TECH TODAY

MARCH 2026

FEDERAL INSTITUTE OF SCIENCE AND TECHNOLOGY (FISAT)
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

OUR VISION

To become a centre of excellence in computer science, developing competent and socially responsible professionals with strong problem-solving skills, catering to the dynamic requirements of industry and society by promoting sustainable development and quality research.

VISION & MISSION

OUR MISSION

Department of Computer Science and Engineering is committed to:

M1 – (Teaching – Learning):

Inculcate a passion for academic excellence through innovative and industry-aligned teaching-learning practices that foster critical thinking and problem-solving.

M2 – (Research & Innovation):

Create opportunities for students to pursue research, innovation, and entrepreneurial initiatives that address real-world challenges with sustainable and impactful solutions.

M3 – (Values & Social Responsibility):

Nurture the students to be technically competent, morally upright and socially responsible computer science engineers to meet global challenges.

THE EDITORIAL BOARD

STAFF EDITORS

DR.PAUL P MATHAI
HOD,CSE

JISMY MATHEW
ASSISTANT PROFESSOR,CSE

NITHYA PAUL
ASSISTANT PROFESSOR,CSE

STUDENT EDITORS

JUDE ABI PYNADATH
S8 CSE B

JOYAL JINNY
S6 CSE B

LEKSHMIPRIYA S
S6 CSE B

ADITHYA KRISHNA J NAIR
S4 CSE A

ANNLIA LIXON
S4 CSE A

HOD'S DESK

It gives me immense pleasure to present the latest edition of our annual technical magazine **"TechToday 2026."** This magazine is a reflection of the creativity, innovation, and technical enthusiasm of our students and faculty members.

Technology is evolving at an extraordinary pace, and platforms like TechToday play a vital role in encouraging young minds to explore new ideas, share knowledge, and express their technical insights. I am delighted to see our students actively contributing articles, project ideas, and research perspectives that showcase their talent and curiosity.

I congratulate the editorial team and all the contributors who have worked tirelessly to make this publication meaningful and inspiring. Your dedication and teamwork have made this edition a valuable source of knowledge and motivation for our academic community.

I hope that TechToday continues to inspire innovation, critical thinking, and a passion for learning among students in the years to come.

My best wishes to the entire team for the success of this magazine.

Dr. Paul P Mathai
Head of the Department
Computer Science and Engineering, FISAT

STAFF EDITOR'S WORD

We are delighted to present the latest edition of the Technical Magazine of Computer Science and Engineering.

This publication serves as a platform to showcase the creativity, technical knowledge, and innovative spirit of our computer science community.

Within these pages, you will find articles, technical write-ups and projects that highlight emerging trends and advancements in computer science and engineering. Each contribution reflects the curiosity, dedication, and talent of our academic community, while also emphasizing the broader impact of technology on society.

We extend our sincere gratitude to the team for their dedication and critical insight, to the contributors for their creativity and hard work, and to the college management for their unwavering support. Together, we continue to foster a culture of excellence and innovation that will define the future of technology. It is our hope that this magazine not only informs and inspires but also motivates readers to explore new ideas and contribute meaningfully to the ever-evolving digital world.

Ms. Jismy Mathew & Ms. Nithya Paul
Chief Editors

STUDENT EDITOR'S WORD

As the Student Editor, it is both an honor and a privilege to present Tech Today '26, the annual magazine of the Department of Computer Science and Engineering. This edition stands as a reflection of the enthusiasm, creativity, and intellectual curiosity that define our student community.

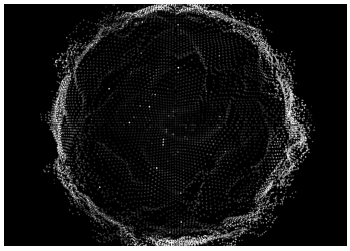
Within these pages, you will find a collection of articles that highlight emerging ideas and innovations in the field. Each contribution reflects the dedication and passion of our students.

I extend my sincere gratitude to all contributors, the editorial team, and our faculty for their constant support.

I hope this magazine inspires readers to explore new ideas and continue pushing the boundaries of technology.

Jude Abi Pynadath
Student Editor

Table Of CONTENTS



07 AI-Generated Art: Creativity or Theft?
-Allen Martin

10 From Tools to Teammates: The Psychological Shift of Working With AI
-Sreya Sreejith

12 Brain–Computer Interface (BCI): Bridging the Human Brain and Machines
-Adel Joby, Adarsh N A

15 Edge Computing: Redefining Real-Time Intelligence
-Aleena K J

17 Beyond Speed: How 5G is Transforming Today and 6G is Designing Tomorrow Data in AI
-Chinmayi V S

19 From Chatbots to Coworkers: Why 2026 is the Year AI Gets a Job
-Sharika S

22 Generative AI: Bridging Human Creativity and Intelligent Machines
-Henna Kuriakose

25 The Role of Color Psychology in UI/UX Evaluating the Effects of Dark Mode on User Engagement and Visual Comfort
-Krishna Jyothish, Rueben Joseph Rex

27 Digital Twin Technology: Creating Virtual Replicas of the Real World
-Lekshmipriya S

30 Cybersecurity in the Age of the Internet of Things (IoT)
-Pournami P

32 Differential Privacy in Large-Scale Data Systems
-Rachel Elsa

34 Artificial Intelligence and Cybersecurity: Defending the Digital World
-Abhishek Murali

37 The double-edged sword of AI
-Aiswarya S Kumar

40 Recommendation Systems (Netflix & YouTube): How AI Decides What You Watch Next
-Akshai M

43 2025: The Indie Year
-Anpu Saramsh

45 ARE WE CODING OUR OWN REPLACEMENTS?
-Fathima Hana

48 The Future of Engineering: Can AI Design Better Engineers Than Humans?
-Fathima Hannah M T

50 The Age of Autonomous Agents: When AI Starts Managing AI
-Hannah Pullan

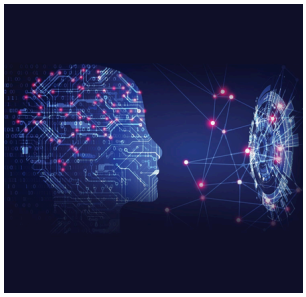
53 The Silicon Traffic Jam: Why AI is Running Out of Gas
-Mohammed Mahir Mobin

56 AI in Exam Systems: Smart Evaluation or Smart Cheating?
-Meenakshi S

59 Ni8mare: A Remote Code Execution Flaw in the Age of AI Agents
-Niranjana S

62 The Silent Data We Give Away: How Everyday Apps Predict Our Behavior
-Alwin Liju

65 Artificial Intelligence in Automotive Systems
-Ann Mary George



68 Zero Trust Architecture: Rethinking Cybersecurity in the Digital Age
-Jane Joe

70 The Future Is Engineered: Designing Tomorrow's Intelligent World
-Rohan Rajesh

72 The Neural Program Synthesis and the Evolution of Git
-Adithi Harish

74 Artificial Intelligence in Automotive Systems
-Anshal Shaju

76 Inside a Ransomware Attack: How Hackers Breach, Move, and Monetize
-Mohammed Faraz KS

79 Quantum Computing: The Next Digital Revolution
-Muhammed Aadil C S

81 Revolutionizing the Future of Medicine
-Anjana Roy

84 The AI Chip Wars: Inside the Battle Powering the Age of Artificial Intelligence
-Ibadh Rahman K P

87 DEAD INTERNET THEORY:
A Conspiracy or the New Reality?
-Ann Maria Tenson

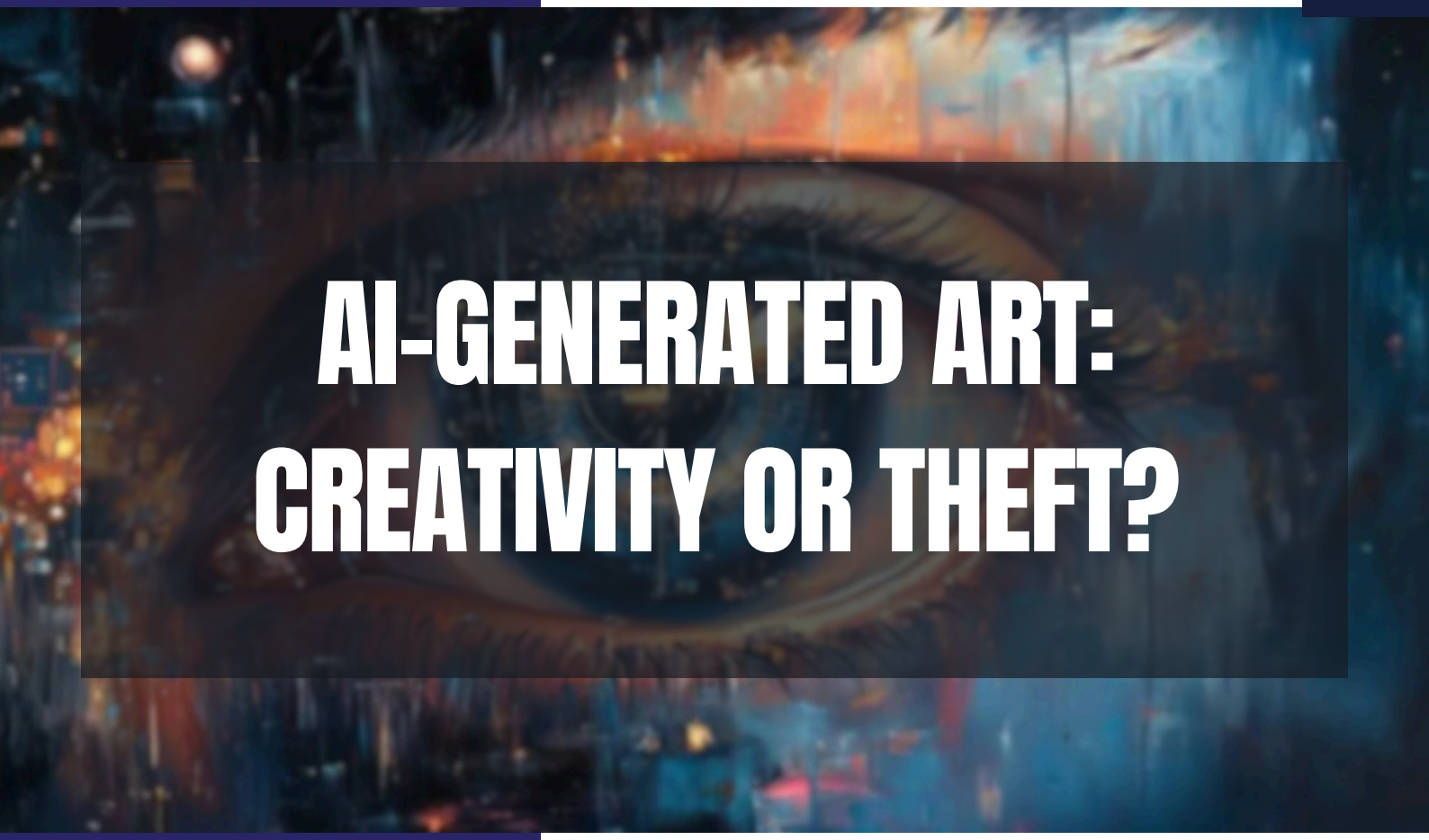
89 Recent Trends in Technology: Shaping the Future in 2026
-Kajol Joby

92 The AI Bubble: Hype, Hardware, and the Hidden Economic Shift
-Haniya Jahan K Z

95 Log Chain Technology
-Nayana Girish M

97 Ethical Hacking
-Helen Maria Jomon

98 Internet of Things (IoT)
-Neha Savithri



AI-GENERATED ART: CREATIVITY OR THEFT?

Allen Martin
S8 CSE A

Introduction

Art created by artificial intelligence has developed at an accelerated pace from rudimentary algorithmic designs to extremely advanced, hyper-realistic, and abstract works. While some segment of the audience accepts AI as a new means of artistic expression, critics argue that it is largely based on available human-made art. The moral challenge comes into play when AI mimics styles of art without explicit permission, raising issues regarding intellectual property rights and just compensation for human artists. This study explores AI-created art through technological, ethical, and legal lenses to ascertain whether it is a means of creative advancement or an act of digital plagiarism.

The Function of AI in Artistic Creation

AI as a Creative Tool

Artificial intelligence-based software like Deep Dream, Runway ML, and DALL·E use machine learning algorithms to create stunning images. AI algorithms, particularly Generative Adversarial Networks (GANs) and diffusion models, browse through massive collections of paintings to create new art based on learned styles and patterns. Artists view AI as an assisting tool and not an alternative to human imagination and can explore new unknown dimensions of art.

The Case for AI as Innovation

Supporters claim that AI democratizes art creation because it enables individuals without the conventional skills of an artist to create effective images. Artists such as Refik Anadol, who employs AI in his data-based art installations, demonstrate how AI can be a partner and not a mere imitator.

Ethics and Copyright Issues

As potential as it is, AI-made art is brimming with profound ethical and legal issues. Large data pools accessed from the internet by most AI algorithms are gathered without the knowledge or permission of the owners. This has triggered legal battles, such as the 2023 Stability AI and MidJourney lawsuits, when artists claimed AI companies profited from the unapproved use of copyrighted content. Additionally, art created by AI can copy the unique style of an artist, leading to confusion in the marketplace and possible economic loss to the human artist.

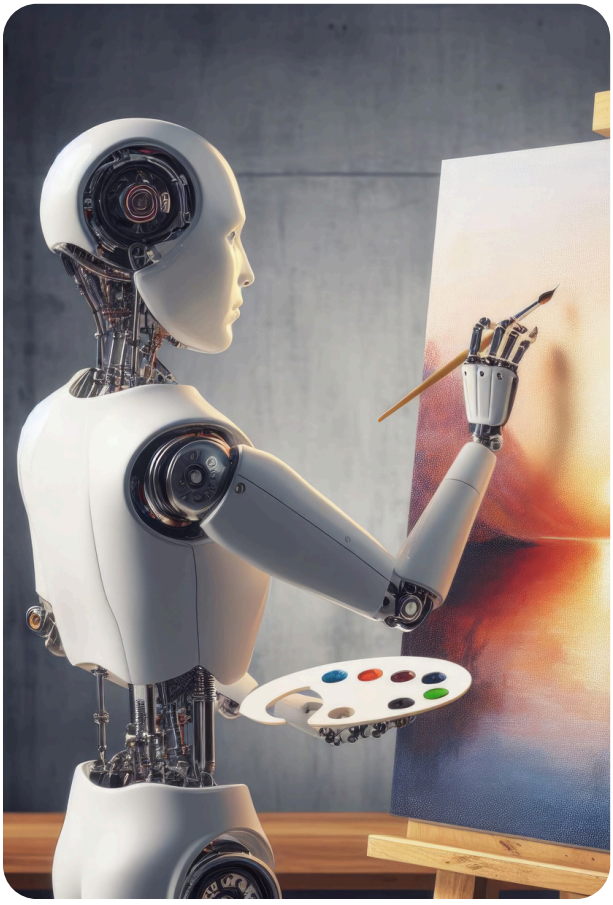
Copyright Law and AI-Generated Works

The existing law on works produced by artificial intelligence is characterized by uncertainty. The U.S. Copyright Office (2023) clarifies that works produced by AI independently are not eligible for copyright protection unless they are combined with notable human contribution. This ruling has been controversial about AI as a standalone creator or as a human tool.

The Need for Regulatory Mechanisms

With more AI-generated content on the rise, new licensing models and regulatory schemes must be established to safeguard both AI creators and human artists. Some proposed solutions are:

- Opt-in databases for AI training – Allowing artists to decide if their creations are appropriate to be used within AI training sets.
- Royalty-based models of compensation – Compensation of artists if their work is utilized to produce an AI-generated work.
- Legally unambiguous definitions of AI authorship – Determining whether works created by AI are owned by the programmer, the user, or no one.



The Future of AI-Generated Art

The future of art produced by artificial intelligence will most certainly be a hybrid path, where artificial intelligence is a co-creator and not an independent artist. Anticipated trends are:

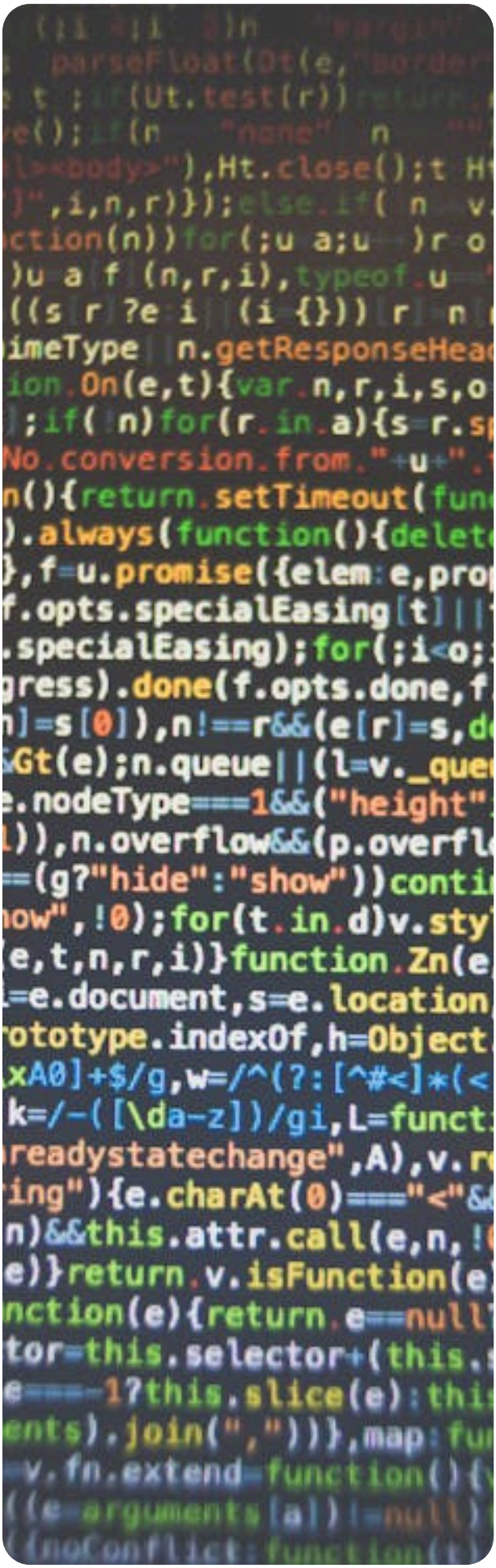
• Ethically trained AI – AI models trained on open-source or ethically obtained artwork.

•AI-human collaboration – Artists leveraging artificial intelligence to enhance their creative process rather than replace it.

• More robust legal protections – More defined global laws regulating the rights of AI content creators.

Conclusion

Art generated by artificial intelligence challenges conventional concepts of creativity and ownership, igniting fiery debates about its place in the world of art. Although AI may democratize art and open creative doors, it also raises critical ethical and legal concerns. There is a need to balance innovation and justice to ensure that AI is used as an assistant to human creativity and not as an instrument of artistic exploitation. The future will depend on how artists, legal academics, and technology experts create systems to ensure proper utilization of AI in the creative industry.



From Tools to Teammates: The Psychological Shift of Working With AI

By 2026, AI is no longer just a tool—it's a teammate, shaping how work gets done across industries. Once, technology was a set of instruments—calculators, computers, software—designed to speed up tasks. Today, intelligent systems are becoming collaborators in thought, creativity, and decision-making. Around 72 % of professionals now use AI at work, up from 48 % just two years ago, and more than half of global businesses are integrating AI into core workflows.

Interactions with AI increasingly feel human. Tools like GitHub Copilot—now used by over 20 million developers worldwide—do more than execute code; they suggest logic, fill gaps, and anticipate needs. Design platforms like Figma generate editable layouts from simple prompts, while AI-driven analytics summarize massive datasets in seconds. According to LinkedIn and Microsoft surveys, 75 % of knowledge workers report AI enhances their productivity and creativity, a figure that continues to rise as adoption spreads.

This partnership transforms problem-solving. In software development, AI helps write and review code, automate repetitive tasks, and identify potential issues before they arise. In creative and analytical roles, AI proposes layouts, drafts insights, and uncovers patterns that might otherwise remain hidden. Across organizations, 68 % of remote workers now use three or more AI tools daily, reporting measurable time savings and improved efficiency. Over time, users begin to see AI not merely as a helper but as a teammate in cognition, influencing how they think and make decisions.

Yet this collaboration comes with challenges. Overreliance can erode core skills and raises
questions of accountability: when an AI suggestion fails, who bears responsibility? Balancing trust and critical thinking remains essential. Human judgment must stay central, ensuring AI amplifies rather than replaces our abilities.
The psychological impact is profound. Working with AI encourages meta-cognition,
prompting reflection on assumptions, evaluation of alternatives, and critical assessment of suggestions. Collaboration with AI fosters patience, adaptability, and humility—similar to human teamwork, but with the unique task of interpreting machine "thinking."

Cultural shifts in workplaces reflect this evolution. Some organizations now link employee advancement to AI fluency, signaling that adapting to AI is a key career skill. At the same time, companies debate how to safely integrate AI on sensitive devices, highlighting ongoing regulatory and ethical considerations.

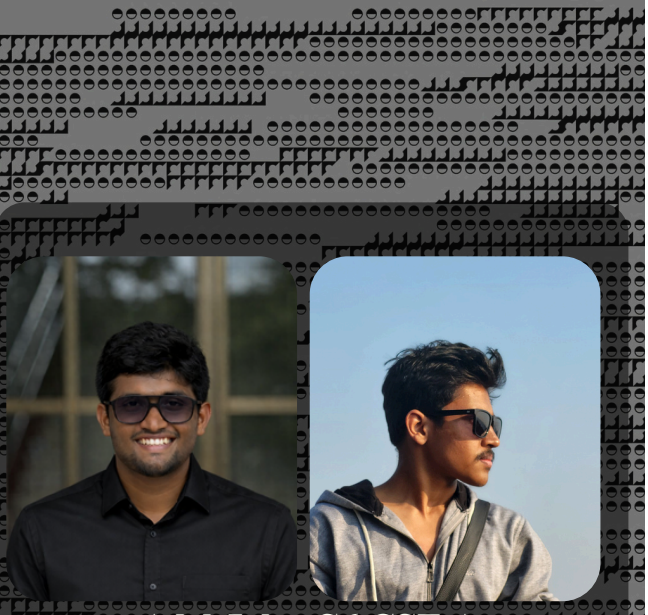
Moving from tools to teammates is more than a technological upgrade—it is a cognitive and cultural transformation. It reshapes what we do and how we perceive creativity, intelligence, and human potential. For students and professionals alike, AI is an opportunity to develop new skills, guide systems effectively, and embrace a future where collaborative thinking with machines is essential.

The essence of creation, decision-making, and innovation remains distinctly human. Yet the way we create is changing as AI becomes a constant partner. The future of work is not simply about using AI—it is about thinking with it, learning from it, and growing alongside it. In a world where AI partners are increasingly capable, the key skill is human judgment: knowing how to steer these partnerships wisely and responsibly.

Sreya Sreejith
S6 CSE C

BRAIN-COMPUTER INTERFACE (BCI):

BRIDGING THE HUMAN BRAIN AND MACHINES



Adel Joby S6 CSE A
Adarsh N A S6 CSE A

Abstract

Brain–Computer Interface (BCI) is an emerging technology that enables direct communication between the human brain and external devices such as computers, prosthetics, and robots. By interpreting neural signals and converting them into machine-readable commands, BCI systems aim to restore lost motor functions, enhance human–machine interaction, and revolutionize healthcare and computing.

Introduction

Traditional human–computer interaction relies on physical inputs such as keyboards, mice, or touchscreens. However, for individuals with severe motor or neurological disabilities, these interfaces are inaccessible. Brain–Computer Interface technology overcomes this limitation by allowing users to interact with machines using brain signals alone, eliminating the need for muscular activity.

Working Principle of BCI

A typical BCI system operates in four main stages:
Signal Acquisition: Brain signals are recorded using sensors, most commonly through Electroencephalography (EEG). Signal Processing: The raw signals are filtered to remove noise and unwanted artifacts. Feature Extraction & Classification Important signal patterns are extracted and classified using algorithms and machine learning models.

Device Output
The interpreted signals are translated into commands to control devices such as cursors, wheelchairs, or robotic arms.

Types of Brain–Computer Interfaces:
1. Non-Invasive BCI
- Sensors placed on the scalp
- Safe and painless
- Lower signal accuracy

Example: EEG-based headsets
2. Invasive BCI
- Electrodes implanted directly into the brain
- High accuracy
- Requires surgery

Example: Brain implants developed by Neuralink
3. Semi-Invasive BCI
- Electrodes placed on the brain surface
- Balance between safety and accuracy

Applications of BCI
- Medical Applications
- Communication for paralyzed or ALS patients
- Brain-controlled prosthetic limbs
- Stroke rehabilitation
- Assistive Technology
- Brain-controlled wheelchairs
- Hands-free computer operation
- Research & Future Computing
- Cognitive state monitoring
- Human-AI interaction
- Virtual and augmented reality systems
- Real-Life Implementations

BCI systems have enabled paralyzed patients to type messages, control robotic arms, and interact with digital environments. Recent experiments have shown humans typing text and moving cursors using implanted brain chips, marking a major milestone in neurotechnology.

Challenges and Ethical Concerns
Despite its potential, BCI faces several challenges:
- High development cost
- Signal instability and noise
- Privacy and data security of brain signals
- Ethical concerns regarding brain data misuse

Future Scope
With advances in artificial intelligence, neuroscience,and hardware miniaturization, BCIs are expected to become more accurate, affordable, and widely available. In the future, BCIs may redefine how humans communicate with machines, leading to smarter healthcare systems and enhanced human capabilities.

