Vita Digital Journal

Life through Technology & Innovation

Computer Science Department Monthly

Vol. 1 | Issue 6 | July 2026

VITA DIGITAL JOURNAL

Life through Technology & Innovation

Computer Science Department Monthly

Volume 1 | **Issue 6** | **July** 2026

Published by:
Department of Computer Science,
Marian College of Arts and Science,
Thiruvananthapuram.

Chief Editor: Livin M Miranda
Student Editors:
Santhipriyan M
Joel George Mathew

Disclaimer & Copyright

The views expressed in Vita Digital Journal are those of the respective authors. Authors are solely responsible for the originality, accuracy, and authenticity of their work. The Editorial Board and the institution are not liable for any claims, errors, or interpretations arising from published content.

Contributors must ensure originality and proper citation of sources. Any issues related to plagiarism or copyright infringement remain the author's responsibility.

mcasmedia123@gmail.com
https://www.mcas.ac.in/

EDITORIAL

Technology continues to transform the way we learn, work, and solve real-world problems. Among the many advancements shaping the future, Artificial Intelligence(AI) has emerged as one of the most influential technologies of our time. From healthcare and education to agriculture, finance, and scientific research, AI is creating opportunities that were once considered impossible.

As students of science and technology, we are not merely observers of this transformation—we are future innovators who will shape it. While technical knowledge is essential, equally important are creativity, ethical responsibility, critical thinking, and a commitment to lifelong learning. The ability to adapt to new technologies and use them for the benefit of society will define the professionals of tomorrow.

Vita Digital Journal continues to provide a platform for students and faculty across science disciplines to exchange ideas, share knowledge, and celebrate academic achievements. Every article, project, and innovation featured in these pages reflects our collective pursuit of excellence and our readiness to embrace the challenges of an ever-changing technological world.

As we present the July issue, let us remain curious, continue learning, and use technology responsibly to build a future that is innovative, inclusive, and beneficial to humanity.

- Chief Editor
Mr. Livin M Miranda
Head, Department of Computer Science

Index

Simulating a Fruit Fly's Brain: A Milestone in Digital Neuroscience

Aldin Brillian Castro
S3 BSc Computer Science

INTRODUCTION

One of the most remarkable scientific achievements in recent years has been the successful digital reconstruction and simulation of the brain of the fruit fly (Drosophila melanogaster). Although a fruit fly's brain is tiny compared to that of a human, it contains an intricate network of neurons that enables learning, memory, navigation, and decision-making. By creating a detailed digital model of this brain, scientists have taken a major step toward understanding how biological intelligence emerges from neural circuits. This breakthrough has implications not only for neuroscience but also for artificial intelligence, medicine, and robotics.

WHY THE FRUIT FLY?

The fruit fly has long been one of biology's most valuable model organisms. Despite having a brain of only about 140,000 neurons, it performs surprisingly complex behaviors, including recognizing odors, learning from experience, avoiding danger, communicating, and navigating its environment. Unlike the human brain, which contains approximately 86 billion neurons, the fruit fly's nervous system is manageable with today's imaging and computing technologies.

Metric	Fruit Fly	Human
Total Neurons	~140,000	~86 billion
Synaptic Connections	>20 million	~100 trillion
Brain Volume	~1 mm^3	~1,400 cm^3
Scanning Status	Completely Mapped	Mapping in Progress

BUILDING THE DIGITAL BRAIN

Scientists preserved fly brain tissue and scanned it using electron microscopy, producing millions of high-resolution images.

Artificial intelligence helped identify neurons and trace their connections, while researchers verified the results. The final connectome maps more than 50 million synaptic connections.

Stage	Description
1. Tissue Preservation	Fly brain tissue chemically fixed to prevent degradation
2. Electron Microscopy	Ultra-high resolution scanning produces millions of serial sections (40 nm slices)
3. Image Processing & AI	Machine learning algorithms segment and reconstruct neuron boundaries from 2D slices
4. Manual Verification	Researchers manually verify AI-traced connections to ensure accuracy
5. Connectome Mapping	Complete 3D neural network map with >50 million synaptic connections catalogued

Table 1: Digital Brain Reconstruction Methodology

SIMULATING BRAIN ACTIVITY

Researchers built computational models that simulate how neurons exchange signals. These simulations reproduce neural computation, allowing scientists to study behavior and perform virtual experiments that would be difficult in living organisms. However, the simulation is not a conscious digital fly.

SCIENTIFIC SIGNIFICANCE

The project helps researchers understand complete neural circuits, inspires more efficient artificial intelligence, and may contribute to future medical advances by revealing principles of nervous system function.

