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

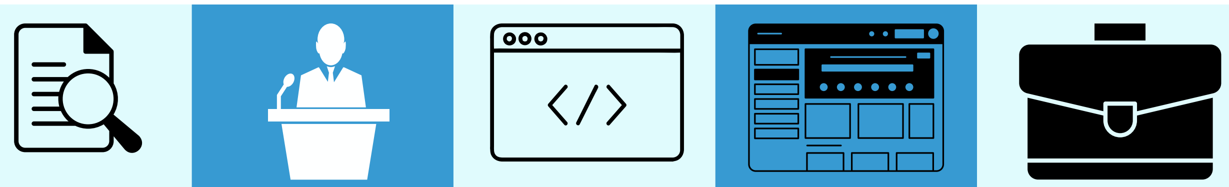
Designing & Digital Art

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

- **Sustainable and Intelligent Time-Series Models for Epidemic**
  May 2024
  Anureet Chhabra, Sunil Kr Singh, Akash Sharma, Kwok Tai Chui
- **SEIR-driven semantic integration framework: Internet of Things-enhanced epidemiological surveillance in COVID-19 outbreaks using recurrent neural networks**
  Apr 2024
  Saket Sarin, Sunil Kr Singh, Sudhakar Kumar, Kwok Tai Chui
- **Metaversal 6G: Deciphering Complex Requirements and Multivariate KPIs in High-Performance Computing**
  Jan 2024
  Sudhakar Kumar, Sunil Kr Singh, Ayushi, Brij B. Gupta

Book Chapters

- **Next Gen Security with Quantum-Safe Cryptography**
  July 2024
  Nipun Singh, Sunil Kr Singh, Sudhakar Kumar, Kwok Tai Chui
- **Homomorphic Encryption in Smart City Applications for Balancing Privacy and Utility**
  July 2024
  Sudhakar Kumar, Sunil Kr Singh, Brij B. Gupta, Jinsong Wu
- **FuzzyBack—A Hybrid Neuro-Fuzzy Ensemble for Concept Drift**
  July 2024
  Saket Sarin, Sunil Kr Singh, Sudhakar Kumar, F. Colace

Conference Papers

- **Exploring Advanced Neural Networks For Cross-Corpus Fake News Detection**
  May 2024
  Manya Girdhar, Sunil Kr Singh, Sudhakar Kumar, Kwok Tai Chui
- **Hyperdimensional Consumer Pattern Analysis with Quantum Neural Architectures using Non-Hermitian Operators**
  May 2024
  Shivam Goyal, Sunil Kr Singh, Sudhakar Kumar, Kwok Tai Chui
- **Revolutionizing Healthcare Systems: Synergistic Multimodal Ensemble Learning & Knowledge Transfer for Lung Cancer Delineation & Taxonomy**
  Jan 2024
  Aishita Sharma, Sunil Kr Singh, Sudhakar Kumar, Kwok Tai Chui
- **Towards Sustainable Consumer Electronics: DL-based SoH and RUL Prediction for E-Waste Reduction**
  Jan 2024
  Anureet Chhabra, Sunil Kr Singh, Akash Sharma, Kwok Tai Chui

EVENTS

JAVASCRIPT BOOTCAMP

Date: 22nd January, 2025
Number of attendees in the event: 19

The JavaScript Bootcamp, organized by the CCET ACM Student Chapter on January 22, 2025, was a successful event that introduced participants to the fundamentals of JavaScript. The session, held in the seminar hall, began at 2:30 PM and covered essential topics such as variables, data types, operators, conditional statements, loops, functions, and event handling. Attendees actively engaged in hands-on coding exercises, making the learning experience interactive and practical.

The event provided an excellent opportunity for students to enhance their web development skills and gain confidence in JavaScript programming. Participants appreciated the clear explanations and practical demonstrations, making the session both informative and engaging. The bootcamp concluded with a Q&A session, allowing attendees to clarify doubts and explore further learning opportunities.

GLIMPSE FROM THE EVENT

Articles

Revolutionizing Healthcare with Deep Learning: CT Scan Interpretation Across Diseases

Introduction

Computed Tomography (CT) scans are imaging tests that help medical professionals to detect, analyze and evaluate diseases in different parts of our body. These scans use X-rays to create accurate imaging of the patient's body. The CT scan is primarily used to identify tumors, injuries or inner bleeding in various organs such as kidneys, brain, heart, lungs etc. However, interpreting CT scans can be at times time-consuming and prone to human error due to the volume and complexity of image data. To overcome such complications AI (Artificial Intelligence) is being widely used in the modern medical field. Deep Learning models such as Convolutional Neural Networks (CNNs) are transforming diagnostics by accurately analyzing CT images, identifying patterns and detecting disease. These models not only help in detection but also helps in reducing the radiation exposure to the patient every time a CT scan is done using advanced reconstruction abilities.

Rise of AI in Medical Industry

The rise of Artificial Intelligence in CT imaging has reshaped how diagnostic medicine is practiced. As the amount of medical imaging continues to grow, AI has emerged as a powerful friend capable of rapidly analyzing complex CT scans and assisting in the detection of diseases such as tumors, hemorrhages, lung conditions, and more.