Conclusion

Brain–Computer Interface technology represents a significant step toward integrating the human brain with digital systems. While still in its developmental stage, BCI holds immense promise in improving quality of life and shaping the future of computing.

Why These Experiments Matter

They aim to restore functions like communication and digital interaction to people with paralysis or disabilities.

They push BCI tech from lab demonstrations to real human use. Successful trials could lead to major advances in medicine and human–machine interfaces.

References

Brain-Computer Interface Research: A State-of-the-Art Summary

Edited by Christoph Guger, Brendan Z. Allison, Aysegul Gunduz.

This book provides a broad overview of key BCI research projects and developments.

Brain-Computer Interface Research

Ed*ited by Christoph Guger, Brendan Z. Allison, Günter Edlinger (earlier edition).*

A foundational book summarizing various BCI technologies and projects.

EDGE COMPUTING: REDEFINING REAL-TIME INTELLIGENCE

Aleena K J
S6 CSE A

"Processing data where it happens is no longer an option—it's the key to innovation."

In an era defined by digital transformation, the world is generating data at an unprecedented pace. By 2025, it is projected that over 175 zettabytes of data will be produced annually, challenging traditional centralized cloud computing systems. To address this, edge computing is emerging as a crucial technology, bringing computation and data storage closer to the devices that generate data.

Edge computing represents a distributed computing model that handles data processing close to its origin—such as IoT gadgets, industrial sensors, or self-driving cars—rather than depending exclusively on centralized cloud servers. This methodology facilitates quicker processing, minimizes latency, enhances bandwidth efficiency, and strengthens security.

Edge computing is vital for low latency applications, such as AR, VR, and real-time gaming, by minimizing data travel and enhancing performance. It optimizes bandwidth by locally preprocessing data, reducing costs and congestion. Enhanced security is achieved by managing sensitive data locally, aiding compliance with privacy regulations. Additionally, edge computing facilitates AI and machine learning applications for real-time analytics and automation across various sectors. It also supports 5G networks, enabling ultra-low latency capabilities for connected technologies like vehicles and drones.

Edge computing is revolutionizing various industries by enabling real-time capabilities. In healthcare, it supports monitoring and telemedicine; in automotive, it facilitates autonomous vehicles; manufacturing leverages predictive maintenance; retail enhances personalized experiences; and energy sectors optimize distribution. The future of edge computing includes expanded use of Edge AI, smart city infrastructure, Industrial Automation under Industry 4.0, integration with advanced

Countless connected devices—from smart wearables to industrial sensors—produce enormous volumes of data. Processing this information locally guarantees immediate responses which are crucial for applications responses, which are crucial for applications like autonomous driving, remote healthcare, and industrial automation. Telecommunications like 5G/6G, improved data privacy through local data processing, energy efficiency through reduced data transfer, and innovation prospects in hardware and software solutions. These advancements are set to drive significant changes across multiple domains over the next decade.

Edge computing presents significant challenges including high infrastructure costs, management complexity, and security risks due to an increased number of endpoints. However, it is a vital enabler of real-time intelligence and low-latency applications, particularly in IoT innovation. By 2025-26, organizations adopting edge computing are expected to enhance their competitive capabilities in speed, efficiency, and data security. Its integration with AI and 5G technology is poised to transform various industries, establishing it as a key component of future digital infrastructure.

With the growing adoption of Edge AI and real-time analytics, experts predict that over 75% of enterprise-generated data will be processed at the edge by 2030. For businesses, governments, and innovators, edge computing represents not just the present, but the future of digital transformation.

Beyond Speed: How 5G is Transforming Today and 6G is Designing Tomorrow

In the digital age, connectivity is no longer a luxury — it is the foundation of education, business, healthcare, and communication. Whether we are attending online classes, streaming content, making digital payments, or collaborating on cloud platforms, reliable internet plays a central role in our daily lives. The emergence of 5G marks a significant leap in this journey, promising not only faster data speeds but also a smarter and more responsive digital ecosystem. Even more exciting is the development of 6G, the next generation of wireless communication, which is already being researched for the future.

5G: More Than Just Faster Internet

While many people associate 5G with high-speed downloads, its impact goes far beyond that. Compared to earlier generations, 5G offers extremely high data transfer speeds, ultra-low latency, support for millions of connected devices, and improved reliability. This allows devices to communicate almost instantly, which is essential for applications such as self-driving cars, robotic surgeries, smart factories, and intelligent traffic systems.

How 5G is Changing Industries

Smart Mobility: Connected vehicles can exchange information with each other and with road infrastructure, reducing accidents and improving transportation efficiency.

Digital Healthcare: With minimal delay in communication, doctors can conduct remote consultations and assist in complex medical procedures using robotic systems.

Intelligent Cities: Energy management systems, traffic monitoring, and public safety networks become more efficient through seamless connectivity.

Immersive Experiences: Virtual Reality (VR) and Augmented Reality (AR) applications become smoother and more realistic, enhancing gaming, education, and training.

The Vision of 6G: What Lies Ahead?

Even as 5G networks continue to expand, researchers are actively working toward 6G, expected to become commercially available around 2030. 6G aims to provide data speeds reaching up to 1 terabit per second, almost zero communication delay, AI-integrated networks, holographic communication, and advanced human–machine interaction.

Imagine virtual meetings where participants appear as lifelike holograms instead of flat screens, or networks that automatically optimize themselves using artificial intelligence before congestion occurs. These ideas are gradually becoming research priorities.

Challenges and Considerations

Despite its immense potential, the journey toward next-generation networks comes with challenges such as high deployment costs, cybersecurity risks, increased energy consumption, and uneven access in rural regions. Addressing these concerns will require collaboration between governments, researchers, and private organizations.

Conclusion

The evolution from 4G to 5G — and soon to 6G — represents more than an upgrade in speed. It signifies a transformation in how humans and machines interact. These technologies are shaping smart cities, digital healthcare, autonomous transportation, and intelligent industries. The future of connectivity is not just about being faster — it is about being smarter, more adaptive, and deeply interconnected.

1. International Telecommunication Union (ITU), "IMT-2020 Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond," ITU-R M.2083-0, 2015.
2. 3rd Generation Partnership Project (3GPP), "5G NR Technical Specifications," Release 15 and beyond.
3. Saad, W., Bennis, M., & Chen, M. (2020). "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems." IEEE Network.
4. Nokia Bell Labs, "6G Research Vision Report," 2020.
5. IEEE Communications Society, Research Publications on 5G and 6G Networks.

Chinmayi V S
S6 CSE A

FROM CHATBOTS TO COWORKERS: WHY 2026 IS THE YEAR AI GETS A JOB

Sharika S
S6 CSE C

If 2023 was the year we learned to talk to machines, 2026 is the year they started talking back—and then clocked in for work. Three years ago, the world watched in awe as ChatGPT wrote poetry and debugged Python scripts. It was a "Copilot," a hyper-intelligent encyclopedia that sat passively in a browser tab, waiting for a human to hit the "Enter" key. It was a tool, no different in nature than a very advanced calculator. But tools don't have job titles. Tools don't have goals. And tools certainly don't negotiate with vendors or fix bugs while you sleep.

As we settle into 2026, we are witnessing the end of the "Chatbot Era" and the violent birth of the "Agentic Era." This shift is not just a technical upgrade; it is a fundamental restructuring of the global economy. For students currently navigating university, the implications are stark: The entry-level job you

are studying for is rapidly being filled by a "synthetic employee." The good news? A much more interesting job is opening up in its place.

To understand this economic shift, we must first understand the technical leap. The AI of the early 2020s was a brain in a jar. It could think and process information, but it had no hands. It could not interact with the world outside of a text box. Agentic AI changes this architecture. It gives the brain "hands"—access to tools like web browsers, code editors, email clients, and APIs. It also gives the brain "agency"—the permission to make decisions to achieve a goal. In 2023, you had to ask an AI, "Write an email to the client rescheduling the meeting," and then you had to copy, paste, and send it yourself. In 2026, you simply tell an Agent, "Manage my calendar conflicts for the week." The Agent perceives the conflict, checks the client's availability, decides on the best slot, drafts the email, sends it, and updates your invite—all without you opening a single tab. This is the difference between a tool and a worker. A tool waits for input; a worker pursues an outcome.

Economists are calling this the "unbundling" of white-collar work. Corporations are realizing that they don't necessarily need a human for every role; they need workflows. And if a workflow can be defined, an Agent can be hired to execute it. We are already seeing the deployment of specialized Agents that function as "Synthetic Employees." Instead of a human tester clicking through a website to find bugs, a QA Agent navigates the site autonomously 24/7, identifies crashes, writes the bug report, and even attempts a code fix in a new branch. Supply Chain Agents monitor global shipping news; if they see a port strike in Rotterdam, they automatically reroute shipments and update inventory projections before a human manager has even finished their morning coffee. These agents don't take coffee breaks, they don't sleep, and their "salary" is the cost of electricity and compute. For the economy, this represents a collapse in the cost of cognitive labor. For us, it raises the terrifying question: What is left for humans?

The prevailing anxiety is that AI will replace us. This is half-true. AI will replace the doer. It will not replace the owner. For the last twenty years, a Computer Science education focused on syntax. We were tested on our ability to write the code—the "how." But in an agentic world, the "how" is cheap. The value shifts entirely to the "what" and the "why." The graduate of 2026 is not entering the workforce as a Junior Developer or a Junior Analyst. They are entering as a Product Manager of AI. Your future job will not be to write a thousand lines of Java. Your job will be to architect a system where five different AI Agents collaborate to build the software for you. You will be the orchestrator. You will define the constraints, set the ethical guardrails, review the output, and intervene when the Agents get stuck in a logic loop.

The hierarchy of the office is flipping. The "entry-level" work is being automated, meaning that every human entry-level employee is being forced into a mid-level management role from Day One. We are no longer operators of tools; we are managers of fleets. So, how do we prepare for this? If the ability to write boilerplate code or draft standard emails is no longer a competitive advantage, the new skill stack must focus on system architecture and integration. You need to understand how to chain Agents together—how does the "Researcher Agent" pass data to the "Writer Agent"? Understanding APIs and data flows is now more important than memorizing syntax. Furthermore, as Agents can be hallucination-prone and dangerous, a massive industry is emerging around "AI Governance"—writing the rules that prevent an autonomous Agent from accidentally deleting a production database or offending a client.

But perhaps most importantly, when the technical execution is perfect and instant, the only differentiator is the human element. Empathy, negotiation, ethical judgment, and creative strategy become the hardest skills to automate. An Agent can design a bridge, but it cannot convince a city council to pay for it. The year 2026 is a threshold. We are stepping out of the era where we stared at screens and into the era where the screens stare back, waiting for orders. The "Coworker AI" is not coming to steal our careers; it is coming to upgrade them. It offers to take the drudgery—the data entry, the bug fixing, the scheduling—off our plates, leaving us with the terrifying freedom to be purely creative and strategic. The question for every student at this college is no longer, "Can I do the job?" The Agents can do the job. The question is, "Can I manage the outcome?"

Generative AI: Bridging Human Creativity and Intelligent Machines

Abstract

Generative Artificial Intelligence (Generative AI) is an advanced branch of AI that enables machines to create new content such as text, images, audio, video, and code. By learning patterns from massive datasets, Generative AI models can produce human-like outputs and assist in creative, analytical, and technical tasks. This technology is transforming industries including healthcare, education, business, and entertainment, while also raising important ethical and societal questions.

Introduction

Traditional software systems operate based on predefined rules and instructions. However, Generative AI goes beyond rule-based programming by learning from data and generating new, original outputs. Unlike earlier AI systems that focused on prediction and classification, Generative AI can compose essays, design graphics, develop software code, and even generate realistic voices.

The rise of powerful AI models developed by organizations such as OpenAI, Google, and Meta has accelerated innovation in this field, making AI tools widely accessible to individuals and businesses.

Working Principle of Generative AI

A typical Generative AI system operates in four major stages:

1. Data Collection and Training: The AI model is trained on massive datasets containing text, images, or other media. During training, it learns patterns, grammar, structure, and relationships within the data.
2. Model Learning Using deep learning techniques such as neural networks and transformers, the system identifies complex patterns and representations.
3. Prompt Processing When a user provides input (prompt), the model interprets the request and predicts the most relevant output based on learned patterns.

4. Content Generation

The system generates new content whether it is a paragraph, an image, a piece of music, or programming code — in real time.

Types of Generative AI Models

Text Generation Models

1. These models generate human-like text for chatbots, content writing, translation, and summarization. Example: Large Language Models (LLMs).
2. Image Generation ModelsThese models create realistic or artistic images from text descriptions using diffusion techniques.
3. Audio and Music Generation Models AI can compose music, clone voices and generate sound effects.
4. Code Generation Models. AI tools assist developers by writing and debugging code efficiently.

Applications of Generative AI

- Education
  Personalized tutoring
- Automatic content summarization
- Interactive learning tools
- Healthcare
  Medical report drafting
- Drug discovery research assistance
- Patient data analysis
- Business and Marketing
  Content creation for social media
- Automated email drafting
- Customer service chatbots
- Entertainment and Media
  AI-generated art and animations
- Script writing assistance
- Game development support

Real-Life Implementations

Generative AI systems are already being integrated into daily life. AI-powered assistants can write emails, generate reports, create presentations, and design graphics. Businesses use AI tools to improve productivity and reduce operational costs. Developers rely on AI for faster coding and debugging processes. These real-world applications demonstrate how Generative AI is transitioning from experimental research to mainstream adoption.

Real-Life Implementations

Despite its advantages, Generative AI presents several concerns:

- Risk of misinformation and deepfakes
- Copyright and intellectual property issues
- Bias in AI-generated content
- Data privacy and security risks
- Potential job displacement

Responsible AI development and proper regulations are essential to ensure that this technology benefits society while minimizing risks.

Future Scope

The future of Generative AI is promising. With advancements in computing power, algorithm efficiency, and multimodal learning, AI systems are expected to become more accurate, context-aware, and creative.

Future developments may include:

- Fully interactive AI assistants
- Real-time video generation
- Advanced human–AI collaboration tools
- Smarter enterprise automation systems

Generative AI has the potential to redefine digital interaction and reshape the global technology landscape.

Why This Technology Matters

- It enhances human creativity and productivity.
- It democratizes content creation for non-experts.
- It accelerates innovation across industries.
- It bridges the gap between human ideas and machine execution.

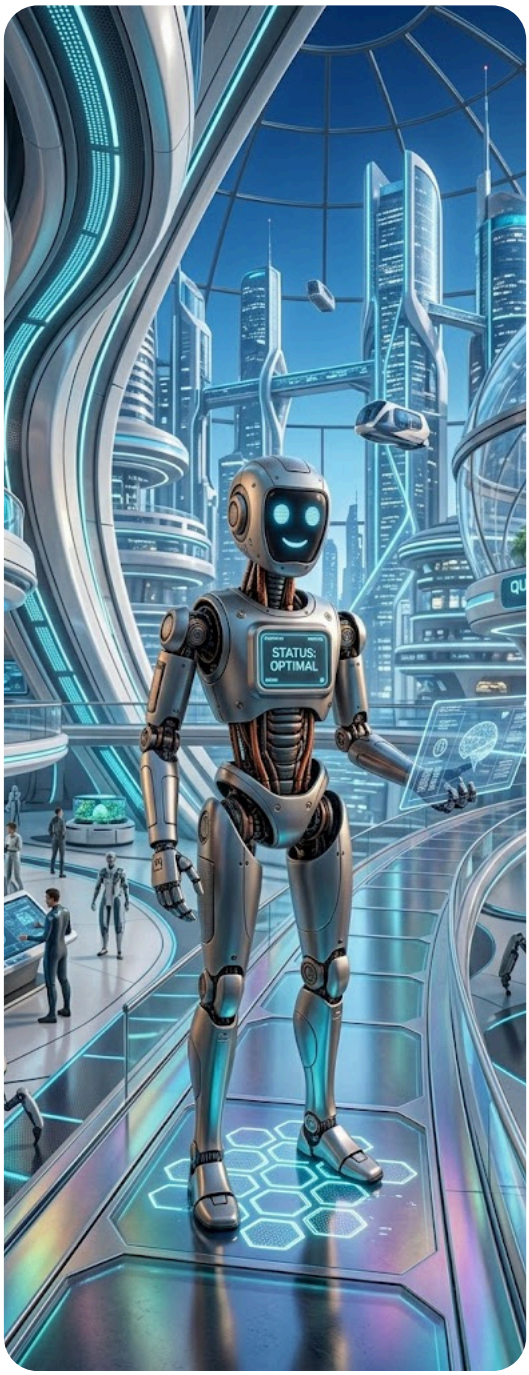
Conclusion

Generative AI represents a revolutionary step in artificial intelligence, enabling machines not only to analyze information but also to create new content. As the technology continues to evolve, it will play a central role in shaping the future of digital communication, business, healthcare, and creative industries.

While challenges remain, responsible development and ethical governance will ensure that Generative AI becomes a powerful tool for human advancement.

References

- Goodfellow, I., Pouget-Abadie, J., Mirza, M., et al. (2014). Generative Adversarial Nets. Advances in Neural Information Processing Systems (NeurIPS).
- Vaswani, A., Shazeer, N., Parmar, N., et al. (2017). Attention Is All You Need. Advances in Neural Information Processing Systems (NeurIPS).
- Brown, T. B., Mann, B., Ryder, N., et al. (2020). Language Models are Few-Shot Learners. NeurIPS.
- Ho, J., Jain, A., & Abbeel, P. (2020). Denoising Diffusion Probabilistic Models. NeurIPS.
- Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th Edition). Pearson.
- OpenAI. (2023). GPT-4 Technical Report. OpenAI Research Publication.



Henna Kuriakose
S6 CSE C

THE ROLE OF COLOR PSYCHOLOGY IN UI/UX:

Evaluating the Effects of Dark Mode on User Engagement and Visual Comfort

Krishna Jyothish
S6 CSD

Rueben Joseph Rex
S6 CSD

In today's digital world, the choice between "Light Mode" and "Dark Mode" has become more than just a matter of looks. It is now an important topic in User Experience (UX) design. Different colors convey meaning and influence behavior. The background type, whether dark text on a light background or vice versa, significantly impacts visual comfort, user engagement, and accessibility.

The Science behind Visual Comfort: Polarity and Fatigue

The dark mode discussion stems from the idea of display polarity. Light mode, or "positive polarity," shows dark characters on a light background. Dark mode, or "negative polarity," features light characters on a dark background.

Traditional thinking suggests that positive polarity (light mode) usually supports better vision and reading performance, especially for tasks with small text. A bright background makes the pupil constrict, which increases the depth of field and reduces optical errors, resulting in a clearer image for the eyes.

However, the way we use screens has changed. Recent studies show that dark mode can greatly reduce visual fatigue, especially in low-brightness settings. Lowering screen brightness in dark mode reduces the contrast between the screen and a dark room, which helps decrease eye strain and minimizes the risks associated with prolonged screen use in the dark.

Cognitive Performance and Demographics

While dark mode is often praised for its comfort, its effect on cognitive performance is more complex. Research shows that cognitive scores, which assess readability and processing speed, are generally higher in light mode among various demographic groups.

Interestingly, user engagement and preferences vary by age and education. Younger adults often do better in light mode, while those with higher education prowess show better performance in dark mode. Additionally, while males typically express comfort with both modes, females tend to prefer light mode more. This tells us that a "one-size-fits-all" coloring strategy in UI design does not exist. Designers must consider the specific characteristics of their users.

The shift to dark mode also relates to the principles of designing for the sake of accessibility, which aims for interactive technologies that support a wide range of users with different visual needs.

For people with certain visual impairments, such as light sensitivity or cataracts, dark mode is not simply a choice but a requirement for accessibility. However, for users with astigmatism, a halo effect called “halation” around bright text on dark backgrounds can make dark mode harder to read.

To promote inclusivity, designers should follow accessibility standards such as the Web Content Accessibility Guidelines (WCAG). These guidelines stress the importance of maintaining enough contrast between text and background so users with low vision or color blindness can easily read the content.

The Psychological Impact of Color

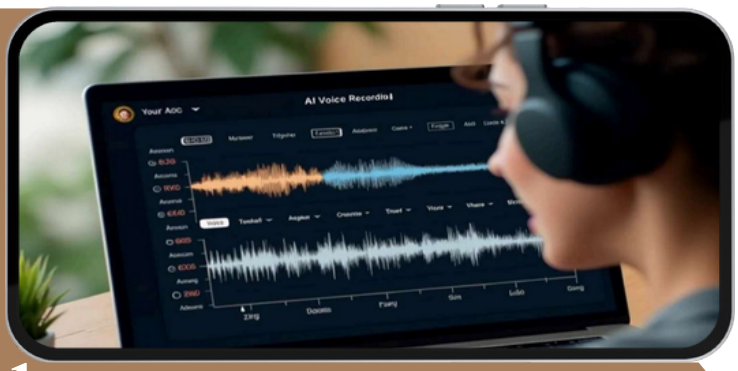
Beyond how easy it is to read, color psychology is crucial for user engagement. Colors do not just serve decorative purposes; they carry meaning and evoke emotions. In dark mode, highly saturated colors may seem overwhelming against a black background, causing visual discomfort.

Good UI design in dark mode means using less saturated accent colors to keep text readable and lessen eye strain. For example, a bright blue that signals "trust" in light mode might need to shift to a softer, lighter blue in dark mode to maintain that connection without causing glare.

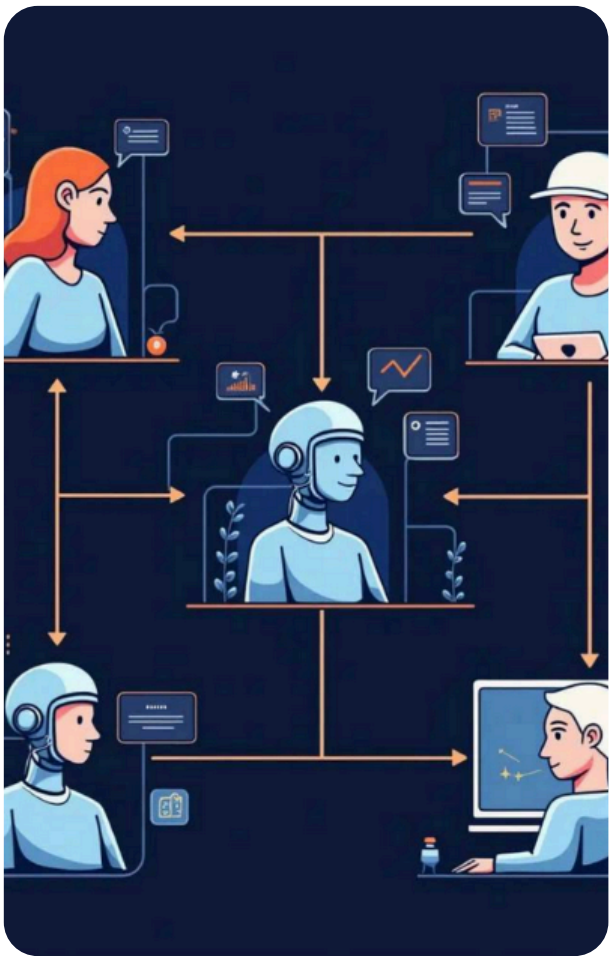
Conclusion: The Case for Adaptive Design

The comparison between dark mode and light mode shows that neither option is obviously better. Light mode typically enhances performance and vision in bright environments, while dark mode provides better comfort in dim settings and appeals to certain users.

Digital Twin Technology: Creating Virtual Replicas of the Real World



Lekshmipriya S
S6 CSE B



Abstract

Digital Twin Technology is an advanced innovation that creates a virtual replica of a physical object, system, or process. By integrating real-time data, simulation models, and artificial intelligence, digital twins enable monitoring, analysis, and optimization of real-world systems. From manufacturing plants and smart cities to healthcare and aerospace, digital twins are transforming how industries design, operate, and maintain complex systems.

Introduction

Digital Twin Technology is an advanced innovation that creates a virtual replica of a physical object, system, or process. By integrating real-time data, simulation models, and artificial intelligence, digital twins enable monitoring, analysis, and optimization of real-world systems. From manufacturing plants and smart cities to healthcare and aerospace, digital twins are

transforming how industries design, operate, and maintain complex systems.

Working Principle of Digital Twin

A Digital Twin system operates through the following stages:

1. Data Collection
   Sensors embedded in physical objects collect real-time data such as temperature, pressure, speed, or health metrics.
2. Data Transmission
   IoT networks and cloud platforms transmit collected data to digital systems.
3. Virtual Modeling
   A digital replica is created using simulation software and 3D modeling tools.
4. Analysis & Optimization
   AI algorithms analyze data to predict failures, improve efficiency, and optimize performance.

Types of Digital Twin

1. Product Digital Twin
   Represents individual products during design and testing phases
2. Process Digital Twin
   Simulates workflows and operational systems for efficiency improvement.
3. System Digital Twin
   Represents entire systems such as power grids or transportation networks.
4. Human Digital Twin
   Models human organs or body systems for medical research and personalized healthcare.

Applications of Digital Twin Technology

- Manufacturing
- Predictive maintenance
- Production optimization
- Quality control
- Healthcare
- Personalized treatment planning
- Surgical simulation
- Organ modeling
- Smart Cities
- Traffic flow optimization
- Energy consumption monitoring
- Infrastructure planning
- Aerospace & Automotive
- Aircraft engine performance monitoring
- Vehicle testing and simulation

Real-Life Implementations

Industries are already using digital twins to monitor equipment performance in real time. For example, manufacturing plants use digital twin models to detect machinery faults before breakdown occurs, reducing downtime and cost.

In healthcare, researchers are developing virtual heart models to simulate treatment outcomes. Smart city projects also utilize digital twins to manage urban infrastructure efficiently.

