



KAS

KONGU ARTS AND SCIENCE COLLEGE

TRANSFORM YOURSELF



**DBT
SPONSORED STAR DEPARTMENT**


DEPARTMENT OF COMPUTER SCIENCE (UG)


***IT UNLIMITED MAGAZINE
(A BI-MONTHLY BONANZA)***

**108TH
ISSUE**

Dec 2025 - Jan 2026

**CYBER CREWS
STUDENTS ASSOCIATION**

 <https://www.kasc.ac.in>

 itunlimitedmagazine@gmail.com



EDITORIAL BOARD

PATRON

Thiru. P. Sachithanandan

Correspondent

EDITORIAL ADVISER

Dr.H.Vasudevan M.Com., M.Phil., Ph.D., MBA., PGDCA., SLET.,

Principal

EDITORIAL IN CHIEF

Prof.P.Ramesh M.Sc., M.Phil.,

HOD

FACULTY EDITOR

Mr.S.Jaganathan M.C.A., M.Phil.,

Assistant Professor

STUDENT EDITORS

Kapil Sanjhiv. A.S

Krishnakumar. S

Kamesh M

Guru Shankar. P.J

Dhanusri.U

Sri Janani.P

G.P. Viswaknithin

Abisree. A.P

Sasmitha Karthikeyan

Anusree.k

Sujit

Srinith K

Dharani S B

Dharshini S

Subiksha Sundaram

Kanishka M

III- B.Sc CS-A

III- B.Sc CS-A

III- B.Sc CS-A

III- B.Sc CS With DA

III- B.Sc CS With DA

III- B.Sc CS With DA

II- B.Sc CS-A

II- B.Sc CS-A

II- B.Sc CS-A

II- B.Sc CS-B

II- B.Sc CS-B

I- B.Sc CS-B

I- B.Sc CS-B

I- B.Sc CS-B

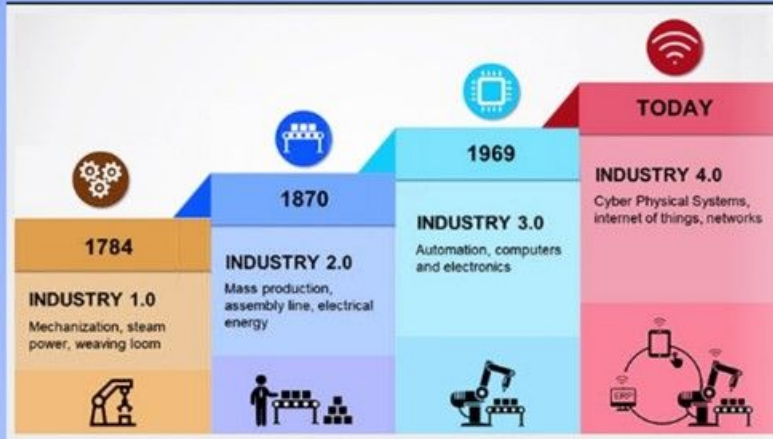
I- B.Sc CS With DA

I- B.Sc CS With DA

TABLE OF CONTENTS

- 02** XR (EXTENDED REALITY)
- 04** PERVASIVE COMPUTING
- 06** CRYPTOGRAPHY
- 08** FUNCTIONAL ROBOTS
- 10** TRANSFORMING REALITY
- 12** THE ETHICS OF AI
- 15** LEARN A TOOL
- 17** REVIEW BOX
- 18** MIND PUNCH
- 19** IT VITA
- 20** FAMOUS AND FAVOURITES
- 21** ANSWERS

THOUGHTS OF THE ISSUE



Remember

Free advice

PROVIDE TECHNICAL ADVICE

- There are three main areas in which project teams need advice:
 - Understanding the intent and meaning of an organization's policies, procedures, standards and guidelines
 - Determining the best method for using the organization's hardware and software
 - Assessing the impact of the application being developed on other applications currently in operation or under development

When you enter a room and forget what you were going to do



Just For Fun

Message

"Just for the record darling, not all positive change feels positive in the beginning."

—S. C. Lurie

Digital Payment System



In an era where digital interactions define everyday life, the sight of hefty wallets bulging with cash has become a rarity. From the moment you tap your smartphone at a street-side tea stall to the instant scan of a merchant's QR code at a high-end boutique, a symphony of sophisticated technologies works behind the scenes to ensure that each transaction is seamless, secure, and virtually instantaneous. As you ride the wave of this cashless revolution, it's worth exploring the key components—some decades old, some cutting-edge—that collectively underpin the global digital payments ecosystem.

Near the foundation of every digital transfer lies robust **Internet and Mobile Connectivity**. Fast, reliable networks—whether 4G/5G cellular, Wi-Fi, or fiber-optic broadband—serve as the nervous system, relaying transaction data between your device, payment platforms, banks, and clearing houses in real time. Without this connectivity, scanning a QR code or tapping an NFC-enabled card reader would be impossible; every millisecond of latency and every dropped packet could lead to delays or failed transactions. Today's networks, with speeds measured in gigabits per second and latencies in mere milliseconds, enable the instantaneous push and pull of authorization requests, fund holds, and settlement confirmations that make cashless payments feel frictionless.

One of the most visible enablers of the contactless era is **Near Field Communication (NFC)**. Embedded in virtually all modern smartphones and many payment cards, NFC uses electromagnetic induction to exchange data when two devices come within a few centimeters of each other. Its brevity of range

is a virtue: it guards against eavesdropping, theft, and unintended transactions. The technology has revolutionized checkout lines—quick taps complete purchases for coffee, groceries, transit fares, and more—while secure elements within NFC chips store tokenized payment credentials so that your actual card number never leaves the device.

Meanwhile, **QR Code Payments** have democratized digital acceptance for merchants of all sizes. A simple black-and-white square carries encrypted merchant or personal account information; customers scan it through their banking or wallet apps, enter the amount owed, and confirm with a PIN or biometric. For small vendors—from street hawkers to neighborhood tea shops—printing a customizable QR code is a cost-effective strategy to capture digital payments without investing in expensive hardware. Across emerging markets, QR codes have propelled financial inclusion by making digital wallets accessible on even the most basic smartphones.



India's **Unified Payments Interface (UPI)** has set a global standard for interoperability and convenience. Developed by the National Payments Corporation of India, UPI links multiple banks through a single app layer, enabling peer-to-peer and peer-to-merchant transfers using a Virtual Payment Address (VPA) instead of cumbersome account numbers and IFSC codes. Real-time settlements, request-to-pay features, built-in mandates for recurring billing, and integration with utility and financial services (including instant IPO subscriptions) have made UPI a

one-stop digital finance hub. Its open architecture has inspired similar initiatives worldwide.

When you shop online, your checkout funnel leads through one or more **Payment Gateways and APIs**—secure portals that orchestrate the authorization, authentication, and settlement phases of a transaction without exposing your raw card details. Gateways leverage SSL/TLS encryption, PCI DSS compliance, and advanced tokenization to protect sensitive data in transit. APIs connect e-commerce sites, mobile apps, and in-store systems to issuing banks, acquiring banks, and card networks, translating customer-facing actions (like entering a card number) into standardized settlement instructions that financial institutions understand.

Underpinning user-friendly logins and approvals is **Biometric Authentication**. As fingerprint readers, facial-recognition cameras, and even iris scanners become standard on smartphones, digital wallets integrate these modalities to confirm that the person initiating a transaction is indeed the authorized user. Biometrics add a robust second factor beyond “what you know” (passwords/PINs) and “what you have” (cards or devices), delivering both enhanced security and smoother customer experiences—no need to punch in lengthy passcodes for everyday micro-payments.

To defend against data breaches and unauthorized use, **Tokenization and Encryption** work hand-in-glove. Tokenization scrambles a real card number into a surrogate alphanumeric string that’s useless if intercepted, while encryption ciphers data in transit so that only endpoints with the correct keys can decrypt it. Together, they ensure that card-on-file breaches and MITM (man-in-the-middle) attacks cannot expose actual payment credentials, drastically reducing the risk and fallout of potential hacks.

Behind every approval or decline message, **Artificial Intelligence (AI) and Machine Learning (ML)** models sift through mountains of transactional data to identify

patterns, flag anomalies, and predict fraudulent behavior. By continuously learning from user habits—preferred merchants, typical purchase amounts, locations, and time-of-day trends—AI engines can intervene automatically when a transaction deviates sharply from the norm, sending alerts, requesting additional verification, or outright blocking suspicious activity. Over time, this adaptive risk scoring becomes more accurate and less intrusive, balancing security with customer convenience.

Finally, **Cloud Infrastructure** provides the elastic backbone for today’s digital payment platforms. From global content delivery networks (CDNs) that cache static assets closer to users, to containerized microservices handling API requests, to distributed databases logging transaction ledgers, the cloud offers the resiliency, scalability, and geographic redundancy that brick-and-mortar data centers struggle to match. In the event of localized outages, cloud-based failover systems redirect traffic seamlessly, ensuring uninterrupted payment flows and rapid disaster recovery.

Together, these technologies form an intricate web that underlies every swipe, scan, tap, and click in our cashless world. As connectivity speeds, security protocols, and intelligent risk-mitigation techniques continue to evolve, digital payments will grow ever faster, safer, and more intuitive—ushering in an era where money moves as effortlessly as thought itself.

Quantum Computing – The Future

Quantum computing has journeyed from an abstract curiosity in theoretical physics to one of the most exciting technological frontiers of our time. At its heart lies the qubit—a quantum analog of the classical bit that, thanks to superposition, can exist in a simultaneous blend of 0 and 1, and through entanglement can become inextricably linked with fellow qubits. This extraordinary behavior unlocks computational pathways that classical machines can only dream of, enabling certain complex problems to be tackled in seconds rather than millennia.

The story begins in the cradle of quantum mechanics, when pioneering 20th-century physicists unraveled the counterintuitive laws governing atoms and sub-atomic particles. Yet it wasn't until the 1980s that a radical proposal emerged: Richard Feynman observed that simulating quantum systems on classical hardware is inherently inefficient, and he challenged the community to build a “quantum simulator” powered by the same rules it sought to emulate. Soon after, David Deutsch formalized the concept of a universal quantum computer—one capable of executing any algorithm that respects quantum laws.

Through the 1990s, theory leapt ahead of practice. Peter Shor's algorithm for factoring large integers exposed a glaring vulnerability in modern cryptography, showing that a sufficiently powerful quantum computer could shatter RSA and ECC systems. Lov Grover followed with a quantum search protocol that reduced search times in unsorted databases from $O(N)$ to $O(\sqrt{N})$. These blueprints galvanized hardware researchers, but the path was treacherous: qubits are delicate, vulnerable to environmental noise that introduces errors and destroys quantum coherence.

Early 21st-century efforts yielded promising qubit platforms: trapped ions suspended in electromagnetic fields, superconducting loops chilled to near absolute zero, and exotic topological states that promise built-in error resistance. D-Wave Systems even commercialized a quantum annealer optimized for solving specific optimization tasks—

arguably the first glimpse of quantum technology in industry. Then, in 2019, Google's 53-qubit “Sycamore” processor achieved a landmark demonstration of quantum supremacy, performing a contrived sampling computation in 200 seconds that would take the world's fastest supercomputer thousands of years to mimic.



Today, quantum computing sits at a thrilling inflection point. IBM, Microsoft, Amazon, Intel, and myriad startups are racing to scale qubit counts, improve coherence times, and develop fault-tolerant architectures. Roadmaps from IBM target hundreds of qubits in the next few years, coupled with rising “quantum volume,” a holistic measure of a machine's error rates, connectivity, and gate fidelity. At the software layer, quantum SDKs and languages—Qiskit, Cirq, Q#—have democratized access, while cloud-hosted simulators and real machines let students and developers experiment in the quantum realm from anywhere on Earth.

The promise of quantum advantage—practical, real-world speedups over classical methods—looms on the horizon. Cryptographers prepare by designing post-quantum algorithms immune to Shor's onslaught. Chemists and materials scientists envision quantum engines that model molecular interactions with precise fidelity, revolutionizing drug discovery and novel material design. Financial institutions explore quantum portfolio optimization, and climatologists dream of simulating global weather systems at quantum detail to better predict and mitigate climate change.

Overcoming Technical Challenges Despite tremendous strides, quantum hardware still grapples with fragility. Qubits decohere rapidly—losing their quantum state in

microseconds—so maintaining coherence long enough to perform deep calculations demands extreme isolation from heat, vibration, and electromagnetic interference. Superconducting circuits require dilution refrigerators chilling to millikelvins, while trapped-ion setups rely on ultra-high vacuum and precise laser control. Scaling from a few dozen qubits to the hundreds or thousands needed for practical error correction multiplies these engineering hurdles. Control electronics must generate millions of high-precision microwave or laser pulses, all synchronized to sub-nanosecond accuracy.

Towards Fault-Tolerant Quantum Computation Natural qubits are imperfect: every gate, measurement, or idle period introduces a small probability of error. Quantum error-correcting codes—like the surface code—encode a single “logical” qubit into dozens or even hundreds of physical qubits, detecting and correcting errors on the fly. While the overhead seems daunting, it’s a necessary trade-off to achieve truly fault-tolerant operations. Progress in materials science, fabrication techniques, and low-noise electronics steadily drives down physical error rates, lowering the number of physical qubits required per logical qubit. Meanwhile, alternative architectures—such as topological qubits leveraging exotic anyon braiding—promise intrinsic resilience, potentially slashing overheads. Achieving threshold error rates below $\sim 1e-3$ is the immediate milestone toward constructing small logical qubit arrays that can run scaled demonstrations of real-world algorithms.

Building the Quantum Ecosystem Hardware advances alone won’t deliver quantum advantage—it must be matched by an ecosystem of software tools, algorithms, and a skilled workforce. Open-source frameworks like IBM’s Qiskit, Google’s Cirq, and Microsoft’s Q# SDK have democratized toolchains for circuit design, simulation, and benchmarking. Cloud-based quantum services let developers prototype hybrid quantum-classical workflows—delegating subroutines

such as variational eigensolvers to quantum processors while offloading classical optimization loops to conventional servers.



Ethical and Societal Implications As quantum computing nears practical utility, societies must grapple with its broader impact. Cryptographers are racing to deploy post-quantum encryption standards before Shor-style attacks become feasible. Industries from pharmaceuticals to finance are strategizing how to integrate quantum models into existing infrastructures. Policymakers face questions about equitable access: Will only large corporations leverage early quantum breakthroughs, worsening digital divides? How should governments regulate dual-use quantum technologies that can accelerate both medical research and advanced weapons design? Proactive frameworks for responsible quantum R&D—covering privacy, security, and workforce displacement—will be critical to harness quantum’s promise for the public good.

Combating Misinformation in the AI Age

DEEPPFAKE



In a world awash with video feeds and viral sound bites, deepfakes represent a ticking time bomb for truth itself. These hyper-realistic forgeries—videos, audio, or images crafted entirely by artificial intelligence—can depict people saying or doing things they never did, sowing confusion and distrust across social media, traditional news outlets, and private communications. Powered by deep learning architectures known as Generative Adversarial Networks (GANs), deepfake models pit two neural networks against each other—one creating increasingly convincing fakes, the other learning to spot telltale signs of manipulation. Over time, this digital arms race has produced forgeries so seamless that even experts struggle to tell real from synthetic.

At their core, deepfakes exploit the same statistical patterns that allow AI to recognize faces and voices. A “generator” network learns to produce an image of a target face superimposed on a source video, while a “discriminator” network examines the result and feeds back corrections. Through thousands of iterations, the generator refines its output until the discriminator can no longer distinguish fake from genuine. Voice deepfakes follow a similar path: given enough audio samples, an AI model captures vocal tone, cadence, and accent, then reanimates speech with any words you choose. The result is a new breed of digital imposter—utterly convincing, yet entirely devoid of authenticity.

The societal stakes of deepfakes are alarmingly high. A doctored clip of a political leader uttering inflammatory remarks can galvanize violence or disrupt election cycles.

Fabricated audio of a CEO authorizing a multi-million-dollar transfer can turn corporate treasuries into open vaults. Worse still, malicious actors can use synthetic pornographic videos to harass or ruin reputations—often targeting marginalized individuals who lack the resources to fight back. As deepfakes proliferate, people begin to doubt everything they see, a paradox known as the “liar’s dividend,” where even genuine evidence is dismissed as AI trickery.

Detecting deepfakes fast enough to prevent harm remains a monumental challenge. Early forensic tools hunted for glitches—warped pixels, inconsistent lighting, or unnatural blinking patterns—but modern models learn to eliminate these flaws. Watermarks and digital signatures can certify legitimate footage, yet require widespread adoption to be effective. Meanwhile, social platforms struggle to flag and remove harmful content at scale: by the time a deepfake is identified, it may already have spread to thousands or millions of viewers.

Combating this threat calls for a multi-pronged approach. On the technological front, researchers are refining detection algorithms that scrutinize biometric cues—subtle micro-expressions, heartbeat fluctuations captured in skin color, or audio-visual synchronization errors that escape human eyes. Emerging architectures employ federated learning: detection models improve by sharing anonymized insights across platforms without exposing user data. Blockchain-based provenance systems promise immutable records of a file’s origin, allowing viewers to verify authenticity through cryptographic stamps.

Legal and regulatory frameworks must evolve in parallel. Some jurisdictions have begun criminalizing the malicious creation and distribution of deepfakes, imposing fines and

prison terms for identity theft, defamation, or election interference. Yet laws often lag behind technology, and cross-border enforcement remains murky. International treaties or harmonized digital policy standards could close loopholes in global networks, ensuring that perpetrators cannot simply relocate to evade prosecution.