Articles

Deep learning models, especially convolutional neural networks (CNNs), have shown remarkable accuracy in identifying patterns that are most of the time overlooked by the human eye. With increasing advancements, AI is moving from experimental tools to active clinical support systems across hospitals and imaging clinics worldwide. The CT scan, a tool created in 1972 that is used as a basic necessity in today's time for any diagnoses is a boon on one side but simultaneously infiltrates the human body with constant radiation every time it is performed potentially increasing the risk of fatal diseases such as cancer. AI models on the rise not only help detect tumors but also help reconstruct low level images into more defined versions without needing the patient to undergo multiple scans, significantly reducing exposure while also keeping the process accurate and efficient.

Integration of Deep Learning in CT Imaging

The incorporation of deep learning into CT imaging is revolutionizing diagnostic radiology by automating and enhancing the interpretation process:

1. Automated Feature Extraction :

Traditional image processing relied on manual feature identifications–such as edge detection or shape analysis–to identify abnormalities. Deep learning, like Convolutional Neural Networks (CNNs), eliminates this step by learning and implementing relevant features directly from the data. These networks progressively identify simple to complex patterns as the image passes through layers.

Articles

2. Real-Time Interpretation :

Deep learning systems are now being deployed in real-time workflows, especially for critical conditions. For example, **Viz.ai** and **Aidoc** have developed FDA-cleared AI platforms that analyze CT brain scans within seconds to detect stroke or intracranial hemorrhage, alerting specialists instantly.[1]

3. Disease-Specific models :

Deep learning models are now trained for organ- or disease-specific CT analysis:

- Lung nodules (lung cancer screening): Optellum, Google LYNA [2]

- Kidney tumors and stones: Research models using custom CNNs

Recent Applications and Research

In the last five years the industry has witnessed a significant rise in usage of AI models for efficient and precise diagnosis not only in the radiology department but also many other clinical domains. These models are not only textbook limited but rather are being deployed across various different hospitals and clinics all around the world. Furthermore, continuous research is being conducted on a daily basis for the advancements of these models so that they can become our primary source of diagnosis and not just second opinions.

1. COVID-19 and Pneumonia Severity Estimation:

During the COVID-19 pandemic, AI-based CT analysis became critical in assessing pulmonary involvement and disease

Articles

e severity. CT shows greater sensitivity for early pneumonic change, disease progression, and alternative diagnosis, making it one of the most important methods in COVID-19 detection. Tools by Infervision, Qure.ai, and RADLogics were used across China, India, and Europe for triaging patients in overloaded healthcare systems.[3]

2. Stroke and Brain Hemorrhage Detection:

In emergency radiology, Viz.ai and Aidoc have developed FDA-cleared tools to detect acute ischemic stroke, hemorrhage, and large vessel occlusion directly from non-contrast head CT scans. These AI models reduce the time from scan to clinical decision, crucial in stroke care where minutes matter.

3. Lung Cancer Screening:

One of the most impactful applications is in low-dose chest CT (LDCT) for early lung cancer detection. Models like Google's LYNA and Optellum's AI decision support system are trained to detect and assess pulmonary nodules, often outperforming radiologists in detection of tumor cells and also with excellent time efficiency. A recent study proposed a novel lung cancer detection framework that utilizes a Flower Pollination Algorithm (FPA) to dynamically weight the outputs of a CNN ensemble comprising VGG16, ResNet101V2, and InceptionV3. Its adaptive weighting strategy led to significantly improved diagnostic accuracy, offering a new direction for performance-tuned AI in radiology. [5]

4. Multi-Organ Detection and Generalized Models:

A growing research direction is the development of generalized CT models trained across multiple organs and diseases. These models aim to function as universal triage assistants, flagging abnormalities in various body regions.[6]

Challenges and Limitations

Despite all the progress that is being made in the field of medicine relating to AI there are still many challenges that are being encountered by professionals in the practical implementation of all these models. These challenges are not only limited to technical issues but also bring in the social security concerns under the umbrella. Some of the challenges that are faced are:

1. Data Scarcity:

The models that are used for medical purposes require a large amount of already available data in order to create reliable and efficient algorithms. This leads to a problem since such data is not always available for diseases that are rare and thus cannot be implemented in the models. [4]

2. Overfitting:

The models that are used for medical purposes require a large amount of already available data in order to create reliable and efficient algorithms. This leads to a problem since such data is not always available for diseases that are rare and thus cannot be implemented in the models. [4]

Articles

3. Data Privacy:

Although AI models are used for advanced treatments, it should also be noted that these models are not immune to data theft. The images that are provided to the models are intimate CT scans of patients and could easily be used in criminal ways in case of any security breaches. This severely violates HIPAA laws made for the protection of a patient's identity.

Future Improvements

As new and better models are developed in the field of machine learning it becomes essential to incorporate them in the medical department. Future models must not only be accurate but also interpretable, they should not only provide the final decisions but also show and prove how that specific result was concluded.