Challenges and Ethical Concerns

Despite its advantages, Digital Twin technology faces challenges such as:

- High implementation cost
- Data security and privacy concerns
- Integration complexity
- Need for high-quality real-time data
- Dependence on cloud infrastructure

Ensuring secure data transmission and maintaining system reliability are essential for long-term success.

Future Scope

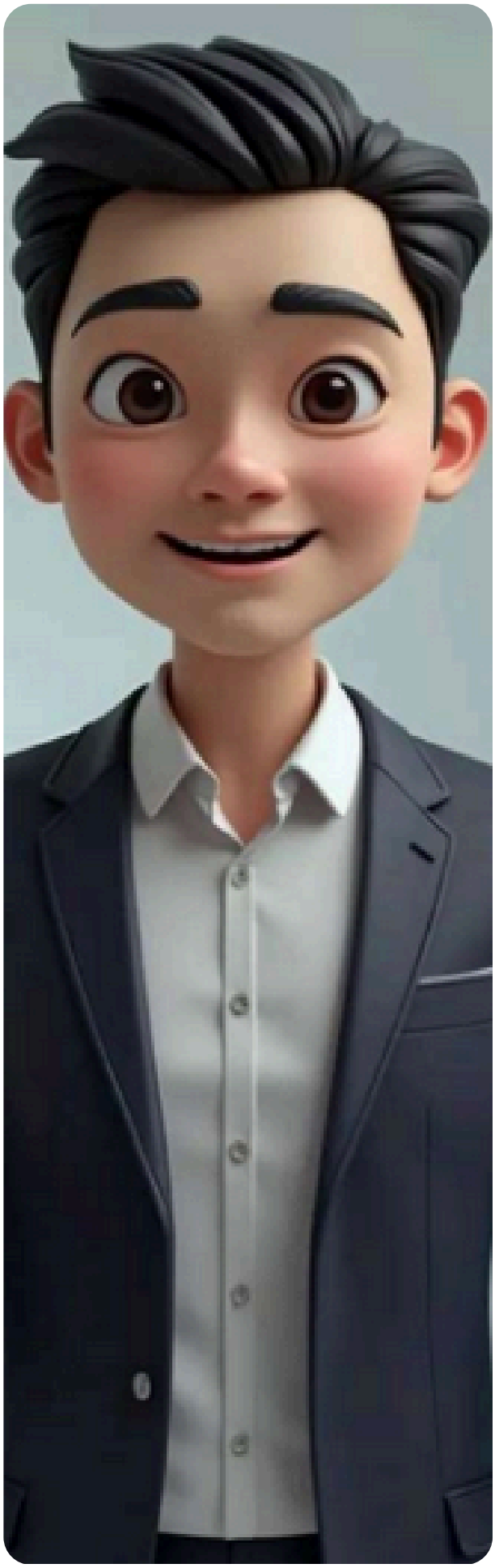
With advancements in AI, 5G connectivity, and edge computing, digital twins are expected to become more intelligent and responsive. Future developments may include:

- Fully automated industrial systems
- Real-time city-scale digital simulations
- Personalized digital healthcare replicas
- Enhanced sustainability and energy management

Digital Twin technology will likely become a foundational component of Industry 4.0 and smart infrastructure.

Why This Technology Matters

- Improves efficiency and reduces operational cost
- Enables predictive maintenance
- Enhances decision-making with real-time insights
- Supports sustainable development



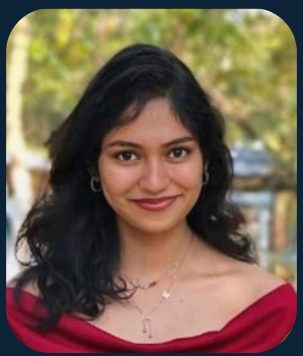
Conclusion

Digital Twin Technology represents a powerful step toward integrating physical systems with intelligent digital environments. By creating accurate virtual replicas, industries can predict, analyze, and optimize real-world performance more effectively. As technology evolves, digital twins will play a critical role in shaping smarter industries and cities.

References

- Grieves, M., & Vickers, J. (2017). Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In Transdisciplinary Perspectives on Complex Systems.
- Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital Twin in Industry: State-of-the-Art. IEEE Transactions on Industrial Informatics.
- Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE Access.
- Siemens Digital Twin Solutions – Official Publications.

CYBERSECURITY IN THE AGE OF THE INTERNET OF THINGS (IOT)



Pournami P
S6 CSE C

The rapid growth of the Internet of Things (IoT) has transformed everyday life by connecting ordinary devices to the internet. From smart home appliances and wearable fitness trackers to industrial sensors and autonomous vehicles, IoT technology enables seamless communication between devices. However, this convenience comes with significant cybersecurity challenges that individuals, organizations, and governments must address.

IoT devices often prioritize functionality and low cost over security. Many devices are shipped with weak default passwords, limited encryption, and infrequent software updates. As a result, they become easy targets for cybercriminals. Once compromised, a single insecure device can serve as an entry point to an entire network, allowing attackers to steal sensitive data, spy on users, or launch large-scale cyberattacks.

One of the most concerning threats associated with IoT is the formation of botnets—networks of infected devices controlled remotely by hackers. These botnets can be used to carry out Distributed Denial-of-Service (DDoS) attacks, overwhelming websites and online services with massive traffic. In recent years, major online platforms have experienced outages caused by compromised IoT devices such as cameras and routers.

Privacy is another major concern. Smart devices continuously collect data about user behavior, location, health, and daily routines. If this data is intercepted or misused, it can lead to identity theft, financial loss, or physical safety risks. For example, hacked smart locks or surveillance systems could allow unauthorized physical access to homes or facilities.

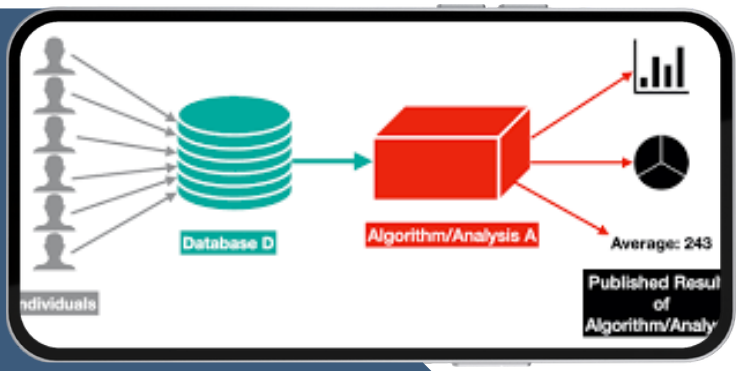
To mitigate these risks, manufacturers must adopt security-by-design principles. This includes implementing strong authentication methods, regular firmware updates, secure communication protocols, and vulnerability testing. Governments and regulatory bodies are also introducing standards that require minimum security features in connected devices.

Users play a critical role as well. Simple practices such as changing default password, enabling automatic updates, using secure Wi-Fi networks, and isolating IoT devices on separate network segments can significantly reduce risk. Awareness and responsible usage are essential in maintaining a secure digital environment.

Looking ahead, emerging technologies such as artificial intelligence and blockchain may strengthen IoT security by detecting anomalies in real time and ensuring tamper-proof data exchange. However, cybersecurity will remain an ongoing challenge as attackers continuously evolve their techniques.

In conclusion, while the Internet of Things offers remarkable benefits in efficiency, convenience, and innovation, it also expands the attack surface for cyber threats. Building a secure IoT ecosystem requires collaboration among manufacturers, policymakers, cybersecurity experts, and users. Only through proactive measures can society fully enjoy the advantages of connected technology without compromising safety and privacy.

Differential Privacy in Large-Scale Data Systems



Rachel Elsa
S6 CSE C

The rapid growth of large-scale data systems has significantly transformed modern computing environments. Organizations today rely on vast volumes of user data to power analytics platforms, recommendation systems, fraud detection mechanisms, and machine learning models. While these systems generate substantial value, they also introduce serious privacy concerns. Even when explicit identifiers are removed, individuals can often be re-identified using auxiliary information and statistical inference techniques. As a result, traditional anonymization methods are no longer sufficient for ensuring data protection.

Differential Privacy has emerged as a rigorous framework designed to address these challenges. Instead of attempting to conceal identities through heuristic approaches, it provides a formal guarantee that the output of a computation remains nearly unchanged whether or not a single individual's data is included. This ensures that participation in a dataset does not significantly increase the risk of privacy exposure. Importantly, this guarantee holds even if an adversary possesses additional background knowledge.

The central mechanism behind differential privacy is the introduction of controlled randomness into data analysis processes. When a query is executed on a dataset, a carefully calibrated amount of noise is added to the result before it is released. The magnitude of this noise depends on how much influence a single data record could exert on the outcome. If one individual's data can substantially change the result, more noise must be injected to protect privacy. This balance between sensitivity and randomness forms the foundation of the differential privacy model.

A privacy parameter, commonly denoted as epsilon, determines the strength of the privacy guarantee. Smaller values correspond to stronger privacy protection, as they restrict how much the output can vary when one record changes . However,

stronger privacy requires greater randomness, which may reduce the accuracy of analytical results. Choosing an appropriate privacy level therefore involves evaluating the acceptable trade-off between data utility and confidentiality.

In practical systems, differential privacy is typically implemented using structured noise-addition techniques. Mechanisms based on Laplace and Gaussian distributions are widely adopted. The Laplace approach is commonly applied to numerical queries such as counts and totals, while the Gaussian mechanism is often used in machine learning applications. Integrating these techniques into large-scale systems requires careful design to maintain computational efficiency and reliability.

Another critical concept in large-scale deployments is the privacy budget. Each query performed on a dataset consumes a portion of the overall privacy guarantee. When multiple analyses are conducted, the total privacy loss accumulates over time. Effective privacy management therefore requires tracking and limiting cumulative exposure. Without proper accounting mechanisms, repeated data access may gradually weaken privacy protection.

Differential privacy has gained particular importance in machine learning systems. Models trained on sensitive datasets can unintentionally memorize specific training examples, creating potential information leakage risks. Privacy-preserving training techniques limit the influence of individual data points and introduce randomness during model updates. This approach reduces the likelihood that trained models reveal sensitive information while still maintaining acceptable performance.

Despite its theoretical robustness, implementing differential privacy in real-world systems presents several challenges. Increasing privacy strength often reduces analytical accuracy. Large-scale distributed environments introduce additional complexity in terms of computation, coordination, and secure random number generation. System designers must carefully balance privacy guarantees, performance constraints, and scalability requirements.

In conclusion, differential privacy represents a structured and mathematically grounded approach to protecting individual information within large-scale data systems. By ensuring that analytical outputs remain stable under small dataset changes, it provides meaningful and quantifiable privacy assurances. Although practical trade-offs exist, differential privacy continues to play a critical role in advancing responsible and secure data engineering practices.

Artificial Intelligence and Cybersecurity:

Defending the Digital World

Cyber Threat

Abhishek Murali
S4 CSE A

In today's digital era, technology has become deeply embedded in everyday life. From online banking and digital payments to cloud storage and social media, almost every activity depends on software systems connected through the internet. While this connectivity brings convenience, it also exposes systems to cyber threats. Cyberattacks are becoming more frequent, sophisticated, and damaging, affecting individuals, organizations, and even governments.

To counter these evolving threats, Artificial Intelligence has emerged as a powerful tool in cybersecurity. AI-driven security systems are transforming how cyber threats are detected, analyzed, and prevented. The integration of AI into cybersecurity is not just a technological upgrade but it represents a fundamental shift in digital defense strategies.

The Changing Nature of Cyber Threats

Earlier, cyberattacks were relatively simple and often relied on known vulnerabilities. Antivirus software and firewalls based on predefined rules were sufficient to handle most threats. However, modern cyberattacks are far more complex. Attackers now use automation, social engineering, and advanced malware that can adapt and evolve to avoid detection.

Cyber threats such as ransomware attacks, data breaches, phishing scams, and Distributed Denial of Service (DDoS) attacks have increased drastically in recent years. These attacks can cause financial loss, data

theft, and disruption of essential services. Traditional security systems struggle to keep up because they depend heavily on known attack signatures and manual updates.

This is where AI becomes essential. Instead of relying solely on predefined rules, AI systems can learn from data, recognise patterns, and adapt to new threats in real time.

Role of Artificial Intelligence in Cybersecurity

AI enables cybersecurity systems to move from reactive to proactive defense. Machine learning models analyze large volumes of data, including network traffic, system logs, and user behavior, to identify anomalies that may indicate a cyberattack.

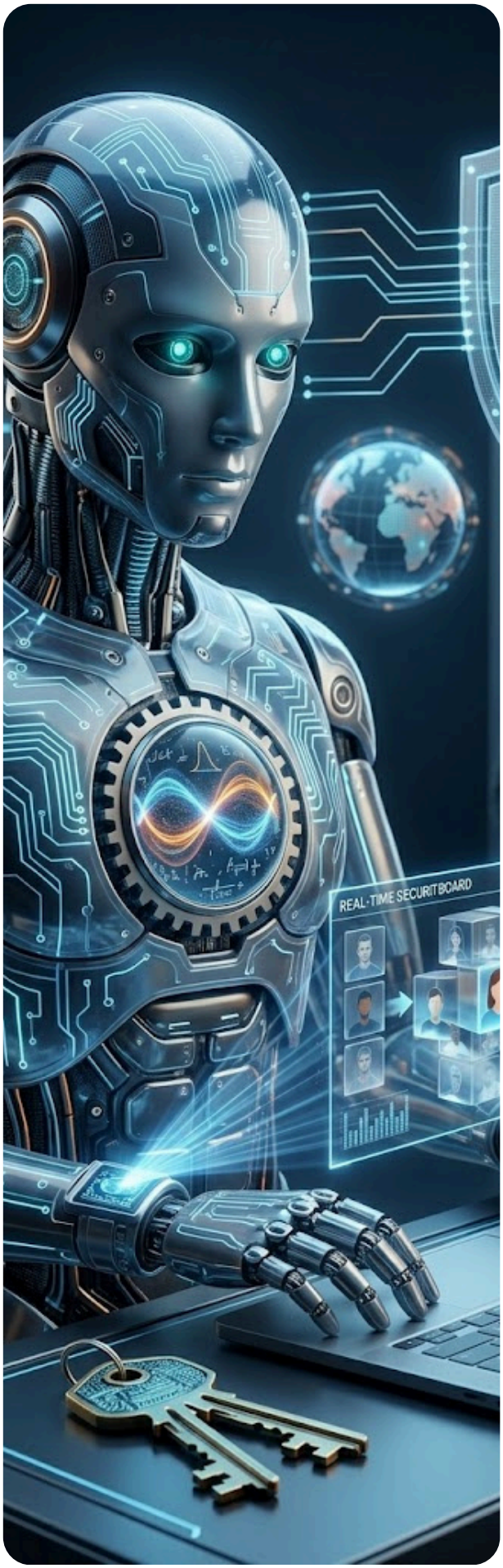
One of the biggest advantages of AI is speed. AI-powered systems can process massive amounts of data within seconds, something that would be impossible for human analysts. This allows faster detection and response, reducing the damage caused by attacks.

AI is also capable of continuous learning. As new threats emerge, AI systems update their models based on new data, making them more effective over time. This adaptability is crucial in a constantly changing threat landscape.

AI in Threat Detection and Prevention

Threat detection is one of the most important applications of AI in cybersecurity. AI models monitor network activity and establish a baseline of normal behavior.When unusual activity is detected, such as abnormal login locations, sudden spikes in data transfer, or suspicious file access, the system immediately raises alerts or blocks the action. AI is also widely used in malware detection. Traditional malware detection relies on known signatures, which makes it ineffective against new or modified malware. AI based systems focus on behavior analysis, identifying malicious actions rather than specific code patterns. This allows detection of zero day attacks that have never been seen before.

Phishing attacks have also become more sophisticated, often using convincing language and realistic websites. AI-powered email filters analyze email content, sender reputation, and user interaction patterns to detect phishing attempts. With the rise of AI generated phishing emails, defensive AI tools have become even more critical. AI plays a key role in cloud security by monitoring workloads, detecting misconfigurations, and identifying suspicious behavior across distributed systems. AI-driven intrusion detection systems (IDS) and intrusion prevention systems (IPS) continuously analyze traffic to prevent unauthorized access. In network security, AI helps in identifying DDoS attacks by analyzing traffic patterns and detecting abnormal spikes. Once detected, automated mitigation strategies can be deployed instantly, ensuring service availability.



Challenges and Ethical Concerns

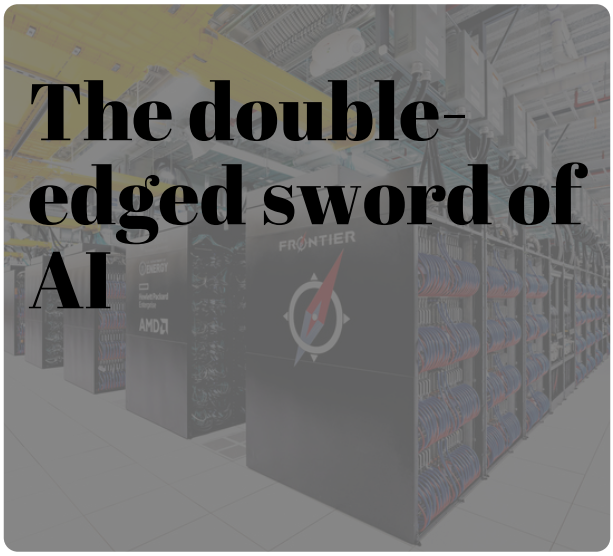
Despite its advantages, AI in cybersecurity also comes with challenges. One major concern is that attackers themselves are using AI to automate attacks, generate convincing phishing messages, and bypass security systems. This has led to an ongoing arms race between attackers and defenders.

Data privacy is another critical issue. AI systems require large amounts of data to function effectively, raising concerns about how user data is collected, stored, and used. Bias in AI models and lack of transparency in decision making processes are additional ethical challenges that must be addressed.

As future engineers, it is important to balance innovation with responsibility, ensuring that AI-powered security systems are ethical, transparent, and fair.

Conclusion

Artificial Intelligence has become a cornerstone of modern cybersecurity. Its ability to analyze data in real time, detect threats proactively, and adapt to evolving attack techniques makes it indispensable in today's digital world. As cyber threats continue to grow in complexity, the role of AI in defending digital infrastructure will only become more significant. For computer science students, the convergence of AI and cybersecurity presents both an opportunity and a responsibility. By building strong technical foundations and understanding real-world security challenges, future engineers can contribute to creating safer, more resilient digital systems.



Artificial Intelligence is no longer a futuristic dream from science fiction movies. It has quietly become a powerful part of our everyday lives. From unlocking smartphones using facial recognition to receiving personalized recommendations on streaming platforms, AI works silently in the background. For students, AI tools can now explain complex topics, generate code, and even help in writing assignments. Organizations like OpenAI have developed advanced systems such as ChatGPT that can interact with humans in a surprisingly natural way. As Artificial Intelligence continues to grow rapidly, an important question arises is AI our greatest technological friend, or is it a potential threat to our future?

AI as a Powerful Ally

On one side, AI has proven itself to be an extraordinary ally. In education, AI-powered platforms provide personalized learning experiences. Every student learns at a different pace, and AI systems can adapt accordingly, offering customized explanations and practice exercises. This makes learning more accessible and inclusive.

As a Computer Science student, I see how AI tools can assist in debugging code, understanding algorithms, and exploring new technologies more efficiently. Instead of replacing learning, AI can enhance it when used responsibly.

In healthcare, the role of AI is even more impactful. Machine learning algorithms can analyze medical images and detect diseases such as cancer at early stages, sometimes with higher accuracy than humans. AI-powered robotic systems assist in surgeries, reducing risks and improving precision. In the field of cybersecurity, AI monitors large networks in real time, identifying unusual activities and preventing cyberattacks before they cause damage. Without AI, managing such massive amounts of data would be nearly impossible.

AI also simplifies daily life. Virtual assistants like Google Assistant and Siri help us set reminders, answer questions, control smart devices, and navigate traffic efficiently. Businesses use AI for automation, improving productivity and reducing human error. Clearly, Artificial Intelligence has the potential to improve efficiency, accuracy, and convenience in countless areas of life.

The Challenges and Risks

However, despite its advantages, AI also brings serious concerns. One of the biggest fears is job displacement. Automation is replacing repetitive and routine tasks in industries such as

Aiswarya S Kumar
S4 CSE A

manufacturing, customer service, and even content creation. While AI creates new job opportunities in fields like data science and AI development, not everyone has equal access to reskilling and education. This could widen economic inequality if not managed carefully.

Another major issue is privacy. AI systems depend on vast amounts of data to function effectively. This data often includes personal information, browsing habits, and even biometric details. If misused, such data can lead to surveillance, identity theft, and loss of personal freedom. Moreover, the rise of deepfake technology allows AI to generate realistic fake videos and images, spreading misinformation and damaging reputations. In a world where digital content can be manipulated so easily, distinguishing truth from falsehood becomes increasingly difficult.

There is also the psychological aspect to consider. Students and professionals may become overly dependent on AI tools. While AI can assist with problem-solving, excessive reliance may weaken critical thinking and creativity. If we allow machines to think for us entirely, we risk losing essential human skills such as independent reasoning and emotional intelligence.

The Human Responsibility Behind AI

Despite these challenges, labeling AI as a "threat" may oversimplify the issue. Artificial Intelligence, by itself, has no intention or morality. It is a tool created and controlled by humans. Just as electricity can power cities or cause harm depending on how it is used, AI's impact depends on human decisions. Governments, organizations, and developers must work together to create ethical guidelines, regulations, and transparent systems to ensure responsible usage.

The future of AI does not have to be frightening. Instead of fearing technological advancement, society must focus on adaptation and education. Schools and universities should prepare students not just to use AI tools, but to understand their limitations and ethical implications. By promoting digital literacy and responsible innovation, we can ensure that AI remains a supportive partner rather than a destructive force.

In conclusion, Artificial Intelligence is neither a hero nor a villain. It is one of the most powerful tools humanity has ever created. Whether it becomes a friend that enhances our lives or a threat that disrupts them depends entirely on how wisely we choose to use it. The true power of AI lies not in the intelligence of machines, but in the responsibility of the humans who guide them.

Recommendation Systems (Netflix & YouTube):

How AI Decides What You Watch Next

Akshai M
S4 CSD

Every time users log in to Netflix or YouTube, they are exposed to a curated list of movies, TV shows, and videos. The ease and simplicity of this process belie the fact that it is one of the most advanced applications of Artificial Intelligence. The primary function of a recommendation system is to predict the type of content that a user is most likely to consume and enjoy in the future. The sheer volume of content on these platforms makes it unreasonable to manually traverse through it. Recommendation systems solve this problem by creating intelligent filters for users.

Understanding User Data

The first step in creating a recommendation system is to accumulate a large volume of user data. This includes:

- Videos that the user has watched
- Videos that the user has searched for
- Videos that the user likes or dislikes
- The time for which the user watched the videos
- The type of device and time of usage

Each of these actions creates a data point. Over time, these data points coalesce to form a detailed digital profile that characterises a user.

Collaborative Filtering

The most common of these is collaborative filtering. The idea behind this technique is that users who behaved in a similar manner in the past will continue to do so in the future. To illustrate this, assume that several users who have watched Series A have also watched Movie B. Consequently, if a new user watches Series A, they will be recommended to watch Movie B. The strength of this technique is that it does not require an understanding of content semantics. However, this technique is only successful if there is access to considerable data and computational power

Content-Based Filtering

The alternative to collaborative filtering is content-based filtering. This technique focuses on content features rather than similarities between users. Each movie/video has features such as:

- Genre
- Language
- Actors/creators
- Keywords
- Time duration

If a user has been watching English romance comedy movies, this technique will recommend them to watch such movies.

Deep Learning and Neural Networks in Modern Platforms

In modern platforms, deep learning is used in combination with neural network architectures to analyse complex relationships between users and their content. These platforms learn new patterns that may not be captured by other conventional methods, and their accuracy improves over time with new data. Deep learning can enable several features, including:

- A better understanding of user intent
- Predictions about users' changing interests
- The ability to rank thousands of items in real time

The type of recommended content changes over time, e.g., for users who were previously interested in comedies, they can now see an increasing number of documentaries.

Real-Time Recommendation Pipeline

The recommendation process is done in almost no time at all. The process can be outlined as follows:

- User initiates an interaction with an application
- User profile and latest activity are obtained
- A wide range of content options is evaluated by AI models
- Content is ranked according to predicted user interest
- Recommended content is displayed to users

The entire process takes only milliseconds to complete, thanks to cloud-based platforms that utilise distributed computing systems.

Personalisation at Scale

The ultimate goal of recommendation systems is to maximise user interaction with their platforms. For instance, platforms can experiment with:

- Thumbnail images
- Video title
- Position of content on the home interface
- Autoplay settings

All these elements can be tested to determine which one improves user experience. This shows that recommendation systems are intrinsically linked to user experience design, which is an integral part of business strategy

Benefits of Recommendation Systems

- Saves users time
- Facilitates user discovery
- Improves user satisfaction
- Improves user engagement on platforms
- Generates revenue through increased user viewing sessions

From observations, it is evident that most of the time users spend watching videos on platforms is through recommended content, not through direct searches by users.

Challenges and Ethical Concerns

Despite their effectiveness, recommendation systems face several challenges. They include the generation of filter bubbles that present users with parallel content. There is also the problem of algorithmic bias that may favor popular content. The concern overoptimizing user engagement that may lead to addiction is also important. The problem of privacy that arises due to the collection of personal information is also relevant. Finding an equilibrium between personalization and ethics remains an important area of research in artificial intelligence.

