SEPT-OCT 2025 VOLUME 6 | ISSUE 5

DIGITAL OUTLET

REVOLUTIONIZING INDUSTRIES, TRANSFORMING LIVES

CYBER FUTURE

HOW TECHNOLOGY IS SAFEGUARDING THE DIGITAL WORLD

GREEN TECH

SUSTAINABILITY MEETS SMART SOLUTIONS

Unlocking the Potential of Augmented Reality

Space Tech

Smart Gadgets to Simplify Your Life

Cybersecurity 2025

Are We Prepared?

PUBLISHED BY-
CCET ACM STUDENT CHAPTER
CCET, DEGREE WING, SECTOR 26
CHANDIGARH

acm CET STUDENT CHAPTER ccet.acm.org

CONTENT

LET'S START

1

WHERE TO NEXT?

2

CONCLUSION

3

Note from our *Mentors*

Dr. Manpreet Singh

Principal CCET (Degree Wing)

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

Dr. Sunil K. Singh

Professor and HOD, CSE | Faculty Mentor

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

Dr. Sudhakar Kumar

Assistant Professor, CSE | Faculty Sponsor

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

"The greatest achievement of technology is not how it changes life, but how it improves it."

ACM'S VISION AND MISSION

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 make the department a smart centre for learning, innovation and research, creativity, and entrepreneurship for the stakeholders (students/scholar, 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.

ASSOCIATION FOR COMPUTING MACHINERY AT CCET

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.

Student Speaker Program

Designing & Digital Art

Research and Development

Competitive Codong

Internship & Career Opportunity

CCET ACM STUDENT CHAPTER

ABOUT

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.

Student Speaker Program

Designing & Digital Art

Research and Development

Competitive Codong

Internship & Career Opportunity

CCET ACM-W STUDENT CHAPTER

ABOUT

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.

Student Speaker Program

Designing & Digital Art

Research and Development

Competitive Codong

Internship & Career Opportunity

ACHIEVEMENTS

Our team's recent publications showcase notable progress in diverse areas of Computer Science, including deep learning, security, and intelligent systems. These works have appeared in high-impact journals, conferences, and book chapters during the initial part of 2025.

Journal Articles

- Advanced Web Traffic Modelling and Forecasting with a Hybrid Predictive Approach
  Author- Ujjwal Thakur, Sunil Kr Singh, Sudhakar Kumar, Kwok Tai Chui

- Cardiovascular Sound Classification Using Neural Architectures and Deep Learning for Advancing Cardiac Wellness
  Author- Deepak Mahto, Sudhakar Kumar, Sunil Kr Singh, Bassma Saleh Alsulami

- Quantum-Resistant Cryptographic Primitives Using Modular Hash Learning Algorithms for Enhanced SCADA System Security
  Author- Sunil Kr Singh, Sudhakar Kumar, Manraj Singh, Brij B. Gupta

- FPA-based weighted average ensemble of deep learning models for classification of lung cancer using CT scan images
  Author- Liang Zhou, Achin Jain, Arun Kumar Dubey, Brij B. Gupta

- Neural Network Architectures for Machine Translation: Enhancing Quality Education Through Improved Access to Multilingual Resources
  Author- Ayushi, Sudhakar Kumar, Sunil Kr Singh, Brij B. Gupta

- Advanced Tools and Technologies for Phishing Prevention
  Author- Kashish Preet Kaur, Sunil Kr Singh, Sudhakar Kumar, Sunil Kr Sharma

- Advanced Techniques and Best Practices for Phishing Detection
  Author- Ravina Mittal, Sunil Kr Singh, Sudhakar Kumar, Konstantinos Psannis

- Foundations of Phishing Defense: Comprehensive Strategies for Digital Asset Protection
  Author- Raj Kanwar, Sumit Bawa, Sunil Kr Singh, Abhay Ratnaparkhi

- Phishing Prevention Solutions and Mechanisms
  Author- Abhavya Muku, Sunil Kr Singh, Sudhakar Kumar, Vandana Sharma

Book Chapters

- Integrating Machine Learning into Cardiovascular Disease Risk Prediction: A Comprehensive Analysis of Cholesterol, Heart Rate, and Gender Impact on Disease Prevalence
  Author- Abdul Rahim, Amit Chhabra, Manya , Karan Sharma

Conference Papers

- Application of Green IoT in Digital Oilfields for Achieving Sustainability in the OnG Industry
  Author- Soumya Sharma, Sunil Kr Singh, Sudhakar Kumar, Tarun Vats

- Blockchain Based Election System Using Fingerprint Recognition
  Author- Uday Madan, Sunil Kr Singh, Sudhakar Kumar, Himanshu Setia

EVENTS

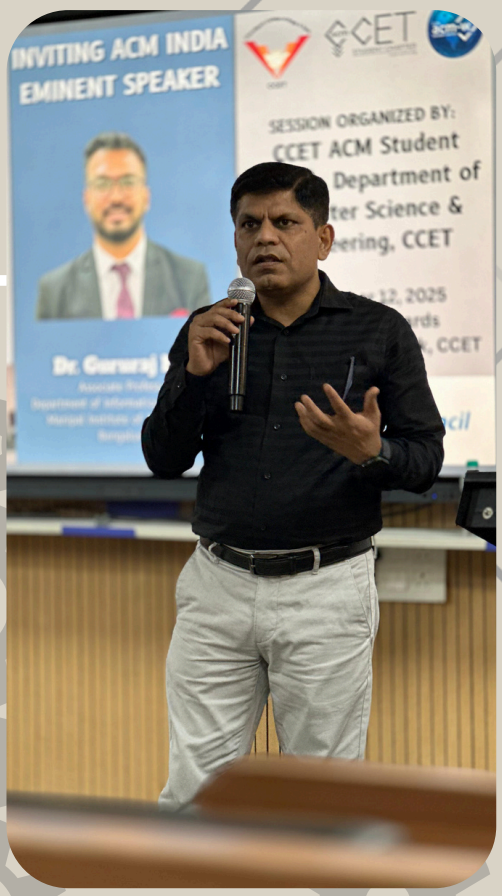
Distinguished Talk on AI and Generative AI in Cybersecurity: From Insight to Foresight through Critical Thinking and Generative Innovation