1. Fine-Tune Radiation Optimization Models:

Future AI models, especially those related to CT scan, need to incorporate low-dose CT protocols so that it can reduce the amount of radiation exposure to the patient without hindering the efficiency.

2. Regulatory and Ethical Frameworks:

Push for more standardised rules and regulations incorporated within the models that include FDA approvals, clinical trials and real-world deployment.

3. Enhance Explainability:

PIncorporate visual interpretation tools like Grad-CAM, SHAP, and LIME to provide clinicians with clearer insights into AI predictions, thereby improving trust and clinical adoption.

Articles

4. Expand Multi-Disease Capabilities:

Develop more AI models so that a single CT scan can help detect various different diseases/injuries in different organs .This advancement will not only reduce the radiation levels as mentioned above but also help models move towards a general purpose diagnostic assistant.[5]

The next way of progress should focus more on gathering large amounts of relevant data necessary for creation of newer models with much better efficiency, reliability, accuracy and speed. The models should aim for large-scale, multi-center clinical validations and successful regulatory approvals.

Conclusion

The integration of deep learning into CT imaging has transformed the landscape of medical diagnostics, offering remarkable gains in speed, accuracy, and consistency. Integration of modern machine learning methods with medical advancements truly have opened endless possibilities to take our current diagnostic practices to a whole another level. However, this progress is accompanied by challenges such as data scarcity, class imbalance and privacy risks that must be responsibly addressed. With continued research, interdisciplinary collaboration, and clinical validation, these models have the potential to not only assist physicians but also redefine diagnostic standards in healthcare.

References

[1] Windecker D, Baj G, Shiri I, et al. Generalizability of FDA-Approved AI-Enabled Medical Devices for Clinical Use. JAMA Netw Open. 2025; https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2833324

[2] Ardila D, Kiraly AP, Bharadwaj S, Choi B, Reicher JJ, Peng L, Tse D, Etemadi M, Ye W, Corrado G, Naidich DP, Shetty S. End-to-end lung cancer screening with three-dimensional deep learning on low-dose chest computed tomography. https://pubmed.ncbi.nlm.nih.gov/31110349/

[3] Fusco R, Grassi R, Granata V, Setola SV, Grassi F, Cozzi D, Pecori B, Izzo F, Petrillo A. Artificial Intelligence and COVID-19 Using Chest CT Scan and Chest X-ray Images: Machine Learning and Deep Learning Approaches for Diagnosis and Treatment. https://pmc.ncbi.nlm.nih.gov/articles/PMC8540782/

[4] Hossain, M. M. et al. (2024). A hybrid CNN-based method for kidney disease classification. https://arxiv.org/pdf/2502.04367

[5] Zhou, L., Jain, A., Dubey, A. K., Singh, S. K., Gupta, N., Panwar, A., Kumar, S., Althaqafi, T. A., Arya, V., Alhalabi, W., & Gupta, B. B. (2025). FPA-based weighted average ensemble of deep learning models for classification of lung cancer using CT scan images. Scientific Reports, 15, 19369. https://doi.org/10.1038/s41598-025-02015-w

[6] Khan, H., Ilyas, M., Muneer, M., & Almotiri, S. H. (2023). Deep learning in diagnostic imaging: A review on the detection of liver, lung, and breast

Articles

cancers. Cancers, 15(9), 2573. https://doi.org/10.3390/cancers15092573

Eshmeet Singh

Developing the Conscious Network for 6G and Beyond

Introduction

Speed, capacity, and connectivity have all played a key role in the development of mobile networks. Every generation has changed how we interact with technology, from 1G's analog voice to 5G's ultra-low latency and high throughput. The story is changing now that 6G is expected to arrive by 2030. In addition to being faster, the network of the future will be intelligent. According to this new paradigm, a network is capable of sensing, adapting, learning, and acting intentionally. The conscious network is aware of its users, surroundings, context, and ethical limitations, but it is not a sentient entity. It represents the combination of adaptive protocols, ubiquitous sensing, artificial intelligence, and sustainable engineering [1][2].

CONSCIOUS NETWORK

The term "consciousness" in networking describes how context-aware intelligence is woven into the structure of communication networks. A conscious network can sense its operating environment, decipher user intent, predict system states, and modify its behavior accordingly. It transmits purpose instead of raw data, optimizing not just performance but also ethics, efficiency, and meaning [3]. In a smart city, for instance, a conscious network might reduce its operating energy when powered by finite renewable

Articles

resources, prioritize emergency traffic over entertainment, or reroute data to avoid crowded nodes. This type of dynamic awareness is made possible by advancements in digital twin technology, AI, and semantic communication [1].

CONSCIOUS 6G NETWORK FOUNDATIONS

1. Pervasive Intelligence

With machine learning models integrated throughout the network, from the core to the edge, 6G will be AI-native. In addition to forwarding packets, base stations will also anticipate traffic trends, proactively distribute resources, and instantly identify anomalies. By processing data close to the source, edge computing will lower latency and allow for context-sensitive decision-making [1][2].

2. Semantic Communication

Conventional networks send bits without regard to their significance or relevance. Semantic communication, or transmitting only what is necessary to sustain an intent of a message, is adopted by aware networks. To save data load and keep bandwidth, a monitoring network might, for instance, transmit an alert that "an object crossed a boundary" instead of passing through the whole video data [3]

3. Digital twins and massive sensing

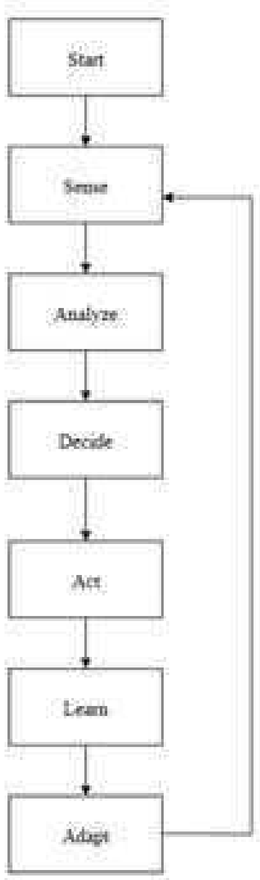
With sensors incorporated into devices, environments, and infrastructure, the 6G network will be deeply integrated. Digital twins, which are virtual representations of physical systems, will receive real-time data from these sensors. By continuously learning from these twins, networks will be able to predict failures before they happen and optimize performance [2].

4. Designing for Sustainability

Climate awareness is also necessary for a conscious network. This includes support for energy-harvesting devices, load balancing based on the carbon intensity of electricity, and intelligent energy use. Energy-efficient routes will be given priority by protocols, which will also cut down on pointless transmissions and modify transmission power according to the environment [3].

5. Ethical Adaptation and Trust

Consciousness revolves around security and trust. These networks will be capable of independently identifying threats, enforcing privacy regulations, and adhering to moral and legal requirements. For instance, data routing may take user consent preferences or geopolitical boundaries into account in addition to speed. [1].



Operational Flow of a Conscious 6G Network

The flow chart shows the essential operation cycle of a 6G conscious network. It starts with environmental, user, and context sensing with deep, imbedded sensors. It processes the gathered information by applying sophisticated AI to infer meaning and identify priorities. This determines the best actions to optimize performance, ethics, and sustainability on which the network acts by dynamically remapping configurations, routes, and resources. These results are continuously learned and cycled back into the system in order to refresh predictions and actions. Ultimately, the network is updated in real time, making sure it remains context-sensitive, effective, and in compliance with environmental and moral standards – entering this loop again in order to truly be 'conscious'.

ENGINEERING CONSCIOUS NETWORKS PRESENTS DIFFICULTIES

The shift from intelligent to conscious networks presents a number of philosophical and engineering difficulties:

Computational Overhead: Energy usage rises when AI is integrated into every node. It is essential to design efficient, low-power models [1].

Ethical Ambiguity: Who establishes the moral guidelines that the network must adhere to? Can these regulations be applied in different jurisdictions and cultures?

Protocol Innovation: AI-based routing and real-time semantic negotiation were not supported by legacy networking stacks. It might be necessary to create entirely new layers.

Data Governance: Massive data is a byproduct of digital twins and massive sensing. It becomes crucial to guarantee explainability, equity, and privacy [3]

USE CASES AND APPLICATIONS

Disaster-Aware Communication

Autonomous drones that prioritize emergency responders, create temporary networks, and dynamically allot bandwidth to mission-critical communications could be deployed by conscious networks in disaster-affected areas [1].

Conscious Healthcare Systems

By distinguishing between routine telemetry and life-threatening anomalies, a hospital's 6G network could adjust resource allocation while maintaining patient privacy and adhering to legal requirements [2].

Green and Intelligent Cities

During energy shortages, urban networks may prioritize sensors that monitor traffic, pollution, or weather anomalies, or they may turn off non-essential services. These actions would be morally consistent with city regulations and context-driven [3].

Data Sovereignty and Ethical Roaming

Conscious networks could enforce cross-border data constraints, ensuring user data is not routed through or stored in unauthorized regions, complying with local laws and respecting user-defined ethical boundaries

FROM IDEATION TO ACTUALITY

The conscious network will need to be achieved by: · Interdisciplinary Research:

Cooperation between human–computer interaction, energy systems, ethics, networking, and artificial intelligence [1].

· New Protocol Stacks: Protocols need to facilitate semantic relevance, context interpretation, and intent negotiation.

· Standardization and Governance: International initiatives to specify and control how these networks function, including accountability and transparency systems.

· Sustainability benchmarks include calculating the environmental impact of network choices and creating self-optimizing systems [3].

CONCLUSION

Not only are we expanding the capabilities of networks as we progress toward 6G and beyond, but we are also rethinking their function. The conscious network signifies a significant shift in the way systems think, communicate, and develop. In addition to being quick and dependable, it pushes us to design connectivity that is conscious, flexible, and consistent with both human and environmental values. In networking, the path to consciousness is both ambitious and essential. Our networks must improve not only in performance but also in awareness in a world that demands ethics, intelligence, and resilience. Let's create networks that are more thoughtful as well as smarter.