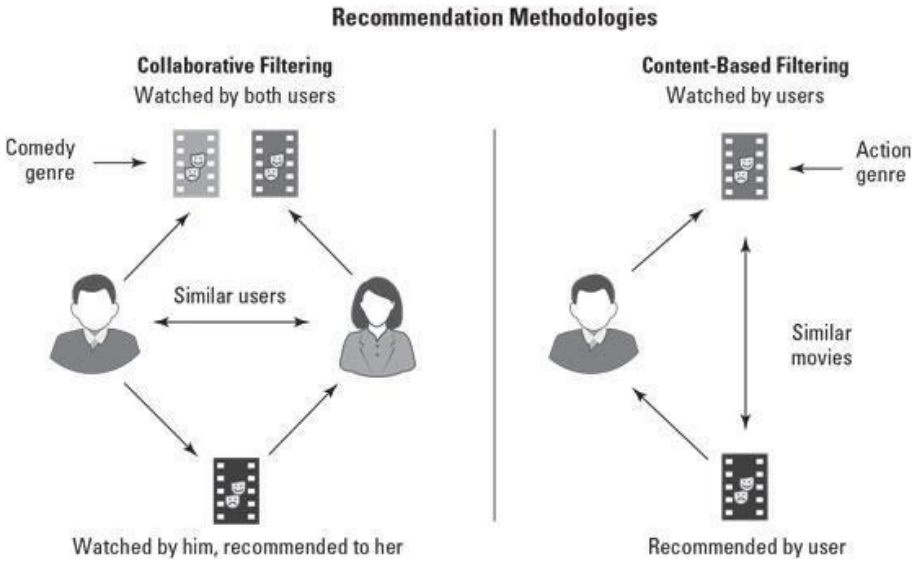
Future Prospects of Recommendation Systems

The future of recommendation systems appears to be highly positive. The systems in use in the future will be highly contextual. They will include factors such as user moods, location, and circumstances. There is also an expectation that future recommendation systems will be highly transparent. They will allow users to understand why they receive specific content recommendations.

Conclusion

Recommendation systems form one of the most important applications of artificial intelligence in the world. The simple list of suggested content is underlined by complex algorithms, huge databases, deep learning models, and high-performance computing infrastructure. Recommendation systems form an important area of study for computer science students.

They demonstrate how computer science theory impacts the lives of billions of users every day.



2025: The Indie Year

Anpu Saramsh
S4 CSE A

2025 has been a year full of ups and downs, but for certain industries, it was a year of great growth and even better representation. I am talking about the gaming industry and to be more specific the indie gaming industry and how they came out on top this year.

2025 Game Awards wrapped up back in December and with it Sandfall Interactive made history.
Claire Obscure Expedition: 33 won the International Game Awards by a Landslide, and with it won 8 more categories. The Last time such a dominant display was seen was back in 2020 with Last of Us Part II. It remains the most awarded game in the history of the game awards

2025 has been a year full of ups and downs, but for certain industries, it was a year of great growth and even better representation. I am talking about the gaming industry and to be more specific the indie gaming industry and how they came out on top this year.

2025 Game Awards wrapped up back in December and with it Sandfall Interactive made history.
Claire Obscure Expedition: 33 won the International Game Awards by a Landslide, and with it won 8 more categories. The Last time such a dominant display was seen was back in 2020 with Last of Us Part II. It remains the most awarded game in the history of the game awardsIn terms of technology the gaming industry is both different and similar to other applications of computer science. When a revolutionary piece of hardware is created or a software is created it sparks a whole new category with it and that much is similar for video games, as an example take Wolfenstein 3D.

It was the first game to pivot into the 3 dimensional world and opened the door to 3D games as we know them today. But the gaming industry has a different form of breakthroughs, when people take already existing tools and create something that no one could even imagine was possible to do in the first place. Expedition: 33 falls squarely in the 2nd category. A game that took existing game engines and existing combat systems and made it something more. By doing something as simple as adding a parry mechanic or a dodge counter-option, they revolutionized the once-thought-to-be-saturated turn based combat and made it into something fresh. 2025 seemed the perfect year for indie games to take home the win, after major controversy surrounding AAA games (games made by major companies, such as Rockstar, Ubisoft, EA, etc.)
With all their anti-consumer practices such as raising prices, the active use of generative AI in the production of AAA games or the CEO of Ubisoft publicly stating how “gamers should get comfortable not owning games”, and such which lit a fire under the companies, giving birth to pro-consumer movements like the “Stop Killing Games” initiative.

Claire Obscure Expedition: 33 was a game that not only had an amazing story with the theme of leaving a better world for ‘those who come after’ and amazing art to boot, but it took an existing system of turn based combat, and completely turned it into something original. Coupled with Unreal Engine 5, a game engine capable of simulating graphics stunning enough to fool someone into thinking it might be reality, the game itself is not just an artistic masterpiece,

but a true testament to the immense technological marvel of graphics processing.

2025 was proof that AAA game studios and publishers were not the end-all be-all for releasing a successful game and that a very important, core part of the video game industry is held up by the indie community, who with their creativity take video games to a whole other level. It is proof that anyone with enough love for the game can do it too.

ARE WE CODING OUR OWN REPLACEMENTS?

Fathima Hana
S4 CSE B

Imagine walking into your future workplace, only to find that your colleague is not a human, but a machine. It writes cleaner code than you. It debugs faster than you. It learns from millions of data points in seconds. And it never gets tired. Now imagine something even more unsettling, you helped build it. Artificial Intelligence is no longer a distant concept from science fiction. It is designing software, optimizing systems, generating content, and reshaping industries. As engineering students and future innovators, we must confront a bold and uncomfortable question :**ARE WE CODING OUR OWN REPLACEMENTS?**

THE RISE OF INTELLIGENT AUTOMATION:

AI today is far more than a simple tool. Modern systems can write functional programs in multiple languages, detect and fix logical errors, suggest performance improvements, automate testing and deployment and analyze large-scale data with remarkable accuracy. In cybersecurity, AI identifies unusual patterns faster than many human analysts. In hardware design, it helps optimize chip layouts and energy efficiency. In software development, it assists with architecture planning and documentation. The productivity gains are undeniable. AI acts like a highly efficient assistant by processing information at speeds no human can match. Engineers can now build faster, test quicker, and deploy smarter systems. However, increased efficiency does not automatically mean human replacement.

WHAT AI CANNOT REPLACE:

Despite its capabilities, AI operates within clear boundaries.

It learns from data, recognizes patterns, and predicts outcomes based on probabilities. But it does not truly understand meaning, intention, or consequences in the human sense. Engineering is not merely about executing instructions. It involves ethical decision-making, accountability, creativity, strategic thinking and understanding real-world complexity. When a bridge collapses, a financial system crashes, or a medical device fails, responsibility does not lie with an algorithm. It lies with human engineers. AI can assist in design and testing, but it cannot take moral or legal responsibility for outcomes. Creativity remains another deeply human strength. While AI can generate variations of existing ideas, true innovation often emerges from imagination, lived experience, and interdisciplinary thinking. Breakthrough ideas frequently come from questioning assumptions, something machines are not designed to do independently.

LESSONS FROM HISTORY:

The fear of technological replacement is not new. During the Industrial Revolution, machines transformed manufacturing, and many feared mass unemployment. Instead, new professions emerged. When calculators became common, mathematicians were not replaced. When computers automated accounting tasks, the demand for IT professionals increased dramatically. Technology tends to remove repetitive tasks, not entire professions. AI is following a similar pattern. Routine coding, basic debugging, and repetitive analysis are increasingly automated. But this shift allows engineers to focus on higher-level responsibilities such as system design, innovation, scalability, and ethical oversight. Rather than eliminating engineers, AI is reshaping what engineering means.

THE ERA OF COLLABORATIVE INTELLIGENCE:

Instead of a competition between humans and machines, the future appears to favour collaboration. In this model of collaborative intelligence, AI handles speed, scale, and pattern recognition. Humans provide creativity, direction, ethics, and judgment. For example, an AI tool may generate a software prototype. A human engineer evaluates its security risks, long-term maintainability, and user impact. The combination of computational speed and human reasoning produces stronger results than either could achieve alone. Engineers who learn how to effectively integrate AI into their workflow will likely become more productive and more competitive in the job market.

NEW OPPORTUNITIES IN AN AI-DRIVEN WORLD:

AI is not shrinking opportunities, it is transforming them. New roles are emerging in areas such as AI safety and alignment, machine learning operations, algorithmic fairness and bias detection and data ethics and governance. Engineers are increasingly expected to understand not only how to build systems, but also how to ensure those systems are transparent, secure, and socially responsible. The demand for technical professionals remains strong, but the required skill set is evolving.

WHAT THIS MEANS FOR STUDENTS:

For engineering students, adaptability is becoming the most valuable skill. Strong foundations in programming, data structures, algorithms, and system design remain essential.

However, understanding AI tools and machine learning concepts is equally important. Engineers must learn how AI works, where it can fail, and how to use it responsibly. At the same time, human–centered skills are gaining importance. As AI automates technical repetition, engineers must focus on innovation, problem-solving, and long-term strategic thinking. The goal is not to compete with AI on speed, but to complement it with insight.

THE REAL RISK:

The real danger is not that AI will replace engineers. The real danger is that engineers who refuse to adapt may become less relevant. Every technological shift rewards those who evolve with it. Just as previous generations adapted to computers and the internet, this generation must adapt to artificial intelligence. Engineers who embrace AI can become more creative, more efficient, and more impactful than ever before.

CONCLUSION:

So, are we coding our own replacements? No. We are coding our evolution. Artificial Intelligence is not the end of engineering, it is the next chapter. Machines may generate code, analyze data, and optimize systems, but they do not dream, question, or imagine beyond their programming. They do not carry responsibility. They do not define purpose. The future will not belong to AI alone. It will belong to engineers who understand it, guide it, and use it to build something greater than themselves. **AI** will not **REPLACE ENGINEERS**, it **REPLACES** those who **STOP GROWING**.

The Future of Engineering: Can AI Design Better Engineers Than Humans?

Fathima Hannah M T
S4 CSE B

Introduction

In the rapidly evolving landscape of technology, artificial intelligence (AI) is no longer a concept confined to science fiction. Its applications are expanding into nearly every sector, from healthcare to finance, and now, we stand at the precipice of its potential impact on engineering education and development. The intriguing question arises: can AI design better engineers than humans?

The answer isn't a simple yes or no, but rather a nuanced exploration of AI's capabilities and its role as a powerful augmentative tool.

AI as a Personalized Learning Architect

One of the most compelling arguments for AI's role in shaping future engineers lies in its ability to personalize learning experiences. Traditional engineering education, while robust, often follows a standardized curriculum. AI, however, can analyze an individual student's learning style, strengths, weaknesses, and even career aspirations. Imagine an AI tutor that adapts course material, suggests supplementary resources, and provides targeted feedback in real-time. This level of personalized instruction could optimize knowledge retention and skill development, ensuring each aspiring engineer receives the most effective training tailored to their unique needs.

Simulating Complex Engineering Challenges

AI-powered simulations can revolutionize how engineers are trained to tackle complex problems. It can generate incredibly realistic and dynamic scenarios, exposing students to a wider array of challenges from structural failures in extreme conditions to optimizing energy grids under fluctuating demand without the risks and costs associated with real-world experimentation.

This allows engineers to practice problem-solving, decision-making, and critical thinking in a safe, yet highly challenging, environment.

Identifying and Nurturing Talent

AI algorithms are adept at pattern recognition. By analyzing performance in various tasks and innovative approaches to problems, AI could identify exceptional potential that might otherwise go unnoticed. It could guide individuals toward specialized fields where their strengths would be most impactful, fostering a new generation of highly specialized and effective engineers.

Automating Repetitive Tasks, Focusing on Innovation

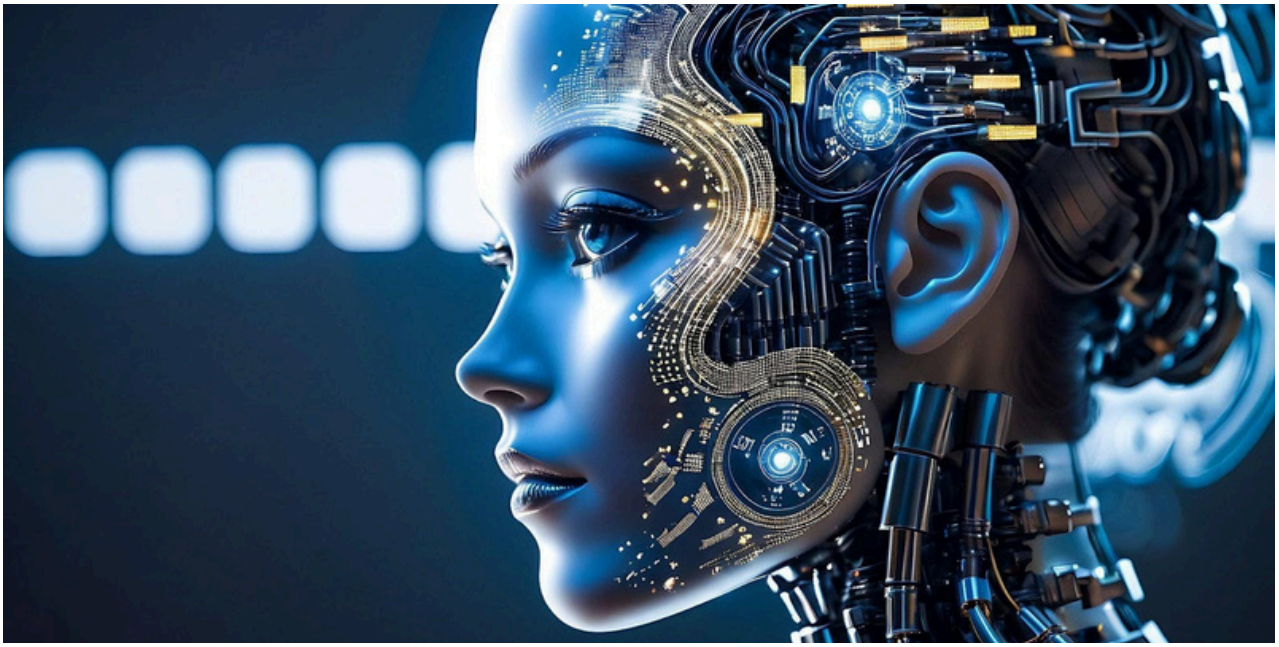
By automating repetitive tasks and calculations that consume significant time in engineering studies, AI can free learners to focus on higher-order thinking, creativity, and innovative problem-solving. This enables deeper conceptual understanding and interdisciplinary approaches essential for addressing complex global challenge

The Human Element Remains Paramount

AI cannot replace empathy, ethical reasoning, leadership, and the ability to understand societal needs. These deeply human attributes remain central to engineering. AI serves as a sophisticated tool that enhances human capabilities while educators focus on mentoring and ethical guidance.

Conclusion

While AI may not literally design engineers, it holds immense potential to design better engineers by optimizing learning, simulating complex challenges, identifying talent, and streamlining education. The future of engineering lies in intelligent collaboration between human ingenuity and artificial intelligence.



The Age of Autonomous Agents: When AI Starts Managing AI

Hannah Pullan
S4 CSE B

Artificial Intelligence is no longer confined to answering questions or generating text on command. It is evolving into something far more dynamic — systems that can interpret goals, design strategies, execute tasks, evaluate outcomes, and refine their own processes with minimal human intervention. This new paradigm is defined by autonomous agents.

Unlike earlier AI tools that functioned reactively, autonomous agents operate with intent. They do not simply wait for instructions; they pursue objectives. When given a complex task, they deconstruct it into manageable components, coordinate resources, interact with digital tools, and adapt their approach based on results. In doing so, AI is beginning to manage not just data — but other AI systems and entire computational workflows.

This transition represents one of the most profound architectural shifts in modern computing.

From Reactive Systems to Goal-Driven Intelligence

The first generation of AI systems primarily served as assistants. Platforms such as ChatGPT or cloud-based automation services integrated into Microsoft Azure were designed to respond to prompts. They generated outputs efficiently, but their interaction cycle ended once the response was delivered.Autonomous agents, however, extend beyond single interactions. If assigned a broad objective such as launching a product campaign or developing a software module, an agent does not require step-by-step guidance. It formulates a plan, allocates subtasks, gathers relevant information, and iteratively adjusts its strategy based on feedback. The process becomes continuous rather than transactional.

This shift from prompt-response behavior to goal-oriented execution is what distinguishes autonomous agents from traditional AI systems. Intelligence is no longer confined to output generation; it becomes embedded in decision-making and workflow management.

When AI Coordinates AI

Perhaps the most revolutionary development in this space is the emergence of layered, multi-agent architectures. Instead of relying on a single model, systems are increasingly designed as collaborative networks of specialized agents.

One agent may function as a planner, outlining the roadmap toward achieving a goal. Another may focus on data retrieval and analysis. A third could generate code or creative content, while a separate evaluation agent assesses the quality and accuracy of outputs. Overseeing them all is a coordinating agent responsible for maintaining coherence and ensuring alignment with the primary objective.

Organizations such as OpenAI and Google are actively exploring these multi-agent frameworks, where models critique, refine, and improve one another's outputs in iterative cycles. In effect, AI systems are beginning to manage and optimize other AI systems — forming structured, digital workforces capable of operating at scale.

The Technical Architecture Behind Autonomy

Autonomous agents are not powered by a single breakthrough but by the convergence of multiple technologies. At their core are large language models that provide reasoning and contextual understanding. Surrounding these models are memory systems that allow agents to retain information across sessions, creating continuity rather than isolated interactions.

Tool integration plays a crucial role as well. Agents can access APIs, browse databases, execute code, and interact with digital environments. Reinforcement learning and feedback mechanisms enable adaptation, allowing agents to learn from outcomes and refine future decisions. Orchestration frameworks coordinate these components, ensuring that multiple models work together coherently rather than in isolation.

The result is not merely a smarter chatbot, but a dynamic ecosystem of interacting systems capable of sustained, independent operation.

Transforming Industries

The implications of autonomous agents extend across technical domains. In software engineering, agents can generate code, test it, identify bugs, and deploy updates in rapid cycles. In cybersecurity, they monitor networks continuously, detect anomalies, and initiate responses before human teams can intervene. Financial systems leverage adaptive algorithms that recalibrate strategies based on real-time market signals, while scientific research environments use AI to generate hypotheses and analyze experimental data.

In high-performance data centers powered by companies like NVIDIA, these agent-driven systems operate with immense computational capacity. The scale at which they function transforms them from experimental tools into operational infrastructures.

The Complexity of Control

Yet autonomy introduces new layers of complexity. Systems capable of independent decision-making must be aligned with human objectives and constrained within ethical and operational boundaries.Without careful design, errors can propagate rapidly through interconnected agents.

Computational demands may escalate, and security vulnerabilities could emerge if permissions are not tightly controlled. As a result, research increasingly focuses on alignment strategies, monitoring frameworks, and fail-safe mechanisms. The challenge lies not merely in building more capable agents, but in ensuring that they remain controllable, transparent, and efficient.

Toward Digital Workforces

As architectures mature, the concept of AI-based digital organizations moves closer to reality. Coordinated networks of autonomous agents may handle repetitive technical operations, data processing, infrastructure management, and even elements of research and development. Human roles will not vanish, but they will evolve — shifting toward oversight, ethical governance, and strategic direction. The next frontier lies in self-improving systems: agents capable of analyzing and optimizing aspects of their own architecture.

If achieved responsibly, this could accelerate technological progress at unprecedented speed. However, such capability also demands rigorous safeguards and responsible deployment.

Conclusion

The rise of autonomous agents marks a structural transformation in artificial intelligence. We are moving beyond reactive tools toward interconnected, goal-driven systems capable of sustained, coordinated action. AI is no longer simply assisting human workflows; it is beginning to design and manage them.

This evolution signals the emergence of intelligent ecosystems — digital networks that collaborate, adapt, and execute with increasing independence. The central question is no longer whether AI can respond to us. It is whether we are prepared to collaborate with systems that can increasingly act on their own. The age of autonomous agents is not a distant possibility. It is already unfolding.

The Silicon Traffic Jam: Why AI is Running Out of Gas

The global technology industry is currently living through a paradox. On one side, we have the fastest race in human history. On the other, we have the world's most expensive traffic jam.

Welcome to the **Great AI Memory Shortage of 2026.**

In this high-stakes poker game, the chips are quite literally computer chips. But we aren't talking about the processors that do the thinking. We are talking about the "gasoline" that keeps them running: a scarce, ultra-expensive, and incredibly hard-to-build technology called High-Bandwidth Memory (HBM). Without it, the $100 billion AI revolution is just a very expensive paperweight.

Act I: The New Ferraris (and the Empty Tank)

To understand the crisis, you have to look at the cars on the track.

Back in 2024, the "Ferrari" of AI was the NVIDIA H100. But that's ancient history. Today, in early 2026, the new king of the road is the NVIDIA Blackwell B200.

It's a dual-chip monster that is effectively two silicon brains smashed together to act as one. It is faster, smarter, and hungrier than anything we've ever seen.

Then there's the other racer: Google is racing its own custom fleet: the workhorse TPU v6 (Trillium) for training, and the brand-new TPU v7 'Ironwood'—a specialist chip designed solely to run the massive reasoning models of 2026.

But here is the problem: Both the B200 and the TPU v7 share the same addiction. They need massive amounts of data fed to them instantly. If you use standard computer memory, it's like trying to fill a Formula 1 car with a garden hose. The engine stalls.

To run at full speed, these chips need HBM—specifically the new HBM3E and the cutting-edge HBM4. And right now, the world is running on fumes.

Act II: The Skyscraper Revolution

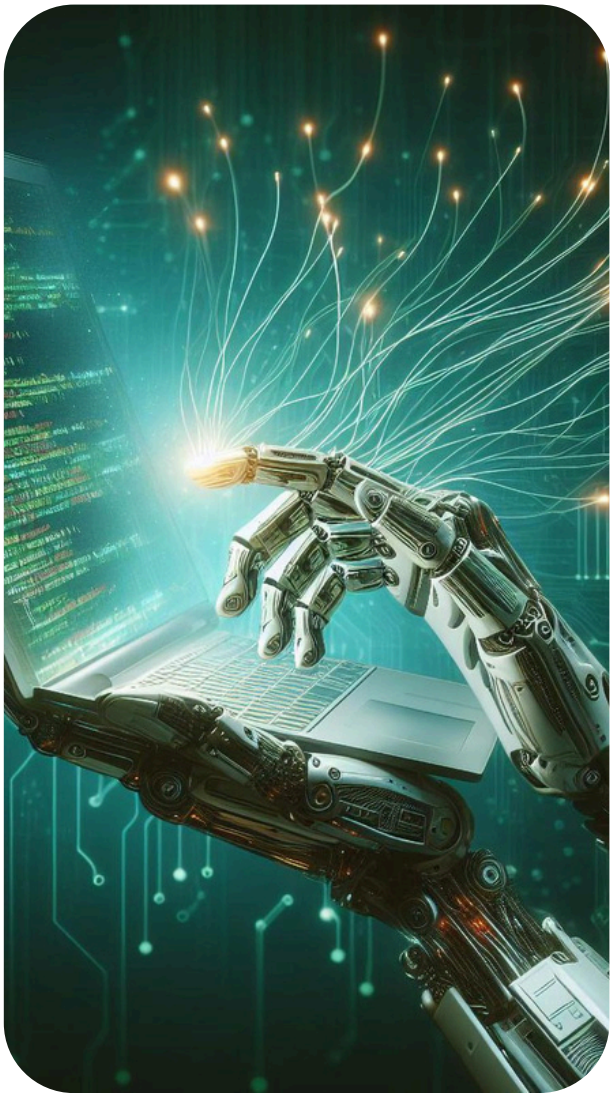
So, what exactly is this magical memory?
For decades, computer memory (DRAM) was like a sprawling, flat parking lot. Data cars would drive in, park, and drive out.

HBM is a skyscraper.

Instead of spreading chips out, engineers stack them vertically—12 to 16 stories high—right on top of the processor. They then drill thousands of microscopic elevators, called **Through-Silicon Vias (TSVs)**, straight through the floors.

On Feb 12, 2026, Samsung pulled off a massive upset. They shipped the industry's first commercial HBM4 memory, beating their rival SK Hynix to the punch. This isn't just a taller building; it's a smarter one. For the first time, the "foundation" of the building (the base die) is made of logic processors (4nm), not just memory.

It's an engineering marvel. It's 40% more power-efficient. And it is incredibly difficult to manufacture.



Act III: "RAMmageddon"

This is where the story hits home for you and me. Because HBM is so profitable and so vital for AI, the "Big Three" memory makers—Samsung, SK Hynix, and Micron—are making a ruthless calculation. They are ripping out the machines that make standard RAM for your PC and phone to make room for HBM lines.

Micron recently dropped a bombshell: their entire HBM supply for 2026 is already sold out. To meet demand, they are pivoting aggressively away from consumer electronics.

The result is what analysts are calling **"RAMmageddon."**

- Price Spikes: The cost of standard DRAM has skyrocketed 80-90% in just the first six weeks of 2026.
- Gadget Inflation: PC makers like Dell are reportedly eyeing 15-20% price hikes. If you're planning to buy a new laptop or smartphone this year, prepare to pay the "AI Tax."
- The "Parking Lot" is Closed: The industry is digging up the parking lot to build more skyscrapers. If you just wanted to park your car (i.e., use a normal computer), you're out of luck.

Act IV: The Billionaire's Dilemma

The desperation at the top is palpable.

In January, **Elon Musk** gave the crisis a slogan. Facing the prospect that Tesla might not get enough chips to train its self-driving AI, he bluntly stated: **"We have two choices: hit the chip wall or make a fab."**

He's not joking. The "chip wall" is the point where money no longer matters because there simply isn't any hardware left to buy.

Google is trying to sidestep the wall by buying huge chunks of the market—projections show Google alone could consume 30% of the world's HBM supply this year for its TPUs. They are betting the farm on custom silicon to keep Gemini growing.

The 2027 Horizon

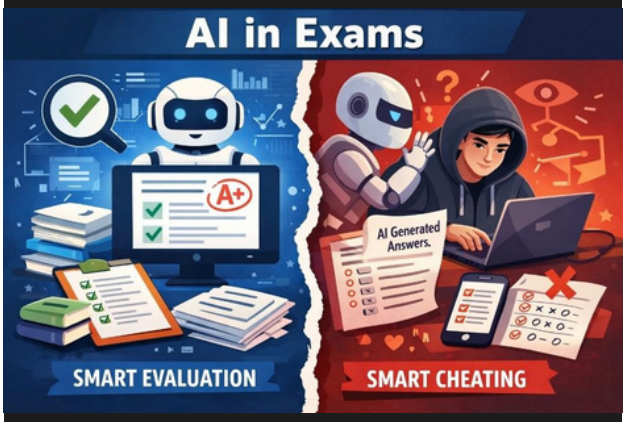
As we look toward the end of the year, the race is only getting faster. NVIDIA's next-generation **"Rubin"** platform is already on the roadmap for 2027, promising to stack even more memory.

As we look toward the end of the year, the race is only getting faster. NVIDIA's next-generation **"Rubin"** platform is already on the roadmap for 2027, promising to stack even more memory.

For now, the lesson is clear: The cloud isn't weightless. It is built on heavy, expensive, hot silicon. And right now, the most valuable real estate in the world isn't in Manhattan or Mumbai—it's the vertical stack of memory sitting inside a server rack, keeping the AI dream alive. So, if your new phone costs a bit more this year, you know who to blame. The gas station is empty, and the Ferraris are drinking it all.

Mohammed Mahir Mobin
S4 CSD

AI in Exam Systems: Smart Evaluation or Smart Cheating?



Meenakshi S
S4 CSE B

Artificial Intelligence is rapidly transforming education. From automated grading tools to AI-powered proctoring systems, technology is redefining how exams are conducted and evaluated. But as AI becomes more integrated into assessment systems, a pressing question emerges:

The Rise of AI in Exam Systems

Educational institutions worldwide are adopting AI to improve efficiency and accuracy in evaluation. Platforms powered by AI can now:

- Automatically grade multiple-choice and short-answer questions
- Evaluate essays using natural language processing
- Monitor students through AI-based proctoring systems
- Detect plagiarism with advanced pattern recognition

Companies like Turnitin use AI-driven algorithms to identify copied content, while online learning platforms such as Coursera integrate automated assessments for scalable learning. The goal is clear: reduce human bias, save time, and standardize evaluation.

Smart Evaluation: The Advantages

1. Faster and Efficient Grading

AI can evaluate thousands of answer sheets in minutes. This is especially useful in large-scale exams and online courses with massive enrollment.

2. Reduced Human Bias

Human evaluators may unintentionally favor certain writing styles or interpretations. AI systems apply consistent grading criteria across all students.

3. Detailed Performance Insights

AI can analyze patterns in student performance, identifying weak areas and recommending personalized improvement strategies.

4. Remote Accessibility

AI-based proctoring allows students to take exams from anywhere, making education more accessible globally.

In many ways, AI promises a fairer and more efficient examination system.

Smart Cheating: The Other Side of the Story

However, the same AI revolution has opened doors to new forms of academic dishonesty.

1. AI-Generated Answers

Students can use tools like ChatGPT to generate essays, solve coding problems, or even complete entire assignments within seconds.

2. Undetectable Paraphrasing

AI tools can rewrite copied content so effectively that traditional plagiarism detection systems struggle to flag it.

3. Deepfake and Proxy Cheating

With advances in facial recognition bypass techniques and remote access tools, AI-based proctoring systems can sometimes be manipulated.

4. Over-Reliance on Automation

When evaluation is fully automated, students may focus on "gaming the algorithm" rather than truly understanding the subject.

Instead of testing knowledge, exams risk becoming contests of who uses AI more cleverly.

Ethical and Privacy Concerns

AI-based exam monitoring often includes:

- Facial recognition
- Eye movement tracking
- Audio monitoring
- Behavior analysis

These systems raise serious privacy questions. Are students being excessively surveilled? Can AI misinterpret nervous behavior as cheating?

There have been criticisms of AI proctoring systems like those used by ProctorU, where students reported false flags and technical issues during exams.

AI is not perfect — and errors in high-stakes exams can significantly impact students' futures.

The Bigger Question: What Are We Really Testing?

The rise of AI challenges the traditional purpose of exams.

If AI can instantly generate essays, solve equations, and debug code, then perhaps memorization-based exams are becoming outdated. Instead of asking:

"Can students produce the correct answer?"

We may need to ask:

"Can students think critically, apply knowledge, and solve real-world problems?"

Education systems might need to shift toward:

- Open-book exams
- Application-based assessments
- Oral examinations
- Project-based evaluation
- AI-assisted but reasoning-focused tests

Rather than banning AI, institutions may need to redesign exams around it.

Smart Tool or Smart Loophole?

AI in exam systems is neither purely beneficial nor purely harmful. It is a tool — and like any tool, its impact depends on how it is used.

If implemented responsibly, AI can:

- Improve fairness
- Increase efficiency
- Enhance learning outcomes

But without proper guidelines and redesign of assessment models, it can:

- Encourage superficial learning
- Increase sophisticated cheating
- Undermine academic integrity

Conclusion

AI is not just changing exams — it is challenging the very definition of knowledge and assessment.

The real issue is not whether AI makes evaluation smarter or cheating smarter. The real issue is whether educational institutions can adapt quickly enough to ensure that technology strengthens learning rather than weakens it.

In the future, success may not depend on avoiding AI — but on learning how to use it ethically, intelligently, and responsibly.

Ni8mare:

A Remote Code Execution Flaw in the Age of AI Agents

Niranjana S
S4 CSD

When a single flaw opens every door

Recently in 2026, security researchers uncovered a critical vulnerability in n8n, an open source workflow automation platform used by developers and companies around the world. The flaw, later nicknamed Ni8mare, was not just another minor bug. It was a remote code execution vulnerability that allowed attackers to take control of exposed systems without needing any authentication. In simple terms, if a vulnerable n8n instance was connected to the internet, an attacker could send a specially crafted request and make the server run their own commands.

Remote code execution vulnerabilities are considered among the most dangerous in cybersecurity. They allow attackers to move from being an outsider to having full control of a system. In the case of Ni8mare, the situation was even more serious because of where the vulnerability existed. It was not in a simple application or a small utility. It was in a workflow engine that often sits at the center of multiple services, data sources, and automated processes. This meant that the attack was not just about breaking into one system. It was about gaining control over everything connected to it.

What makes n8n such a powerful target

n8n is designed to connect different applications and automate tasks between them. It can read emails, process data, interact with APIs, trigger notifications, and even run AI models as part of its workflows. Many organizations use it to build automated pipelines that run quietly in the background.Because of this, n8n usually holds access to sensitive information. It may store database credentials, API tokens, and authentication keys for various services.

It may also have permission to perform actions such as sending messages, updating records, or running scripts on connected systems.

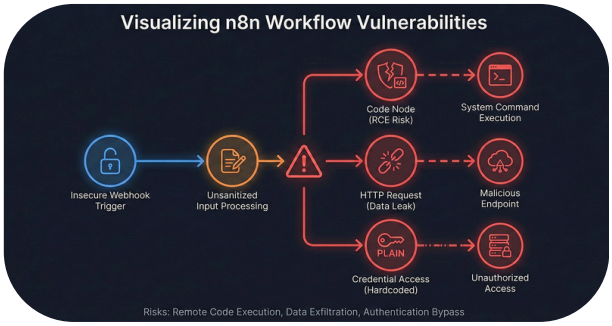
It may also have permission to perform actions such as sending messages, updating records, or running scripts on connected systems.

How the Ni8mare vulnerability worked

The Ni8mare flaw allowed attackers to execute commands on a vulnerable n8n server from a remote location. The most alarming part was that the attack did not require any login credentials. The system would accept the malicious request and run the attacker's code as if it were a legitimate command.

Once the attacker gained control, they could do almost anything the server was allowed to do. They could read stored credentials, modify workflows, access connected services, or install malicious programs. In some cases, they could even use the compromised server as a launching point for further attacks inside the network.

What made the vulnerability especially concerning was the number of exposed instances. Thousands of n8n systems were directly accessible from the internet. Many of them were running without strong authentication or network restrictions. This created a large attack surface where a single vulnerability could affect a huge number of targets.



When automation becomes a weapon

Automation platforms are built to perform actions automatically. They do not wait for manual approval every time a task needs to be completed. This is what makes them efficient, but it is also what makes them dangerous when compromised. If an attacker takes over a normal application, they might gain access to stored data. But if they take over an automation engine, they gain the ability to perform actions across multiple systems. They could send fake emails, alter data in databases, or trigger processes that cause financial or operational damage. The real danger is that these actions happen automatically. Once the attacker modifies the workflow, the system itself carries out the malicious tasks. This makes the attack faster, quieter, and harder to detect.

The growing role of AI in workflows

Modern automation platforms are no longer limited to simple tasks. Many of them now include AI agents that can process text, analyze data, or make decisions. These agents are often connected to emails, customer messages, or internal systems.

This creates a new kind of risk. If an attacker compromises an automation platform that uses AI, they can manipulate the decision making process itself. Instead of manually controlling every action, they can alter the logic and let the AI handle the rest.

For example, an attacker could modify a workflow so that an AI system starts sending misleading messages, leaking sensitive information, or approving requests that should have been rejected. Because the system is automated, these actions could continue for a long time before anyone notices.

A new attack surface in modern systems

For years, cybersecurity focused on protecting operating systems, web servers, and databases. These were the main components that attackers targeted. But the rise of automation and AI has created a new layer in modern computing. Workflow engines now sit at the center of many digital environments. They connect services, manage data flows, and execute automated actions. They often have high privileges and broad access across systems. This makes them an attractive target. A single vulnerability in such a platform can lead to widespread compromise. Instead of attacking each system separately, an attacker can simply take over the automation engine and let it do the work. The Ni8mare incident is a clear example of this shift. It shows that the security focus must expand beyond traditional components to include automation and AI driven systems.

Why the vulnerability spread so easily

One of the main reasons Ni8mare became a serious threat was the way many systems were deployed. Automation platforms are often installed quickly for convenience. Developers may expose them directly to the internet to allow remote access or integration with cloud services. In many cases, these systems were running without proper authentication or network restrictions. Some were not updated regularly, leaving them vulnerable to known flaws. Basic security practices could have reduced the impact. Limiting access to trusted networks, enabling authentication, and keeping software updated are simple steps that can prevent many attacks. However, as automation tools become easier to use, security is sometimes treated as an afterthought.

Lessons for the age of AI agents

The Ni8mare vulnerability highlights a deeper issue in modern cybersecurity. As systems become more automated and intelligent, the consequences of a security flaw become greater. A compromised AI driven workflow is not just a technical problem. It can affect business operations, financial transactions, and decision making processes. Automation platforms are becoming the control centers of digital systems. They connect services, store credentials, and execute actions. This makes their security critical. The incident serves as a reminder that convenience should never come at the cost of security. As organizations adopt AI agents and automation tools, they must also adopt stronger security practices. Protecting these systems is no longer optional. It is a necessity.

How the issue was fixed

After the vulnerability was discovered, the developers of n8n released security updates to close the flaw. Users were advised to update their systems as soon as possible so that attackers could no longer exploit the weakness. Security teams also encouraged people not to leave automation platforms exposed directly to the internet. Many organizations reviewed their setups, added proper authentication, and restricted access to trusted networks to prevent similar incidents.

The Silent Data We Give Away: How Everyday Apps Predict Our Behavior

In the modern digital era, smartphones and apps have become an integral part of our daily lives. From social networking to online shopping, from navigation to entertainment, technology is always interacting with us. However, beneath the convenience and personalization lies a powerful system that is collecting and analyzing our data. Every click, search, and interaction is adding up to what is called "behavioral data." This quiet exchange of information enables apps to forecast our decisions, interests, and even future actions.

Most people are aware that apps are collecting data, but very few people know how detailed this data can be. Location-based services track where we go, search engines track what we search for, and streaming services track what we watch and skip. Over time, this data is analyzed through Artificial Intelligence and Machine Learning algorithms.

These algorithms analyze patterns in user behavior and make predictions.

For instance, an online shopping website may suggest products to us even before we know we need them. Similarly, social networking sites are designed in such a way that our feeds are tailored according to our past behavior, ensuring that we remain engaged for a longer period of time. This predictive technology is not all negative.

Advantages of Low-Code/No-Code Development

1. Speed and Efficiency

One of the biggest advantages of LCNC platforms is the ability to rapidly develop applications. Traditional software development involves complex coding, testing, and debugging, which can take weeks or months. With LCNC tools, businesses can deploy applications within hours or days, significantly accelerating digital transformation.

2. Accessibility for Non-Developers

LCNC platforms empower business analysts, marketers, and entrepreneurs to create custom applications without relying on IT departments. This democratization of development fosters innovation and allows companies to quickly adapt to changing business needs.

3. Cost Savings

Hiring and retaining skilled software developers is expensive. LCNC platforms reduce development costs by enabling organizations to build applications without requiring a large team of specialized programmers.

4. Seamless Integration

Many LCNC platforms support API integration and third-party service connections, allowing users to link their applications with existing enterprise systems like CRMs, ERPs, and cloud storage solutions.

The Limitations of Low-Code/No-Code

1. Limited Customization and Scalability

While LCNC platforms simplify development, they often lack the flexibility and scalability required for large-scale applications. Traditional programming allows developers to build highly customized, performance-optimized software that LCNC tools struggle to replicate.

2. Security and Compliance Concerns

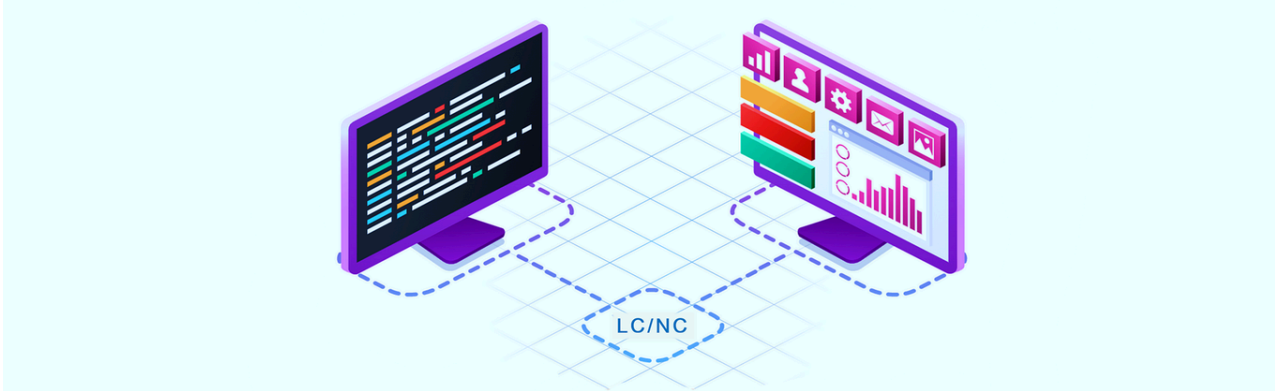
Many businesses handle sensitive data that must comply with regulations such as GDPR, HIPAA, and ISO 27001. LCNC platforms may have limited security controls, raising concerns about data privacy, access management, and compliance.

3. Dependence on Platform Providers

Applications built on LCNC platforms are often locked into specific vendors, making it difficult to migrate to other technologies. This vendor dependency can lead to increased costs and reduced flexibility over time.

4. Lack of Deep Technical Control

For applications that require complex algorithms, real-time processing, or highly customized workflows, LCNC platforms fall short. Traditional coding remains essential for developing AI-powered applications, high-frequency trading systems, and large-scale enterprise software.



Will Low-Code/No-Code Replace Traditional Programming?

While LCNC development is transforming the industry, it is unlikely to replace traditional programming entirely. Instead, LCNC and traditional coding will coexist, each serving different needs:

- LCNC for Rapid Prototyping and Business Applications: Ideal for internal tools, workflow automation, and non-complex applications.
- Traditional Coding for Advanced Software Development: Essential for building scalable, secure, and high-performance applications with deep customization.

The Future of Software Development: A Hybrid Approach

The future of software development lies in a hybrid approach where LCNC and traditional programming complement each other. Many enterprises are adopting citizen development models, where business users build basic applications using LCNC tools while professional developers focus on enhancing them with advanced features.

With AI-powered development tools emerging, LCNC platforms will continue to evolve, integrating machine learning, automation, and natural language processing to further simplify software creation. However, as technology advances, traditional programming skills will remain invaluable for pushing the boundaries of what's possible in software engineering.

Conclusion

Low-code and no-code development platforms are revolutionizing the way software is built, making application development more accessible and efficient. While these tools offer incredible speed and convenience, they cannot fully replace traditional programming, especially for complex, high-performance applications. Instead, the future of software development lies in the collaboration between LCNC and traditional coding, leveraging the strengths of both approaches to drive innovation and efficiency.

As technology continues to evolve, businesses and developers must adapt, learning when to use LCNC for speed and efficiency and when to rely on traditional coding for flexibility and power.The software development landscape is shifting, but coding remains an essential skill in the digital era.

Alwin Liju
S2 CSE A

Artificial Intelligence in Automotive Systems

Ann Mary George
S2 CSE A

Artificial Intelligence is a part of modern car systems. It helps cars drive themselves and make decisions on the road. Artificial Intelligence utilises data and specialised algorithms to achieve this. It is different from programming because it can learn and improve over time.

Artificial Intelligence in systems is used in many things, including Advanced Driver Assistance Systems and fully autonomous vehicles. Artificial Intelligence enables machines to understand their surroundings, make decisions, and take actions while driving.

Autonomous Cars

These are self-driving cars. Drivers don't need to worry about handling the steering wheel. These vehicles operate just like traditional vehicles without the need for human passenger control.

There are six levels of automation:

- LEVEL 0: No Assistance
  Here, automation is manually controlled, just like our traditional cars
- LEVEL 1: Assisted
  Here, there is only a single feature that is being automated, for example, monitoring speed using cruise control.
- LEVEL 2: Partially Automated
  Partially automated, i.e., can perform steering and acceleration tasks
- LEVEL 3: Highly Automated
  Has environment detection capabilities. The vehicle can take on most of the driving tasks, but human override is required.
- LEVEL 4: Fully Automated
  The vehicle performs all driving tasks under specific circumstances. Geofencing is required. Human override is still an option.

- LEVEL 5: Autonomous
  Full automation means the vehicle performs all driving tasks under all conditions. Zero human interaction required.

AI Algorithms in Autonomous Vehicles

Autonomous vehicles rely on three types of algorithms:

- **Regression Algorithm**
  It is used to predict a numerical value based on previous data collected.
  For example:
  Predicting the distance to an object, the speed of another car or the probability that a pedestrian will cross. The system collects historical data while driving and is input by the sensors and estimates how fast a nearby car is moving, or how long before a traffic light changes, or estimates the trajectory of a pedestrian.
- **Clustering Algorithms**
  It is mainly used to group similar data points together, like one cluster could be the data about pedestrians, while another cluster could be about vehicles or the road surface. So basically, it is organizing raw sensor data into meaningful groups
- **Decision Network Algorithms**
  They are basically rule-based systems using probabilistic decision models. The combined sensor input, predicted outcomes and predefined safety rules.
  For example,
  If:
  1) Object detected ahead
  2) Distance < safe threshold
  3) Speed > braking limit
  Then:
  Apply brakes

Application of AI in Autonomous Vehicles

1)Data Collection (Perception)

Autonomous vehicles collect real-time data using sensors such as cameras, radar, LiDAR, ultrasonic sensors, and GPS. These sensors detect objects, road conditions, traffic, and vehicle position. All collected data is sent to the central onboard computer for processing.

2) Path Planning (Decision Making)

After processing sensor data, the AI system predicts object movements and calculates the safest and most efficient path from point A to point B. It evaluates multiple possible actions and selects the one with the highest safety and efficiency.

3) Action (Control Execution)

Once a decision is made, the vehicle executes commands such as braking, steering, accelerating, or lane changing. This control process is continuously repeated to ensure safe and smooth driving.

Benefits of AI in Automotive Manufacturing

AI is making car manufacturing smarter and more efficient. One major benefit is predictive maintenance. Instead of waiting for machines to break down, AI analyses sensor data and detects problems early. This helps companies avoid unexpected downtime and saves money. AI also improves quality control by automatically spotting defects during production. This ensures better vehicle quality and higher customer satisfaction. In addition, AI helps with testing and demand forecasting, making production planning more accurate and reducing unnecessary inventory. Overall, AI helps manufacturers save time, reduce costs, and build better cars.

Challenges of AI Integration in the Automotive Industry

Bringing AI into the automotive industry isn't easy. There are a few major challenges companies face:

Data Collection Issues

Car manufacturers generate huge amounts of data from sensors, machines, and customer feedback. But this data is often:

- Scattered across different departments
- In different formats
- Not always accurate or clean
- Stored in isolated systems

Combining all this data properly is complicated but necessary for AI to work effectively.

Data Privacy and Security

The industry handles sensitive information like customer data and trade secrets. Companies must protect this data and follow strict regulations like the GDPR.

Without strong data security and privacy policies, AI implementation can become risky.

Infrastructure Requirements

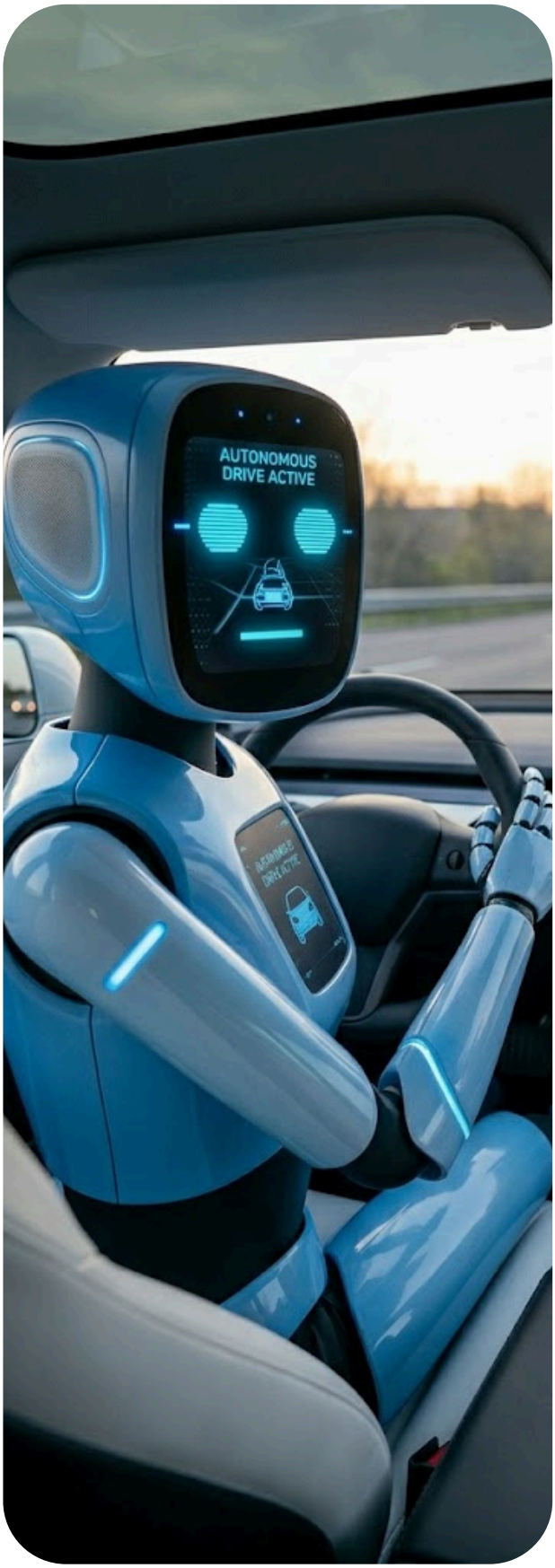
AI needs powerful systems to process large amounts of data. This means companies must invest in:

- High-performance computing
- Large data storage (cloud or on-site)
- Strong networking systems

This can be expensive and technically demanding.

Skilled Workforce

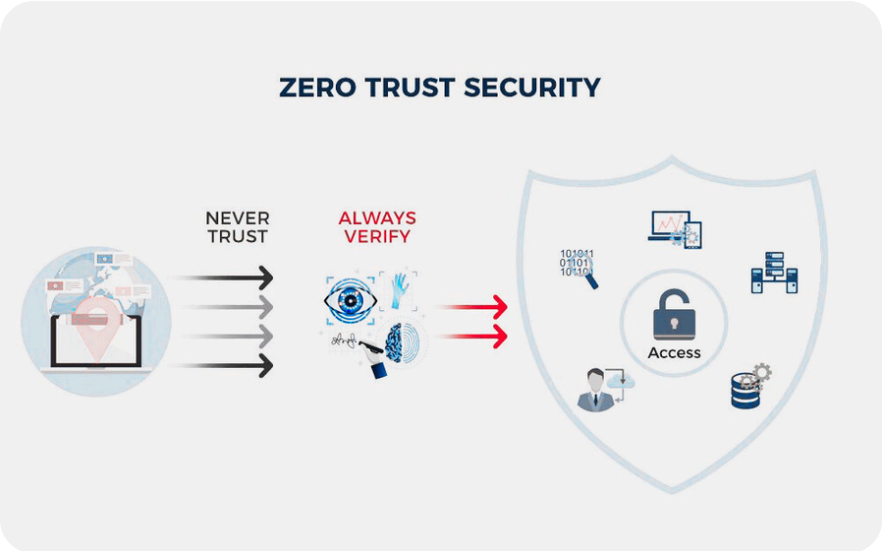
AI requires trained professionals like data scientists and engineers. Many companies face a skills gap, so they must train employees and encourage collaboration between technical and manufacturing teams.