Equally crucial is fostering a culture of digital literacy. Educators and community leaders are integrating media-fluency modules into school curricula, training students to question the provenance of viral clips and to verify content through reliable news outlets or reverse-image searches. Public awareness campaigns remind everyday users not to become unwitting amplifiers of falsehoods: before clicking “share,” pause, reflect, and ask whether the footage you’re about to spread makes sense.

Finally, platform accountability must be non-negotiable. Social networks, video-sharing sites, and messaging apps hold immense power in controlling the flow of information. By deploying real-time scanning tools, user-reporting mechanisms, and transparent content-moderation reports, these companies can detect and quarantine deepfakes before they spiral out of control. Incentivizing industry alliances—such as coalitions that define open standards for media provenance—will also help smaller platforms integrate best practices without reinventing the wheel.

Collectively, these strategies can turn the tide against the deepfake dilemma. Technology, law, education, and corporate responsibility must align to safeguard the integrity of our

digital commons. Only then can we continue to reap AI’s benefits—creative filters, realistic avatars, immersive virtual worlds—without sacrificing our shared commitment to truth.

Beyond these measures, a sustainable defense against deepfakes hinges on fostering a resilient socio-technical ecosystem where technology, policy, and public engagement evolve in concert. Governments must allocate funding for independent labs and challenge grants that reward breakthroughs in real-time deepfake detection and provenance verification. At the same time, industry leaders should adopt standardized AI-transparency labels, disclosing the datasets and architectures behind generative models so regulators and researchers can trace—and penalize—misuse. Civil society organizations and newsrooms can collaborate on rapid-response “debunking networks” that analyze viral clips, fact-check their origins, and distribute corrections through trusted community channels. Educational institutions must go beyond one-off workshops to integrate ongoing media-literacy modules across disciplines, equipping students with mental “inoculation” strategies so that they instinctively question sensational content. Technologists, meanwhile, should explore adversarial watermarking—embedding invisible, tamper-resistant signals into authentic recordings that survive recompression and editing. International bodies like UNESCO and the Council of Europe can spearhead multilateral treaties to harmonize legal definitions of malicious deepfakes, clarify cross-border enforcement protocols, and protect citizens’ rights to both free expression and digital security. By weaving together technical safeguards, policy frameworks, and societal norms, we can outpace the threat of synthetic deception and fortify the very trust that digital media was designed to enhance.

AI - Friend or Foe?



AI's arrival in creative fields has sparked a debate as old as technology itself: is it a dazzling new partner in human expression or a stealthy threat to originality, fairness, and the very heart of artistry? Across writing, music, film, design, and visual arts, powerful neural networks now assist with composing melodies, drafting scripts, generating images, and even editing scenes. Tools like ChatGPT offer instant first drafts of articles or dialogue, while image generators such as DALL·E and Midjourney conjure entire landscapes from a few words. These tools accelerate workflows, spark ideas when inspiration runs dry, and democratize creation for those without formal training—yet they arrive with profound ethical questions about authorship, authenticity, and equity in the creative economy.

On one side of the argument, AI shines as a benevolent collaborator. By automating repetitive or technical tasks—from transcribing interviews and color-grading footage to filling in background harmonies or suggesting plot twists—AI frees human creators to focus on emotional depth, thematic coherence, and innovative leaps that machines cannot replicate. An independent game designer can now prototype art assets overnight, while a small press writer can iterate on several cover designs without hiring an illustrator. Musicians routinely use AI-driven mastering plugins to achieve radio-ready sound, and filmmakers leverage AI to storyboard entire sequences in minutes. In each example, AI magnifies human potential, lowers barriers to entry, and invites voices that might otherwise have remained silent to participate in the cultural conversation.

Yet on the other side lurk serious pitfalls. At the heart of the controversy lies the question of who truly owns an AI-generated masterpiece. Most generative models learn from massive datasets that include copyrighted music, paintings, articles, and photographs—often ingested without explicit permission or compensation to the original creators.

When an AI uses Van Gogh's brushstrokes or Beyoncé's vocal inflections as building blocks, does the credit belong to the user who typed the prompt, the engineers who built the model, or the countless artists whose work fueled its training? Without clear legal frameworks, AI-generated art risks trampling on intellectual property rights and undermining the livelihoods of the very creatives who inspired it.

The specter of job displacement intensifies these concerns. Freelance illustrators, editorial writers, graphic designers, and voice actors now compete with cost-effective AI alternatives that can produce basic deliverables in seconds. In crowded markets, clients may opt for an AI cover image or AI-written blog post simply because it fits a tighter budget, leaving human professionals scrambling to prove their unique value. This economic pressure threatens to hollow out mid-level creative roles and concentrate opportunity among those with either deep pockets to invest in proprietary AI or rare skills that machines cannot easily emulate.

Compounding the dilemma is the issue of bias and representation. AI models mirror the patterns in their training data, which often reflects historical and cultural prejudices. As a result, default image-generation algorithms may overrepresent certain skin tones, body types, or gender roles, while underrepresenting or stereotyping marginalized communities. Without careful curation and ongoing oversight, AI outputs risk perpetuating the very inequities that society strives to overcome, undermining diversity in creative industries and alienating underheard voices.

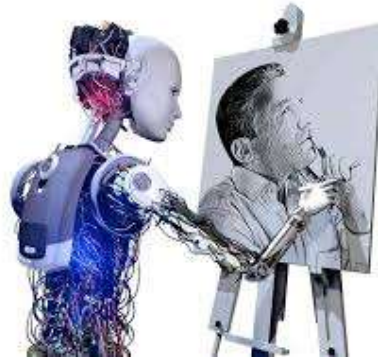
Perhaps most insidious is the erosion of authenticity itself. Audiences may grow

uncertain about whether a film’s trailer was AI-edited, whether a viral poem was penned by a human soul or an algorithmic remix, or whether the illustrator behind a bestselling graphic novel truly sketched every line. This “authorship ambiguity” can devalue genuine human effort: if any aspiring novelist can use an AI co-writer to accelerate drafts, what distinguishes a human storyteller’s insight from a machine’s statistical prediction?

Reconciling AI’s promise with its perils demands a balanced, ethical framework. First and foremost, transparency must become the norm: platforms and creators should clearly label AI-generated or AI-augmented content so audiences can make informed judgments. Equally important is the establishment of fair compensation and attribution mechanisms for artists whose work contributed to AI training sets. Licensing agreements and revenue-share models could ensure that musicians, illustrators, and writers receive royalties whenever their styles or voices inform AI outputs.

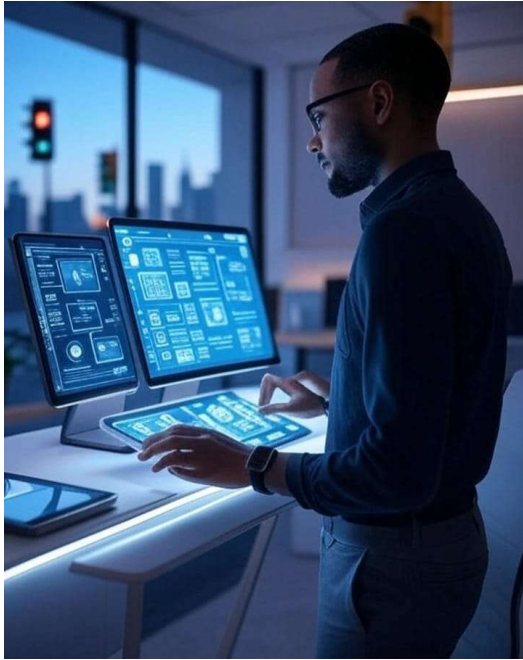
Education and public dialogue also play pivotal roles. Creative communities, academic institutions, and industry bodies should collaborate on best practices for responsible AI use, offering workshops on prompt-engineering ethics, dataset curation, and auditing for bias. By equipping both seasoned professionals and emerging creators with the tools to interrogate AI outputs critically, the industry can foster a culture where human ingenuity remains the driving force.

Finally, thoughtful regulation can help safeguard against misuse without stifling innovation. Policymakers should work with technologists and artists to craft rules that protect copyright while encouraging open research, penalize malicious deep-fakes or fraudulent AI-assisted claims, and incentivize the development of AI systems that enhance, rather than replace, human creativity. Clear legal definitions of authorship, along with streamlined dispute-resolution processes, will give creators confidence to experiment with AI tools without fearing unjust appropriation.



In the end, AI in the creative industries need not be a gladiator’s duel between human and machine. When wielded with respect for original creators, guided by transparent practices, and underpinned by fair compensation and robust policy, AI can become a loyal comrade—amplifying human voices, diversifying artistic expression, and unlocking new realms of possibility that neither artists nor algorithms could achieve alone. Only by embracing this nuanced partnership can we ensure that the future of creativity remains as authentic and equitable as the artistry it seeks to enhance.

Beyond the Screen



The way we interact with technology is undergoing a profound transformation. Where once our lives revolved around lit screens, clicking icons and typing commands, we're now moving toward a world where computing fades into the background—always present but almost invisible. This is ambient computing: a seamless fusion of artificial intelligence, the Internet of Things, pervasive sensors, and cloud services that anticipates our needs and acts on our behalf without demanding direct input. Imagine stepping into your home after a long day and finding lights, temperature, and your favorite music already adjusted to your mood, or leaving for a meeting and knowing that your car will navigate the least-congested route, all without you lifting a finger. At its core, ambient computing relies on a network of interconnected devices—smart thermostats, cameras, microphones, wearable health trackers, connected appliances, and more—all feeding data into AI-driven engines in the cloud or at the edge. Machine-learning algorithms sift through patterns of behavior—when you wake, how you move through your home, what you listen to, even subtle biometric cues—to build a dynamic profile

that informs real-time decisions. Voice assistants maintain conversational context, home hubs recognize individual occupants, and mobile apps hand off tasks to environmental controllers. The result is an ecosystem that responds to you, rather than waiting for you to issue a command.

The evolution of ambient computing accelerated with the rise of smartphones and smart speakers, but it's now extending far beyond personal devices. In smart offices, occupancy sensors and intelligent HVAC systems join forces to optimize comfort and reduce energy waste. Wearable medical monitors track vital signs and proactively alert caregivers if anomalies appear. Connected retail spaces analyze foot traffic and purchasing behavior to tailor promotions as you browse.

Even urban infrastructure is waking up: streetlights adjust their brightness according to pedestrian flow, and public transport apps communicate directly with traffic signals to prioritize buses and trams during rush hours.

In healthcare, ambient systems are proving life-saving. Continuous glucose monitors relay readings to AI platforms that predict dangerous spikes or dips and automatically adjust insulin pumps. Post-operative patients wear discreet patches that monitor wound healing, sending alerts at the first sign of infection. In eldercare facilities, motion detectors and pressure-sensitive mats ensure that residents receive prompt assistance if they fall or wander. These non-intrusive monitors free up medical staff to focus on complex care tasks while preserving patient dignity.

Education and work environments are also benefiting. Classrooms equipped with ambient mics and cameras can gauge student engagement—adjusting lesson pace or suggesting breaks when attention wanes. Hybrid-work offices use desk-booking systems and environmental sensors to allocate space efficiently and maintain safe distancing.

Agriculture using AI and IOT



From the earliest days of human civilization, agriculture has been defined by innovation—from shifting cultivation to plow-driven tillage, from manual transplanting to mechanized combines. Today, we stand at the cusp of a new revolution: one driven not by horsepower but by petabytes and algorithms. The convergence of Artificial Intelligence (AI) and the Internet of Things (IoT) is transforming every facet of farming, enabling growers to monitor, analyze, and act on data in real time. What was once intuition and experience is now precision metrics and predictive models, ushering in an era where food production becomes smarter, more efficient, and more sustainable.