On September 12, 2025, the CCET ACM and ACM-W Student Chapter hosted a talk by Dr. Gururaj H. L. on "AI and Generative AI in Cybersecurity." The event, a collaboration with the Department of Computer Science and Engineering, drew a large audience of students and faculty.

Dr. Gururaj's lecture emphasized the shift from insight (analyzing existing threats) to foresight (anticipating future risks) in cybersecurity. He highlighted how traditional, rule-based systems are being replaced by AI and machine learning models that can adapt to new threats. A key theme was Generative Innovation, using AI to proactively design new defenses and explore hypothetical attack patterns, staying ahead of cybercriminals.

The talk also stressed the importance of critical thinking and ethical responsibility. Dr. Gururaj cautioned against blindly trusting algorithms and urged attendees to consider the societal impact of AI, especially with the rise of misinformation and privacy concerns. The event successfully inspired participants, reinforcing the need for continuous learning and innovation in the field, and highlighting the importance of the human element in an increasingly automated world.

GLIMPSE OF THE EVENT



EVENTS

Cyber Awareness Week 2025: Cyber Wellness Clinic (CWC) Workshop: Getting Real About Digital Safety

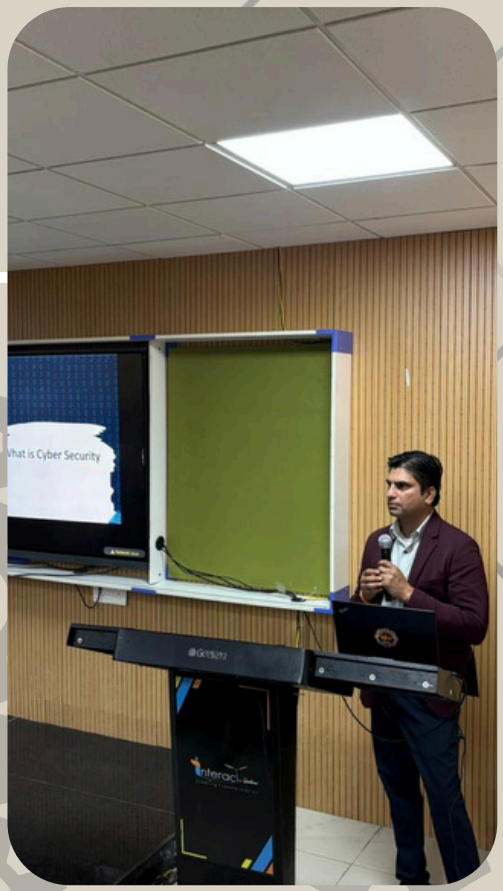
On October 14, 2025, the CCET ACM/ACM-W Student Chapters and CSE Department, partnering with NITTTR, Chandigarh, hosted a crucial Cyber Wellness Clinic. Expert Mr. Tarun Malhotra guided students and faculty through modern cyber threats.

Key topics covered included Social Media Safety and Digital Hygiene, emphasizing personal habits as the primary defense. The session then took a serious turn, dissecting the anatomy of malicious attacks like Phishing, Scams, and Frauds. A major "aha" moment came with the chilling demonstration of how Generative AI is now weaponized to create ultra-realistic deepfakes, bypassing common sense.

Mr. Malhotra shared the defense playbook, focusing on Email Security and Data Protection, underscoring the non-negotiable necessity of Multi-Factor Authentication (MFA) and robust password management using dedicated tools. He also addressed the human cost of online harm, detailing Cyberbullying and clarifying relevant sections of the Information Technology (IT) Act, 2000. The expert concluded by presenting a practical toolkit, including apps like the Government of India's Kavach and professional security solutions, while also highlighting Career Opportunities in Cybersecurity.

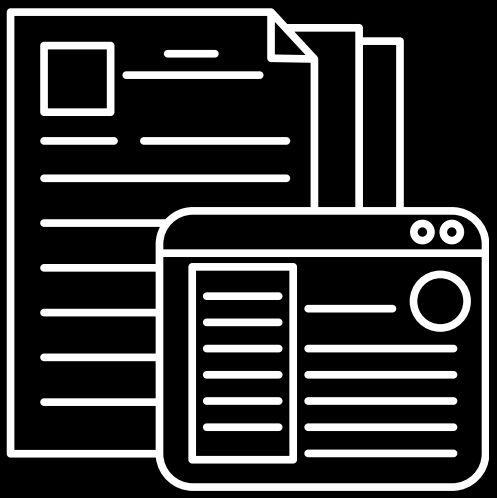
The event successfully demystified digital responsibility, transforming it into a personal, actionable priority and setting a strong standard for future campus outreach. The attendees left with a concrete toolkit and a profound, lasting awareness of modern cyber dangers.