Articles

REFERENCES

[1] Saad, W., Bennis, M., & Chen, M. (2020). A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Network, 34(3), 134-142. https://doi.org/10.1109/MNET.001.1900287

[2] Strinati, E. C., Barbarossa, S., Gonzalez-Jimenez, J. L., Ktenas, D., Cassiau, N., & Dehos, C. (2019). 6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication. IEEE Vehicular Technology Magazine, 14(3), 42-50. https://doi.org/10.1109/MVT.2019.2921162

[3] Dang, S., Amin, O., Shihada, B., & Alouini, M. S. (2020). What Should 6G Be? Nature Electronics, 3(1), 20-29. https://doi.org/10.1038/s41928-019-0355-6

Simar Atwal

Multi-Agent Systems in AI: Collaboration, Communication, and Emergent Intelligence

INTRODUCTION

Intelligence is rarely a singular occurrence in nature. Complex systems frequently result from the interactions of several independent agents, as seen in human social behaviour and the coordinated flight of birds. Artificial intelligence researchers have created Multi-Agent Systems (MAS) as frameworks for distributed communication, problem solving, and emergent behaviour, motivated by these ideas. A multi-agent system is fundamentally made up of several intelligent entities, or agents, that interact with one another, perceive their surroundings, and make decisions in order to accomplish individual or group objectives. These agents could be software entities negotiating over cloud resources, financial bots in a market, or even robots in a fleet. MAS systems must deal with partial observability, distributed knowledge, and coordination among entities with potentially conflicting objectives, in contrast to single-agent systems that optimize behaviour based on a single perspective. They become more powerful and in line with the dynamics of the real world as a result, but they also become more complex.

Articles

COMMUNICATION AND COORDINATION

Effective communication is a major problem in MAS. To coordinate activities, prevent confrontations, and share observations, agents need to communicate with one another. Communication protocols can be implicit, depending on environmental cues or stigmergy,- an indirect method of communication employed by social insects, or explicit, involving the direct passing of messages. The complexity of coordination mechanisms varies. Coordination may be predicated on established rules in simple systems. In more complex systems, agents bid for resources or tasks through market-based methods, consensus algorithms, or even negotiation. To maximize efficiency, for instance, agents may bargain over which robot retrieves which package in a multi-robot warehouse. Coordination in swarm robotics is frequently emergent, with agents adhering to basic local laws that produce global order.

These communication strategies need to be designed with efficiency, scalability, and robustness in mind. While insufficient communication can result in coordination issues, excessive communication can overload bandwidth and impair system performance.

LEARNING IN MULTI AGENT SYSTEMS

Compared to single-agent systems, learning in MAS is much more complicated. In addition to learning about its surroundings, each agent also needs to learn about the behaviour of other agents, which may be changing at the same time.

Articles

Multi-Agent Reinforcement Learning (MARL)

is one of the fundamental methods in this field. While taking other people's policies into account, agents in MARL learn policies that optimize their own rewards. This frequently results in learning environments that are non-stationary, meaning that the best course of action for each agent is contingent upon the strategies of other agents as they evolve. There are several learning paradigms:

- Independent learning: Every agent picks up its own policy on its own.
- Joint action learning: Using shared rewards as a basis, agents discover the best joint strategies.
- Centralized training with decentralized execution: Agents can access centralized data while training, but they function independently during runtime.

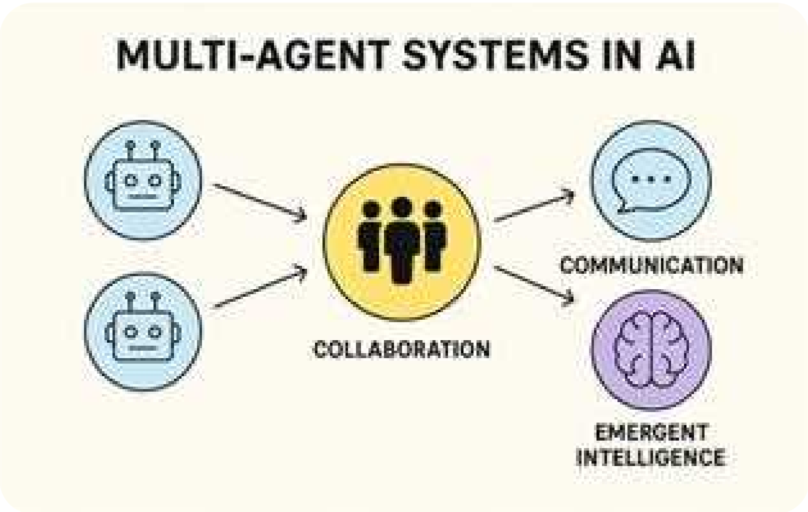
Deep MARL systems are now able to solve intricate coordination tasks in real time thanks to recent developments in deep learning. In contexts ranging from autonomous traffic systems to strategic games, algorithms like COMA (Counterfactual Multi-Agent Policy Gradients), QMIX, and MADDPG (Multi-Agent Deep Deterministic Policy Gradients) exhibit scalable performance.