Zero Trust Architecture: Rethinking Cybersecurity in the Digital Age

Jane Joe
S2 CSE B

In today's digital world, where cloud computing, remote work, and mobile devices dominate, cybersecurity has become more critical than ever. Traditional security models, which trust users and devices once they enter a network, are no longer effective against modern cyber threats. This has led to the rise of a new and powerful security approach known as Zero Trust Architecture (ZTA).



What is Zero Trust Architecture?

Zero Trust Architecture is a cybersecurity framework based on the principle "Never trust, always verify." Unlike traditional models that assume internal network users are safe, Zero Trust treats every user, device, and application as untrusted by default. Every access request is carefully verified, regardless of whether it originates from inside or outside the organization.

The core idea behind Zero Trust is to assume that threats can exist anywhere in the network. Therefore, continuous authentication, authorization, and monitoring are essential. This approach significantly reduces the chances of unauthorized access and data breaches.

What is Zero Trust Architecture?

The rapid growth of cloud services, IoT devices, and remote working environments has expanded the digital boundaries of organizations. Employees now access sensitive data from multiple locations and devices, increasing exposure to cyberattacks. Traditional perimeter-based security models struggle to handle these challenges effectively.

Once attackers break through the network perimeter, they can move freely inside the system. Zero Trust prevents this by implementing strict access control and continuous verification. This makes it harder for attackers to exploit vulnerabilities and ensures better protection of sensitive data.

What is Zero Trust Architecture?

Zero Trust operates by continuously verifying users and devices before granting access. When a request is made, the system evaluates multiple factors such as user identity, device health, location, and behaviour patterns. Access is granted only if all security requirements are met.

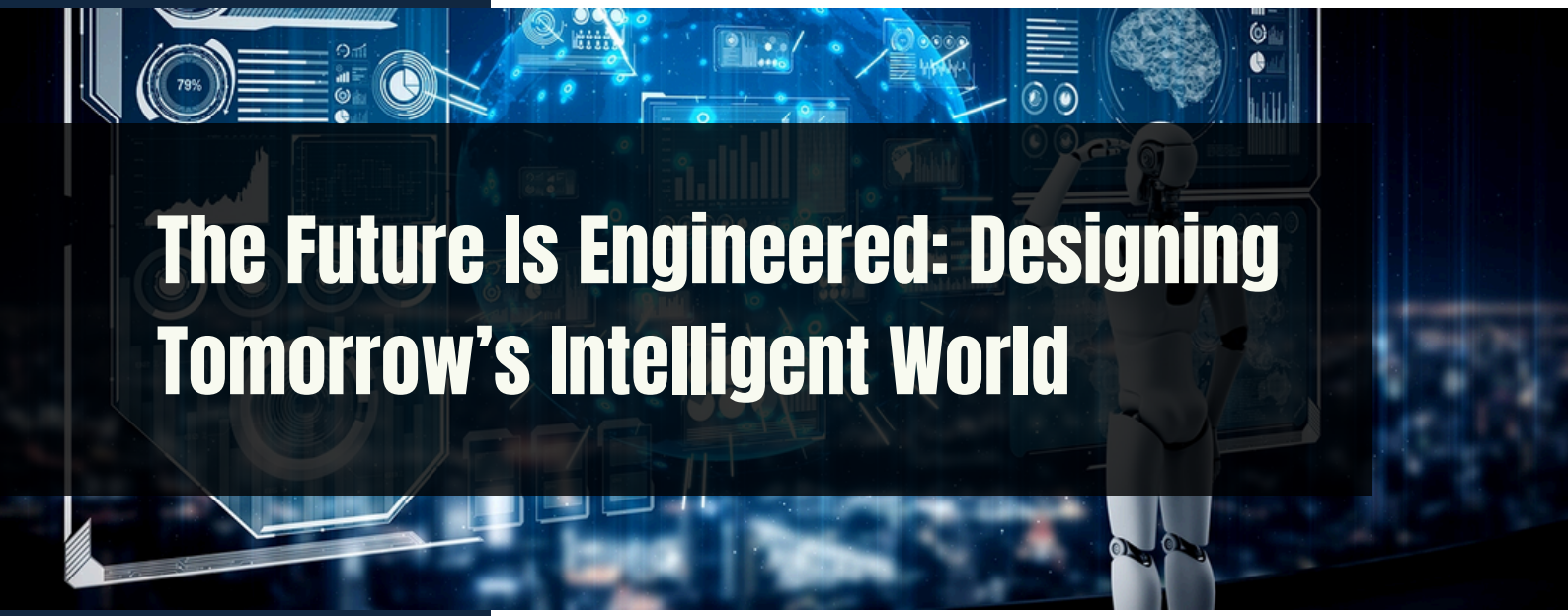
Another key concept is least privilege access, which means users receive only the permissions necessary to perform their tasks. This minimizes potential damage if an account is compromised and limits attackers from accessing critical systems.

Key Components of Zero Trust

Zero Trust Architecture consists of several integrated security components:

- Identity and Access Management (IAM): Controls user authentication and authorization.
- Multi-Factor Authentication (MFA): Adds an extra verification layer beyond passwords.
- Endpoint Detection and Response (EDR): Ensures device security compliance.
- Micro-segmentation: Divides networks into smaller isolated zones to prevent lateral movement.
- Continuous Monitoring and Analytics: Tracks real-time activity to detect anomalies and threats.
- These components collectively create a highly secure and resilient architecture.

In conclusion, Zero Trust Architecture represents a major shift in cybersecurity strategy. By replacing implicit trust with continuous verification, it provides stronger protection against modern cyber threats. As digital systems continue to expand and evolve, Zero Trust will play a crucial role in safeguarding data and infrastructure. For aspiring computer engineers, gaining knowledge about Zero Trust is not just an advantage—it is a necessity in the modern tech landscape.



The Future Is Engineered: Designing Tomorrow's Intelligent World

Rohan Rajesh
S2 CSE C

The future is not something we wait for. It is something we design.

Across the globe, technology is advancing at a pace faster than any other period in human history. Artificial Intelligence is learning patterns beyond human perception. Quantum computing is redefining computational limits. Autonomous systems are beginning to think, decide, and adapt. What once belonged to science fiction is rapidly becoming scientific reality.

We are not merely living in the Digital Age — we are constructing the Intelligent Age.

Intelligence Beyond Humans

Artificial Intelligence is evolving from simple automation to systems capable of reasoning, predicting, and self-improving. In healthcare, intelligent systems can detect diseases earlier than traditional diagnostics. In finance, algorithms predict risks in milliseconds. In education, adaptive platforms personalize learning for every individual.

The future belongs not to machines alone, but to collaboration between human creativity and machine precision.

Intelligence Beyond Humans

Traditional computers process information in bits — zeros and ones. Quantum computers use qubits, allowing them to perform multiple calculations simultaneously. This breakthrough has the potential to revolutionize climate modeling, drug discovery, cybersecurity, and space exploration.

When computational limits disappear, innovation becomes limitless.

A Hyper-Connected World

The Internet of Things (IoT), 5G networks, robotics, and cloud computing are merging into a unified ecosystem. Smart cities will regulate traffic automatically, optimize energy consumption, and respond to emergencies in real time. Wearable technologies will continuously monitor health. Autonomous vehicles will transform transportation.

Technology will no longer be just a tool we use. It will become an invisible layer embedded into everyday life.

A Hyper-Connected World

With advanced innovation comes ethical responsibility. Data privacy, cybersecurity threats, AI bias, and digital inequality are challenges that demand thoughtful solutions.

The engineer of the future must not only be technically skilled but ethically aware.

Progress without responsibility creates risk. Innovation with integrity creates impact.

The Role of Students: Architects of 2040

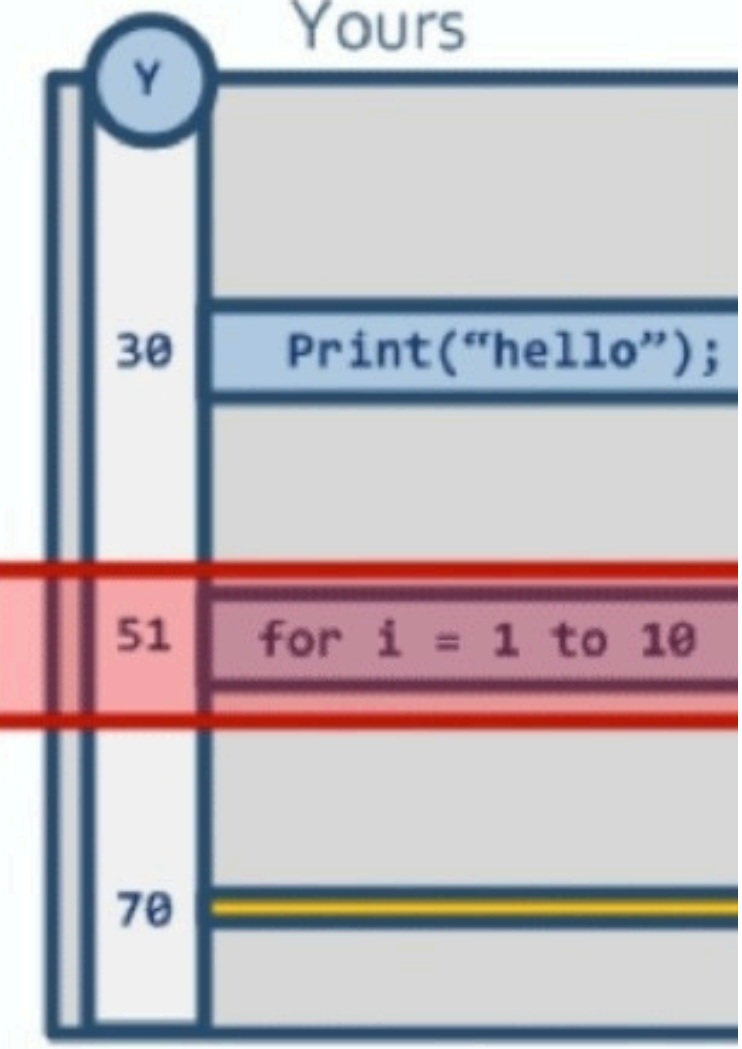
Universities today are incubators of transformation. Every project, research paper, startup idea, or hackathon solution holds the potential to shape industries. Students are not preparing for the future — they are actively building it. The technologies of 2040 are being coded, tested, and imagined in classrooms today.

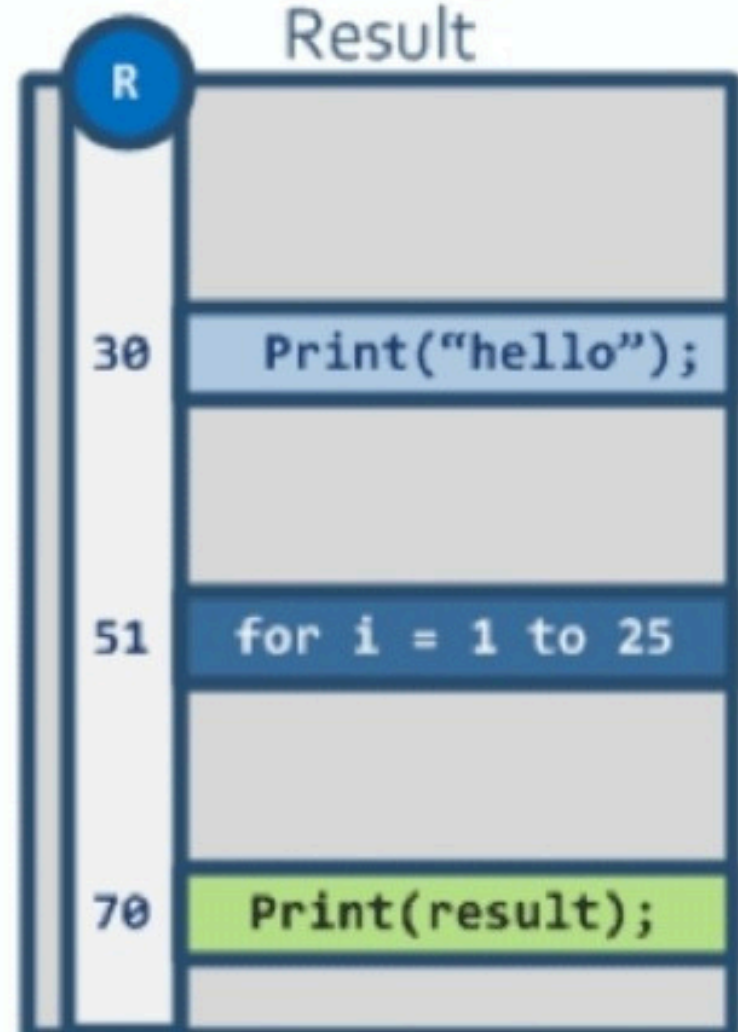
Conclusion: Build Beyond Limits

The coming decade will redefine humanity's relationship with technology. Intelligent systems will assist us. Quantum breakthroughs will accelerate discovery. Connected ecosystems will transform societies. But above all, the most powerful innovation will remain human imagination.

The future is not arriving on its own. It is being engineered — by thinkers, creators, and bold innovators willing to challenge limits.

And that journey begins now.





THE NEURAL PROGRAM SYNTHESIS AND THE EVOLUTION OF GIT

Adithi Harish
S2 CSE A

1. Introduction: The Persistence of the Merge Conflict

In the discipline of software engineering, the "Merge Conflict" represents the primary point of friction in collaborative development. Every developer has experienced the frustration of Git halting a deployment because it cannot reconcile two versions of the same file. While version control systems have evolved significantly in terms of hosting and UI, the core logic behind merging remained largely stagnant for decades.

A landmark project from Microsoft Research, titled "Program Merge: What's Deep Learning Got to Do with It?", signals a fundamental shift in this field. We are currently moving away from traditional rule-based merging toward a more sophisticated approach: **Neural Program Synthesis.**

2. The Technical Bottleneck: Syntax Blindness

Traditional tools like Git utilize a "three-way merge" algorithm. This process compares a "Base" version (the common ancestor) with "Branch A" and "Branch B." However, this logic is strictly textual. If two developers modify the same line of code, the system throws a conflict error, even if their changes are logically compatible.

Current tools are essentially "syntax-blind." They process text strings but do not comprehend the underlying logic. They cannot distinguish between a vital security patch and a minor style adjustment. This creates a bottleneck in large-scale projects, requiring manual, often error-prone intervention from engineers to "stitch" the logic back together.

3. The DeepMerge Framework: From Text to Tokens

Researchers at Microsoft developed **DeepMerge** to transition from viewing code as text to treating it as a **Sequence Prediction Problem**. Instead of relying solely on rigid mathematical rules (known as Symbolic Methods), they applied Deep Learning to the problem.

How the System Functions:

- **Token-Level Surgery:** Instead of evaluating entire lines, the AI analyzes "tokens" (the smallest units of code, such as variable names, operators, or semicolons). This allows the model to "interleave" changes, mixing fragments from two different branches into a single, functional line of code.

Empirical Learning: The model was trained on millions of real-world merges from GitHub. The AI essentially observed how professional human developers resolved conflicts over the last decade and learned to mimic their decision-making processes.

4. The 70/30 Rule: Semantic vs. Social Conflicts

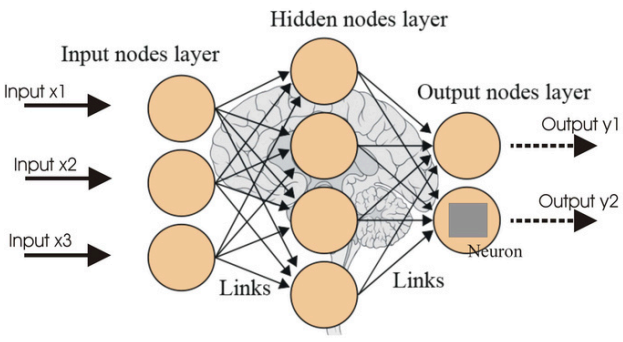
Research revealed a significant statistic: 70% of the time, a merge conflict is resolved by simply selecting one developer's version and discarding the other. This usually occurs for social reasons or because one update makes the other obsolete.

The true engineering challenge lies in the remaining 30%. These are Semantic Conflicts, where both pieces of code are correct individually but must be woven together to maintain program integrity. DeepMerge uses neural training to predict the most likely "correct" way to integrate these two logic paths without breaking the build.

6. Conclusion

The transition from "Classic Software Engineering" to "AI-Augmented Engineering" is an ongoing evolution. Projects like DeepMerge demonstrate that the future of Computer Science involves building systems that can understand and repair code alongside human developers.

The merge conflict is finally being addressed not through more complex rules, but through better learning. For students and future engineers, mastering these AI-driven tools will be essential for managing the complex, collaborative codebases of the future.



ARTIFICIAL INTELLIGENCE IN AUTOMOTIVE SYSTEMS

Spend a little time in any college library or classroom and you'll see it. Laptops open. Tabs switching. Someone typing, pausing, then typing again. And somewhere in that routine, an AI tool quietly doing its part..

It has slipped into our academic lives so naturally that we hardly question it anymore.

Don't understand a concept from today's lecture? Ask AI. Not sure how to begin an assignment? Ask AI. Feel like your paragraph sounds awkward? Ask AI to improve it.

It saves time. And in college, time feels like the one thing we never have enough of between internal exams, projects, presentations, internships, and personal commitments, the pressure to keep up is constant. When something can make work easier and faster, it feels practical to use it. In many ways, it is practical.

But learning has never been only about finishing quickly. Think back to a topic you once struggled with but eventually understood.Chance are, the understanding didn't come instantly. You probably reread the material. You may have made

You might have discussed it with friends or stayed up a little longer trying to make sense of it . That uncomfortable phase confusion the trial and error is not wasted time. It is the point where brain is actually working.

When we turn to AI at the first sign of difficulty, we sometimes remove that stage completely. The answer appears in seconds organized, confident, polished. The assignment moves forward. But the deeper question remains: did we engage with the idea, or did we simply move past it?

This is not an argument against AI. It is an observation about how easily convenience can change our habits.

AI is undoubtedly useful. It can break down complex topics into simpler explanations. It can offer examples when textbooks feel too dense. It can provide guidance when a student feels unsure about asking questions in class. In that sense, it can be supportive and even empowering.

The concern begins when support turns into dependence. Critical thinking does not develop automatically. It grows when we analyze, question, compare, and sometimes disagree. If answers are always provided before we attempt to think through a problem ourselves, we may slowly lose the confidence to form our own conclusions. It becomes easier to accept information than to examine it.

Memory is affected as well . We rely on reminders for important dates. We search for formulas instead of recalling them. We save information rather than store it in our minds.Access to information is undoubtedly valuable, but the habit of recalling and connecting ideas strengthens understanding in ways that simple retrieval cannot.

Creativity also requires space. Many meaningful ideas come during quiet moments—while walking back to the hostel, sitting alone after class, or reflecting before sleep. When every pause is filled with instant answers and generated suggestions, those reflective moments become rare.

Still, it would be unrealistic to suggest that students avoid AI altogether. Technology has always influenced education. Calculators changed how mathematics was practiced. The internet transformed research. In the same way, AI is reshaping how we approach learning.

The difference lies in how we choose to use it.

If we attempt first and consult later, AI becomes a guide. If we allow it to replace our effort entirely, it becomes a shortcut that may limit growth. The distinction is subtle, but important.

AI will continue to evolve. It will become more efficient and more integrated into everyday academic life. That progress is inevitable.

What remains within our control is the choice to continue exercising our own minds.

AI does not automatically weaken us. But if we stop challenging ourselves—if we stop reflecting, analyzing, and thinking deeply—we risk losing the very skills that education is meant to strengthen.

In the end, the responsibility is not with the technology, but with us.

Anshal Shaju
S2 CSE A

INSIDE A RANSOMWARE ATTACK: HOW HACKERS BREACH, MOVE, AND MONETIZE

Mohammed Faraz KS
S2 CSE C

Imagine waking up to find your company's computers locked, critical files encrypted, and a message flashing on every screen demanding millions in cryptocurrency. Operations stop. Customers panic. News spreads. This is not a movie scene — this is ransomware.

Ransomware has become one of the most dangerous and profitable forms of cybercrime in the modern world. From hospitals to fuel pipelines, no organization is immune. One of the most famous cases was the Colonial Pipeline attack, which disrupted fuel supply across parts of the United States. But how exactly does a ransomware attack happen? Let's take a step-by-step journey inside a cyber breach.

Step 1: Initial Access – The Entry Point

Every ransomware attack begins with entry. Attackers do not magically appear inside a system they find a weakness. The most common methods include:

- Phishing emails with malicious attachments or fake login pages
- Weak or reused passwords
- Exploiting outdated software vulnerabilities
- Remote Desktop Protocol (RDP) exposed to the internet

A single employee clicking a malicious link can give attackers the foothold they need. This stage often goes unnoticed because the attacker tries to remain silent and avoid detection.

Step 2: Establishing Persistence

Once inside, attackers ensure they can return even if the system restarts. They may create hidden administrator accounts, install backdoors, or modify system settings. This is called persistence.

At this stage, they are not yet encrypting files. Instead, they are quietly preparing the environment for a larger attack.

Step 3: Privilege Escalation

Most initial access points do not give full control of the system. Attackers need higher privileges to access sensitive data. Through techniques like password dumping, exploiting misconfigurations, or abusing system tools, they gain administrator-level access.

With elevated privileges, they can now control critical systems.

Step 4: Lateral Movement

After gaining control of one machine, attackers spread across the network. This is known as lateral movement.

They scan the network to identify servers, databases, backup systems, and domain

controllers. Using stolen credentials, they move from one device to another. If network segmentation is weak, the attacker can compromise the entire infrastructure.

Step 5: Data Exfiltration
Modern ransomware attacks are no longer just about encryption. Attackers first steal sensitive data such as customer records, financial information, or intellectual property.

This strategy is called double extortion. Even if a company restores its data from backups, attackers threaten to leak stolen data publicly unless the ransom is paid.

Step 6: Encryption and Ransom Demand
Only after fully understanding the system do attackers launch the final stage. They deploy the ransomware payload, which encrypts files across the network.

Users suddenly see a ransom note demanding payment usually in cryptocurrency like Bitcoin within a specific deadline. If payment is not made, attackers threaten to permanently delete or leak the stolen data.

At this point, the organization faces a difficult decision:
• Pay the ransom and hope for decryption
• Refuse and risk data loss and public exposure

Many cybersecurity experts advise against paying, as it encourages more attacks and does not guarantee full recovery.

Why Ransomware Is So Effective
Ransomware works because it targets what organizations value most — their data and operations. Businesses depend on digital systems. When systems stop, revenue stops.
Attackers also exploit human psychology:
• Urgency (“Pay within 48 hours!”)
• Fear (“Your data will be leaked!”)
• Pressure on executives and decisionmakers

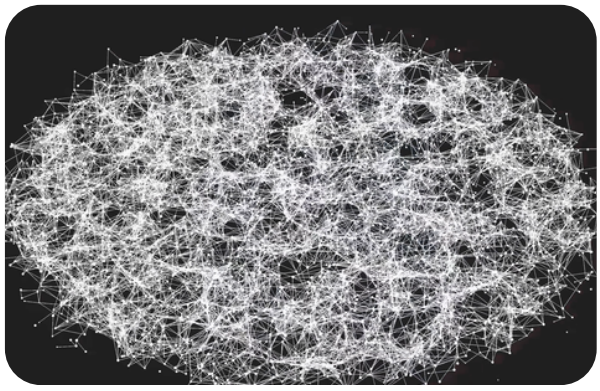
Additionally,ransomware-as-a-service (RaaS) platforms allow even less-skilled criminals to launch sophisticated attacks by purchasing ready-made tools from dark web marketplaces.

How Organizations Can Defend Themselves
While ransomware is powerful, it is not unstoppable. Strong cybersecurity practices significantly reduce risk:

1. Regular software updates and patch management
2. Strong password policies and Multi-Factor Authentication (MFA)
3. Network segmentation to limit lateral movement
4. Regular offline backups
5. Employee awareness training to prevent phishing
6. Continuous monitoring through Security Operations Centers (SOC)

Zero Trust security models are also becoming popular, where no user or device is automatically trusted.

The Bigger Picture
Ransomware is not just a technical issue — it is a business and national security issue. When critical infrastructure is attacked, the impact spreads beyond companies to entire communities.
The Colonial Pipeline attack demonstrated how cyber incidents can affect fuel supply and economic stability. Similar attacks on hospitals have delayed surgeries and endangered lives.



The Colonial Pipeline attack demonstrated how cyber incidents can affect fuel supply and economic stability. Similar attacks on hospitals have delayed surgeries and endangered lives.