GLIMPSE OF THE EVENT



Article

NEUROMORPHIC CHIPS: ENGINEERING THE BRAIN IN SILICON



Introduction

In the rapidly evolving landscape of computing, the pursuit of intelligent processing units has led to the development of neuromorphic chips. Neuromorphic chips are the result of the search for effective, flexible, and intelligent processing units in the quickly changing field of computing. These chips, which prioritize low power consumption, high parallelism, and event-driven processing, are modeled after the composition and operations of the human brain. Neuromorphic computing is a crucial technology to overcome the drawbacks of traditional architectures as artificial intelligence (AI) systems become more intricate and data-intensive. The basic idea behind neuromorphic engineering is to use silicon to simulate biological neural networks. When handling tasks like real-time perception, decision-making, and motor control, traditional von Neumann systems experience bottlenecks due to their sequential processing of instructions. On the other hand, neuromorphic architectures, which closely mimic the functioning of the human brain, enable the simultaneous transmission and processing of information.

PRINCIPLES OF NEUROMORPHIC CHIPS

· Spiking Neural Networks (SNNs), which use spikes—short electrical pulses—for communication, are the foundation for neuromorphic chips. SNNs closely resemble biological neurons in the brain.

· Neuromorphic systems only transmit information when a neuron's internal potential crosses a certain threshold, in contrast to traditional digital systems that run continuously on a clock cycle. Neurons communicate through discrete, asynchronous spikes. The energy efficiency of this event-driven communication is higher.

· Because neuromorphic chips' neurons are dormant until they are stimulated, event-based operation significantly lowers power consumption. This makes the system extremely effective for real-time, always-on applications.

· Unlike traditional processors, which process data step-by-step using synchronized clock signals, neuromorphic chips operate asynchronously. Neuromorphic systems, on the other hand, function asynchronously, more like the brain.

· Continuous, real-time learning from sensory input is made possible by STDP: Unlike conventional AI models, this biologically inspired learning mechanism enables the system to adapt in real-time without requiring frequent retraining.

· Perfect for applications that need real-time, low-power, adaptive processing: In domains where energy efficiency and continuous learning are crucial, such as autonomous robotics, edge AI devices, and neuromorphic sensors, neuromorphic chips are especially helpful.

NOTABLE ARCHITECTURE AND SYSTEMS

IBM's TrueNorth is among the first and best-known instances of neuromorphic computing. TrueNorth, which was unveiled in 2014, has 256 million synapses and more than a million neurons. Pattern recognition, image classification, and object detection are all possible with this low-power device, which uses only 70 milliwatts. An important advancement was made in 2018 with the release of Intel's Loihi. Loihi facilitates on-chip learning using SNNs, in contrast to TrueNorth, which mainly functions as an inference engine. Use cases like robotic navigation, smart edge devices, and gesture recognition have showcased Loihi's energy-efficient architecture and programmable plasticity rules. Another commercial neuromorphic solution made especially for edge AI applications is BrainChip's Akida platform. Akida has been incorporated into voice recognition, cybersecurity, and biometric analysis devices and offers real-time learning and inference in a small package.

APPLICATIONS IN ROBOTICS AND AI

· One of the most promising applications for neuromorphic chips is robotics. Neuromorphic processor-equipped robots are incredibly efficient at motion planning, real-time control, and sensory integration. For example, ultra-low-latency visual processing is made possible by event-based vision sensors (also known as Dynamic Vision Sensors, or DVS), which detect changes in brightness to replicate the retina. These sensors are used in conjunction with neuromorphic processors.

· Neuromorphic chips allow adaptive behaviours like target tracking, obstacle avoidance, and real-time environmental mapping in mobile robotics. These systems are perfect for exploration and surveillance missions because of their power efficiency, which prolongs their operational duration.

· Additionally, neuromorphic systems are being investigated for cognitive robotics, in which robots demonstrate complex decision-making, memory recall, and interaction-based learning. Robots can perceive and interact with their environment more effectively when neuromorphic vision and tactile sensors are integrated, which supports applications in home automation, healthcare, and assistive robotics.

· Beyond robotics, neuromorphic chips are also being tested for AI applications. They are employed, for instance, in cybersecurity for anomaly detection, where their capacity to pick up on typical behavioural patterns enables the effective identification of anomalies. SNNs have shown promise in medical imaging for classifying CT and MRI scan data with reduced power consumption and latency.

CHALLENGES AND LIMITATIONS

· Notwithstanding the obvious benefits, neuromorphic computing has a number of issues that need to be resolved before it can be widely used. First of all, programming frameworks and standardized development tools are lacking. Neuromorphic platforms frequently rely on proprietary SDKs with challenging learning curves, in contrast to conventional AI systems that use TensorFlow or PyTorch.

· Furthermore, specific training algorithms are needed for SNNs. Despite being the foundation of contemporary deep learning, backpropagation cannot be directly applied to spiking models because spikes are not differentiable. To get around this restriction, researchers are looking into hybrid training schemes, biologically inspired rules, and surrogate gradient techniques.

· Co-designing software and hardware is another crucial issue. It takes a thorough grasp of the algorithm and the hardware limitations to map neural network models to neuromorphic chips effectively. Many developers are discouraged from experimenting with neuromorphic systems because of their complexity.

· Commercial viability and scalability are also issues. Neuromorphic chips are not yet general-purpose processors, despite their superiority in certain tasks. Another challenge is ensuring robustness and fault tolerance, particularly in safety-critical applications like medical devices or driverless cars.

FUTURE DECISIONS

· One promising direction for the future is the combination of neuromorphic computing and traditional AI accelerators. By fusing the computational power of GPUs or TPUs with the low-latency, event-driven processing of neuromorphic cores, hybrid systems can benefit from the advantages of both paradigms.