CHALLENGES AND LIMITATIONS

The model does not capture every biochemical process or the full complexity of living brains. Simulating biological systems also requires significant computational power, and applying findings directly to humans remains challenging.

FUTURE PROSPECTS

Scientists aim to create increasingly realistic simulations that incorporate more biological detail and eventually model larger nervous systems, advancing neuroscience, AI, and medicine.

CONCLUSION

The digital simulation of the fruit fly brain is a landmark achievement that combines microscopy, artificial intelligence, and high-performance computing. While it does not recreate a living organism, it offers an unprecedented tool for understanding how brains work and lays the foundation for future discoveries.

REFERENCE

- Dorkenwald, S., McKellar, C. E., Macrina, T., et al. (2024). Neuronal wiring diagram of an adult brain. Nature.
- FlyWire Consortium. (2024). FlyWire: A complete wiring diagram of the Drosophila brain.
- Janelia Research Campus, Howard Hughes Medical Institute. (2024). FlyEM Project: Mapping the Drosophila Brain.
- Howard Hughes Medical Institute. (2024). Researchers Complete the First Wiring Diagram of an Adult Fly Brain.
- Kornfeld, J., & Denk, W. (2018). Progress and Remaining Challenges in High-Throughput Volume Electron Microscopy. Current Opinion in Neurobiology.

Practical Defensive Security: Building Systems That Anticipate Failure

Alin Antony
S3 BSc Computer Science

INTRODUCTION

Defensive security is the art of building systems that respond to attacks after they have happened. Software development practices that focus on the offensive side (pentesting, ethical hacking, etc) enjoy greater recognition. But ultimately what makes our systems safe is not the ability to detect and react to exploits, but engineering practice aimed at eliminating successful attacks altogether. A common theme across defensive security practices is to build software with security in mind at all stages of the development cycle, not as an afterthought.

DEFENSE IN DEPTH

The principle is simple : one point of failure is intrinsically unsafe.

Another way to put it: any security measure that relies on not being exploited can be exploited. The Defense in Depth (DoD) principle suggests that applications should be designed such that the failure of any one security measure does not compromise the overall security of the system. For instance, if an attacker manages to circumvent the Web Application Firewall (WAF) in some way, then the database encryption, the network micro-segmentation and Role-Based Access Control (RBAC) should stop the database from being hijacked.

PRINCIPLE OF LEAST PRIVILEGE (POLP)

The Principle of Least Privilege (PoLP) states that every user, process, or system should be provided with only the services and

information they need to do their work. One example of privilege escalation vulnerability is the use of the admin account to run a web backend. It's much better to run the backend as some restricted user with access to application specific directories.

SECURE BY DEFAULT AND FAIL SECURELY

Security software ought to be designed and put in place so that getting around its controls feels as difficult as possible. This idea is really tied to the notions of "secure by default" and "fail securely" practices, in a way that often sounds similar but lands differently in real use. Software should, out of the box, demand real effort to loosen those protections, not the other way around. For runtime errors, the rule stays steady: when something goes wrong the system should fail securely, basically denying access rather than "playing safe" by accident and granting it.

Defensive Error Handling Example:

```python
# Defensive Error Handling: Fail Closed
try:
 user_authorized = verify_user_token(auth_token)
except SignatureExpiredError:
log_security_event("Token expired")
user_authorized = False except Exception as e:
# Fail closed: treat unexpected system errors as unauthorized
log_system_error(e)
user_authorized = False
if not user_authorized:
raiseUnauthorizedAccessError("Access Denied") ```
```

DEFENSIVE CODING: STOPPING INJECTIONS AT THE SOURCE

Most of the well-known software weaknesses come from bad input handling done by the application itself. Parameterized queries and prepared statements are a kind of defensive coding practice, they help stop database injections like SQL injection (SQLi) which typically abuse improperly formatted user inputs. It's basically like you control how the data is treated before it even reaches the database.

MODERN AUTHENTICATION REQUIREMENTS

Here's a slightly expanded version:
Authentication standards such as NIST SP 800-63B continue to evolve as new security threats emerge and technology advances. Many older authentication practices, while once considered effective, are now known to have limitations in protecting users against modern attacks such as phishing, credential stuffing, and password reuse. As a result, these standards are regularly updated to recommend stronger, more user-friendly authentication methods that better address today's cybersecurity challenges. The following table illustrates how authentication practices have shifted over time.