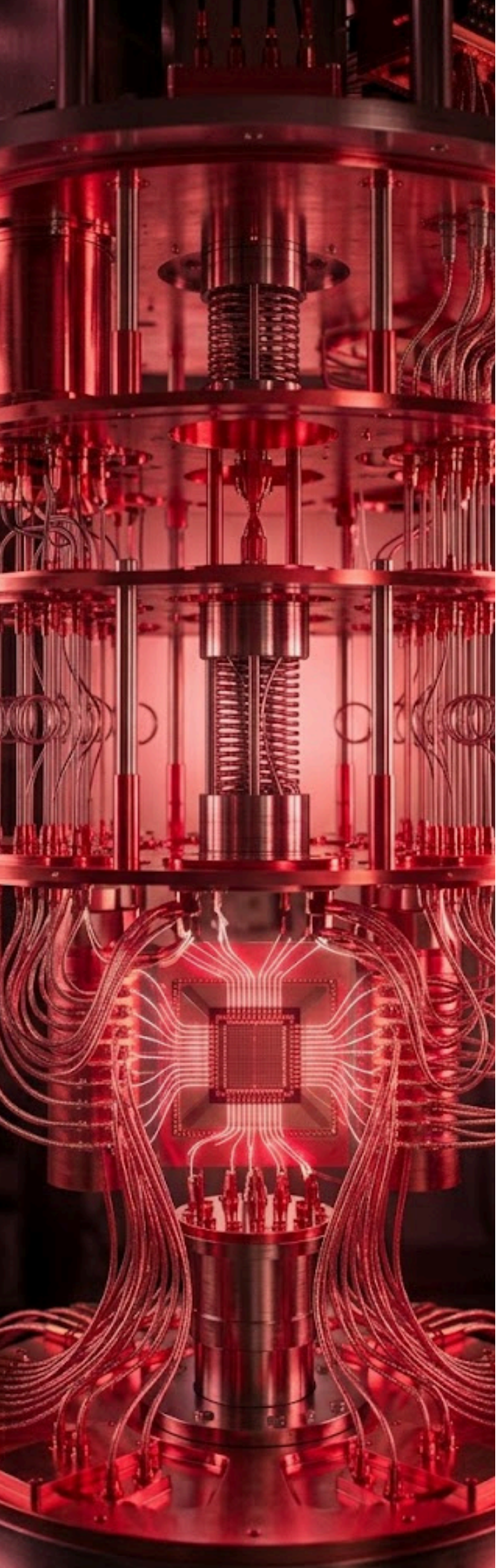
Cybersecurity is no longer optional. It is a necessity.

Conclusion

Understanding how a ransomware attack unfolds helps us see that cybersecurity is not just about installing antivirus software. It is about strategy, awareness, and continuous defense.

From initial access to data encryption, ransomware is a carefully planned operation. But with strong security practices, informed employees, and proactive monitoring, organizations can reduce the risk dramatically.

From initial access to data encryption, ransomware is a carefully planned operation. But with strong security practices, informed employees, and proactive monitoring, organizations can reduce the risk dramatically.



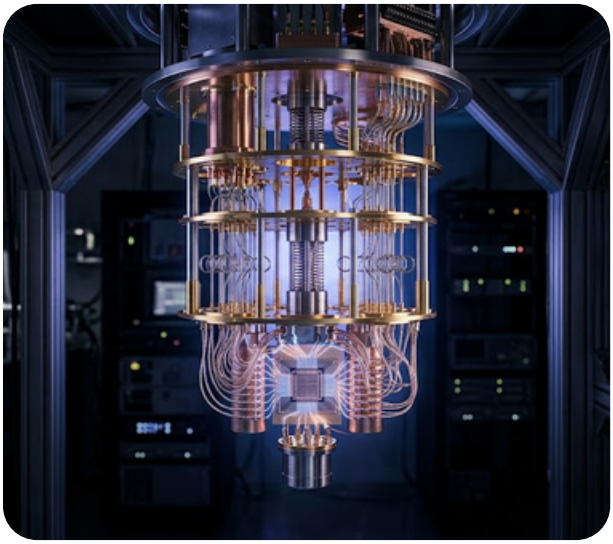
QUANTUM COMPUTING: THE NEXT DIGITAL REVOLUTION

Muhammed Aadil C S
S2 CSE C

In the world of modern technology, computing power has always been the driving force behind innovation. From early mechanical calculators to today's powerful supercomputers, each advancement has transformed how humans solve problems. Now, scientists and engineers are exploring a groundbreaking frontier known as quantum computing a technology widely considered the next digital revolution. Traditional computers use bits as the smallest unit of data, which can exist in one of two states: 0 or 1. Quantum computers, however, use quantum bits or qubits. Unlike classical bits, qubits can exist in multiple states simultaneously due to a phenomenon called superposition.

This allows quantum computers to process vast amounts of information at once, making them exponentially more powerful for certain tasks. Another important principle behind quantum computing is entanglement. When qubits become entangled, the state of one qubit instantly influences another, even if they are far apart. This property enables incredibly fast and complex calculations that would take classical computers thousands of years to solve. As a result, quantum computing has the potential to revolutionize fields such as cryptography, medicine, artificial intelligence, climate modeling, and financial analysis. One of the most exciting applications of quantum computing lies in cryptography. Current encryption systems rely on mathematical problems that are difficult for classical computers to solve. Quantum computers could potentially break these systems quickly, which is why researchers are also developing quantum-resistant encryption methods. This race between computing power and security is shaping the future of digital communication. In healthcare and drug discovery, quantum computing could dramatically accelerate research. Scientists could simulate molecular interactions at an atomic level, leading to faster discovery of new medicines and materials. Similarly, in environmental science, quantum simulations may help predict climate patterns more accurately and design sustainable solutions for global challenges. Despite its enormous promise, quantum computing is still in its early stages. Building stable quantum systems is extremely difficult because qubits are highly sensitive to environmental disturbances such as temperature and electromagnetic radiation. Researchers worldwide are working to overcome these challenges and create scalable, reliable quantum machines.

Technology giants, research institutions, and governments are investing billions of dollars into quantum research. Their goal is not only to achieve quantum supremacy the point where a quantum computer outperforms the best classical computer but also to make quantum technology practical for everyday use. While fully functional quantum computers may still take years to become mainstream, progress is happening faster than ever before. The impact of quantum computing on society could be as transformative as the invention of the internet or the smartphone. It promises to solve problems that are currently impossible, optimize complex systems, and unlock new scientific discoveries. For students and future engineers, understanding quantum computing today means preparing for the technological world of tomorrow. In conclusion, quantum computing represents a revolutionary leap in computational science. Though still developing, its potential applications span countless industries and could reshape the digital landscape. As research advances and technology matures, quantum computing is poised to become one of the most powerful tools humanity has ever created truly marking the beginning of the next digital revolution.



Revolutionizing the Future of Medicine

Anjana Roy
S2 CSE A

Artificial Intelligence is transforming nearly every industry, but its impact on healthcare is particularly profound. By combining computer science with medicine, AI is helping doctors diagnose diseases earlier, personalize treatments, reduce medical errors, and improve patient outcomes. What once seemed like science fiction—machines assisting in surgeries or predicting diseases—is now becoming everyday reality.

AI in Medical Imaging and Diagnosis

One of the most successful applications of AI in healthcare is medical imaging. Machine learning and deep learning models analyse X-rays, MRIs, CT scans, and ultrasounds with remarkable accuracy.

AI systems can:

- Detect tumours in early stages
- Identify fractures in X-rays
- Recognize signs of stroke or heart disease
- Assist radiologists in faster diagnosis

For example, researchers at Stanford University have developed deep learning models that can detect skin cancer with accuracy comparable to dermatologists. These systems reduce diagnostic time and help in areas where specialists are limited

Predictive Analytics and Early Disease Detection

AI models trained on large healthcare datasets can predict potential health risks before symptoms appear. By analysing patient history, lifestyle data, and genetic information, AI can:

- Predict diabetes risk
- Detect heart disease patterns
- Identify patients likely to develop complications
- Forecast disease outbreaks

Organizations like Mayo Clinic use AI-based predictive tools to enhance clinical decision-making. Early detection not only saves lives but also reduces healthcare costs.

Personalized Medicine

Traditional medicine often follows a "one-size-fits-all" approach. AI is changing that by enabling personalized treatment plans tailored to individual patients.

Through data analysis, AI can:

- Recommend specific drug combinations
- Adjust treatment plans based on genetic profiles
- Predict how patients will respond to certain medications

This approach increases treatment effectiveness and minimizes side effects.

Virtual Health Assistants and Telemedicine

AI-powered chatbots and virtual assistants help patients schedule appointments, monitor symptoms, and receive medical advice remotely. Telemedicine platforms integrate AI to:

- Analyse patient-reported symptoms
- Provide preliminary health assessments
- Monitor chronic conditions in real time

During global health crises such as the COVID-19 pandemic, AI played a vital role in tracking infection rates and accelerating vaccine research.

Ethical Challenges and Data Privacy

Despite its advantages, AI in healthcare raises critical concerns:

- Data Privacy: Medical records are highly sensitive.
- Algorithmic Bias: Biased training data can lead to unequal treatment.
- Accountability: Who is responsible if an AI system makes an error?
- Security Risks: Healthcare systems are targets for cyberattacks.

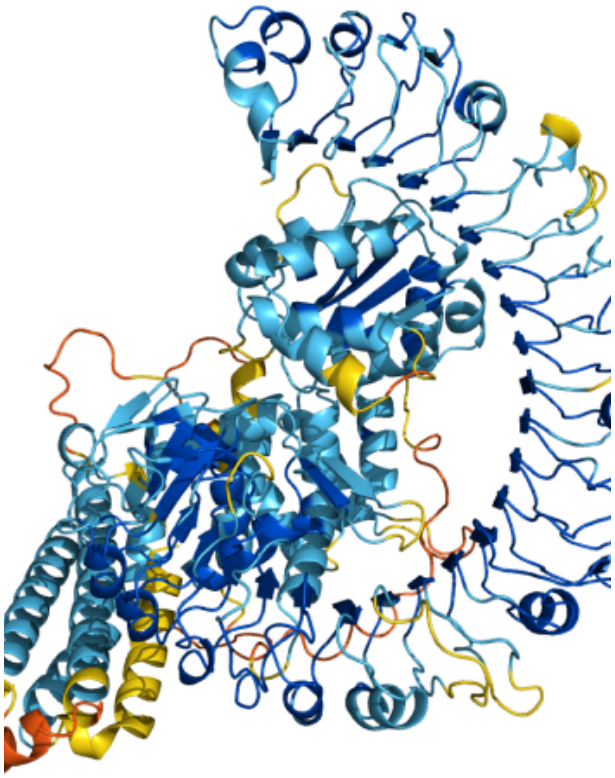
Computer scientists must design systems that are secure, transparent, and ethically responsible.

The Future of AI in Healthcare

The future holds exciting possibilities:

- AI-powered wearable devices for continuous monitoring
- Integration of AI with genomics
- Smart hospitals with automated systems
- Advanced brain-computer interfaces

As computing power grows and healthcare datasets expand, AI will become even more integrated into everyday medical practice.



Conclusion

Artificial Intelligence is not replacing doctors—it is empowering them. From early diagnosis and robotic surgery to personalized medicine and drug discovery, AI is revolutionizing healthcare. For computer science students, this field offers opportunities in machine learning, data science, cybersecurity, biomedical engineering, and software development. More importantly, it offers a chance to contribute to saving lives and improving global health. The future of medicine is intelligent, data-driven, and deeply connected to computer science.

THE AI CHIP WARS:

INSIDE THE BATTLE POWERING THE AGE OF ARTIFICIAL INTELLIGENCE

Ibadh Rahman K P
S2 CSE B

Artificial Intelligence may appear as software — chatbots answering questions, image generators creating art, or recommendation systems predicting what we watch next. But behind every intelligent response lies an enormous physical infrastructure. At the heart of this revolution are specialized semiconductor chips designed to process massive amounts of data simultaneously. Today, the global technology industry is locked in an intense competition often described as the AI Chip Wars. Companies such as NVIDIA, AMD, Intel, Apple, and emerging startups are racing to build faster, more efficient processors capable of powering the next generation of artificial intelligence. The outcome of this battle may determine who controls the future of computing itself.

From CPUs to GPUs: Why AI Needed New Hardware

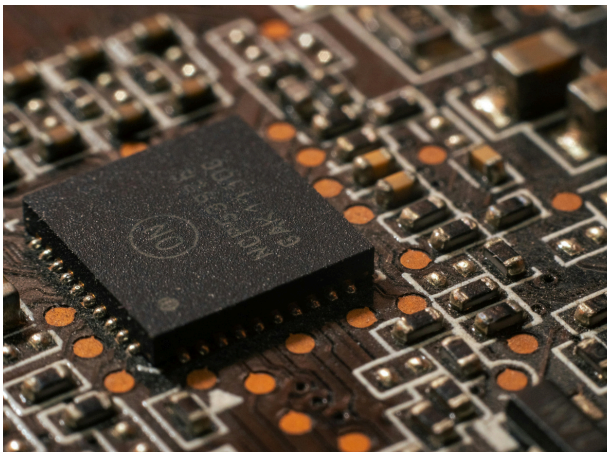
For decades, central processing units (CPUs) powered computers through sequential execution performing one operation after another at extremely high speed. This model worked well for traditional software tasks such as spreadsheets or web browsing.

Artificial intelligence changed everything.

Modern AI models rely on neural networks containing billions or even trillions of parameters. Training these systems requires performing millions of mathematical operations simultaneously, particularly matrix multiplications. Graphics Processing Units (GPUs), originally designed to render video game graphics, turned out to be perfect for this work. Unlike CPUs, GPUs contain thousands of smaller cores capable of parallel computation.

NVIDIA: The Unexpected King of AI

Few companies benefited from the AI boom as dramatically as NVIDIA. Long before artificial intelligence became mainstream, NVIDIA invested heavily in parallel computing software through its CUDA platform, allowing researchers to program GPUs easily for scientific workloads.



Today, NVIDIA's data-center accelerators dominate AI training workloads across major cloud providers.

AMD and Intel Strike Back

AMD has aggressively entered the AI accelerator market through competitive hardware and open software ecosystems.

Intel is attempting a comeback through specialized AI processors and manufacturing investments aimed at large-scale AI training efficiency.

Apple Silicon

While cloud data centers dominate AI headlines, another revolution is happening quietly inside personal devices. Apple's custom silicon integrates neural engines designed specifically for machine learning tasks, enabling on-device AI that improves privacy and reduces latency.

The Hidden Battlefield: Manufacturing and Geopolitics

The AI chip war is not only technological but geopolitical. Advanced semiconductor manufacturing requires extreme precision and massive investments. Governments increasingly view access to advanced chips as essential for economic and national security competitiveness. Energy, Heat, and the Cost of Intelligence Training advanced AI models consumes enormous electricity. Large data centers require sophisticated cooling systems and dedicated power infrastructure. Engineers are exploring liquid cooling and specialized architectures to improve efficiency.

Can AI Power Demand Break the Grid? - The Energy Cost of Intelligence

Artificial intelligence is often described as a digital revolution, but behind every intelligent response lies a massive physical cost "electricity".

Training modern AI systems requires enormous computational power, and that power comes from data centers consuming energy at unprecedented levels. Large language models and advanced image generators are trained using thousands of specialized GPUs running continuously for weeks or even months. Some large training clusters consume as much electricity as small towns. As companies race to build more capable AI systems, energy demand has rapidly become one of the industry's biggest hidden challenges. Modern hyperscale data centers now require advanced cooling infrastructure to prevent overheating. Traditional air cooling is increasingly insufficient for high-performance AI hardware. Engineers are turning toward liquid cooling systems, where coolant flows directly around processors to remove heat efficiently.

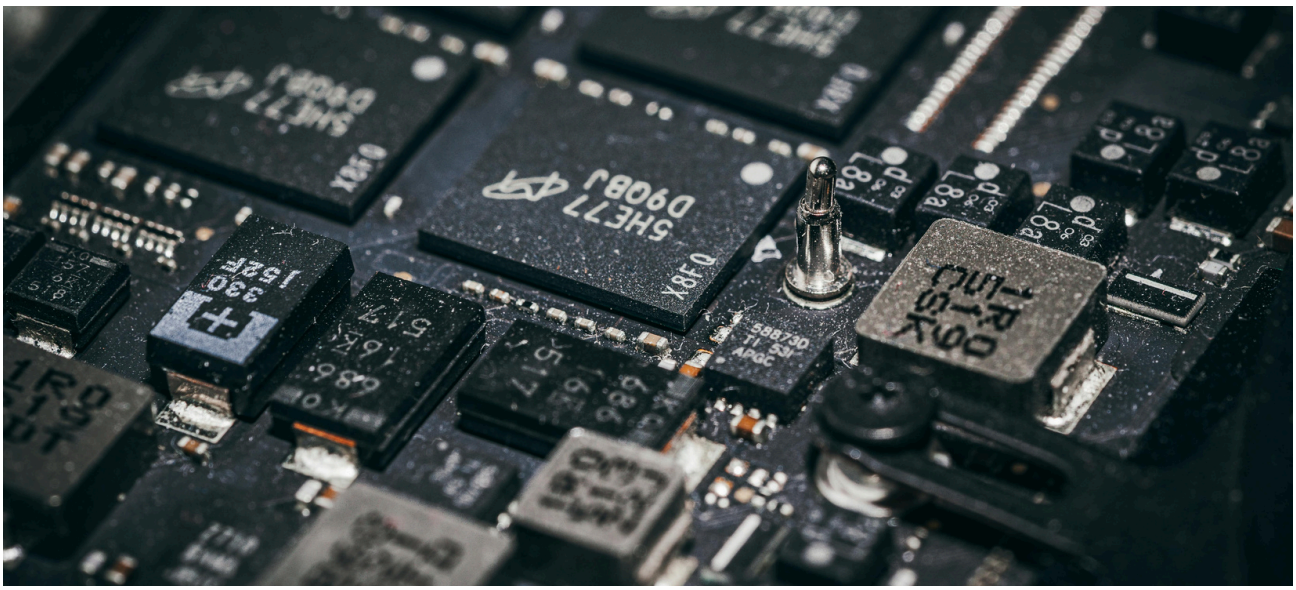
Energy consumption is not only an economic concern but also an environmental one. Increased electricity demand raises questions about carbon emissions and sustainability. Technology companies are therefore investing heavily in renewable energy contracts, solar farms, and even nuclear power partnerships to support future AI expansion.

Water usage has also emerged as a concern. Cooling large server facilities can require millions of liters of water annually, creating challenges in regions already facing water scarcity.The future of artificial intelligence may ultimately depend not only on faster chips but also on smarter energy solutions. Efficiency improvements, specialized AI accelerators, and greener power sources could determine whether AI growth remains sustainable in the decades ahead. In the race to build smarter machines, humanity may first need to solve how to power them responsibly.

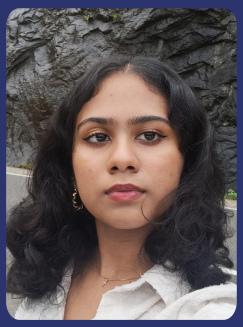
What Comes Next?

The future of AI hardware may include photonic processors, neuromorphic chips inspired by the human brain, and custom accelerators optimized for specific AI workloads.

Artificial intelligence is no longer just a software competition. It is a battle fought in silicon, factories, supply chains, and power grids, a race to build the machines capable of thinking alongside humanity.



DEAD INTERNET THEORY: A CONSPIRACY OR THE NEW REALITY?



Ann Maria Tenson
S2 CSE A

Introduction

The Dead Internet Theory was a theory which claims that since around 2016, the internet has consisted primarily of bot activity and automated content manipulated by algorithmic curation. Allegedly, it aims to reduce genuine interaction and enhance search results to influence consumers, slowly turning the internet from a human space to something that's mainly controlled by AI and bots.

But what was merely just a conspiracy theory gained renewed interest following the AI boom that began in the 2020s, with AI chatbots and generative AI becoming heavily commonplace and popularized.

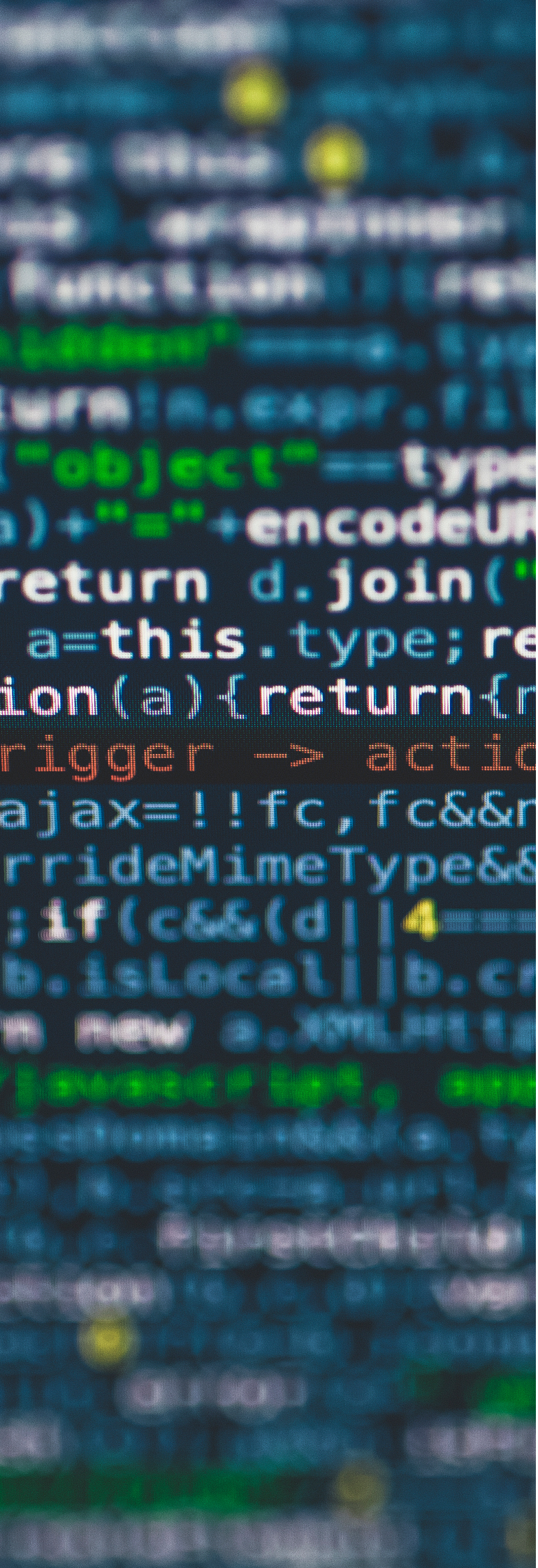
Since then, people have watched in real-time as the quality of AI gradually increased, blurring lines between what's real and what's fake, and social media sites having an exponential increase in bot activity with algorithms displaying AI slop instead of actual user-generated content. Users may not even be interacting with real individuals, but with automated systems designed to generate information. Likes, comments and shares which indicate human engagement and show people's opinions may be partially manufactured, indicating that online spaces may be becoming more artificial than authentic by the day. One of the most concerning and visible shifts is AI creating art, which is one of the most human acts-- as art imitates life itself, where people convey emotions and experiences. And art made by humans will always be imperfect, which ironically makes it perfect in a way that's human and in a way that AI could never replicate.

Beyond creative fields, AI has significantly taken over the advertising field. While passing by the street or scrolling on the internet, there's an increasing amount of AI generated ads. What was once the place of models and actors are now replaced by AI generated faces, and what was once somebody's hand drawn illustration is now just an AI generated illustration.

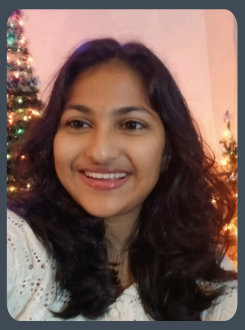
There are even social media accounts that are entirely AI, with thousands of followers. These accounts can respond to comments, post daily with no sleep, and maintain engagement with no human intervention. While swallowing the fact that artificial influencers even exist feels dystopian, more of these "influencers" are generating content by the hour to keep their audience hooked-- some of whom don't even realise that it's just AI.

Another terrifying aspect of this theory is the possibility of a recursive digital ecosystem. As AI generated content becomes more prevalent, AI starts feeding off AI generated content- coming in full circle and creating a version of the internet that evolves entirely independently of human input.

Despite its unsettling implications, the Dead Internet Theory remains partially speculative. The internet is far from entirely automated, and human presence continues to play a central role in shaping digital culture. But the significance of the Dead Internet Theory lies not in whether it is entirely true, but in the questions it raises. If art can be generated without artists, conversations conducted without consciousness, and influence exerted without human intent, the boundaries between the real and the artificial may become increasingly blurred. The internet may continue to expand and evolve, but the central concern remains whether it will retain its authenticity and human-ness.



RECENT TRENDS IN TECHNOLOGY: SHAPING THE FUTURE IN 2026



KAJOL JOBY
S2 CSE B

Technology continues to evolve at an unbelievable pace. Every year brings innovations that redefine how we live, work, learn, and connect. In 2026, the world is experiencing breakthroughs that are not just futuristic — they are transforming reality right now. From artificial intelligence to space tech, recent trends are reshaping human life across the globe.

1. Artificial Intelligence Everywhere

Artificial Intelligence (AI) is no longer limited to smart assistants or chatbots — it has become pervasive.

Generative AI

Generative AI tools can create realistic text, images, music, and even software code. They help students write essays, designers generate artwork, and developers build apps faster.

We now see AI in:

- Healthcare diagnostics
- Personalized learning systems
- Smart manufacturing
- Language translation
- Autonomous vehicles.

AI continues to evolve, making machines capable of performing complex tasks that once required human intelligence.

2. Metaverse and Extended Reality (XR)

The concept of the metaverse — a virtual world where people interact through digital avatars — is gaining major traction.

Virtual Reality (VR)

VR creates immersive digital environments that users can explore using headsets. These are used in:

- Gaming
- Virtual meetings
- Remote training

Augmented Reality (AR)

AR overlays digital objects onto the real world — like filters in apps or AR navigation on smartphones.

Together, VR and AR are called Extended Reality (XR), and they are redefining entertainment, education, and work.

3. 5G and Beyond Connectivity

5G (fifth-generation mobile network) is rapidly rolling out worldwide. It offers:

- Faster internet
- Reliable connections
- Ultra-low latency

This means smoother streaming, better online gaming, smarter cities, improved remote work, and advanced IoT (Internet of Things) systems.

4. Edge Computing

Edge computing brings processing power closer to where data is generated — such as smart devices, sensors, and machines.