· More effective neuromorphic systems could also result from developments in materials science and nanotechnology. The goal of memristor and spintronic device research is to physically mimic synaptic behaviour while further minimizing component size and energy consumption.

· On the software side, work is being done to create neural compilers, simulation tools, and high-level programming languages that can abstract the intricacy of neuromorphic systems. This gap is being filled in part by platforms such as NEST, BindsNET, and Lava.

· Integrating neuromorphic chips into brain-machine interfaces (BMIs) is another potential future path. Real-time neural signal decoding capabilities of these chips open up new avenues for neuroprosthetics, rehabilitation, and even cognitive improvement.

Conclusion

By taking direct inspiration from the functioning of the human brain, neuromorphic computing represents a revolutionary change in the way we approach information processing. The development of AI systems that are not only incredibly energy-efficient but also flexible, scalable, and able to continuously learn from interactions in the real world is made possible by these brain-inspired chips. Neuromorphic technologies will be crucial as domains such as autonomous systems, robotics, and edge computing develop because they will allow machines to function in real-time, with higher intelligence and less energy consumption.

Neuromorphic computing holds promise for bridging the gap between artificial systems and biological intelligence. These systems can process information in a fundamentally new way by utilizing spiking neural networks and concepts like synaptic plasticity. This can lead to breakthroughs in areas where traditional AI is challenged, especially in environments with limited power and latency. However, overcoming persistent obstacles in algorithm development, hardware innovation, and the establishment of strong software ecosystems will be necessary to fully utilize this technology. Overcoming these obstacles will require interdisciplinary cooperation between researchers, engineers, and business executives. Neuromorphic chips have the potential to completely transform artificial intelligence in the future with continued work and investment. They will provide more effective solutions that are also better suited to the intricacies of real-world interaction and cognition. This development could revolutionize the way intelligent systems function in our day-to-day lives, propelling social and technological advancement.

References

[1] Indiveri, G., & Liu, S. C. (2015). Memory and information processing in neuromorphic systems. Proceedings of the IEEE.

[2] Furber, S. B. (2016). Large-scale neuromorphic computing systems. Journal of Neural Engineering.

[3] Davies, M., et al. (2018). Loihi: A neuromorphic manycore processor with on-chip learning. IEEE Micro.

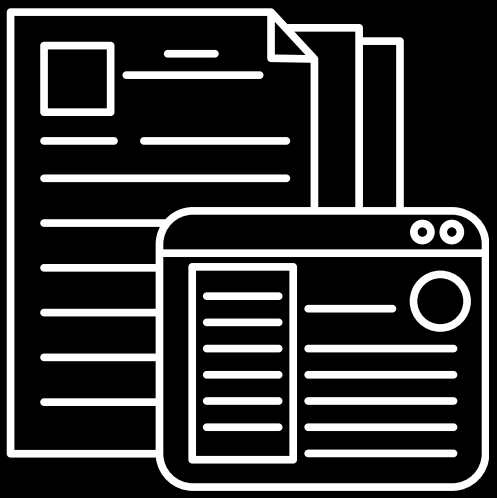
[4] Roy, K., Jaiswal, A., & Panda, P. (2019). Towards spike-based machine intelligence with neuromorphic computing. Nature.

[5] Qiao, N., et al. (2015). A reconfigurable on-line learning spiking neuromorphic processor. Frontiers in Neuroscience.

Samriti sharma

Article

NEURO-SYMBOLIC AI FOR REASONING TASKS



Introduction

Artificial intelligence has seen rapid development in both neural network-based learning and symbolic reasoning. While deep learning systems excel at recognizing patterns from massive datasets, they often struggle with tasks requiring logic and reasoning. On the other hand, symbolic AI, which uses formal logic and rules, lacks the ability to learn from raw data. Neuro-symbolic AI represents a hybrid approach that seeks to integrate the strengths of both systems. This article delves into how neuro-symbolic systems are transforming reasoning tasks and why they may represent the future of general-purpose AI.

Understanding Neuro-Symbolic AI

Neuro-symbolic AI combines neural networks (deep learning models) with symbolic reasoning mechanisms. Neural components handle perception-based tasks such as vision, speech, and natural language processing, while symbolic components interpret logical structures, infer relations, and apply rules. By fusing these paradigms, neuro-symbolic AI aims to achieve both robustness in data-driven learning and transparency in decision-making.

Why Reasoning Matters

Reasoning is a fundamental component of human intelligence. It allows us to deduce conclusions, solve problems, and make sense of complex situations using logic. Traditional deep learning models can classify images or generate text, but they lack the ability to apply commonsense reasoning or explain their decisions. For example, understanding that 'if A is bigger than B, and B is bigger than C, then A is bigger than C' requires reasoning, not just pattern recognition.

Recent Advances (2022–2024)

Recent research has shown significant promise in neuro-symbolic integration. IBM’s Neuro-Symbolic Concept Learner (NSCL) is one such example, using neural networks to parse visual scenes and symbolic programs to answer questions about them. Stanford and MIT researchers have explored neural-symbolic models for solving algebra, understanding diagrams, and performing visual question answering (VQA). These models outperform purely neural approaches in tasks requiring structured logic and inference.

Applications

1.Education and Tutoring Systems: Neuro-symbolic AI is being applied in intelligent tutoring systems that explain math or logic problems step-by-step using both visual cues and symbolic reasoning.
2.Healthcare Diagnostics: These systems can analyze medical imagery with deep learning while using symbolic rules to cross-reference symptoms and historical data, improving diagnostic accuracy.
3.Robotics: Robots that use neuro-symbolic AI can understand instructions like "Pick up the red block next to the green one" and reason about spatial relationships and object properties.
4.Legal and Compliance: By combining natural language processing with rule-based logic, these systems help automate compliance checking and interpret regulations contextually.