EMERGENT BEHAVIOUR AND SELF ORGANISATION

The development of complex behaviour from basic local interactions is one of the most intriguing features of MAS. Emergent behaviour is a phenomenon that is replicated in artificial systems and seen in nature. For example, in ant colonies, no individual ant is aware of the overall foraging strategy, but the group as a whole determines the best routes to food. Similar to this, agents in MAS can accomplish complex goals like collective mapping, flocking, and surveillance by adhering to basic rules. Numerous applications in swarm robotics, environmental monitoring, and disaster response have been sparked by this idea of self-organization. These systems are appropriate for dynamic or hostile environments because they have high fault tolerance and little need for centralized control.

APPLICATIONS OF MAS

- Autonomous Vehicles and Robotics Drone or autonomous car fleets need to coordinate in order to share data, optimize routes, and prevent collisions. Swarm-like coordination is made possible by MAS in situations where GPS is unavailable or during relief efforts. To accomplish global goals, agents communicate locally, improving resilience and scalability. Applications in space exploration, the military, and search and rescue depend on such systems.



Articles

- Financial markets Because trading bots communicate with one another in real time, MAS is perfect for managing and simulating high-frequency markets. These systems are capable of simulating market equilibria, price formation, and competition. MAS assists in locating possible cascading failures and market vulnerabilities. Through simulation, it also aids in the design of financial infrastructures that are more resilient.
- Healthcare Distributed diagnostic agents can work together to suggest interventions and track patients across multiple health indicators. MAS facilitates effective resource allocation in hospital logistics. To enhance patient care and cut down on wait times, agents can collaborate across departments. Additionally, MAS facilitates remote healthcare and real-time monitoring for the management of chronic diseases.
- Multi-Agent Simulation for Social Sciences Traffic dynamics, epidemic spread, social behaviour, and even election results are all frequently modeled using MAS. These simulations provide insights into intricate systems in which social trends are shaped by individual behaviours. Policy interventions are tested in controlled virtual environments by researchers using MAS. These simulations offer data-driven projections to help guide choices.
- Cyber Security and Intrusion Detection Real-time threat detection, network patrolling, and anomaly detection are all capabilities of MAS agents. In distributed systems, autonomous agents work together to identify and eliminate malware. They offer quick, dispersed reactions to complex cyberattacks. By facilitating proactive defence across sizable, intricate infrastructures, MAS improves resilience.

CHALLENGES

- Scalability: Coordination becomes more challenging as the number of agents increases. Both computational complexity and communication overhead are growing quickly. In large-scale systems, this may result in bottlenecks, delays, and inefficiencies.
- Security and Robustness: Agents may deceive people or mimic harmless behaviour in hostile environments. For real-world deployments, resilience against such threats is essential. One agent's flaws could jeopardize the system's overall security. Adversarial training, trust systems, and continuous observation are necessary for robustness.
- Ethical and Governance Issue: As agents behave on their own, concerns about decision transparency, bias, and accountability surface. The ethical framework that directs agent behaviour becomes crucial in systems that involve human interaction.

Ignoring these issues can damage one's reputation and undermine trust.To guarantee responsible deployment, transparent governance models and moral AI standards are required.

FUTURE DIRECTIONS

MAS that is neurosymbolic
More interpretability and generalization are provided by hybrid systems that combine neural learning and symbolic reasoning. These methods hold particular promise for applications that demand transparency and involve high stakes.
Multi-Agent Federated Learning
Decentralized AI model training while maintaining data

Articles

privacy is made possible by combining federated learning and MAS; this makes it perfect for applications such as collaborative healthcare.

Teams of Humans and Agents
Humans will be agents in future MAS, working in dynamic teams with AI. To sustain these human-AI ecosystems, research in explainable AI, trust modeling, and shared autonomy is essential.

CONCLUSION
A fundamental change in the way we develop and implement intelligent systems is represented by multi-agent systems. More resilient, scalable, and cross-domain solutions are made possible by the shift from isolated intelligence to collaborative, distributed intelligence. MAS provides a blueprint for next-generation AI systems that are collective by design, whether they are used to manage decentralized energy systems, coordinate fleets of robots, or simulate human societies. Both technological innovation and philosophical investigation are necessary for the future. The design principles guiding these interactions will influence the future of autonomy, accountability, and shared intelligence as machines work together more and more—and with humans. In this way, multi-agent systems represent a vision for how intelligence itself can develop in a networked world, not just a branch of artificial intelligence research.

Articles

REFERENCES

1. Busoniu, L., Babuska, R., & De Schutter, B. (2008). A comprehensive survey of multi-agent reinforcement learning. IEEE Transactions on Systems, Man, and Cybernetics, Part C, 38(2), 156–172.
2. Shoham, Y., & Leyton-Brown, K. (2009). Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. Cambridge University Press.
3. Lowe, R., et al. (2017). Multi-Agent Actor-Critic for Mixed Cooperative-Competitive Environments. Advances in Neural Information Processing Systems (NeurIPS).
4. Zhang, K., Yang, Z., & Basar, T. (2019). Multi-Agent Reinforcement Learning: A Selective Overview of Theories and Algorithms. Handbook of Reinforcement Learning and Control.
5. Wooldridge, M. (2009). An Introduction to MultiAgent Systems (2nd ed.). Wiley.

