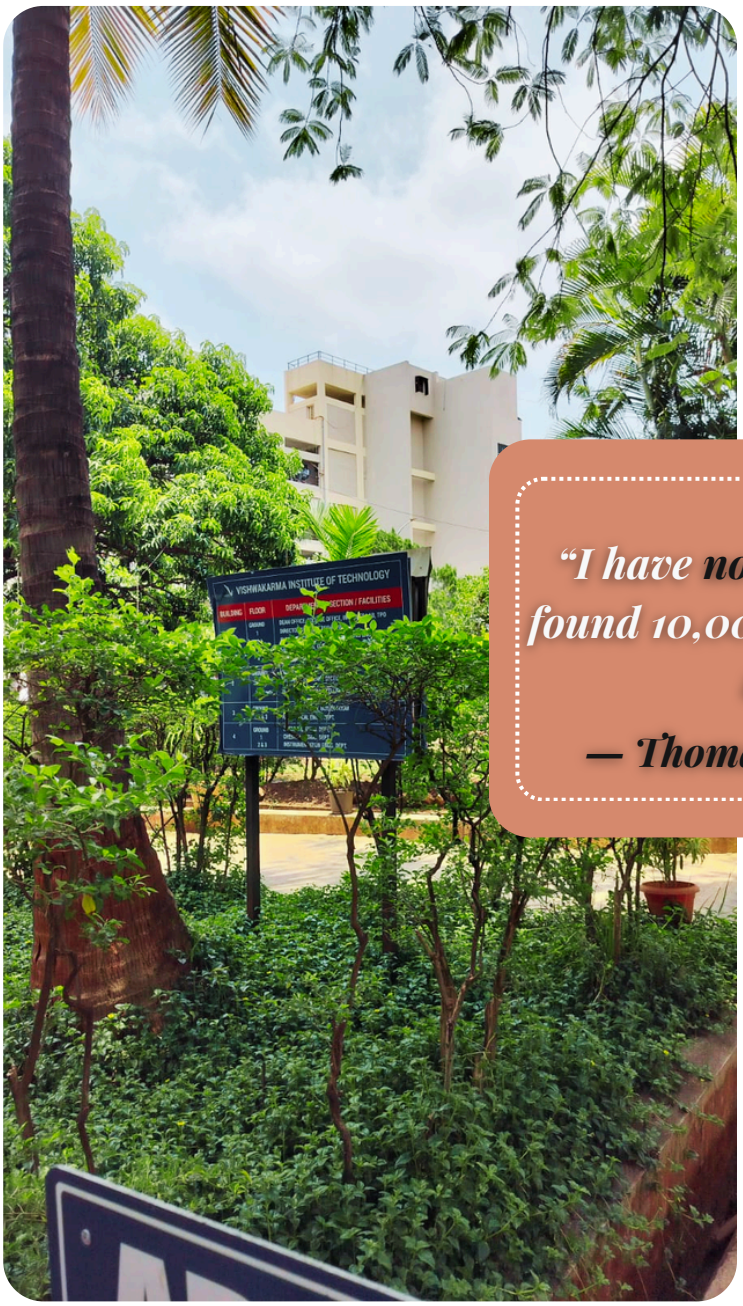
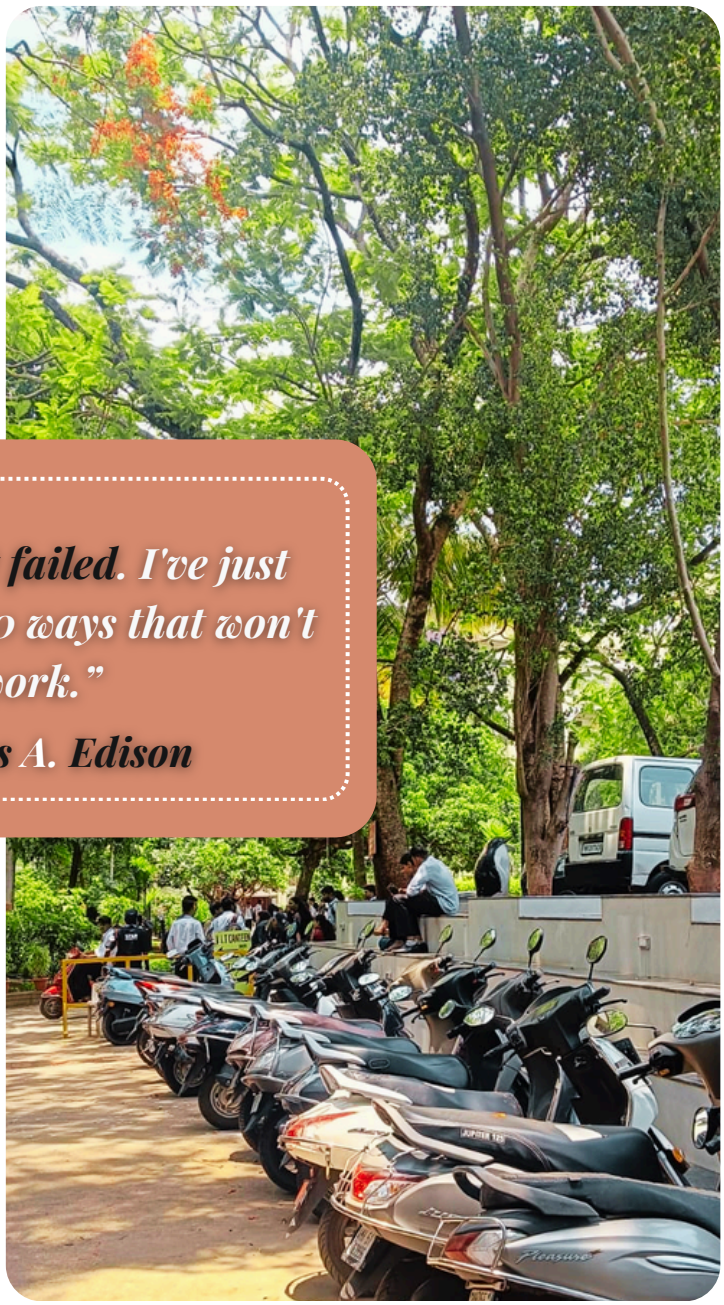
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE

Monthly Awareness Bulletin

ISSUE 2.10 June 2026

AI&DS INSIGHTS





"I have not failed. I've just found 10,000 ways that won't work."

— Thomas A. Edison

Achievement Spotlight

National-Level Achievement in Artificial Intelligence

We are delighted to celebrate the outstanding achievement of Mr. Pranav Doshi, a B.Tech Semester VIII (Artificial Intelligence & Data Science) student, who secured 1st Prize at Semtech's Pune AI Hackathon 2026, a prestigious National-Level Technical Hackathon held on 16–17 April 2026.

Competing against talented participants from institutions across the country, Pranav demonstrated exceptional innovation, technical proficiency, and problem-solving skills in the field of Artificial Intelligence. His AI-based solution impressed the judges with its creativity, practical impact, and technical excellence.

Achievement Highlights

- Position Secured: 1st Prize
- Event: Semtech's Pune AI Hackathon 2026
- Date: 16–17 April 2026
- Level: National-Level Technical Competition
- Cash Prize: ₹10,000
- Student: Pranav Doshi
- Program: B.Tech (Artificial Intelligence & Data Science)

This remarkable accomplishment reflects Pranav's dedication, creativity, and commitment to technological innovation. His success not only brings honor to the institution but also serves as an inspiration to fellow students aspiring to excel in Artificial Intelligence and emerging technologies.

The institute extends its heartfelt congratulations to Pranav Doshi on this outstanding achievement and wishes him continued success in all his future endeavors.

Student Article

Your Data Is Already Stolen — You Just Don't Know It Yet

Every message you've ever sent, every password you've ever typed, every transaction you've ever made — is protected by mathematics that a quantum computer could shatter. And adversaries may already be collecting it.