At the heart of this transformation lies the deployment of IoT sensors across fields, greenhouses, and ranches. Soil probes measure moisture, pH, and nutrient levels at granular intervals; microclimate stations record temperature, humidity, solar radiation, and wind speed; livestock wearables track location, activity, and health metrics. These devices stream a continuous torrent of data to edge gateways and cloud platforms, creating an always-on view of the farm ecosystem. No longer must farmers rely solely on visual inspection—every furrow, vine, and animal can be observed remotely, day or night, providing actionable insights down to the square meter.

But raw data alone cannot solve complex agronomic challenges. This is where AI steps in. Machine-learning algorithms ingest sensor feeds, historical yield maps, satellite imagery, and weather forecasts to forecast crop stress, pest outbreaks, and nutrient deficiencies days—or even weeks—ahead of human detection. Deep-learning models trained on

thousands of labeled images can identify early signs of disease on leaves with over 90% accuracy, enabling targeted treatment that saves chemicals, cuts costs, and protects beneficial insects. Predictive analytics optimize planting schedules and variety selection by simulating growth patterns under different climate scenarios, helping farmers hedge against drought, flood, or extreme temperatures.

Precision irrigation offers one of the most tangible benefits of AI-IoT synergy. Smart valves and drip systems receive irrigation commands based on soil-moisture sensors and evapotranspiration models, delivering water exactly where and when it's needed. Such systems can reduce water use by up to 40%, a critical advantage in water-scarce regions. Fertigation—delivering soluble fertilizers via irrigation—can also be dynamically controlled, matching nutrient delivery to the real-time uptake rates of crops. The result is healthier plants, higher yields, and significantly lower environmental impact.

Field operations themselves are becoming increasingly autonomous. GPS-guided tractors plant, cultivate, and harvest with centimeter-level precision, minimizing soil compaction and overlap. Drones equipped with multispectral and thermal cameras survey fields in minutes, generating high-resolution maps of canopy vigor and water stress. Robotic harvesters, once a distant dream, are now picking strawberries, apples, and tomatoes in controlled environments, using computer vision to distinguish ripe fruit and gentle mechanical grips to avoid damage. These technologies not only boost labor productivity but also address seasonal labor shortages and rising wage costs.

Beyond the farm gate, AI and IoT also streamline supply chains. Smart packaging embeds RFID tags or QR codes that record temperature, humidity, and handling events during transit. Blockchain platforms can verify provenance—showing consumers exactly which plot their produce came from and documenting pesticide testing, organic certifications, or fair-trade compliance. In

retail, AI-driven demand forecasting reduces spoilage by aligning inventory with real-time sales trends, while dynamic pricing engines adjust offers based on quality and shelf-life predictions.

Despite these advances, challenges persist. Many smallholder farmers lack reliable connectivity, high-performance sensors, or the technical skills to manage complex digital platforms. Data privacy and ownership pose thorny questions: when a sensor network collects performance data, who controls it—and who benefits from the insights? Interoperability gaps between different IoT standards and agricultural management software can create vendor lock-in, limiting farmers’ flexibility. Moreover, the upfront costs of deploying AI-IoT solutions—sensors, gateways, drones, and analytics subscriptions—remain a barrier for resource-constrained operations.

earth-orbit satellite networks expand, connectivity deserts will shrink, bringing these capabilities to remote regions.

Ultimately, the fusion of AI and IoT promises to elevate agriculture from an art of guesswork to a science of precision. By harnessing continuous sensor data, machine-learning insights, and autonomous machinery, farmers can produce more with less: higher yields with fewer inputs, superior quality with reduced waste, and resilient systems that adapt to a changing climate. The seeds of this digital revolution have already been sown; in the seasons ahead, as these technologies mature and scale, they will help feed a growing global population while preserving the planet’s precious resources. As we cultivate this smart-farm future, the age-old craft of agriculture will reach new pinnacles of productivity, sustainability, and profitability—powered by AI, IoT, and the human ingenuity that guides them.



Looking ahead, the next frontier lies in fully integrated, AI-powered digital-twin farms. By combining real-time IoT streams with high-fidelity crop and soil simulations, growers will be able to run “what-if” scenarios at the click of a button—evaluating, for instance, the impact of switching to a new cover crop or altering irrigation schedules under different ENSO forecasts. Advances in edge computing will push more intelligence onto devices themselves, reducing latency and ensuring critical decisions—like frost protection or automated pesticide applications—occur even without cloud connectivity. As 5G and low-

Learn A Tool



Introduction

Cisco Packet Tracer is a powerful, cross-platform network simulation tool that empowers students, engineers, and IT professionals to design, configure, and troubleshoot virtual networks without ever touching physical hardware. Whether you're preparing for a Cisco certification such as the CCNA or simply exploring networking fundamentals, Packet Tracer provides a risk-free environment where you can experiment with routers, switches, protocols, and end devices. In this two-page guide, we'll explore what makes Packet Tracer an industry favorite, highlight its standout features, walk through a hands-on mini lab, and point you toward advanced applications that will sharpen your skills and boost your confidence.

What Is Cisco Packet Tracer?

At its core, Cisco Packet Tracer is an educational simulation tool developed by Cisco Systems for the Networking Academy program. It replicates real-world network components and behaviors, letting you:

- **Build virtual topologies** of routers, switches, firewalls, and end devices
- **Configure protocols** like OSPF, EIGRP, VLAN tagging, and IPv4/IPv6 addressing
- **Observe packet flows** in real time or step-by-step simulation modes

- **Troubleshoot errors** using built-in diagnostic tools such as ping, traceroute, and console logging

Packet Tracer caters primarily to CCNA aspirants, networking students, and hobbyists. While a full license is free for Cisco Networking Academy learners, a limited version is publicly available at no cost—making it an accessible first step for anyone curious about networking.

Key Features

Packet Tracer's beginner-friendly design conceals a robust feature set capable of advanced labs:

1. **Drag-and-Drop Interface** Easily add routers, switches, PCs, wireless devices, and specialized modules (e.g., hubs, printers) onto a canvas, then connect them with appropriate cables.
2. **Real-Time & Simulation Modes** Switch between instant packet forwarding and slowed-down “playback” that visualizes each frame of traffic, helping you dissect protocol behaviors.
3. **Multi-Protocol Support** Practice DHCP and DNS deployments, establish secure management via SSH/Telnet, and implement routing protocols such as RIP, OSPF, and EIGRP.
4. **Activity Wizard & Pre-Built Labs** Access guided exercises that walk you through step-by-step scenarios, reinforcing concepts from basic IP addressing to complex WAN setups.
5. **Collaboration & File Sharing** Export .pkt files to share network topologies with classmates or instructors, enabling collaborative troubleshooting and peer learning.

Unlike heavyweight emulators like GNS3 or EVE-NG, Packet Tracer requires minimal configuration and runs smoothly on modest hardware—ideal for beginners who seek

instant gratification without steep setup hurdles.

Getting Started – A Mini Lab

Lab Title: Building a Simple LAN

1. **Launch Packet Tracer** and open a new blank workspace.
2. **Add Devices**
 - Drag one 2960 switch and two generic PCs onto the canvas.
3. **Interconnect**
 - Choose **Copper Straight-Through** cables and connect PC0 → FastEthernet0/1, PC1 → FastEthernet0/2 on the switch.
4. **Configure IP Addresses**
 - Click PC0, go to the **Desktop** tab → **IP Configuration**, and set:
 - IP Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
 - Repeat for PC1 with IP 192.168.1.2.
5. **Test Connectivity**
 - Switch to **Simulation Mode**, generate an ICMP ping from PC0 to 192.168.1.2, and observe the echo request/reply frames traversing your virtual switch.
6. **Troubleshooting Tip**
 - If the ping fails, verify that IP addresses and subnet masks match and that the correct cable type is used.

Visual Aid: Imagine two PCs flanking a switch, each linked by a grey cable, with

successful ping arrows lighting up in Simulation Mode.



Advanced Applications

Once you've mastered the basics, Packet Tracer scales to complex scenarios:

- **CCNA Certification Prep** Practice VLAN segmentation, trunking protocols, inter-VLAN routing, and Access Control Lists (ACLs) in multi-switch environments.
- **IoT & Automation** Simulate smart sensors, cameras, and actuators using Packet Tracer's IoT device library. Configure simple Python scripts on edge devices to automate data collection.
- **Wireless Networking** Deploy wireless routers, set up SSIDs, apply WPA2 security, and roam between access points to understand ESS and BSS architectures.
- **Enterprise-Scale Labs** Design campus networks with redundant Layer-3 switches, implement HSRP/VRRP for high availability, and test QoS policies for voice and video traffic.

These advanced use cases not only deepen your networking understanding but also prepare you for real-world IT roles where hands-on troubleshooting is paramount.

Review Box



Introduction

Adobe Firefly, the AI-powered creative suite long revered on desktop, now lives in your pocket. With its mobile app for iOS and Android, Firefly brings generative AI artistry to designers, marketers, and hobbyists alike. Tap a prompt, and in seconds you'll have high-quality images, stylized text effects, or seamless photo edits—no PC required. Whether you're crafting social-media visuals on the subway or retouching photos between meetings, Firefly mobile promises professional results with minimal learning curve. In this two-page deep dive, we'll unpack what Firefly offers, examine its performance and interface, weigh its pros and cons, and help you decide if it deserves a permanent place on your home screen.

What Is the Adobe Firefly Mobile App?

At its core, Adobe Firefly Mobile is a standalone generative-AI art engine optimized for smartphones. It taps Adobe's proprietary Firefly models—trained exclusively on licensed Adobe Stock and public-domain assets—to ensure ethically sourced outputs free of copyright entanglements. Unlike browser-only or desktop-bound tools, the mobile app delivers:

- **Text-to-Image Generation:** Convert simple descriptions like “sun-lit

mountain lake at dawn” into stunning, 4K-capable visuals.

- **Generative Fill:** Remove unwanted objects, extend backgrounds, or insert new elements by painting over areas of your existing photos.
- **Text Effects:** Transform plain typography into neon, watercolor, or chrome-embossed masterpieces with a single tap.
- **Ecosystem Integration:** Sync your creations to Adobe Express, Creative Cloud Libraries, or Photoshop on desktop, preserving seamless workflows.



In comparison to giants like MidJourney or DALL·E, Firefly mobile's claim to fame is its ethical stance: every image generation abides by strict licensing, and Content Credentials metadata tracks provenance, model versions, and user attribution.

Features & Performance

1. User Interface & Experience

Firefly Mobile adopts the familiar clean lines of Adobe Express. A bottom prompt bar anchors the canvas, while tabs across the top switch between generation modes—Image, Fill, Text Effects. Prompt suggestions and style-preset carousels guide novices, and real-time low-resolution previews let you refine iterations before committing your credit. The minimalist design ensures that complex AI controls never clutter the screen, keeping creativity front and center.

2. AI Generation Quality

Under typical network conditions, Firefly Mobile returns polished, photorealistic renders in **5–10 seconds**. The engine excels at natural scenes—landscapes, portraits, product mockups—and produces painterly or abstract styles without explicit training. Advanced sliders let you nudge “Style Intensity,” adjust “Lighting Mood,” or switch aspect ratios on the fly. In head-to-head tests, Firefly’s outputs rival some desktop-only models, with accurate lighting, coherent textures, and minimal artifacts in complex compositions.

3. Editing Tools

Generative Fill empowers on-the-go retouching: simply paint over an unwanted background object, hit “Generate,” and watch AI seamlessly reconstruct the scene. Expansion tools let you extend horizons or add context beyond the original frame. A suite of presets—vintage film, cyberpunk neon, pastel watercolor—applies cohesive color grading and grain effects that feel handcrafted.

4. Pricing & Limitations

Firefly Mobile uses a credit system: the **Free tier** grants a modest monthly allotment for testing; heavy users will quickly need the **Premium plan (\$4.99/month)** for higher priority processing and more credits. Unlike some competitors, there’s no offline mode—an internet connection is mandatory. Video and 3D model generation are also absent, limiting the app to stills and basic photo edits.