Benefits:

- Faster response time
- Reduced network traffic
- Better performance for real-time apps

This trend is crucial for technologies like autonomous cars, industrial automation, and remote monitoring.

5. Cybersecurity Advancements

As digital threats grow more sophisticated, cybersecurity is becoming more advanced too.

Current trends include:

- AI-based threat detection
- Behavioral analytics
- Zero-trust security models
- Multi-factor authentication

Security is moving from reactive defense to proactive protection.

6. Quantum Computing

Traditional computers use bits (0 or 1), but quantum computers use qubits, allowing them to handle massive calculations far faster.

Quantum computing shows promise in:

- Drug discovery
- Cryptography
- Climate simulations
- Financial modeling

While still emerging, quantum computing could revolutionize science and technology.

7.Blockchain Beyond Crypto

Blockchain technology the backbone of cryptocurrencies is now being used in many other areas:

- Secure digital identities
- Supply chain transparency
- Voting systems
- Decentralized apps (dApps)

Blockchain ensures trust, traceability, and data integrity across platforms.

8. Sustainable Technology

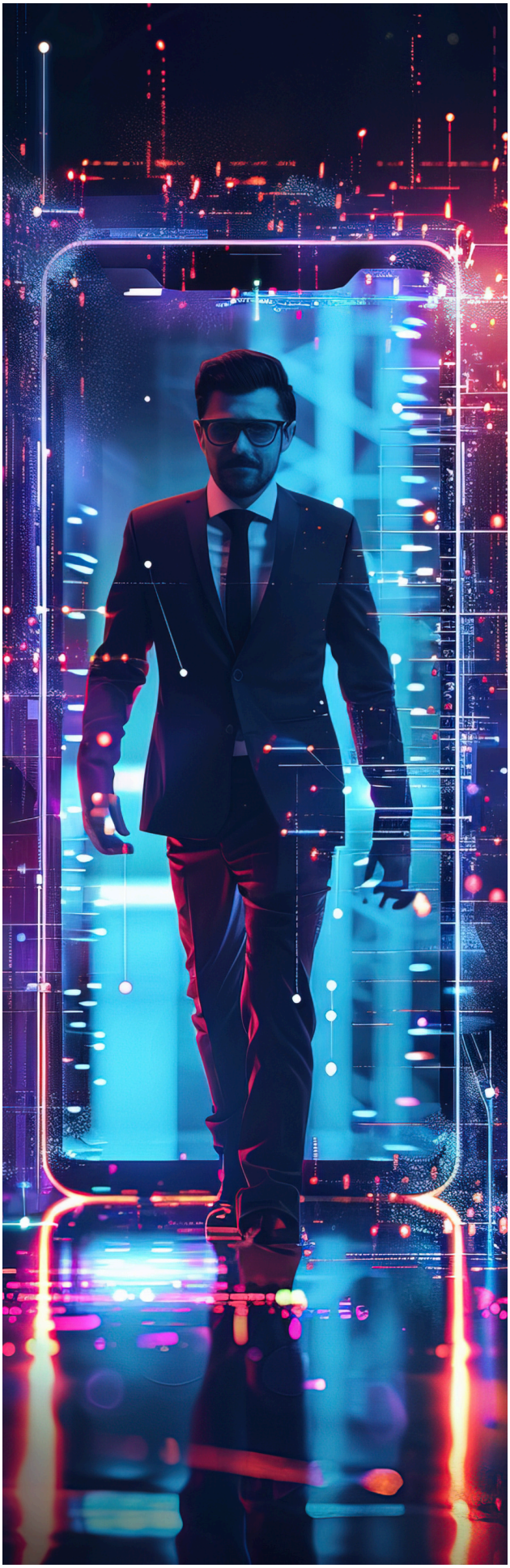
Green tech is trending as the world prioritizes environmental sustainability.

Examples include:

- Energy-efficient data centers
- Renewable energy solutions
- Advanced battery tech
- Eco-friendly electronics

Technology and sustainability now go hand-in-hand.

2026 is a remarkable time for technology. Recent trends like AI, 5G, XR, cybersecurity, quantum computing, and sustainability are not just shaping innovation — they are redefining human progress. As we continue to explore and adopt these technologies, the possibilities for tomorrow are endless.



THE AI BUBBLE: HYPE, HARDWARE, AND THE HIDDEN ECONOMIC SHIFT

Haniya Jahan K Z
S2 CSE B

In the last three years, conversations about an "AI bubble" have intensified across technology forums, financial markets, and academic discussions. Artificial Intelligence has shifted from being a research concept to becoming one of the main drivers of global technological investment. From generative AI tools to automation systems and large data models, AI is now a key part of modern digital infrastructure.

But as this expansion accelerates, an important question arises: Are we witnessing genuine long-term innovation, or are we inflating an economic bubble?

The Rise of the AI Boom (2020–2024)

Since 2020, investment in AI has grown at an extraordinary pace. The release of advanced generative models and breakthroughs in machine learning efficiency have pushed companies to invest aggressively.

Major technology corporations are building massive AI data centers, acquiring chip manufacturers, and expanding cloud computing capabilities.

Governments are also entering the race, funding AI research as a matter of national competitiveness. This global competition further accelerates capital flow into the sector.

2. Metaverse and Extended Reality (XR)

While strong investment can indicate confidence in innovation, rapid valuation increases can also signal speculative enthusiasm. Startups with minimal products are receiving billion-dollar valuations. This environment raises concerns about long-term sustainability.

Historical Parallels: Lessons from the Dot-Com Era

The dot-com bubble of the late 1990s offers an important comparison. During that period, internet-based companies attracted massive funding despite lacking stable revenue streams. When expectations exceeded reality, markets corrected sharply.

However, unlike many dot-com firms, AI companies today often provide tangible services with measurable impact. The difference lies in whether current growth reflects sustainable transformation or inflated expectation.

The Hardware Effect: Rising RAM and Memory Prices

One of the clearest real-world consequences of the AI boom is the rising price of RAM and High Bandwidth Memory (HBM). AI models require enormous computational resources. GPUs process massive datasets, but their efficiency depends heavily on high-speed memory systems.

As AI training workloads increase, demand for advanced memory chips has surged globally.

Manufacturers are prioritizing HBM production for AI accelerators, which reduces supply for traditional consumer memory markets. This shift has driven up RAM prices and increased infrastructure costs for businesses and data centers.

Energy Consumption and Environmental Concerns

Beyond financial markets, AI expansion raises environmental questions. Training large AI models consumes vast amounts of electricity. Data centers require cooling systems and continuous energy supply. If investment continues to grow without efficiency improvements, sustainability may become a major concern.

Infrastructure Imbalance and Market Pressure

AI infrastructure relies on GPUs, high-speed RAM, storage systems, and networking technologies. As demand rises, supply chains face bottlenecks. Semiconductor production is geographically concentrated, making it vulnerable to geopolitical instability.

This can lead to unequal competition between major corporations and smaller startups that cannot afford expensive infrastructure.

Broader Economic and Social Implications

If AI investment continues expanding rapidly, several outcomes are possible:

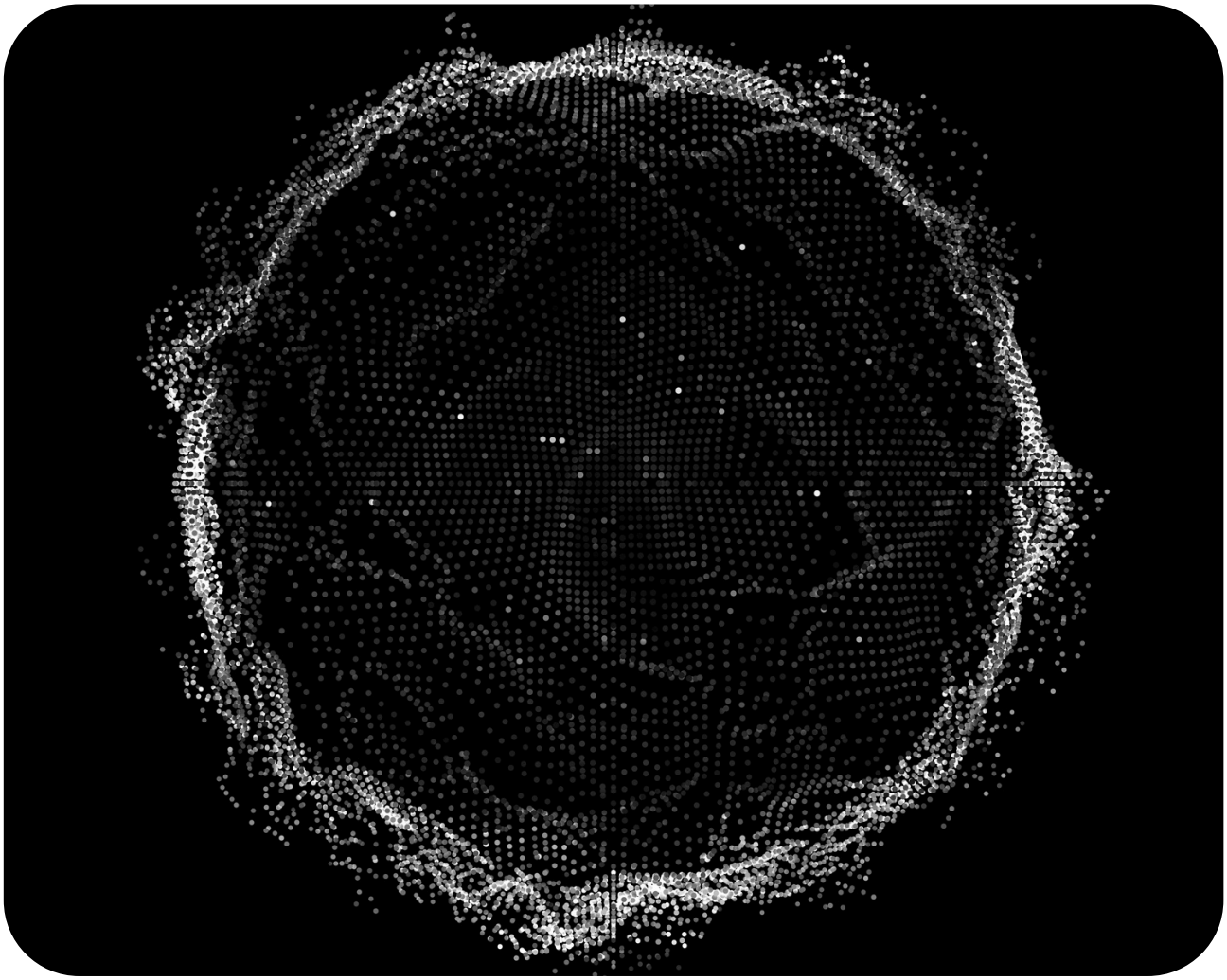
- Sustained productivity growth across industries
- Increased automation and workforce shifts
- Stronger regulatory oversight
- Market correction if returns fail to justify valuations

The AI bubble debate is therefore not limited to investors. It influences employment patterns, education systems, government policy, and global economic stability.

Broader Economic and Social Implications

The AI boom stands at a crossroads between speculation and structural transformation. Rising RAM prices demonstrate how deeply AI demand is reshaping hardware markets. At the same time, rapid valuations and concentrated investment raise legitimate concerns.

Whether history will describe this period as an AI bubble or the beginning of a new industrial revolution depends on how effectively innovation translates into long-term, sustainable value.



LOG CHAIN TECHNOLOGY

Nayana Girish M
S2 CSD

Log Chain Technology is a structured method of recording, verifying, and maintaining logs in a secure and sequential manner. It is inspired by blockchain principles, where data is stored in linked blocks that form a continuous chain. Each log entry is connected to the previous one, ensuring transparency, traceability, and integrity.

1. Introduction to Log Chain Technology

Log Chain Technology ensures that every event or transaction is recorded in chronological order. Each log contains a timestamp, data payload, previous log reference, and a unique hash value. This linking mechanism prevents tampering, as modifying one log would require changing all subsequent logs in the chain.

2. Core Components

- The core components of Log Chain Technology include:
- Log Block: A unit containing data and metadata.
- - Hash Function: Ensures data integrity.
- Timestamp: Records the time of log creation.
- Chain Link: Connects each log to the previous one.

3. Working Mechanism

When a new event occurs, it is recorded as a new log block. The system calculates a cryptographic hash based on the current log data and the hash of the previous log. This creates a secure chain. Verification mechanisms ensure that logs are validated before being permanently added to the chain.

4. Advantages of Log Chain Technology

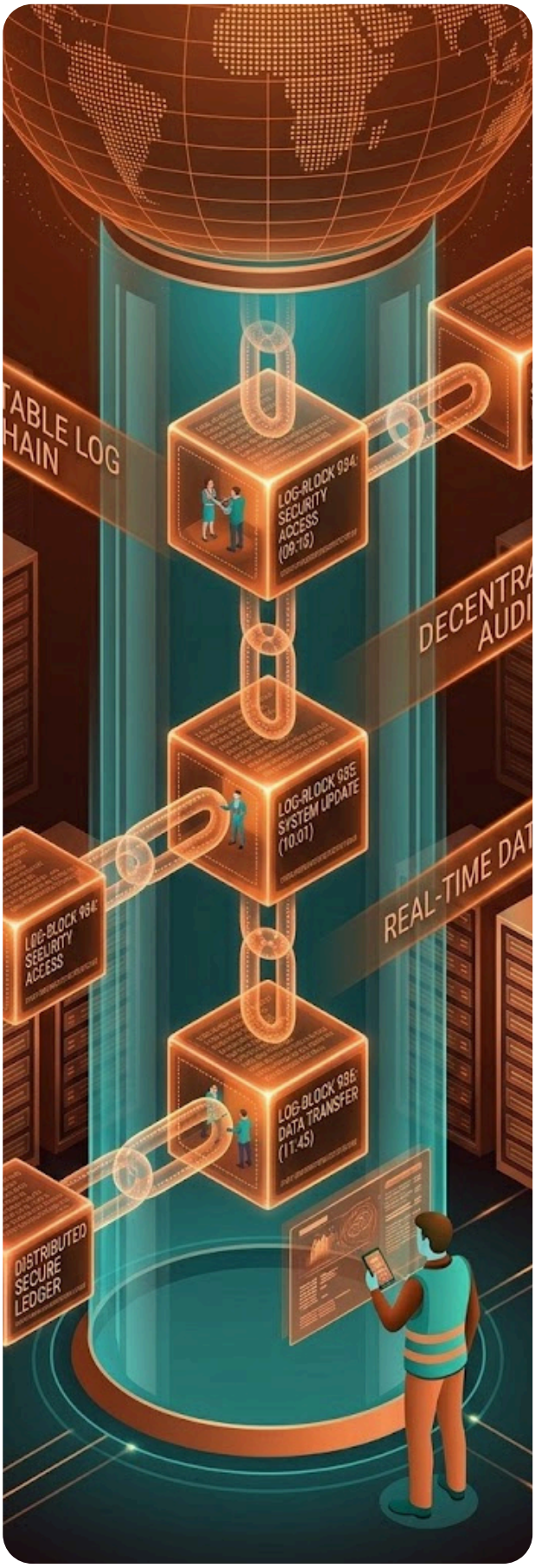
- Data Integrity: Prevents unauthorized modifications.
- Transparency: Provides a clear audit trail.
- Security: Uses cryptographic principles.
- Decentralization: Can be implemented across distributed systems.

5. Applications

Log Chain Technology is widely applicable in cybersecurity logging systems, financial transaction monitoring, supply chain tracking, healthcare record management, and cloud infrastructure auditing.

Conclusion

Log Chain Technology represents a modern approach to secure logging and data integrity. By linking records sequentially and protecting them with cryptographic techniques, organizations can ensure transparency, reliability, and tamper-proof documentation.



ETHICAL HACKING

Ethical Hacking?

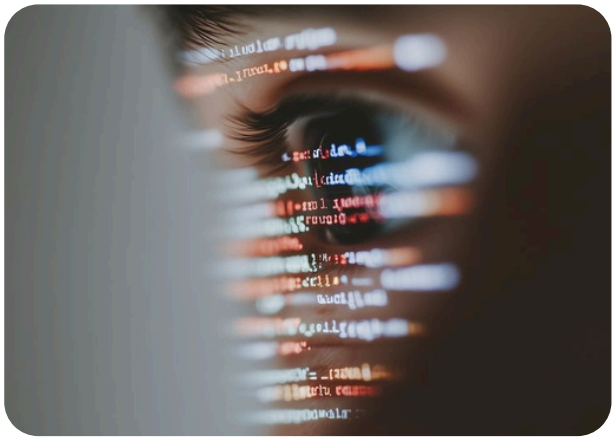
Ethical hacking, also known as penetration testing or white-hat hacking, is the practice of intentionally probing computer systems, networks, and applications to identify security vulnerabilities. Unlike malicious hackers, ethical hackers operate with proper authorization and aim to strengthen an organization's cybersecurity posture.

What is Ethical Hacking?

Ethical hacking involves simulating cyberattacks in a controlled and legal manner. Organizations hire ethical hackers to discover weaknesses before malicious attackers can exploit them. These professionals follow a structured methodology and provide detailed reports with recommendations for improving security.

Phases of Ethical Hacking

The ethical hacking process typically consists of several key phases including reconnaissance, scanning, gaining access, maintaining access, and reporting. Each phase plays a crucial role in understanding the target system and identifying potential vulnerabilities.



Types of Hackers

Hackers are generally categorized into three main types:

1. White Hat Hackers – Security professionals who test systems ethically.
2. Black Hat Hackers – Malicious attackers who exploit vulnerabilities for personal gain.
3. Grey Hat Hackers – Individuals who may violate rules but do not have malicious intent.

Importance of Ethical Hacking

Ethical hacking is essential in today's digital world where cyber threats are constantly evolving. It helps organizations protect sensitive data, maintain customer trust, comply with legal regulations, and prevent financial losses caused by cyberattacks.

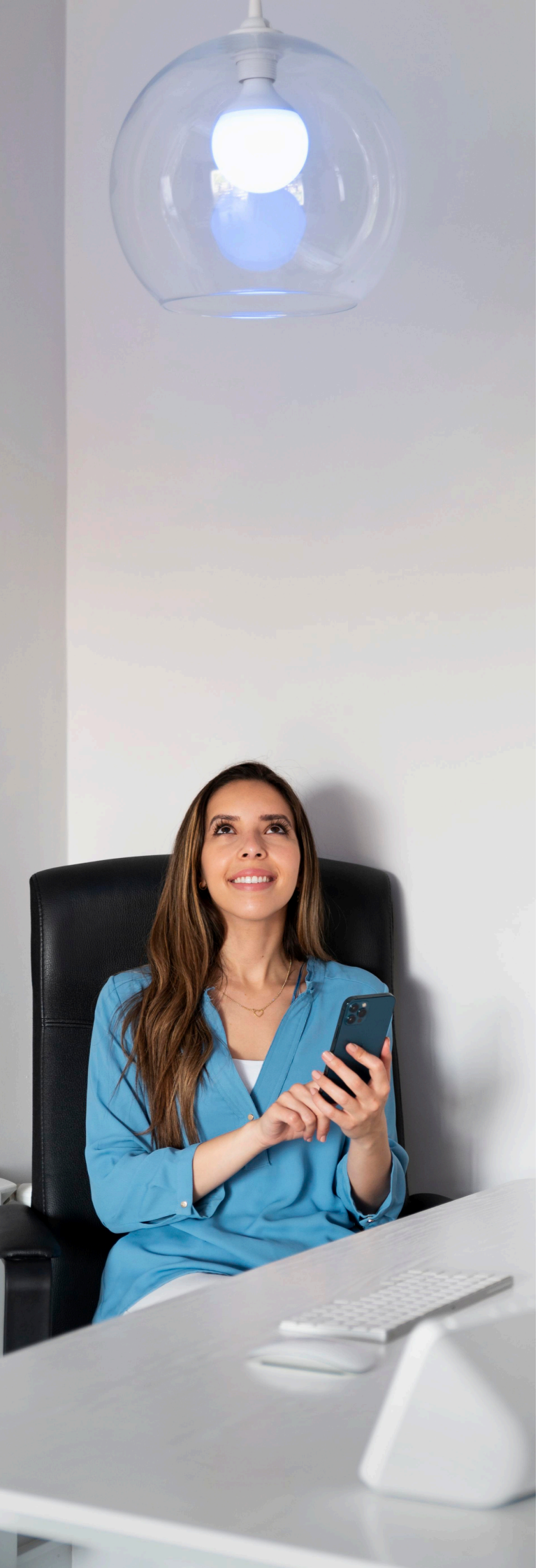
Security Testing Cycle

The security testing cycle is a continuous process that includes identifying vulnerabilities, testing systems, analyzing results, fixing issues, and retesting to ensure security improvements are effective.

Conclusion

Ethical hacking plays a vital role in modern cybersecurity. By proactively identifying and addressing security weaknesses, ethical hackers help organizations build resilient systems and defend against increasingly sophisticated cyber threats.

Helen Maria Jomon
S2 CSD



INTERNET OF THINGS (IOT)

Neha Savithri
S2 CSD

1. Detailed Explanation about IoT

The Internet of Things (IoT) refers to a network of physical devices embedded with sensors, software, and connectivity features that allow them to collect and exchange data over the internet. These devices communicate with each other without human intervention. IoT integrates technologies such as cloud computing, artificial intelligence, big data analytics, and wireless communication to create smart and automated environments.

2. Understanding IoT

IoT works through four key components:

- Devices/Sensors – Collect real-time data.
- Connectivity – Transfers data through Wi-Fi, Bluetooth, or 5G.
- Data Processing – Cloud platforms analyze the information.
- User Interface – Displays insights to users via apps or dashboards.

3. Real-World Applications of IoT

- Smart Homes – Automated lighting, thermostats, and security systems.
- Healthcare – Remote patient monitoring and wearable devices.
- Agriculture – Smart irrigation and crop monitoring systems.
- Smart Cities – Traffic control and waste management systems.
- Industry – Predictive maintenance and automation in manufacturing.

4. Ethical Concerns in IoT

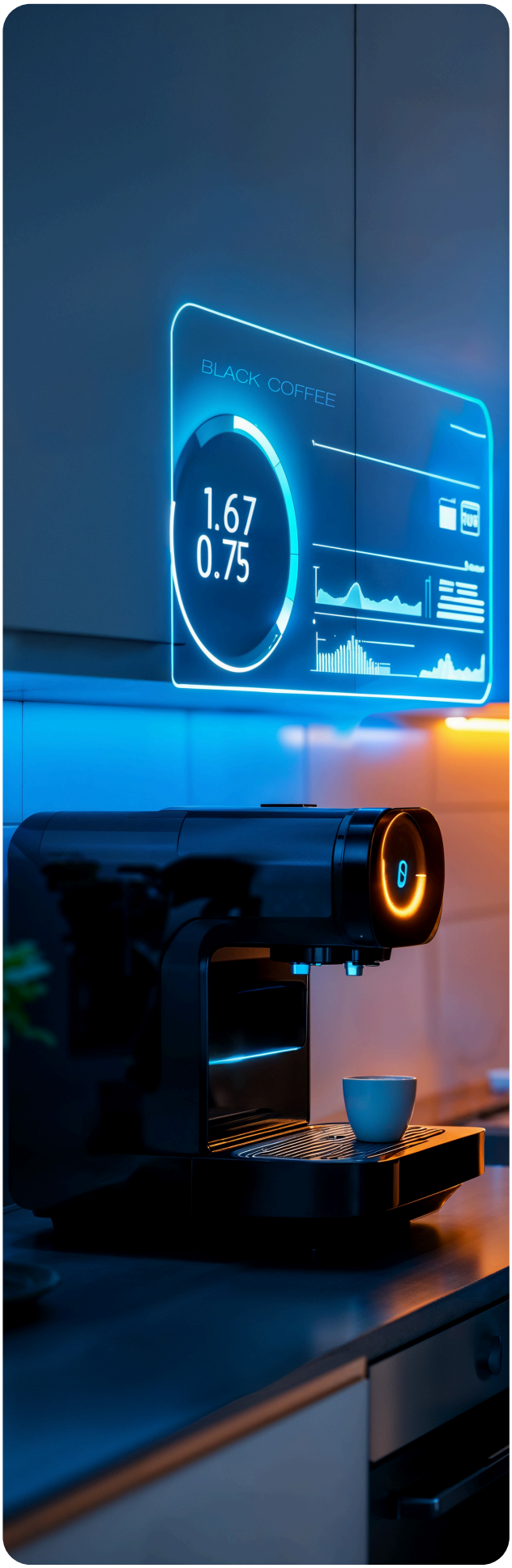
- Data Privacy – Risk of misuse of personal information.
- Security Risks – Devices can be vulnerable to hacking.
- Surveillance – Excessive monitoring may affect personal freedom.
- Data Ownership – Unclear control over collected data.
- Digital Divide – Unequal access to smart technologies.

5. Other Important Fields in IoT

- Artificial Intelligence Integration
- Edge Computing
- 5G and Advanced Connectivity
- Cybersecurity Frameworks
- Sustainability & Green IoT
- Blockchain for Secure Transactions

6. Conclusion

The Internet of Things is transforming the world by connecting devices and enabling smarter decision-making. While it offers innovation, automation, and efficiency, ethical considerations and security challenges must be addressed. With responsible implementation, IoT will continue to shape the future of technology and society.



"Design is not just what it looks like and feels like. Design is how it works."

- Steve Jobs

FEDERAL INSTITUTE OF SCIENCE AND TECHNOLOGY, AUTONOMOUS
Accredited by NAAC with 'A+' Grade & NBA (CSE,ECE,EEE,EIE,CE & ME)
Hormis Nagar, Mookkannoor P O,
Angamaly, Ernakulam Dt.
Kerala, India, Pin - 683 577
Ph: 0484 - 2725272
Email : mail@fisat.ac.in