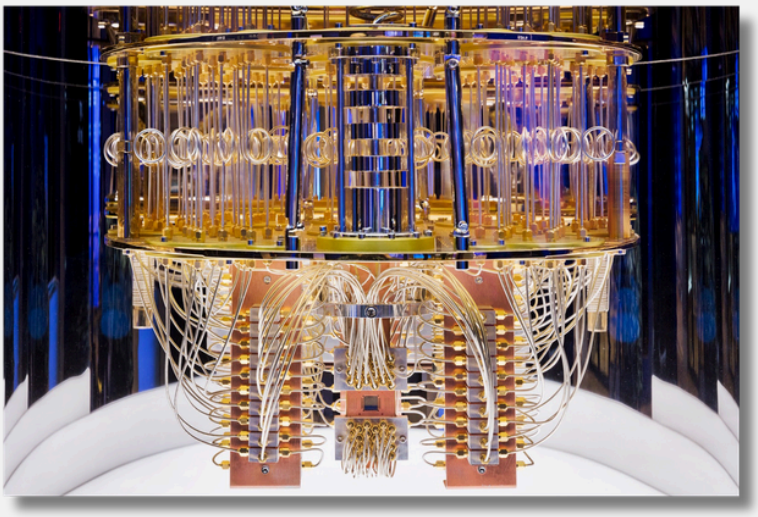
What Quantum Computing Actually Does to Encryption:

Right now, a copy of your encrypted data may be sitting in a server somewhere — patiently waiting. Not for a hacker to crack it. Not for a weak password. Waiting for a quantum computer. This strategy, known as "Harvest Now, Decrypt Later," is not science fiction. It is an active, documented threat and the clock started ticking before most of us even knew what a qubit was.

Think about the last time you opened your banking app, sent a private message, or submitted an assignment on your college portal. Every one of those actions was protected by mathematical locks called RSA and Elliptic Curve Cryptography (ECC); systems so hard to break that even the fastest classical computers would need millions of years. We built the modern internet on that assumption. For decades, it held. Quantum computers are approaching a threshold where it stops holding.

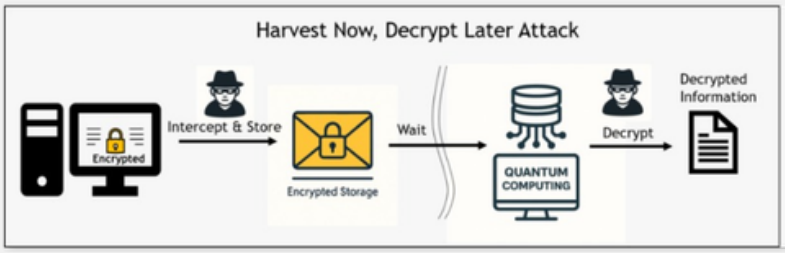
RSA's strength comes from a simple asymmetry: multiplying two large prime numbers is trivially easy, but factoring the result back is extraordinarily difficult. In 1994, mathematician Peter Shor proved that a sufficiently powerful quantum computer could factor those numbers exponentially faster, what takes a classical computer millions of years could take a quantum computer hours. Shor's Algorithm didn't just threaten RSA. It threatened ECC, Diffie-Hellman, and essentially every public-key system protecting the modern internet.

Quantum computers exploit superposition, existing in multiple states simultaneously and entanglement to evaluate enormous numbers of possibilities in parallel. IBM's latest Nighthawk processor has reached 120 qubits, and cracking RSA-2048 may still require far more. But progress is accelerating. Three research papers published between May 2025 and March 2026 reduced the estimated qubits needed from 20 million to potentially as low as 100,000. The goalposts are moving faster than most people realise and adversaries are not waiting for the computers to exist before they act.



The Attack Already Underway:

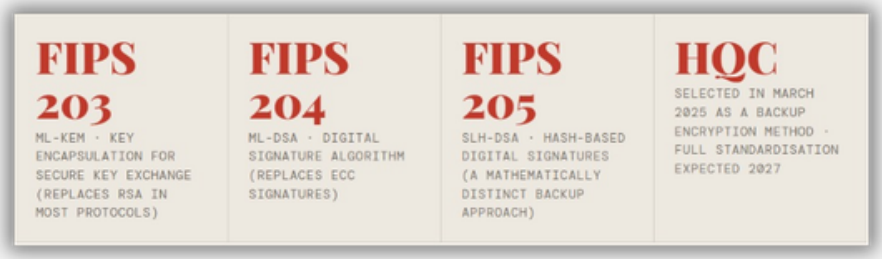
Nation-state actors are intercepting and storing encrypted data today, diplomatic communications, corporate secrets, healthcare records; with the explicit plan to decrypt it once quantum computers mature. The breach happens now. The damage surfaces years later. The US Federal Reserve published a 2025 research paper analysing this "Harvest Now, Decrypt Later" (HNDL) threat to financial networks. CISA has issued public warnings. Palo Alto Networks documented that the fastest attackers reached data exfiltration in just 72 minutes in 2025. This is a present-day, operational risk — not a future one.