Pros & Cons

👍 Pros

- **Top-Tier Output Quality:** Renders often match or exceed desktop-only AI tools.
- **Adobe Ecosystem Sync:** Instant transfers to Express, Photoshop, and Lightroom.
- **Ethical Training Data:** Licensed imagery ensures you’re never building on pirated content.

- **Intuitive Workflow:** Minimal learning curve, thanks to clear prompts and real-time previews.

👎 Cons

- **Limited Free Credits:** Casual users may burn through their allowance quickly.
- **Subscription Push:** Feature set feels gated behind Premium.
- **No Video or 3D Generation:** Falls short of platforms like Canva or Runway for multimedia.
- **Complex Prompt Misfires:** At times struggles with highly detailed or abstract instructions.

Who Should Use It?

Firefly Mobile shines for:

- **Social Media Managers** crafting eye-catching posts on tight deadlines.
- **Digital Marketers** needing rapid ad visuals and mockups.
- **Designers** prototyping concepts during client calls or off-site workshops.
- **Hobbyists & Creatives** exploring AI art without investing in desktop GPU rigs.

However, full-time illustrators or VFX artists requiring granular control over every stroke may find Firefly’s automations too rigid—desktop tools or specialized software remain essential for detailed pipelines.

MIND PUNCH

1) Using only three 4's (and factorial), make 24.

Answer: $4! + 4 - 4$

2) “Chirp” is to “Bird” as “Neigh” is to?

3) What is 25% of 640?

4) Series: 4, 6, 9, 6, 14, 6,...
What comes next?

5) Standard TCP port for HTTPS?

6) If March 1, 2022 was Tuesday, what day was March 1, 2023?

7) Using exactly five 5's, make 50

8) In “ $14 \times 3 + 5 = 47$ ” and “ $16 \times 2 + 9 = 41$,” what is “ $18 \times 2 + 7$ ”?

9) I run all around a field but never move—what am I?

10) Which cannot be spelled from “EXAMPLE”?



1) What is the time complexity of the best-case scenario for the Quicksort algorithm?

2) Who invented the first compiler for a computer programming language?

3) In Big-O notation, what does $O(1)$ denote?

4) What is the default port number for HTTPS?

5) Name the two types of cache mapping techniques.

6) What is the main function of a DNS server?

7) Which data structure is used for implementing recursion?

8) What is the Von Neumann bottleneck?

9) What does the OSI model stand for?

10) What algorithm does RSA encryption use?



FAMOUS AND FAVOURITES



Sir Timothy John Berners-Lee stands among the most transformative pioneers in computing history, forever altering how humanity communicates and shares knowledge. Born June 8, 1955, in London to mathematician parents Conway and Mary Lee—early computer programmers themselves—Tim’s fascination with electronics led him to build his first crude computer in university using a Motorola processor, TTL gates, a soldering iron, and an old television’s CRT. After earning a physics degree from The Queen’s College, Oxford, in 1976, he joined CERN in 1980 and, frustrated by the challenge of sharing documents across the lab’s sprawling network, drafted in March 1989 a proposal for a “distributed information system.” By December he had written the first web server (httpd), the inaugural browser (WorldWideWeb), and defined HTML (HyperText Markup Language), HTTP (HyperText Transfer Protocol), and the URL (Uniform Resource Locator), the three pillars that transformed the internet from a niche academic network into a universal, hyperlinked platform for publishing, commerce, and collaboration. Released free by CERN on August 6, 1991, his code sparked a global explosion in web development. Recognizing the necessity of open standards, Tim founded the World Wide Web Consortium (W3C) at MIT in

1994, guiding the evolution of XML, CSS, DOM, accessibility guidelines, and countless other protocols that ensure interoperability among browsers, servers, and devices. In recent years he has championed data sovereignty through the Solid project—introducing personal “pods” that separate user data from application logic—and co-founded Inrupt to bring enterprise-grade Solid solutions to market, enabling individuals and organizations to reclaim control of their personal information and counter data monopolies. Today, Sir Tim splits his time as a professor of computer science at both MIT and the University of Oxford, mentors the next generation of ethical technologists, and continues to direct W3C while serving as CTO of Inrupt. His vision of an open, accessible, privacy-respecting web has earned him the highest honors: a knighthood from Queen Elizabeth II in 2004; the 2016 Turing Award for inventing the World Wide Web, the first browser, and foundational web protocols; the Royal Society’s Royal Medal; the UK’s Order of Merit; and spots on Time magazine’s lists of the 100 most influential people of the 20th and 21st centuries. Despite his accomplishments, those who know him describe an unassuming, approachable figure—often clad in a T-shirt, jeans, and blazer—who credits the web’s success to a global community and insists technology must amplify human values rather than undermine them. Whether inspiring activists to organize social movements, enabling teachers in remote villages to deliver lessons, or empowering doctors to collaborate on lifesaving research, Sir Tim Berners-Lee’s legacy is an ever-evolving, human-centric internet that continues to unite billions and will inspire generations of innovators to come.

ANSWERS

MIND PUNCH

- 1) $4! + 4 - 4 = 24$
- 2) Horse
- 3) Answer: 160
- 4) 19 (odd positions start at 4 and increase by 5; even positions stay 6)
- 5) 443
- 6) Wednesday
- 7) 50
- 8) 43
- 9) A fence
- 10) AMPLER

IT VITA

- 1 $O(n \log n)$
- 2 Grace Hopper
- 3 constant-time performance
- 4 443
- 5 Direct mapping & Associative mapping
- 6 resolve human-readable domain names into IP addresses.
- 7 stack data structure
- 8 limited throughput between the CPU and memory caused by a single shared data bus
- 9 Open Systems Interconnection model
- 10 Asymmetric

SENSE OF GRATITUDE

THE EDITORIAL BOARD EXPRESSES ITS SINCERE GRATITUDE TO ALL THOSE WHO ARE RESPONSIBLE, EITHER BY BEING ON THE STAGE OR BEHIND THE SCREEN FOR THE SUCCESSFUL LAUNCH OF THE MAGAZINE