Challenges

· Architectural Complexity: Integrating symbolic and neural components requires careful design and coordination between modules to ensure seamless functionality.
· Scalability: Symbolic reasoning can be computationally expensive, especially when used with large-scale knowledge bases, which may slow down performance in real-world applications.
· Dataset Availability: Developing datasets that are suitable for both neural network training and symbolic reasoning remains a significant challenge, limiting the effectiveness of hybrid systems.

Future Outlook

The convergence of neural and symbolic AI is paving the way toward more versatile, interpretable, and intelligent systems. Ongoing research aims to simplify hybrid architectures and embed logic more naturally into neural training processes. With advancements in foundation models and multimodal systems, neuro-symbolic AI may become the default strategy for tasks that require both learning and reasoning in real-world scenarios.

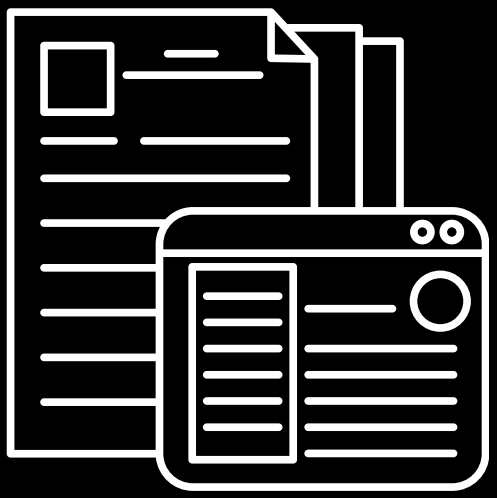
Conclusion

Neuro-symbolic AI bridges the gap between learning from data and reasoning with logic. By combining the best of both paradigms, it opens up new possibilities for AI systems that are not only accurate but also explainable and adaptable. As the field matures, neuro-symbolic approaches are likely to influence a broad range of industries and accelerate the development of truly intelligent machines.

Kritin koundal

Article

ETHICAL IMPLICATIONS OF AI IN DECISION-MAKING PROCESSES



Introduction

Artificial Intelligence (AI) has made stunning progress over the last several decades, transforming from abstract ideas to real-world applications that now form an integral part of a wide variety of industries, ranging from healthcare, finance, and transportation to education. As AI systems increasingly begin to aid or even displace human decision-making, there are several ethical implications which crop up, requiring detailed scrutiny and debate. This piece explores the moral issues involved in the use of AI in decision-making, centering on key issues like bias, accountability, transparency, and the potential for misuse of these powerful technologies. [1]

The Rise of AI in Decision-Making

AI systems, especially those employing machine learning methods, are particularly developed to scan through large amounts of data and generate patterns that can significantly contribute to and improve decision-making processes. For instance, AI algorithms are increasingly used in many applications, such as credit scoring, employment and recruitment procedures, and medical diagnoses. Although these applications can promote increased efficiency and accuracy, they also pose significant ethical problems that need to be resolved in order to produce fair and equitable results. [2]

Ethical Challenges

> Bias and Discrimination: Perhaps the most pressing ethical concern around AI decision-making is bias and discrimination. The AI systems are trained on past data, which will by necessity contain societal prejudices that are embedded into these data. For example, if an AI system is trained on data from biased historical hiring practices, then it will preserve and even amplify these biases in its own decision-making. This can lead to discriminatory results in areas that are important like hiring, lending, and law enforcement, ultimately impacting marginalized groups disproportionately. [3]

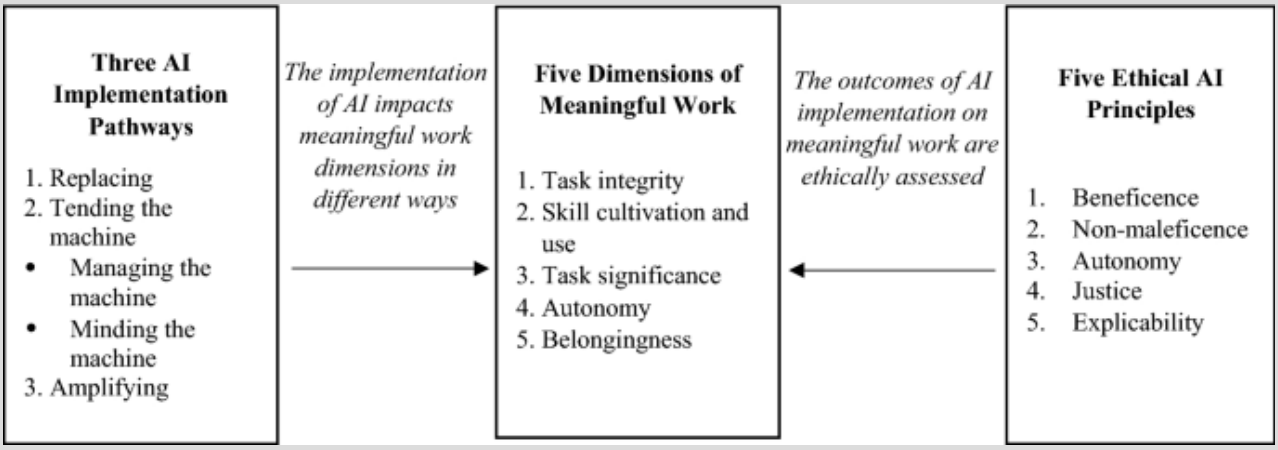
>Accountability: When decisions are made by AI systems, it often becomes challenging to determine who is responsible for the decisions. If an AI algorithm errors and causes harm or adverse effects, it poses complex questions of liability. Should the blame lie with the developers who designed the algorithm, the companies that deploy the AI, or the AI system itself? Having definitive accountability frameworks in place is critical to respond to these pressing issues and provide assurance that mechanisms exist to hold accountable the right parties for the consequences of AI-based decisions. [4]

>Transparency: Transparency of AI decision-making is the utmost critical aspect for building trust among users and stakeholders. Yet, most AI algorithms, especially deep learning-based ones, are "black boxes," and it is extremely hard to know the reason behind particular decisions made by them. It can hamper human and organizational capabilities to challenge and examine AI decisions, and thus, it poses serious ethical issues and can lead to a downfall in people's trust in AI technologies. [5]

>Misuse of AI: The possibility of AI technologies being misused is another serious ethical issue. AI can be used for malicious purposes or weaponized to carry out nefarious activities, such as surveillance, spreading false information, and manipulating public opinion. The ethical use of AI in these areas needs to be thoroughly evaluated to avoid causing harm to individuals and society as a whole. It is essential to have safeguards and ethical principles for preventing AI technologies from being misused.

Steps to overcome these challenges:

- Fairness Audits: Regularly conduct audits of AI systems to identify and mitigate biases. This can involve testing the AI's decisions across different demographic groups to ensure equitable outcomes.
- Diverse Training Data: Ensure that the datasets used to train AI systems are diverse and representative of all groups. This can help reduce the risk of perpetuating existing biases.
- Define Responsibility: Create clear guidelines that outline who is responsible for AI decisions, including developers, organizations, and users.
- Human Oversight: Implement systems where human oversight is mandatory for critical decisions made by AI, ensuring that there is always a human in the loop who can be held accountable.
- User Education: Provide training and resources for users to understand AI systems better, including their limitations and the importance of questioning AI-generated decisions.
- Transparent Reporting: Develop standards for reporting AI decision-making processes and outcomes, making it easier for stakeholders to access and understand how AI systems operate.



Conclusion

While AI is increasingly becoming an essential component in most decision processes, sectors and institutions must address the ethical implications on the use of AI. Proper deployment of AI with fair, accountable, and transparent use with responsibility will avoid all the potential harms as well as bring out positive results. Stakeholders such as developers, organizations, and policymakers need to work together to develop ethical principles and frameworks promoting the use of AI in decision-making in a responsible manner, hence creating a more just and fair society.

Addressing the ethical implications of AI in decision-making requires a multi-faceted approach involving collaboration among developers, organizations, policymakers, and the public. By implementing fairness audits, establishing accountability frameworks, enhancing transparency, and developing ethical guidelines, stakeholders can work towards a more responsible and equitable use of AI technologies. This collaborative effort is essential for fostering trust and ensuring that AI contributes positively to society.

References

[1] Binns, R. (2018). Fairness in Machine Learning: Lessons from Political Philosophy. In Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (pp. 149-158).

[2] Dastin, J. (2018). Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women. Reuters. Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

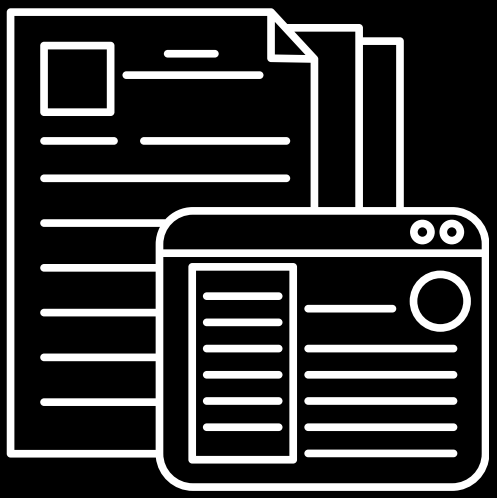
[3] Lipton, Z. C. (2016). The Mythos of Model Interpretability. Communications of the ACM, 61(12), 36-43.

[4] O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group.

[5] Russell, S., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach (3rd ed.). Pearson.

ANSHIKA GOYAL

Article



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.

● 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.

APPLICATIONS

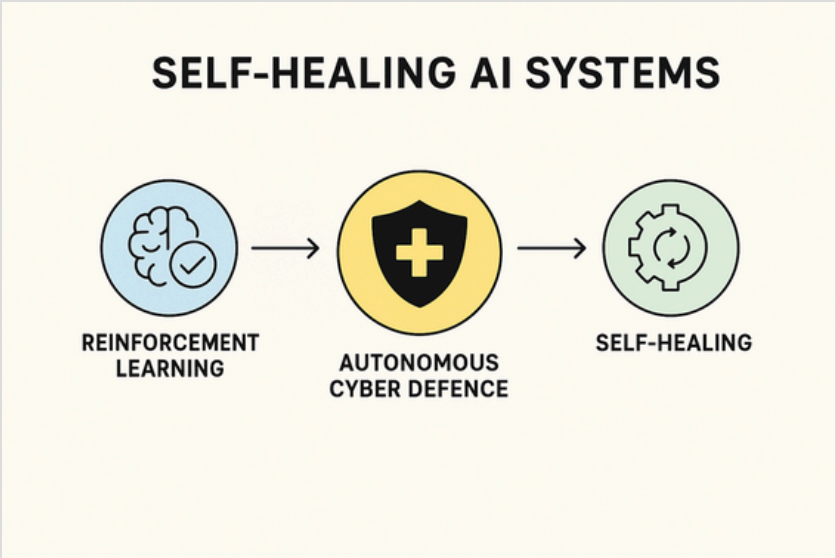
● Cloud Security: Self-healing systems can rotate credentials, isolate compromised components, and monitor service integrity in dynamic cloud environments where services scale up and down continuously. In settings where assets change frequently, they aid in maintaining compliance. Through quick containment, 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.

● Software Supply Chain Security: The software build pipeline can be observed by AI systems. They have the option to rebuild using verified components or roll back to a previous state upon identifying dependency tampering or policy violations. Throughout cycles of continuous integration and deployment (CI/CD), they guarantee integrity. This reduces vulnerability to increasingly frequent supply chain attacks.

● 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.



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.

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.

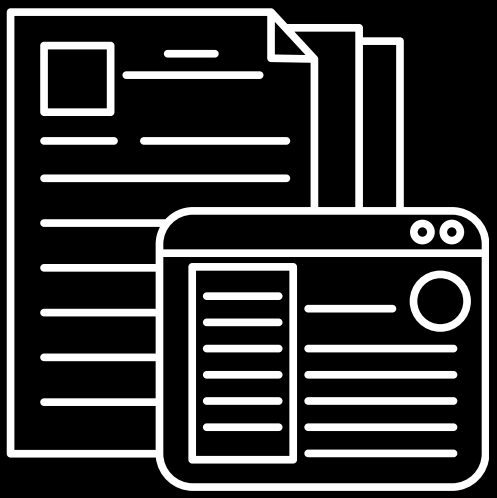
The potential advantages are enormous, despite the fact that there are still difficulties, especially with regard to safety, reward design, and training data. AI agents could soon serve as our digital world's immune system, continuously patrolling, defending, and recovering from attacks without the need 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.
5. DARPA Cyber Grand Challenge. (2016). https://www.darpa.mil

Aarushi Khera

Article



MIGRATION TO POST-QUANTUM CRYPTOGRAPHY: NEEDS AND CHALLENGES

Introduction

With the rapid advancements in quantum computing, the cryptographic techniques that secure our digital infrastructure today are under threat. Algorithms like RSA, DSA, and ECC which secures the internet protocols, banking systems, and confidential communications get their security from mathematical problems that classical computers struggle to solve. But with the use of algorithms like Shor's [1] and Groover's algorithms, quantum computers can solve these problems extremely faster. This threatens modern security which has led to a shift toward Post-Quantum Cryptography (PQC) algorithms. These algorithms are designed to be secure even against quantum computers. Migration to PQC is not an easy task, it is a transformation that affects cryptographic primitives, protocols, standards, and deployment models. This article explores the need for migration to PQC and brings out the key challenges involved in making this transition.

Why Quantum-Resistant Cryptography Is Needed

The most significant reason for adopting PQC are the capabilities of quantum computers to easily decrypt the currently used cryptographic algorithms. Shor's [1] algorithm can be executed on a powerful quantum computer to efficiently factorize large integers thus breaking algorithms like RSA and ECC. Similarly, Grover's [2] algorithm also weakens the symmetric key encryption by reducing key lengths to half of the original.

Quantum computers powerful enough to break current encryption don't exist yet. But the threat still exists. Attackers can collect the encrypted data now and decrypt it once the quantum technology progresses. This puts sensitive information like government confidential information, medical records, and other sensitive information at a major risk. The governments and organizations around the world are taking this potential threat seriously. The National Institute of Standards and Technology (NIST) [3] has already started selecting new algorithms which can provide security against these quantum threats. This marks the beginning of a shift toward post-quantum cryptography.

The Landscape of Post-Quantum Algorithms

Post-quantum cryptographic algorithms are built on mathematical problems that are difficult to solve for both classical and quantum computers [5]. The categories of PQCs include lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, hash-based signatures, and isogeny-based cryptography. Among these, lattice-based cryptography schemes like CRYSTALS-Kyber (for key encapsulation) and CRYSTALS-Dilithium (for digital signatures) are the top contenders [4]. Due to their balance in security and efficiency, these algorithms are under consideration for their robustness, performance, integration capabilities, resistance to attacks, and implementation complexity.

Integration Challenges Across Systems

One of the biggest obstacles in making the transition to PQC is bringing new algorithms into the marketplace. Legacy applications, protocols, and hardware were developed with respect to today's cryptography standards. Implementing new primitives into stacks such as TLS, SSH, VPNs, embedded systems, and industrial control systems could involve complete redesigns [4]. In addition, the signature lengths and key sizes of PQC algorithms may be much larger than their traditional equivalents. For instance, while a 256-byte key is used in RSA-2048, there are PQC algorithms that can demand kilobytes of data, influencing performance and bandwidth, particularly in resource-constrained devices or in applications sensitive to latency.

Moreover, hybrid schemes, integrating classical and post-quantum algorithms, are being explored as a transition solution [6]. But this introduces new issues with respect to trust models, key management, and failure modes, adding to the complexity of implementation and verification.

Standardization and Interoperability

Standardization is a basic requirement for this cryptographic transition. Without globally accepted and tested standards, it is difficult to verify and maintain interoperability. NIST's PQC competition has served an important role in assessing and choosing secure algorithms, but worldwide agreement is still required. Other organizations and governments are creating their own standards and testing frameworks. The European Telecommunications Standards Institute (ETSI) [6], ISO, and IETF are also working to bring updates to protocols and APIs to align with the needs of Post Quantum Cryptography. Maintaining world interoperability while avoiding fragmentation during this transition is an important task. Incompatible cryptographic systems with varying regions or providers can lead to severe vulnerabilities or leave systems inoperable for secure communication.