Bhavya

Self-Healing AI Systems: Reinforcement Learning for Autonomous Cyber Defence

INTRODUCTION

The complexity and interconnectedness of digital ecosystems have led to an exponential growth in the threat landscape in cyberspace. Every development in software-defined networks, cloud computing, and the Internet of Things (IoT) is accompanied by a rise in potential attack points and vulnerabilities. Even though they are still essential, traditional cybersecurity tools like firewalls, intrusion detection systems, and antivirus software are insufficient in the face of increasingly complex, persistent, and automated threats. Systems of the future must be able to respond, adapt, and recover on their own in addition to detecting anomalies.

AI systems that can heal themselves are useful in this situation. These systems, which draw inspiration from biological immunity and homeostasis, are designed to identify, isolate, and fix cyber intrusions on their own without the help of humans. They use reinforcement learning (RL), a subfield of machine learning in which agents discover the best course of action via trial and error, to defend infrastructure in real time. The design, operation, and uses of RL-driven self-healing AI systems are examined in this article. We look at how these agents can respond to attacks, adjust defences, keep an eye on system integrity, and pick up on changing threats. We also go over limitations, practical applications, and the future of autonomous cyber defence.

WHAT IS SELF-HEALING AI SYSTEM?

An intelligent agent that observes its surroundings, recognizes dangers or malfunctions, responds appropriately, and adjusts its approach over time without direct human guidance is referred to as a self-healing AI system.

Key capabilities:

- Detection: Find unusual trends in system behaviour or data.
- Diagnosis: Identify the problem's origin, nature, and extent.
- Remedial action should be taken (e.g., patch vulnerability, block port, isolate node).
- Recovery: Return impacted states or services to normal.
- Learning: Modify policies in light of new data and results. Reinforcement learning is frequently used to implement these features in conjunction with automation APIs, system telemetry, and monitoring tools.

THE NEED FOR AUTONOMOUS AI:

- Complexity and Scale: Clouds, edge devices, containers, microservices, and APIs are all part of modern IT systems, which result in extremely complex and dispersed environments. It is no longer feasible to manage, monitor, and secure this infrastructure by hand; automation is required for accuracy and efficiency.
- Speed of Attacks: There is little time for human intervention when cyberattacks like ransomware, zero-day exploits, and lateral movement tactics happen at machine speed. To identify threats and take immediate action to stop damage, automated defence systems are required.
- Skill shortage: Because of the global

scarcity of qualified cybersecurity specialists, it is difficult for businesses to keep up robust defences. By managing repetitive tasks and improving incident response effectiveness, automation helps close this gap.

- Sophistication Of Threats: Advanced Persistent Threats (APTs) circumvent conventional defences by using multi-stage, covert tactics. Security systems that are AI-driven and adaptive are better able to identify, evaluate, and neutralize such complex threats instantly.

APPLICATIONS

- Cloud Security: Self-healing systems can rotate credentials, isolate compromised components, and monitor service integrity in dynamic cloud environments where services scale up and down continuously. In settings where assets change frequently, they aid in maintaining compliance. Through quick containment, these systems minimize downtime and restrict the blast radius of attacks.
- IoT and Edge Devices: Strong security is frequently absent from low-power IoT devices. Lightweight RL agents are able to initiate localized healing protocols and identify anomalies (such as unexpected data surges or unauthorized access). This proactive defence stops minor breaches from getting worse.

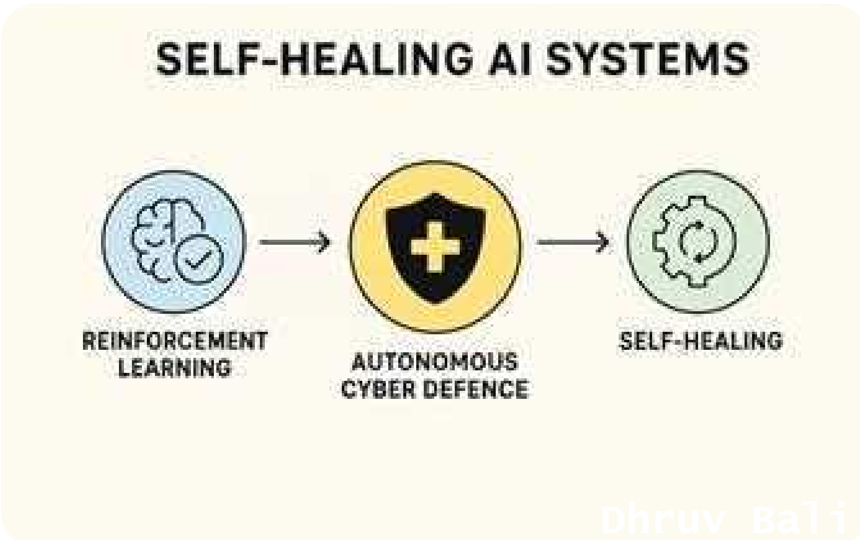
In smart environments and critical infrastructure, self-healing improves resilience.

