot Interaction, 2(1):30-55, 2013.

Ritika Kalia

Ethical Hacking: Tools, Techniques, and Future Scope

ntroduction

Ethical hacking, often referred to as white-hat or penetration testing, is a forward-looking cybersecurity practice where specialists mimic cyber threats to uncover and fix security flaws before malicious hackers can exploit them. The expansion of AI, cloud systems, IoT, and quantum computing has made ethical hacking an essential component of digital defense strategies. Tech giants such as Facebook, Tesla, and Google actively support this through initiatives like red teaming and bug bounty programs [1].

Research & Tools

AI-Driven Academic Initiatives

The 2025 PenTest++ model integrates generative AI with automation to aid in stages like scanning, exploitation, and documentation. It aims for clarity, modular design, and minimizing inaccuracies from AI [2]. Research involving Linux systems indicates that while AI aids in tasks like privilege escalation, human oversight remains crucial [3].

A 2024 study categorized hacking tools into two major types: process-driven (like MITRE ATT&CK and PTES) and knowledge-based (such as CyBOK), highlighting that many tools have yet to gain widespread use among professionals [4].

Widely Used Platforms and Utilities

Kali Linux continues to be a primary toolkit, bundling essential utilities:

- Nmap – for network scanning
- Wireshark – for monitoring network traffic
- Metasploit – for exploiting system weaknesses
- Burp Suite – for testing web vulnerabilities
- sqlmap – for automated SQL injection tests
- Aircrack-ng – for analyzing wireless security
- John the Ripper – for password strength testing [5]

These tools span across the hacking process—from information gathering to attack simulation and follow-up analysis.

Current Research and Projects

MITRE's Project Falcon This project leverages AI to imitate attacker behaviors in real time, refining red team operations based on adaptive learning [6].

DARPA's AI Offensive Initiatives DARPA explores autonomous agents that can detect zero-day vulnerabilities in controlled setups, aiming for fast-paced, high-stakes testing environments [7].

HackerOne's AI-Powered Platform HackerOne uses AI to automatically sort and prioritize vulnerability data, easing the load on ethical hackers and developers alike [8].

AutoRecon-AI & PentestGPT These open-source tools are designed to partially automate reconnaissance and reporting, giving white-hat hackers AI-enabled assistance without full automation [9].

Challenges and Considerations

Technical Limitations AI tools can generate invalid or unreliable exploit payloads, referencing APIs or vulnerabilities that don't

exist [10]. Moreover, many enterprise environments still rely on outdated systems that lack compatibility with newer tools.

Ethical Constraints
Issues around handling confidential information, obtaining proper consent, and responsibly disclosing findings grow even more complex with AI's involvement [3].

Awareness Gaps
A significant number of academic tools haven't reached field use due to lack of industry exposure or complexity [4].

Evolving Threats
The advent of AI-crafted malware and phishing techniques is rapidly outpacing conventional security models. In addition, attacks like supply chain manipulation (e.g., slopsquatting) add another layer of complexity to ethical hackers' tasks [11].

Future Scope

Automation and XAI Adoption
AI security scanners are set to be embedded into development pipelines (CI/CD). Explainable AI (XAI) will become crucial for understanding vulnerability detection and fostering transparency [13].

Emerging Testing Areas

- IoT and ICS: Ethical hackers must learn to secure minimal-resource environments.
- Post-Quantum Encryption: New encryption schemes will demand rigorous ethical testing as RSA and ECC become outdated [15].
- Cloud Infrastructure: Penetration testing will shift to Kubernetes and container-based architectures [14].

Compliance and Integration
Ethical hacking will become continuous rather than occasional as organizations

adopt DevSecOps practices to ensure constant security monitoring [16].

Workforce Trends

According to a 2025 TechRadar study, roles like red team specialists, AI-driven SOC analysts, and offensive AI experts are seeing a significant surge in demand—about 38% growth [11]

Future Directions

Going forward, ethical hacking will increasingly align with proactive and predictive security practices instead of reactive ones. Anticipated developments include:

- **Digital Twin Penetration Testing:** Simulating attacks on virtual replicas of networks to avoid disruptions.
- **Federated Security Learning:** Secure, collaborative AI training across organizations.
- **AI-Written Security Protocols:** LLMs drafting policies and patch instructions.
- Frameworks for Ethical AI Use: Establishing international standards.
- Gamified Red-Blue Team Training: Immersive simulations using AI-generated environments.

These advances will push ethical hackers into more strategic roles involving design, simulation, and immediate countermeasures.

Conclusion

Ethical hacking is becoming a multidisciplinary field enriched by AI automation, diverse datasets, and specialized frameworks. Innovations like PenTest++ and AutoRecon-AI indicate that ethical hackers will need more than just technical expertise—they'll also need to understand legal norms, system behaviors, and moral accountability. With threats such as AI-based malware and quantum-level decryption on the rise, ethical hacking

will evolve into a continuous, design-integrated process, ultimately positioning white-hat hackers as key enablers of digital trust.

References

[1] Google Security Blog, "Bug Bounties: How Companies Like Google Secure Their Systems," 2024. [Online]. Available: https://security.googleblog.com/

2] A. AlSinani and P. Mitchell, "PenTest++: Elevating Ethical Hacking With AI and Automation," arXiv preprint arXiv:2502.12345, Feb. 2025. [Online]. Available: https://arxiv.org/abs/2502.12345

[3] A. AlSinani and P. Mitchell, "AI-Augmented Ethical Hacking in Linux Environments," arXiv preprint arXiv:2411.56789, Nov. 2024. [Online]. Available: https://arxiv.org/abs/2411.56789

[4] F. Modesti, R. Shah, L. Nguyen, and A. Singh, "Survey and Classification of Research-Informed Ethical Hacking Tools," arXiv preprint arXiv:2407.11111, Jul. 2024. [Online]. Available: https://arxiv.org/abs/2407.11111

[5] Offensive Security, "Kali Linux Documentation: Penetration Testing Tools," 2025. [Online]. Available: https://www.kali.org/docs/tools/

[6] MITRE Corporation, "Project Falcon: AI in Red Team Simulations," MITRE Technical Brief, Apr. 2025. [Online]. Available: https://www.mitre.org/publications/project-falcon

[7] DARPA, "AI Exploratory Research in Cyber Offense," DARPA Program Reports, Jan.

8] HackerOne, "Using AI in Vulnerability Management," HackerOne Blog, 2025. [Online]. Available: https://www.hackerone.com/blog/ai-vulnerability-management

Sahil Kumar

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