The Race to Build New Locks:

NIST spent nearly a decade running an international competition to find quantum-resistant encryption. In August 2024, it finalised three Post-Quantum Cryptography (PQC) standards built on lattice mathematics and error-correcting codes that quantum computers cannot efficiently break: FIPS 203 (replaces RSA for key exchange), FIPS 204 (replaces ECC for digital signatures), and FIPS 205 (a mathematically distinct backup). A fourth standard, HQC, was selected in 2025.

The NSA has mandated all new US National Security Systems be quantum-safe by January 2027. Google's internal deadline is 2029. And yet, as of early 2026, only 38% of organisations are taking any meaningful action.



What This Means for CS/AIDS Students:

This is not a distant policy problem: it lands in your career. Every application you build will need to consider cryptographic agility: the ability to swap encryption algorithms like a library dependency rather than rebuilding from scratch. This is already a hiring requirement in security-adjacent roles.

NIST's post-quantum standards use genuinely interesting CS mathematics — lattice cryptography, hash-based signatures, code-based systems — actively implemented in open-source libraries like liboqs that you can explore today. The same quantum mechanics threatening our encryption is also accelerating drug discovery and machine learning. The machine that breaks the lock is the same machine that could change medicine.

Conclusion:

Quantum computing is not arriving with sirens and warnings, it is arriving quietly, in server rooms and research labs, while the data it will one day unlock is already being collected. The mathematics that has silently protected every login, every transaction, and every private conversation for the past three decades is not broken yet. But the countdown has started, and the people setting that countdown are not waiting for the rest of us to catch up. As CS students standing at the exact intersection of this shift, we have a rare and uncomfortable advantage, we understand enough to act before the problem becomes visible to everyone else. The new locks are being built. The question is whether we will be among the people building them, or among those still assuming the old ones hold.

Sources: NIST PQC Standardization (2024) · US Federal Reserve HNDL Working Paper (2025) · Palo Alto Networks Unit 42 Report (2026) · IBM Quantum Roadmap (2025–26) · CISA Quantum Preparedness Guidelines

SRUSHTI ROKADE
SY AIDS E

Faculty Article

Current Trends, Future Scope, and Career Opportunities of Artificial Intelligence in Agriculture

Sheela Chicnhmalatpure
Assistant Professor,
AIDS , VIT Pune

Artificial Intelligence (AI) is revolutionizing modern agriculture by enabling farmers to make smarter and more efficient decisions. Recent advancements in AI-powered precision farming use data collected from drones, satellites, sensors, and IoT devices to monitor crop health, soil conditions, and weather patterns in real time. AI-based image recognition systems can detect plant diseases, pest infestations, and nutrient deficiencies at an early stage, allowing timely intervention and reducing crop losses. Smart irrigation systems powered by AI optimize water usage by analyzing soil moisture and weather forecasts, contributing to sustainable farming practices. These innovations are helping farmers increase productivity while minimizing the use of resources such as water, fertilizers, and pesticides.

The future scope of AI in agriculture is vast and promising. Emerging technologies such as autonomous tractors, AI-driven crop prediction models, digital twins of farms, and climate-smart agricultural systems are expected to transform the farming sector. AI will play a crucial role in ensuring food security for the growing global population while promoting sustainable resource management. The increasing adoption of AI in agriculture is also creating exciting career opportunities for students and professionals. Careers such as Agricultural Data Scientist, AI Engineer, Precision Agriculture Specialist, Drone Analyst, Agritech Researcher, Robotics Engineer, and Smart Farming Consultant are gaining significant demand worldwide. As agriculture becomes more technology-driven, professionals with expertise in AI, machine learning, data analytics, IoT, and agricultural sciences will be at the forefront of innovation, contributing to a smarter, more productive, and environmentally sustainable future.

OUR TEAM

Dr Minal Barhate

Jatin Shende
SY AI&DS -E

Vedank Shinde
SY AI&DS-F

For Feedback
and Query,
Scan this: