MITS
MADANAPALLE

MADANAPALLE INSTITUTE OF TECHNOLOGY & SCIENCE
(UGC-AUTONOMOUS INSTITUTION)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

MAGAZINE

TECHERA 2026



MESSAGE FROM THE CORRESPONDENT



I am exhilarated that the Department of Computer Science & Engineering at MITS is launching a magazine called TECHERA in 2026. This Magazine brings out the intellectual brilliance in various new techniques introduced in Information Technology industry.

"**Hard work, sincerity, dedication, and enthusiastic devotion to your work will bring you unbounded success. May the Lord shower His blessings on you.**"

I warmly congratulate the students and the staff of CSE Department and wish them a grand success.

Dr. N. Vijaya Bhaskar Choudary
Correspondent

MESSAGE FROM THE PRINCIPAL



I am delighted about the magazine **'TECHERA'**, published by the Department of Computer Science & Engineering at MITS. On this momentous occasion, I congratulate all the students and faculty members of the department for their excellent efforts and coordination in making the magazine a great success.

Dr. P. Ramanathan
Principal

MESSAGE FROM THE HEAD OF THE DEPARTMENT



TECHERA is dedicated to addressing emerging topics and challenges in technology. TECHERA is to create great awareness on new innovative ideas and technologies. I thank the readers of **'TECHERA'** for their support and encourage them to provide useful feedback to enhance the magazine's standards.

Dr. M. Sreedevi
Head Of the Department CSE

EDITORIAL DESK

The annual release of the department magazine "**TECHERA – 2026",** mark the spirit of exploration among students in an environment of erudition.

This year's edition of '**TECHERA - 2026**' focuses on current trends in Computer Science & Engineering, key drivers in shaping a new world of science. It is a collection of information and facts, featuring the recent developments of fascinating and conceptual communication.

The editorial team expresses its gratitude to all who have made '**TECHERA - 2026**' a remarkable success.



ABOUT MITS

Madanapalle Institute of Technology & Science was established in 1998 in the picturesque and pleasant surroundings of Madanapalle. It is ideally located on a sprawling 26.17-acre campus along the Madanapalle-Anantapur Highway near Angallu, about 10 km from Madanapalle.

MITS, originated under the auspices of Ratakonda Ranga Reddy Educational Academy, under the proactive leadership of and **Dr. N. Vijay Bhaskar Choudary, Secretary & Correspondent** of the Academy.

MITS is governed by a progressive management that never rests on laurels and has been striving conscientiously to develop it as one of the best centers of Academic Excellence in India. The Institution's profile is firmly based on strategies and action plans that match changing demands of the nation and the student's fraternity. MITS enjoys constant support and patronage of NRI's with distinguished academic traditions and vast experience in Engineering & Technology.



ABOUT DEPARTMENT

The Department of Computer Science & Engineering, established in 1998, has been playing a vital role in producing value-based professionals. The department offers one 4 years undergraduate program to cater to the ever-challenging needs of technical excellence in the emerging areas of Computer Science & Engineering. The curriculum is flexibly designed to meet the IT industry's evolving needs. The CSE department has eminent faculty members with rich academic and industry exposure, who have pursued a Masters/Ph.D. Degree from prestigious institutions like NITs, IITs, and Central Universities within India and abroad. Many research activities in the domain of Artificial Intelligence (AI) and Machine Learning (ML) are under progress. Department of CSE has good interactions and MoUs with leading Industries for technology domain Training & Development Industries. It organizes Symposia, Exhibitions, Conferences, Seminars and Workshops for both students and Faculty belonging to various Technical Educational Institutions, Research Scholars of Research Institutes and Industries all over India.

Our students have secured placement offers from leading MNCs such as TCS, Infosys, IBM, Tech Mahindra, Accenture, Mindtree, etc., with prestigious salary packages ranging from 14 to 24 LPA. The department also offers training in certification programs and encourages students in self-learning with MOOC's such as NPTEL, Microsoft, Coursera, edX, etc. Activities in Research outcomes are presented/published in National / International Conferences / Journals. The students can become members of CSI, IEEE-CS, IEEE-PCS, IEEE-WIE, ACM & IET and participate various activities through these professional body.Department is committed to encourage students/researchers to carry out innovative research in the field of Computer Science & Engineering, keeping excellence in focus and deliver quality servicesto match the needs of the technical education system, industry and society. Students of CSE department are motivated to be innovative in their thinking while being strong in the Computer Science Core Knowledge. The department is also accredited by NBA (NationalBoard of Accreditation) of All India Council for Technical Education (AICTE), New Delhi.

DEPARTMENT VISION

To excel in technical education and research in area of Computer Science & Engineering and to provide expert, proficient and knowledgeable individuals with high enthusiasm to meet the Societal challenges.

DEPARTMENT MISSION

M1: To provide an open environment to the students and faculty that promotes professional and personal growth.

M2: To impart strong theoretical and practical background across the computer science discipline with an emphasis on software development and research.

M3: To inculcate the skills necessary to continue their education after graduation, as well as for the societal needs.

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

The Program Educational Objectives (PEOs) of the department of CSE are given below:

PEO1: Gain Successful Professional career in IT industry as an efficient software engineer.

PEO2: Succeed in Master / Research programmers to gain knowledge on emerging technologies in Computer Science and Engineering.

PEO3: Grow as a responsible computing professional in their own area of interest with intellectual skills and ethics through lifelong learning approach to meet societal needs.

PROGRAM SPECIFIC OUTCOMES (PSOs)

The Computer Science & Engineering Graduates will be able to:

PSO1: Apply mathematical foundations, algorithmic principles and computing techniques in the modelling and design of computer based systems.

PSO2: Design and develop software in the areas of relevance under realistic constraints.

PSO3: Analyze real world problems and develop computing solutions by applying concepts of Computer Science.

CONTENTS

SI.NO	CHAPTER	PAGE NO
1	Chatgpt Astra 6: Beyond Human Intelligence.	11 - 13
2	AI vs AI: The New Battle For Cybersecurity.	14 - 16
3	Beyond The Screen: The Era Of Spatial Computing	17 - 20
4	Brics In The Digital Age: Building A Connected Technological Future	21 - 23
5	Quantum Computing: From Fragile Qubits To Reliable Quantum Computing	24 - 26
6	INDIA'S Semiconductor And Ai Revolution	27 - 28
7	Humanoid Robots: When Ai Enters The Physical World	29 - 30
8	Sovereign Cloud: Why Data And Ai Infrastructure Are Becoming Strategic	31 - 32
9	The Architecture Of Quantum Regions: Building The Deep-Tech Infrastructure Of Tomorrow	33 - 34

CHATGPT ASTRA 6: BEYOND HUMAN INTELLIGENCE

The Next Era Of AI

1. From Generative AI to Agentic AI

Artificial Intelligence has evolved from rule-based systems to machine learning, deep learning, and Generative AI. While traditional AI systems mainly respond to specific inputs, Agentic AI takes a further step by working toward a complete objective.

An AI agent can receive a goal, reason about the required steps, use digital tools, inspect results, and continue working until the task is completed. GPT-6 Astra represents this direction by combining reasoning, computer use, coding, document understanding, and tool interaction within a single system.

This shift is significant because AI is moving from simply generating answers to performing multi-step digital work. Users can increasingly ask AI systems to accomplish complete tasks rather than requesting only information or individual pieces of code.



2. Why GPT-6 Astra Matters

Astra's importance comes from combining several capabilities, including reasoning, computer use, software engineering, browsing, cybersecurity, and professional workflows.