Security, Usability, and Risk

Post-quantum cryptographic schemes are newer and, therefore, less tested in combat compared to well-established standards [4]. Although the mathematical underpinnings can be sound, implementation bugs, side-channel attacks, and fine-grained protocol-level mistakes can still be present. There is a need for more research to make these algorithms resistant to practical attack vectors.

Usability is also an issue. Certain PQC algorithms require additional memory, slower computation times, or increased network usage. For instance, in web applications that have to complete TLS handshakes within milliseconds, a sluggish or heavy post-quantum algorithm may slow down user experience. In addition, cryptographic agility becomes essential. Systems need to be architected such that future cryptographic primitives can be inserted or replaced with a minimum of disruption. This involves improved software design, modular crypto libraries, and dynamic protocol negotiation [5].

Legal, Policy, and Supply Chain Concerns

Migration to PQC is not merely a technical issue. It crosses over with legal and regulatory schemes, particularly in industries such as defense, finance, and healthcare. Governments can require specific algorithms or ban others based on national security interests [6]. Intellectual property rights, export controls, and algorithm origin can affect adoption choices. Vendors and organizations will have to work through a highly complex matrix of compliance and certification while maintaining transparency and supply chain integrity. In addition, as PQC gains increased visibility, attackers can be expected to leverage the transition period to attack legacy systems or improperly configured hybrid deployments. Awareness and cyber hygiene will both take on a decisive role in mitigating these transitional threats.

Roadmap for Migration

Effective migration to post-quantum cryptography must be a phased and well-planned process. Organizations need to start with cryptographic inventory audits determining where and how cryptography is employed throughout systems, applications, and data flows [3]. Second, pilot deployments of PQC algorithms must be tried out in testbed environments. Hybrid deployment approaches can provide a compromise by maintaining backward compatibility while introducing quantum resilience incrementally. Close tracking of international and NIST standards, coordination with suppliers, and education of engineering staff will also be essential. In the long run, cryptographic flexibility has to be accepted as a design philosophy so that systems can grow as cryptography science evolves.

Current Research and Global Initiatives

The international research community, the government, and industry partners have been working to make systems quantum-resistant at an accelerating pace. Leading the pack is the NIST Post-Quantum Cryptography Standardization Project, which reached its last stages in 2024 by shortlisting CRYSTALS-Kyber and CRYSTALS-Dilithium as finalists for standardization. Other alternative candidates such as SPHINCS+ and BIKE are also being considered for particular use cases like stateless signatures or resource-constrained devices [3][4]. Academic institutions are performing continuous cryptanalysis to assess the strength of suggested algorithms against both quantum and classic attacks. In parallel, agencies like CNSA (Commercial National Security Algorithm) Suite 2.0 by NSA, and ENISA (European Union Agency for Cybersecurity), have started providing strategic advice for quantum-safe upgrades.

Large tech firms and consortia—like Google, IBM, Microsoft, and the Open Quantum Safe (OQS) initiative—are offering open-source libraries and implementing experimental PQC algorithms within protocols such as TLS. Google has experimented with hybrid key exchanges in Chrome over TLS, between X25519 and Kyber for increased compatibility. In addition, the Internet Engineering Task Force (IETF) has established the PQUIP (Post-Quantum Use in Protocols) working group to standardize how quantum-resistant primitives can be integrated into current Internet protocols. Academia, governments, and industry cooperation is being found crucial in obtaining secure, practical deployments of post-quantum security.

Conclusion

Post-quantum cryptography is a necessary and imminent effort fueled by the revolutionary promise of quantum computing. Although today's systems are secure, they might become obsolete in the near term, jeopardizing confidential communications, critical infrastructure, and national security. While beset with technical, operational, and regulatory difficulties, the shift to PQC is a proactive move towards future-proofing our digital world. With concerted international efforts, strong standards, and ongoing innovation, a quantum-safe internet is achievable.

References

[1] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. [quant-ph/9508027] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [2] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing. [quant-ph/9605043] A fast quantum mechanical algorithm for database search [3] NIST. (2024). Post-Quantum Cryptography Standardization Project. https://csrc.nist.gov/projects/post-quantum-cryptography [4] Chen, L., et al. (2016) Report on Post-Quantum Cryptography. Department of Commerce and National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8105 [5] Bernstein, D. J., et al. (2009). Post-Quantum Cryptography. Springer. Post-Quantum Cryptography | SpringerLink [6] ETSI. (2023). Quantum-Safe Cryptography. European Telecommunications Standards Institute. https://www.etsi.org/technologies/quantum-safe-cryptography

Hitesh Saini

FUN FACTS


WHEN YOU JOIN ACM THINKING IT'S JUST ABOUT CODING...
Expectation:
I'll just code and chill
EVENT
POSTER
ACM
Reality:
Suddenly managing events, designing posters, debugging life, and still coding at 2 AM
#ACMFunPage #CoderLife #CollegeChronicles
acm

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

Aarushi
2023

Aanshi Bansal
2023

Content Editors

Eshmeet Singh Bhachu
2023

Vanshika Singla
2023

Feature Editors

Khushi
2023

Bhavya
2023

Anshika Goyal
2024

Tanvi
2024

Shiven Sharma
2024

CASC Board

Jaiveer Singh
Chairperson

Satvik Pathak
Vice-Chairperson

Sanatan
Secretary

Shivam Vats
Membership Chair

Dhruv Bali
Treasurer

Abhay
Webmaster

Aarushi
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

- https://ccet.acm.org

- CCET ACM Student Chapter

- /acmccet

- ccet-acm-student-chapter

CCET, Degree Wing | Department of CSE | Sec-26 Chandigarh

Contact Us - www.ccet.ac.in