- Zero Trust Architecture: Self-repair by constantly confirming trust boundaries, AI can uphold the zero trust principles. Policies can be updated instantly to stop untrusted behaviour when anomalies arise. Security postures are strengthened against changing threats through ongoing validation. These systems lessen the need for manual supervision and static rules.

.

- Enterprise Incident Response: Self-healing systems can lock compromised nodes, cut off network segments, and start data restoration procedures without human intervention during ransomware outbreaks

They reduce operational disruption and facilitate quicker recovery. The time between detection and containment is shortened to just a few seconds thanks to this automation.



Articles

CASE STUDIES AND PROJECTS

- **Deep Armor by Spark Cognition:** employs reinforcement learning (RL) to anticipate and stop malware from running on endpoints. Its agents pick up the best answers to system calls and binary behaviours. Through real-time behaviour pattern analysis, it proactively defends against zero-day threats. Through exposure to novel attack vectors, Deep Armor continuously improves its models.

- **IBM Watson for Cybersecurity:** combines playbooks, automation, and machine learning to plan incident responses; RL components are added gradually to adjust defence tactics. By connecting threats with useful insights, it improves SOC efficiency. Over time, IBM Watson hopes to develop security environments that are more contextually aware and adaptive.

- **Microsoft Defender for Endpoint:** makes use of auto-remediation procedures and behavioural cues. By comparing attack graphs and initiating mitigation, it is moving closer to self-healing even though it is not yet entirely RL-based. For proactive defence, it integrates real-time telemetry with threat intelligence. Microsoft is still working to make it more resilient and independent.

- **DARPA's Cyber Grand Challenge:** In competitions, autonomous systems outperformed human teams by scanning, identifying, and patching vulnerabilities in real-time. It demonstrated the viability of machines protecting intricate systems on their own. The foundation for upcoming developments in autonomous cybersecurity was established by this competition.

Articles

CHALLENGES

Reward Function Design: Unexpected or less-than-ideal behaviour can result from poorly constructed reward signals. To prevent false positives, an agent might, for instance, block all external IPs, which would disrupt legitimate services. To match agent actions with actual security objectives, careful reward shaping is required. Agents are better able to prioritize security and operational continuity when they undergo regular testing.

Safety and Explainability: High impact can result from autonomous actions, such as shutting down a system. For decisions to be auditable and comprehensible, explainability is essential. For compliance and trust, security teams must have a clear justification for their decisions. Adoption in regulated industries depends on transparent AI models.

Adversarial Manipulation: To fool agents, attackers could contaminate the learning environment or alter feedback loops. Frameworks for secure reinforcement learning are crucial. Before deployment, vulnerabilities can be found with the aid of thorough adversarial testing. Monitoring systems and fail-safes are necessary to identify manipulation in real time.

Data Scarcity and Simulation: Training robust RL agents requires exposure to diverse threats. Simulated cyber ranges or synthetic data must be used to generate training scenarios. Real-world cyberattack data is rare, sensitive, and difficult to access. Simulations help agents generalize their learning to unpredictable attack patterns.

CONCLUSION

The conventional perimeter-based, rule-driven defence is no longer adequate as cybersecurity threats increase in number, complexity, and speed. We need to transition to autonomous, continuous systems that can think, adapt, and heal themselves. Reinforcement learning-driven self-healing AI systems are revolutionizing cyber defense. These agents can foresee threats, react wisely, and change with the environment by viewing security as a dynamic game of strategy. They provide a proactive, robust, and scalable substitute for manual defences. The potential advantages are enormous, despite the fact that there are still difficulties, especially with regard to safety, reward design, and training data. AI agents could soon serve as our digital world's immune system, continuously patrolling, defending, and recovering from attacks without the need for human assistance.

REFERENCES

1. Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction. MIT Press.

2. Nguyen, N. T., Hoang, D. T., Nguyen, D. N., et al. (2019). Deep Reinforcement Learning for Cyber Security. IEEE Transactions on Neural Networks and Learning Systems, 30(10), 3214-3228.

3. Shrobe, H. E., et al. (2016). Toward a Science of Autonomy for Physical Systems: A Cyber Physical Systems Perspective. MIT Lincoln Laboratory.

4. Fadlullah, Z. M., & Kato, N. (2017). Intrusion Detection System in the Context of Cloud Computing and Internet of Things. IEEE Communications Magazine, 55(3), 64-69.

Articles

5. DARPA Cyber Grand Challenge. (2016). https://www.darpa.mil

Aanshi Bansal

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
2023

Aanshi Bansal
2023

Content Editors

Bhavya
2023

Vanshika Singla
2023

Feature Editors

Khushi
2023

Saksham
2023

Anshika
2024

Tanvi
2024

Shiven
2024

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