One notable capability is its ability to interact with applications that people already use, including applications that may not provide an API. Organizations commonly work with browsers, spreadsheets, documents, internal dashboards, code repositories, and specialized software. An AI that can interact with these environments can potentially become part of existing workflows without requiring every application to be redesigned specifically for AI.

his represents an important change: AI can move from being a separate tool to becoming an active participant in digital workflows.

3. Computer Use: From Instructions to Action

Traditional AI generally provides instructions that a human must execute. Computer-using AI can perform more of these operations directly through digital interfaces, subject to permissions and safeguards.

Such systems can potentially navigate websites, work with documents, prepare spreadsheets, interact with software interfaces, and perform repetitive digital procedures. Instead of describing every individual step, a user can communicate the desired outcome while the AI handles many intermediate operations.

This creates a new model of human-computer interaction. However, human supervision remains essential when AI actions can modify data, share confidential information, delete files, or produce other significant consequences.

4. Impact on Software Engineering

AI is rapidly changing software development. Software engineers normally need to understand requirements, design systems, write code, debug problems, test changes, review code, and maintain documentation. Advanced AI systems can assist with many of these activities.

GPT-6 Astra is designed to support longer and more complex engineering tasks by working across files and understanding relationships within a codebase. OpenAI reports a 57.9% score on Terminal-Bench 4.0, compared with 37.3% for GPT-5.6 Sol, on complex terminal-based tasks involving software engineering, system configuration, and data analysis.

The role of programmers is therefore likely to evolve rather than disappear. Developers may spend more time on system architecture, requirements, verification, security, and decision-making, while AI handles an increasing amount of implementation and debugging.

Human expertise remains essential because AI-generated code must be checked for correctness, performance, maintainability, and security.

5. Beyond Human Intelligence

The phrase “Beyond Human Intelligence” should be interpreted carefully. AI has not surpassed humans in every form of intelligence. Humans continue to possess important abilities involving emotional understanding, social awareness, moral judgment, lived experience, and responsibility.

However, machines can outperform individual humans in particular computational tasks. They can process large amounts of information rapidly, perform repetitive operations without fatigue, compare large quantities of data, and operate digital systems at high speed.

Therefore, the more meaningful idea is that AI can go beyond specific human limitations of speed and scale. Humans remain responsible for defining goals, evaluating consequences, applying values, and making important decisions.

The future is more likely to involve human-AI collaboration than a simple competition between humans and machines.

6. Safety, Security, and Human Control

Greater AI capability also creates greater responsibility. When an AI system can access applications, confidential information, or digital tools, an incorrect action can have real consequences.

Potential risks include exposing confidential information, sharing data too broadly, making unauthorized changes, or deleting important information. Advanced AI systems therefore require strong controls and human oversight.

Enterprise environments can restrict access to approved websites and applications, manage uploads and downloads, and control browsing activity. Confirmation mechanisms can also require human approval before important actions are performed.

Cybersecurity is another major consideration. As AI becomes more capable of interacting with computer systems, security mechanisms must evolve alongside its capabilities. AI development must therefore include safeguards against unauthorized actions, misuse, and security threats.

7. The Future of Human-AI Collaboration

The next generation of AI is expected to focus increasingly on complete workflows rather than isolated answers.

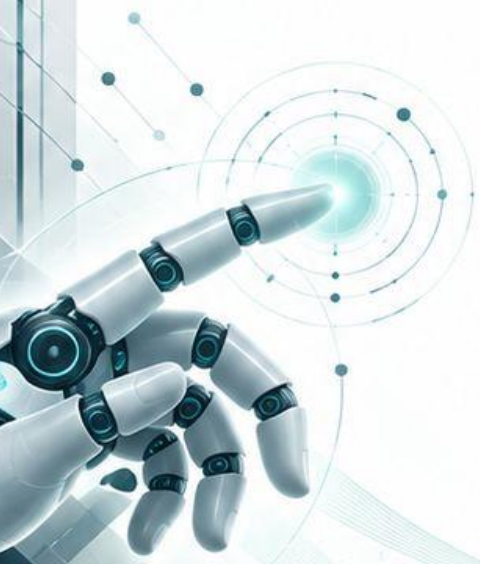
For example, a software engineer could describe a feature and ask an AI agent to inspect a codebase, implement the change, run tests, identify failures, and prepare the changes for review. A researcher could ask an AI system to collect information, analyse data, and organize the findings into a structured report. A business analyst could use AI across spreadsheets, documents, and internal applications.

This does not eliminate the need for human expertise. Instead, it changes where expertise is applied. Humans will increasingly focus on defining objectives, evaluating evidence, designing systems, managing risks, and validating AI-generated results.

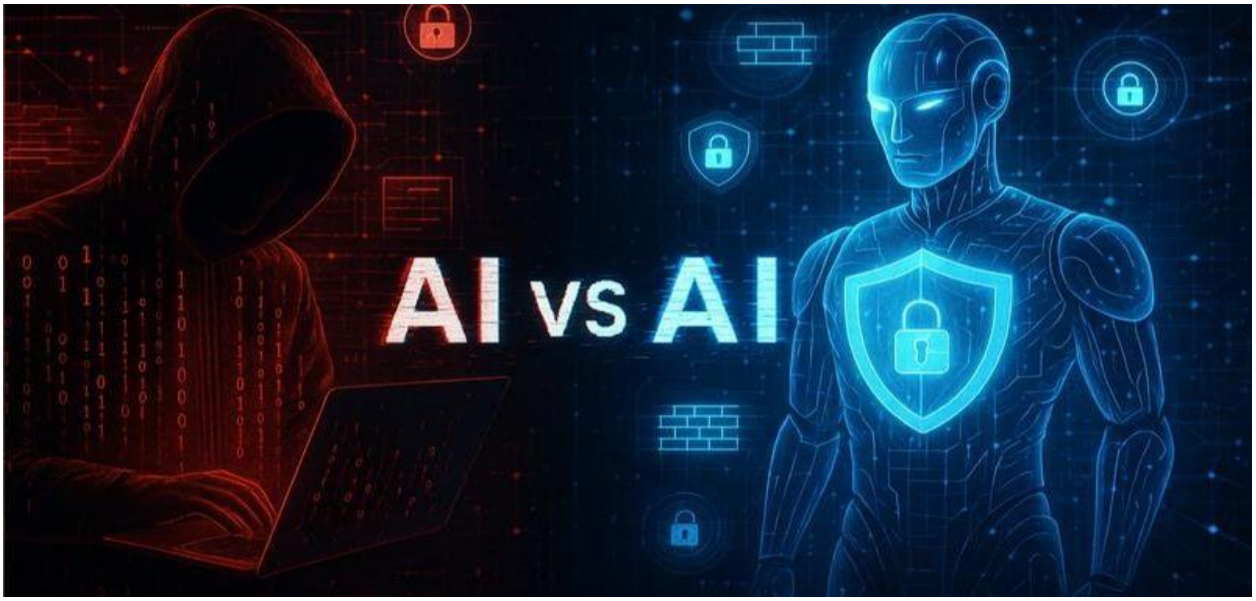
For Computer Science and Engineering students, strong technical fundamentals remain essential. Knowledge of algorithms, data structures, operating systems, databases, computer networks, software engineering, cybersecurity, and AI will help future professionals understand, evaluate, and effectively direct intelligent systems.

Bhojanapu Deva Raj

25695A0514



AI VS AI: THE NEW BATTLE FOR CYBERSECURITY



When Artificial Intelligence Becomes Both the Attacker and the Defender

Cybersecurity is entering a new phase where artificial intelligence is no longer simply a tool used by security teams. The same technology that helps organizations detect cyber threats is also being used by attackers to make attacks faster, more automated and more difficult to identify. This has created a new technological contest: AI versus AI.

For many years, cyberattacks depended heavily on human expertise. Attackers needed to identify vulnerabilities, write malicious code, create convincing phishing messages and analyze the target environment. Generative AI and autonomous AI systems are changing this process. AI can now help automate several stages of an attack, allowing cybercriminals to operate faster and at a much larger scale. Recent cybersecurity discussions in 2026 increasingly describe this as a new AI-driven cyber arms race.

How AI Is Changing Cyberattacks

One of the biggest changes is the ability of AI systems to process enormous amounts of information quickly. An attacker can use AI to analyze publicly available information about an organization, identify potential weaknesses and generate highly personalized social-engineering messages.

Traditional phishing emails often contain obvious warning signs such as poor grammar or generic messages. AI can make fraudulent communication much more convincing by generating messages that match the language, style and context of the intended victim.

AI can also assist attackers in developing malicious scripts, modifying attack techniques and identifying vulnerabilities. Security researchers have warned that AI-enabled malware may become increasingly

adaptive, potentially changing its behavior during an operation.

Another emerging concern is the rise of AI agents. Unlike a conventional chatbot that waits for a human instruction, an AI agent can perform a sequence of tasks with greater autonomy. This creates a new security challenge because attackers may attempt to compromise AI agents themselves or use autonomous systems to attack other systems.

This means organizations must begin thinking about AI systems as part of their security boundary—not simply as software applications.

AI as the Defender

Fortunately, AI is also giving cybersecurity professionals powerful new capabilities.

Modern security platforms can continuously analyze network traffic, user behavior, applications, devices and system logs. Instead of depending entirely on known attack signatures, AI can look for unusual patterns and identify behavior that may indicate a previously unknown threat.

For example, if an employee normally logs in from a particular location during working hours but suddenly attempts to access sensitive information from an unfamiliar device at an unusual time, an AI-based security system can identify the abnormal behavior and generate an alert.

AI can also help security teams prioritize thousands of alerts. Security Operations Centers traditionally require analysts to examine large volumes of security events. AI can analyze these events rapidly, identify relationships between seemingly unrelated incidents and help analysts focus on the most serious threats.

The next step is automated response. Instead of simply informing a security analyst that an attack is occurring, an AI security system may be able to isolate a compromised device, block suspicious communication or temporarily restrict an account.

AI Red Team vs AI Blue Team

One of the most interesting developments is the use of AI for both offensive and defensive security testing. A red team represents attackers and attempts to discover weaknesses in a system. A blue team represents defenders and works to protect the system.

New AI-based approaches are beginning to automate parts of both activities. In 2026, NVIDIA and CrowdStrike announced AI cybersecurity models designed around offensive and defensive roles, including systems that simulate attack behavior and systems focused on remediation and defense. Their approach also uses digital-twin environments to test attack paths before applying defensive measures to real systems.

This creates an interesting feedback loop:

AI attacker → simulated attack → AI defender → detection → response → improved defense

The goal is to allow organizations to identify weaknesses before real attackers exploit them.

Humans Still Matter

Despite the growing capabilities of AI, cybersecurity cannot become completely dependent on automation. AI systems can make mistakes. They may generate false alarms, misunderstand legitimate behavior or make incorrect decisions when the available information is incomplete. A poorly controlled autonomous security system could even create new problems while attempting to solve an existing one.

Therefore, cybersecurity professionals will increasingly need to work with AI rather than compete against it.

Human experts will remain important for security architecture, incident investigation, risk assessment, governance and strategic decision-making. Organizations will also need strong access controls, continuous monitoring, secure AI deployment and clear rules defining what an AI system is allowed to do.

For students and professionals, this means cybersecurity itself is changing. Knowledge of networking, operating systems, cloud computing and security remains essential, but understanding AI systems is becoming equally important.

The Future: Cybersecurity at Machine Speed

The future of cybersecurity will probably not be a simple competition between humans and machines. Instead, it will involve intelligent systems continuously attacking, testing, detecting and defending against one another—with humans supervising the overall process.

The central question is no longer “Can attackers use AI?” They already can. The more important question is whether defenders can deploy AI quickly, safely and intelligently enough to maintain an advantage.

As AI becomes faster and more autonomous, cybersecurity must also become faster and more adaptive. The organizations that succeed will be those that combine artificial intelligence, strong security practices and human expertise.

Nikhitha Y

23691A05C4

BEYOND THE SCREEN: THE ERA OF SPATIAL COMPUTING

1. Computing Beyond the Screen

For decades, people have interacted with computers mainly through screens, keyboards, mice, and touchscreens. Spatial Computing represents a shift toward more natural and immersive forms of digital interaction. It connects digital information with the physical environment, allowing computers to understand and respond to the space around users. Spatial Computing enables digital objects and information to be positioned within a three-dimensional environment. Users can view, move around, and interact with these digital elements as if they are part of their surroundings.

The technology combines Artificial Intelligence (AI), Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR), computer vision, sensors, and 3D graphics to create interactive digital experiences.

2. Understanding the Spatial World

Spatial Computing allows computers to understand the position, shape, movement, and structure of objects and people in a physical environment. Instead of limiting digital interaction to a flat screen, it enables users to interact with information in three-dimensional space.

For example, a user wearing an AR or mixed-reality headset can place a virtual 3D model of furniture inside a room. The user can walk around the model, view it from different angles, and examine how it fits within the available space.

The basic concept can be represented as:

Physical Environment → Sensors → 3D Understanding → Digital Interaction

This approach makes computing more closely connected to the real world and enables digital information to become part of the user's physical surroundings.

3. The Technologies Behind Spatial Computing

Spatial Computing is not a single technology. It combines several technologies that work together to create an interactive spatial environment.

Augmented Reality (AR):

AR adds digital information or objects to the real world. For example, an AR navigation application can display directions and location information over the user's view of a real road.

Virtual Reality (VR):

VR creates a completely computer-generated environment. Users can enter and interact with a simulated three-dimensional world using headsets and controllers.

Mixed Reality (MR):

Mixed Reality combines physical and digital environments. Digital objects can appear within the real environment and respond to physical surroundings.

Computer Vision:

Computer vision enables computers to interpret images and videos. In Spatial Computing, it helps identify objects, surfaces, people, and movements.

Sensors:

Cameras, depth sensors, motion sensors, and other sensing technologies collect information about the environment and the user's movements. This information helps the system understand the surrounding space.

4. From Physical Space to Digital Experience

Spatial Computing generally involves several stages that allow a system to understand and interact with its environment.

Environment Sensing:

Cameras and sensors first collect information about the surrounding physical environment and the user's movements.

Environment Mapping:

The collected information is processed to identify surfaces and objects such as floors, walls, tables, and other structures.

3D Processing:

The system creates a digital representation of the environment. This allows virtual objects to be positioned accurately within the physical space.

User Interaction:

Users can interact with digital objects through hand gestures, controllers, voice commands, eye movements, or other input methods.

For instance, a user may place a virtual chair inside a room and examine its size, position, and appearance before purchasing the actual product. Similarly, an engineer can view a virtual machine component within a real workspace before manufacturing it.

5. Where Spatial Computing is Making an Impact

Spatial Computing has applications across education, healthcare, engineering, entertainment, and other fields.

Education:

Students can use interactive 3D models and simulations to understand complex concepts. Medical students, for example, can explore three-dimensional models of the human body instead of relying only on textbooks or two-dimensional diagrams.

Healthcare:

Doctors and medical professionals can use 3D visualizations to understand medical information and assist with procedure planning. Spatial technologies can also support medical training and simulation.

Manufacturing:

Engineers can visualize machines, components, and production environments in 3D. Spatial Computing can support product design, assembly, maintenance, and employee training.

Architecture and Engineering:

Architects and engineers can explore 3D models of buildings and structures before construction. Designs can be viewed at realistic scales, helping professionals identify potential design problems at an early stage.

Gaming and Entertainment:

Spatial Computing can provide immersive experiences in which digital objects and environments respond to the user's position and movements.

Navigation:

AR-based navigation can display directions and useful location information directly over the user's view of the real environment, making navigation more intuitive.

6. Transforming the Way We Learn and Work

One of the major benefits of Spatial Computing is better visualization. Complex objects, systems, and environments can be represented as interactive 3D models, making them easier to understand.

It also provides immersive experiences. Instead of interacting with digital information only through a screen, users can move around and interact with virtual objects in a more natural way.Spatial Computing can improve learning and training by providing simulations that allow students and professionals to practice tasks in controlled environments. This can be particularly useful in fields such as medicine, engineering, aviation, and industrial training.

Another benefit is improved productivity. Engineers, designers, and other professionals can visualize and modify digital models directly within a three-dimensional environment. The technology may also reduce the need for some physical prototypes. Designers can create and examine virtual models before producing physical versions, potentially saving time and resources.

7. Challenges in the Spatial Era

Despite its potential, Spatial Computing faces several technical and practical challenges.

Hardware Cost:

Advanced AR, VR, and mixed-reality devices can be expensive, which may limit their adoption among individuals and organizations.

Battery Life:

Spatial devices require power for displays, sensors, cameras, and computing. Maintaining long battery life while providing high performance remains a challenge.

Privacy:

Spatial devices may collect information about users, their movements, surroundings, and physical environments. Protecting this information is an important concern.

User Comfort:

Extended use of VR devices can cause motion sickness, eye strain, or discomfort for some users. Improving display technology and device ergonomics is therefore important.

Tracking Accuracy:

Spatial systems need to accurately understand their surroundings and track user movements. Poor lighting, complex environments, or changes in the physical space can affect tracking performance.

8. The Road Ahead

Spatial Computing is expected to become more capable as AI, computer vision, sensors, AR, VR, and 3D technologies continue to improve. Future devices are likely to become smaller, lighter, and more comfortable. Improved AI and computer vision can enable systems to understand physical environments with greater accuracy and respond more intelligently to users.

Spatial Computing may become increasingly important in education, healthcare, manufacturing, remote collaboration, entertainment, architecture, and professional training.

Human-computer interaction may also become more natural. Instead of depending mainly on keyboards, mice, and touchscreens, users could interact with computers through gestures, voice, eye movements, and physical movement.

The combination of Spatial Computing and Artificial Intelligence is particularly promising. AI can help systems understand not only the user's instructions but also the surrounding environment. This could lead to intelligent applications that respond to both human needs and physical context.

Manasa Bysani

23691A0599

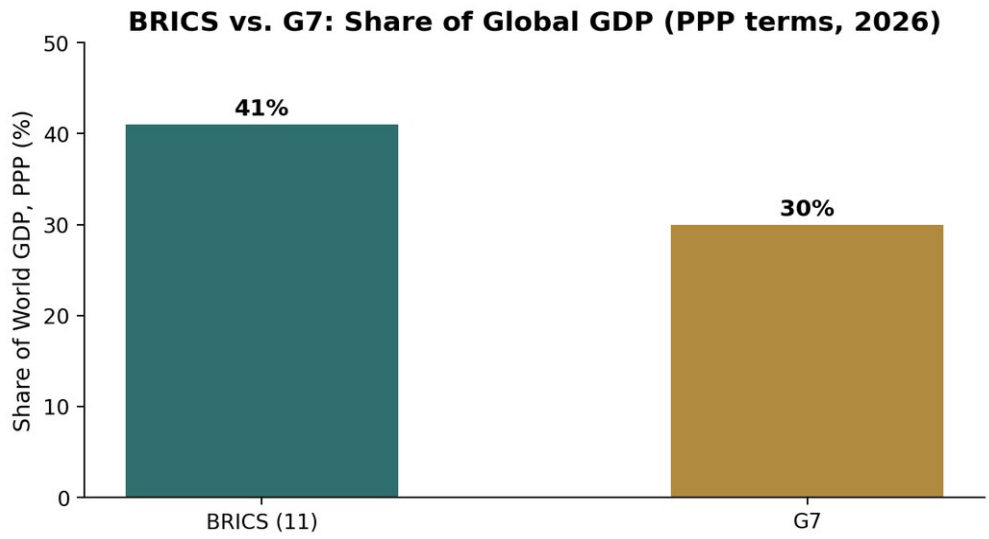
BRICS IN THE DIGITAL AGE: BUILDING A CONNECTED TECHNOLOGICAL FUTURE

BRICS began in 2009 as an informal grouping of Brazil, Russia, India, and China, joined shortly after by South Africa. Following an expansion in 2024 and 2025 that added Egypt, Ethiopia, Iran, Saudi Arabia, the United Arab Emirates, and Indonesia, the bloc now comprises eleven full members. Together, official 2026 figures put the group at roughly half the world's population and around 40% of global GDP measured at purchasing power parity (PPP) — a scale that puts it on par with, or ahead of, the G7 by that same measure.

Beyond the eleven full members, a ten-country "partner" tier — Belarus, Bolivia, Cuba, Kazakhstan, Malaysia, Nigeria, Thailand, Uganda, Uzbekistan, and Vietnam — lets additional economies engage with BRICS initiatives without full accession. Turkey, Pakistan, Bangladesh, and Azerbaijan are among several countries with active membership bids, though no further expansion round was announced at the 2026 summit.

Share of Global GDP

On a PPP basis, BRICS' combined economic output now exceeds the G7's share of world GDP, driven largely by China and India's growth alongside the bloc's 2024–2025 expansion. The chart below reflects figures widely cited around the 18th BRICS Summit, hosted by India in New Delhi in September 2026.



Source: BRICS 2026 chair (India) figures; PPP-basis estimates widely cited at the 18th BRICS Summit, Sept 2026.

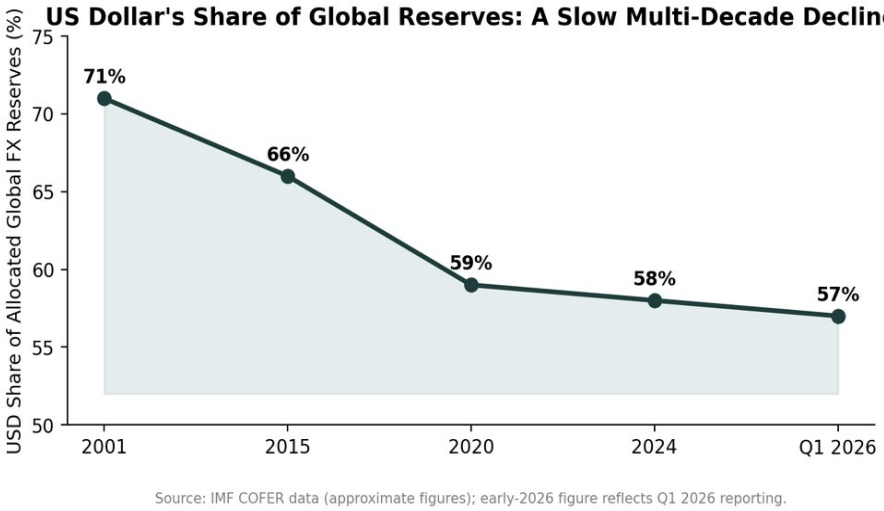
Trade Settlement and De-Dollarization

The most closely watched economic trend within BRICS is the gradual shift toward settling trade in members' own currencies rather than the US dollar. Russia and China already conduct roughly 90% of their bilateral trade in rubles and yuan, by Vladimir Putin's own account. At the September 2026 New Delhi summit, leaders formally adopted

BRICS Pay, a payment-messaging system linking national networks — Russia's SPFS, China's CIPS, and India's UPI — to route cross-border transactions outside the dollar-denominated SWIFT system.

This should be read carefully. There is no single BRICS currency, and several members — India most explicitly — have stated they have no policy aimed at replacing the dollar. BRICS Pay itself is not a currency and does not replace the dollar as a reserve asset; it is payment infrastructure, not a substitute for the system it runs alongside.

The aggregate data is more stable than the "de-dollarization" framing suggests. IMF COFER figures put the dollar's share of allocated global FX reserves at roughly 57% in early 2026 — essentially flat to slightly up quarter-on-quarter, a move the IMF attributes mainly to the dollar's own appreciation rather than active diversification. The chart below shows the broader multi-decade trend.



Gold and the "Unit" Settlement Pilot

Alongside payment infrastructure, BRICS has floated a gold-backed settlement instrument nicknamed the Unit. It is not a currency and not a reserve-replacement project: the New Delhi Declaration describes it as entering a technical feasibility study, several steps short of deployment, with no BRICS central bank yet committed to using it operationally. The concept draws on the bloc's substantial collective gold reserves — estimated above 6,000 tonnes — as potential backing. For now, it is best treated as a pilot concept rather than working financial infrastructure.

Washington's Response

US President Donald Trump has repeatedly threatened tariffs of up to 100% on BRICS members that back a currency intended to replace the dollar — a threat first issued in late 2024 and reiterated since, including immediately after the New Delhi summit's BRICS Pay announcement. That pressure is itself part of the bloc's economic story: it raises the stakes for members weighing how far to lean into alternative payment systems, and helps explain why BRICS initiatives are framed as diversification and efficiency rather than a currency challenge to the dollar.

The New Development Bank

Less prominent than de-dollarization headlines but arguably more concrete is the New Development Bank (NDB), BRICS' equivalent of the World Bank. It has approved tens of billions of dollars in financing across energy, transport, water, and climate-related infrastructure since its founding, and has been increasing the share of lending issued in members' domestic currencies, targeting roughly a third of its loan book. For borrowers in smaller or credit-constrained economies, an additional lender with different terms than the IMF or World Bank changes the calculus of development financing, even though the NDB remains far smaller than its older counterparts.

Expansion and Its Economic Weight

Each new member shifts the bloc's economic profile in a distinct way:

- **Saudi Arabia and the UAE** add sovereign wealth and energy-export weight (Saudi Arabia's status remains diplomatically ambiguous — India lists it as a full member, while Saudi officials have described their own participation as an “invited country”).
- **Indonesia** contributes a large, fast-growing consumer economy in Southeast Asia.
- **Egypt and Ethiopia** extend the bloc's reach into African trade and infrastructure.
- **Brazil** anchors commodity trade and agricultural exports across Latin America.
- **The ten-country partner tier** — including Belarus, Kazakhstan, Malaysia, Nigeria, Thailand, and Vietnam — lets additional economies plug into BRICS payment and trade initiatives without full membership.

Scepticism Worth Taking Seriously

Coverage of BRICS' economic rise tends to run ahead of the underlying data. Trade and political interests among members frequently conflict outright — India and China remain regional and economic rivals even within the same bloc; Gulf members and Iran do not share the same read on regional security; Saudi Arabia's own delegation described itself as an “invited country” at the 2026 summit even as host India listed it as a full member. There is no unified BRICS fiscal or monetary policy and no mechanism to bind members to common action — and, per the reserve data above, no clear sign yet that the dollar's global dominance is meaningfully eroding at the aggregate level, whatever is happening in specific bilateral trade corridors.

The Bottom Line

What BRICS has built so far is less a rival to the existing economic order than a widening set of alternative channels — payment rails, a development bank, local-currency settlement options, and now a gold-settlement pilot — that give its members more room to makeover, particularly when Western sanctions or tariffs are on the table. That is probably the most accurate way to read its economic impact to date: not a new global financial system, but more off-ramps from the old one, built cautiously enough to avoid the 100%-tariff trigger Washington keeps threatening to pull.

R B BHANU

23691A0521

QUANTUM COMPUTING
FROM FRAGILE QUBITS TO RELIABLE QUANTUM COMPUTING

Introduction

Quantum computing is a Fastly evolving technology which uses the principles of quantum mechanics to process the information. Unlike classical computers, which are represented by 0 or 1, quantum computers are represented by qubits that can exist in superposition and can become entangled. These properties give quantum computers the potential to solve certain problems that are difficult for classical computers.

However, qubits are extremely sensitive to their surroundings. Noise, unwanted interactions, imperfect quantum gates and measurement errors can disturb their quantum states. This makes maintaining reliable quantum information one of the biggest challenges in building useful quantum computers. Quantum Error Correction (QEC) is a collection of techniques designed to detect and correct errors in quantum information without directly destroying the information being protected.

Why Do Quantum Computers Need Error Correction?

A classical bit can be copied and stored. If one-bit changes accidentally, classical error-correction techniques can detect the mistake and recover the original information.

Quantum information is more difficult to protect. A quantum state cannot simply be copied because of the no-cloning theorem. In order to that, measuring a qubit disturbs its quantum state.

Quantum errors can occur because of decoherence, environmental noise, imperfect gates and measurement errors. Two basic examples are the bit-flip error,

Where $|0\rangle \rightarrow |1\rangle$

and the phase-flip error, which changes the phase relationship of a quantum state.

Hence, a quantum computer needs a method of protecting quantum information while it is being processed.

How Does Quantum Error Correction Work?

The idea of QEC is to encode information from one logical qubit into several physical qubits. Instead of depending on one fragile physical qubit, information is distributed across a group of qubits.

For example, a simplified three-qubit bit-flip code can encode:

$$|0\rangle_L \rightarrow |000\rangle$$

$$|1\rangle_L \rightarrow |111\rangle$$

If one of the physical qubits changes, the pattern of the three qubits provides information about where an error may have occurred. Measurements called syndrome measurements can identify the error without directly measuring the logical quantum information.

Real quantum error correction is much more sophisticated because it must protect against different types of errors and

repeated errors during computation. Important approaches include Shor's 9-qubit code, Steane's 7-qubit code and surface codes.

Surface Codes and Logical Qubits

The surface code is one of the most promising methods used for quantum error correction. It arranges physical qubits in a two-dimensional pattern and repeatedly checks groups of nearby qubits. These checks, known as stabilizers, provide information about possible errors without directly disturbing the logical quantum state.

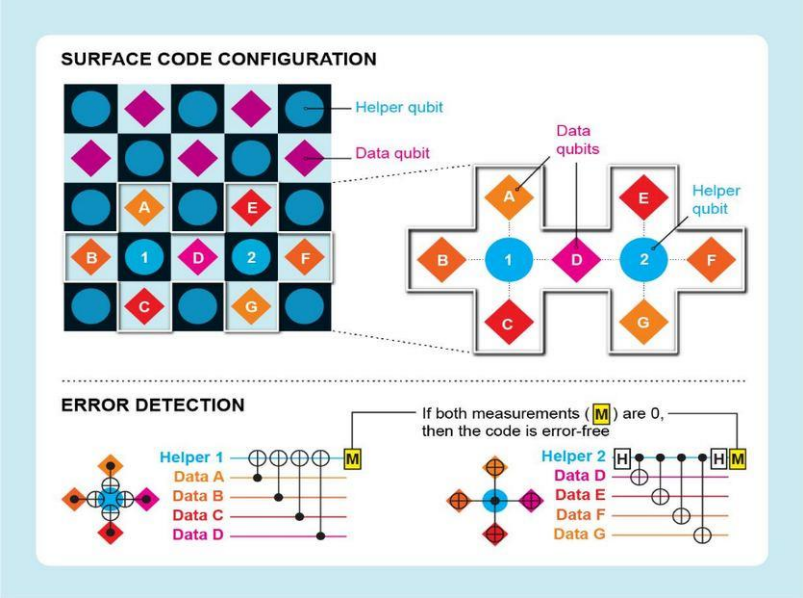
A key idea in the surface code is code distance. A larger code distance usually means using more physical qubits, but it also makes the logical qubit more resistant to errors.

For error correction to become more effective as the number of physical qubits increases, the error rate of the individual physical qubits must stay below a certain threshold. When the error rate is below this threshold, increasing the size of the code can gradually reduce the error rate of the logical qubit.

Recent Progress

A major milestone came from Google Quantum AI's Willow processor.

- In a Nature study published in 2025, researchers demonstrated surface-code quantum memories operating below the error-correction threshold. Their distance-7 logical memory used 101 qubits and achieved a logical error rate of about 0.143% per error-correction cycle. Increasing the code distance from 5 to 7 reduced the logical error rate by more



than a factor of two, demonstrating the desired trend of improving protection as the code becomes larger.

The experiment also demonstrated real-time decoding, which is important because error information must be processed quickly enough to keep up with the quantum computer. However, this does not mean that large-scale fault-tolerant quantum computing has already been achieved. Significant challenges remain in scaling the technology, reducing resource requirements and dealing with correlated errors.

Challenges and Future

The biggest challenge of QEC is overhead. Protecting one logical qubit can require many physical qubits. Some surface-code approaches may require hundreds or even thousands of physical qubits.

Other challenges include improving gate and measurement accuracy, reducing correlated errors, developing fast classical decoders and building hardware that can maintain quantum states for sufficiently long periods.

Researchers are therefore exploring improved surface codes, quantum low-density parity-check (qLDPC) codes, better decoding methods and lower-overhead fault-tolerant architectures. Recent research continues to investigate ways of reducing the number of physical qubits required for reliable logical computation.

Conclusion

Quantum Error Correction is one of the fundamental technologies required to transform fragile experimental qubits into reliable computational systems. Instead of trying to make every physical qubit perfect, QEC uses redundancy, syndrome measurements and carefully designed quantum codes to protect logical qubits from physical errors.

Recent experiments have demonstrated important progress toward operating below the error-correction threshold, but practical fault-tolerant quantum computers still require major advances in hardware, error rates, decoding and scalability. Ultimately, the success of quantum computing will depend not only on creating more powerful qubits, but on protecting quantum information well enough to perform long and reliable computations.

- **N. Ashraf Vali**
24691A0540

INDIA'S SEMICONDUCTOR AND AI REVOLUTION

Why chips are becoming the foundation of the next generation of computing



Artificial Intelligence has changed the importance of semiconductor technology. Modern AI applications require enormous computing power, which depends on powerful processors, GPUs, specialised AI accelerators and high-performance computing infrastructure.

As a result, semiconductors are no longer viewed only as components used in electronic devices. They have become a strategic technology resource.

India is increasingly building capabilities across the semiconductor ecosystem, including chip design, manufacturing, packaging, electronics and supporting infrastructure. These developments are closely connected with the country's growing ambitions in artificial intelligence and advanced computing.

The relationship between AI and semiconductors works in both directions. AI requires powerful chips to train and run complex models. At the same time, AI can assist semiconductor companies with chip design, optimisation, defect detection, predictive maintenance and manufacturing analysis.

The expansion of AI is also increasing demand for data centres. Large AI models require significant computing power, memory, networking and energy. Therefore, the growth of AI is creating demand not only for software engineers but also for semiconductor engineers, hardware designers and infrastructure specialists.

This trend creates new career opportunities for students in areas such as:

- VLSI and chip design
- Semiconductor engineering

- Embedded systems
- AI hardware
- Computer architecture
- Edge computing
- Hardware-software co-design

For computer science students, this development highlights an important change in the technology industry. Understanding software alone may not be enough to understand modern computing. Algorithms, AI models, processors and infrastructure are increasingly interconnected.

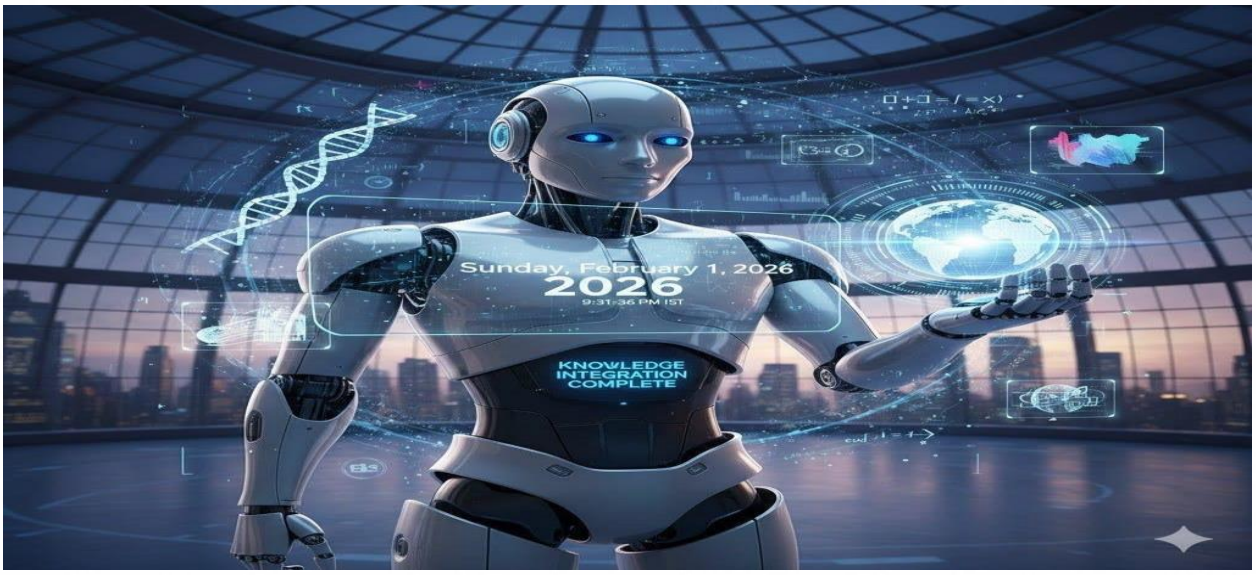
India's semiconductor development is therefore not simply about manufacturing chips. It is about creating the computing foundation for the next generation of AI and digital technologies.

Madaparthi Yaswanth Sai Ganesh

25695A0558

HUMANOID ROBOTS: WHEN AI ENTERS THE PHYSICAL WORLD

The convergence of artificial intelligence, robotics and computer vision



Artificial Intelligence has traditionally operated mainly in the digital world. Today, that is changing rapidly. AI is increasingly being integrated with robotics, allowing intelligent systems to perceive and interact with the physical environment.

One of the most visible developments is the rise of humanoid robots.

Humanoid robots are designed with a human-like body structure so that they can potentially operate in environments created for people. They combine multiple technologies, including artificial intelligence, computer vision, sensors, machine learning, natural-language processing and robotic control systems.

One emerging concept is physical AI. Instead of simply generating text or images, physical AI systems must understand their surroundings and take appropriate physical actions. A robot may need to recognise an object, determine its location, plan a movement and safely manipulate it.

Humanoid robots are being explored for applications in manufacturing, logistics, inspection, healthcare and hazardous environments. Their ability to operate in human-designed spaces could make them useful for tasks that are repetitive, physically demanding or potentially dangerous.

However, several challenges remain. Robots must be able to operate safely around humans and respond to unpredictable situations. Battery capacity, computing power, mechanical reliability and cost are also important limitations.

For computer science students, humanoid robotics provides an excellent example of technological convergence. It brings together:

Artificial Intelligence + Computer Vision + Machine Learning + Robotics + IoT + Embedded Systems

The future may not necessarily involve robots replacing humans. A more practical possibility is human-robot collaboration, where robots perform repetitive or dangerous tasks while humans provide creativity, judgement and supervision.

Humanoid robotics therefore represents a major step in the evolution of AI—from systems that understand digital information to systems that can interact with the real world.

Arveti Yamini

25695A0557

SOVEREIGN CLOUD: WHY DATA AND AI INFRASTRUCTURE ARE BECOMING STRATEGIC

Cloud computing has transformed the way organisations store information and operate applications. Businesses, universities, governments and technology companies increasingly depend on cloud infrastructure for everyday digital services.

However, as cloud computing becomes more important, another issue is receiving greater attention: where is data stored, who controls it and under which laws is it managed?

This has led to growing interest in sovereign cloud.

A sovereign cloud focuses on stronger control over data storage, processing, management and access. It can help organisations meet national or regional requirements related to privacy, cybersecurity and data governance.

The issue is particularly important for Artificial Intelligence. Modern AI systems require large volumes of data and significant computing resources. Sensitive information may need to remain within a particular geographical or legal jurisdiction.

Sovereign cloud does not necessarily mean that organisations must build and operate their own data centres. Hybrid-cloud and multi-cloud approaches can allow organisations to select different environments for different types of workloads.

For example, highly sensitive information may require a tightly controlled environment, while less sensitive applications can continue to use conventional public-cloud infrastructure.

This trend creates opportunities for computer science professionals in:

- Cloud security
- Cybersecurity
- Data governance
- Distributed systems
- AI infrastructure
- Privacy engineering

- Cloud architecture

As artificial intelligence becomes integrated into business and public services, data and computing infrastructure are increasingly becoming strategic assets.

The future of cloud computing will therefore not simply be about more computing power. It will increasingly be about having the right infrastructure, in the right location, with the right security and governance.



Utla Greeshma

24691A05E8

THE ARCHITECTURE OF QUANTUM REGIONS: BUILDING THE DEEP-TECH INFRASTRUCTURE OF TOMORROW

1. The Global Market Trajectory

Quantum computing is rapidly moving from research laboratories toward commercial deployment. The global quantum computing market is estimated at around USD 4.99 billion, with strong growth driven by investments from governments and technology companies.

Large enterprises are exploring quantum computing for logistics optimization, molecular simulation, financial analysis, and complex problem solving. Cloud-based access is also allowing organizations to experiment with quantum processors without owning expensive hardware.

2. The Rise of Quantum Technology Hubs

Quantum development is increasingly concentrated in specialized geographic regions where universities, industries, governments, and infrastructure providers work together.

North America:

North America has a major share of the quantum computing market, supported by companies such as IBM, Google, and Amazon Web Services. Research centers and universities are developing quantum processors, networking technologies, and supporting infrastructure.

Asia-Pacific:

Countries in the Asia-Pacific region are making significant investments in quantum technologies. India's National Quantum Mission (NQM) supports specialized Thematic Hubs and research collaborations. India is also developing quantum communication networks aimed at enabling secure long-distance communication.

Hybrid Computing:

Quantum processors are expected to work alongside classical computers rather than completely replace them. A notable example is the integration of an IBM Quantum System Two with the Fugaku supercomputer at RIKEN, Japan, enabling quantum and classical systems to work together on advanced workloads.

3. Re-Engineering the Physical Infrastructure

Quantum networks require different infrastructure from conventional communication networks. Classical networks can amplify optical signals, but quantum information cannot simply be copied because of the No-Cloning Theorem. Quantum networks therefore use techniques such as entanglement swapping, where intermediate nodes help establish entanglement between distant locations without directly copying the quantum state.

Another major concern is “Harvest Now, Decrypt Later” (HNDL). Attackers may collect encrypted information today and attempt to decrypt it in the future using powerful quantum computers. Algorithms such as Shor's Algorithm could threaten current RSA and ECC encryption.

To address this risk, organizations are adopting Post-Quantum Cryptography (PQC), which uses cryptographic methods designed to resist attacks from both classical and quantum computers.

4. Market Composition

The quantum computing ecosystem can be broadly divided into three major layers:

- Hardware: Quantum processors require highly specialized equipment, including cryogenic systems, control electronics, and sophisticated error-management technologies.
- Cloud Access: Quantum-as-a-Service (QaaS) allows users to access quantum processors remotely through platforms such as IBM Quantum, AWS Braket, and Microsoft Azure Quantum.
- Software and Services: This includes quantum algorithms, programming tools, error-correction techniques, compilers, and consulting services.

This structure means that opportunities in quantum technology are not limited to physicists. Computer science, cybersecurity, software engineering, electronics, and cloud computing all have important roles.

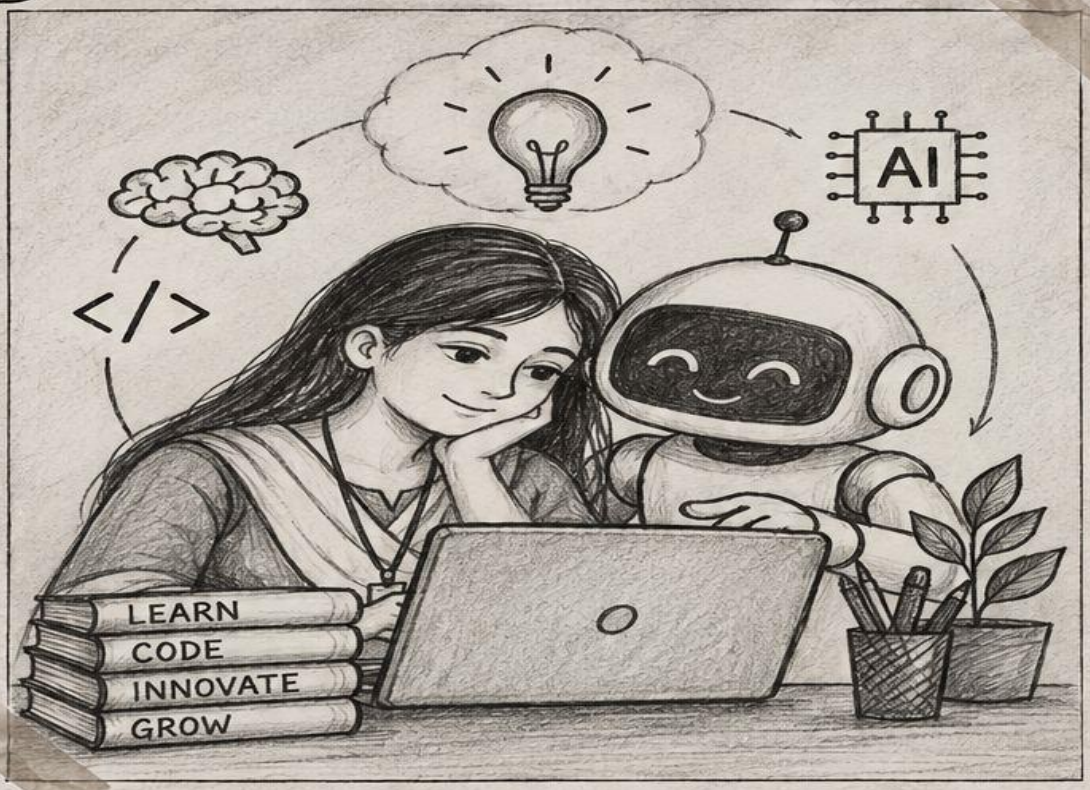
5. Opportunities for Next-Generation Engineers

The growth of quantum infrastructure is creating demand for professionals with interdisciplinary skills:

- Quantum Software Engineers: Develop quantum programs using tools such as Qiskit and Cirq, and design software that connects high-level applications with quantum hardware.
- Post-Quantum Cybersecurity Analysts: Help organizations migrate existing security systems to post-quantum cryptographic algorithms and protect sensitive information against future quantum attacks.
- Cryogenic and Microwave Engineers: Design the specialized hardware, control systems, and low-temperature environments required to operate quantum processors.

Konangi Harshitha

24691A05H9



Good Ideas Take Time

Same Mind Greater Possibilities



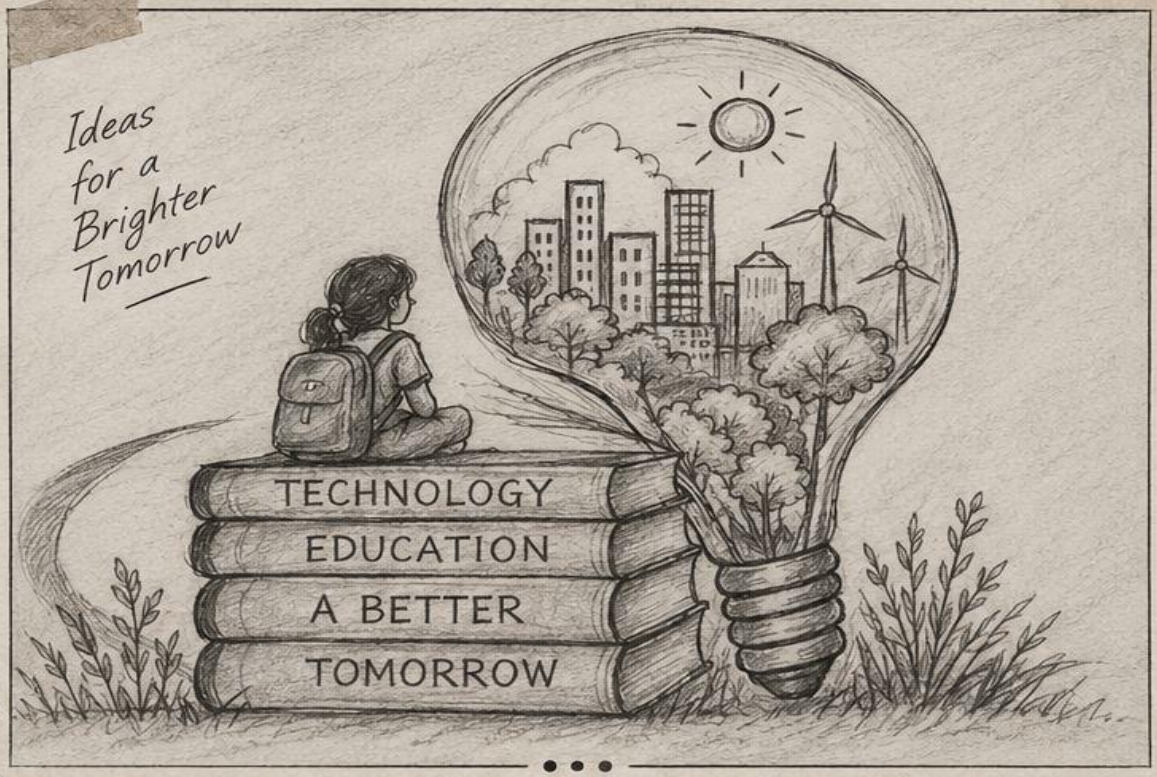
Just a Human Trying My Best

Feel Think Heal Evolve

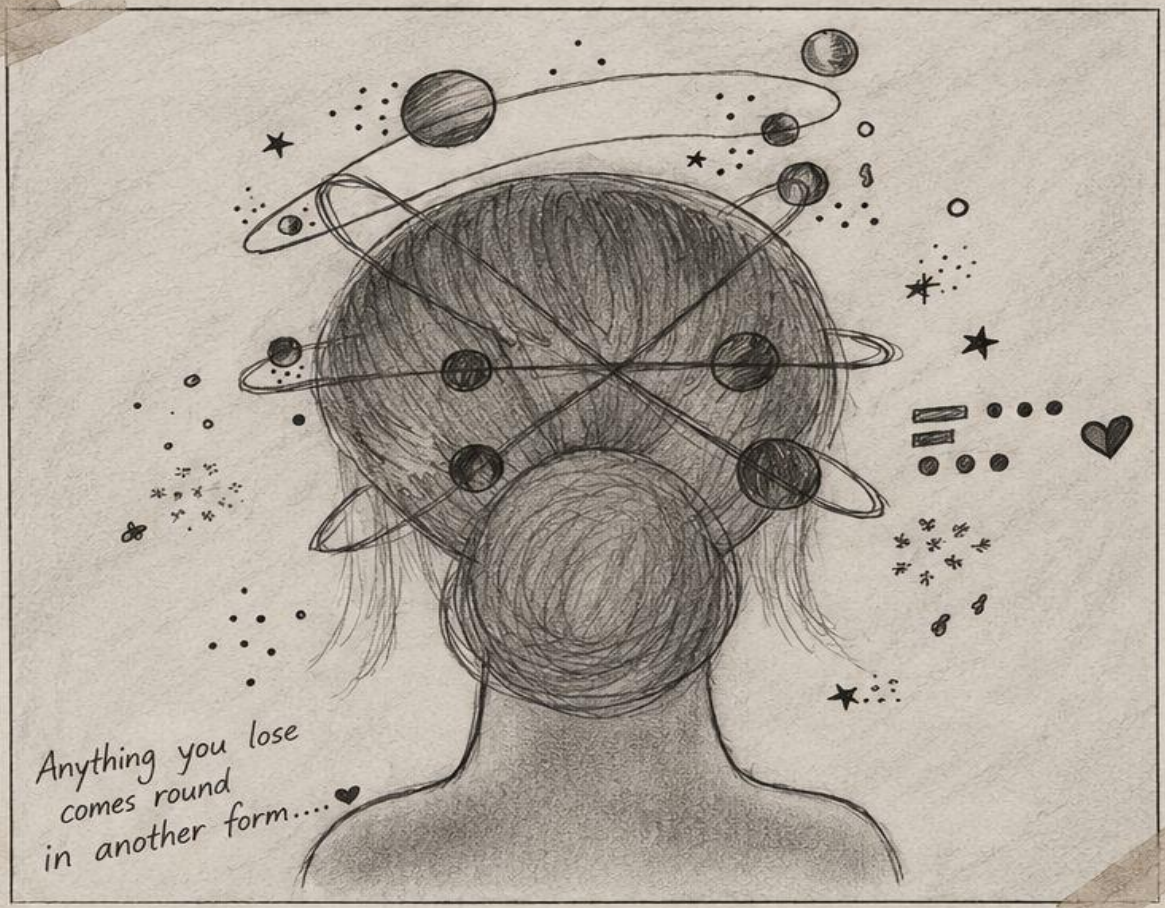
Art By -

KETHA GOWTHAMI

24691A05E6



SAME MIND
GREATER POSSIBILITIES



Art By -
P.HASINI
24691A05I0

Students Editors

BHOJANAPU DEVA RAJ – 25695A0514

Faculty Editors

Dr. M. SREEDEVI,
Professor & HOD
Department of CSE

Mrs. P. JAYASELVI,
Assistant Professor
Department of CSE