Aspect	Traditional Approach	Modern Best Practice
Password Complexity	Mix of uppercase, lowercase, numbers, special characters (8+ chars)	Longer passphrases or passkeys (less reliance on complexity rules)
Password Rotation	Forced rotation every 60–90 days	No automatic rotation; only when compromise is suspected
Breach Database Screening	Not typically checked; relies on complexity rules	Passwords validated against known breach databases (e.g., HaveIBeenPwned)
Authentication Factor	Single-factor (password) authentication	Multi-factor authentication (MFA), biometrics, passkeys

THE GAP IN PRACTICE

Here's a slightly expanded version while keeping it concise:
However, in actual practice, many services still only verify that a candidate password satisfies complexity rules and do not screen it against databases of leaked credentials. This creates a significant security gap, as users often choose predictable passwords or reuse passwords that have already been exposed in previous data breaches. As a result, attackers can exploit these weak or compromised passwords to gain unauthorized access to user accounts.

CONCLUSION

Overall, defensive security is mostly about trying to spot software design and implementation traps, instead of depending on the ability to "jump in" once vulnerabilities pop up as they are found. It includes things like input checking, least privilege, layered principle, and safer development habits.

Key Defensive Security Principles:

Principle	Description
Defense in Depth	Multiple independent security layers ensure that failure of one does not compromise the entire system
Principle of Least Privilege	Users, processes, and systems should have only the minimum permissions needed to perform their tasks
Secure by Default	Security controls should be enabled by default, requiring effort to weaken them
Fail Securely	When errors occur, the system should deny access by default rather than accidentally grant it
Defensive Coding	Input validation and parameterized queries prevent injection attacks at the source

REFERENCE

- National Institute of Standards and Technology. (2020). Digital Identity Guidelines: Authentication and Lifecycle Management.
- National Institute of Standards and Technology. (2024). Secure Software Development Framework (SSDF) Version 1.1.
- OWASP Foundation. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks.
- Bishop, M. (2018). Computer Security: Art and Science (2nd ed.). Addison-Wesley.
- Stallings, W., & Brown, L. (2023). Computer Security: Principles and Practice (5th ed.). Pearson.

Thinking Like a Programmer: The Scarcity of Problem Solving AI Didn't Create — But Will Accelerate

Siva Sajith
S1 BSc Computer Science

INTRODUCTION

For years, a persistent issue has plagued the tech industry: Computer Science graduates frequently enter the workforce struggling to write clean, compilable, and deployment-ready code. The arguments for this disconnect are numerous. Some blame a lack of exposure to real-world applications; others point to the rote memorization of syntax; and many fault outdated syllabi that turn a blind eye to current technological advancements. However, one critical factor is often missing from this debate: Do they think like a Programmer ? Do they think about writing the code or solving the problem 1st ? Do they have the idea of breaking the problem into small pieces ? What exactly does it mean to 'Think like a programmer' ?

IT'S MORE THAN JUST SOLVING PROBLEMS

Being able to think like a programmer isn't only about the approach we use when we're faced with a tough issue, it's the natural way we act and approach things with software in general. And there are 5 primary traits to this :-

1. You think in inputs and outputs

Every situation has something going in , and something coming out. As a programmer you sort of automatically ask:
What do I have? →Input
What do I need? →Output
What turns one into the other ? → The solution
Before you write even a single line of code, you should already be clear about what's going in, what's coming out. Everything else, is just

the bridge , kind of a background detail.

2. You think about edge cases

Normal thinking: “Does it work?”
Programmer thinking: “Does it work when the input is empty ? When it’s negative? When two things happen at the same time? When the user does something kinda unexpected ?”

// Normal thinking stops here: if (customerAge >= 18) { accept order }
// Programmer thinking sort of keeps going:
// What if customerAge is 0?
// What if customerAge is -5 ,
// What if nobody even passed customerAge at all?

Real software fails at the boundaries, not right in the middle.

3. You distinguish WHAT from HOW

This is the highest level.
Programming mindset allows you to see a problem and distinctly separate:

WHAT should be done → the requirement, the logic
HOW it should be done → the implementation, the code

The majority of beginners try to immediately proceed to the HOW – start writing code. The programmer first spends time with the WHAT and thinks about it thoroughly, and then the HOW virtually writes itself.

That is why sometimes senior programmers write less code than junior programmers – they think more and write less.

4. Expect things to break and continue to be interested in why

If one is not a programmer and makes a mistake, he or she feels like he or she has messed up. If one is a programmer, however, he or she thinks that the situation is interesting and tries to understand the information that is presented by the system.

5. You break big problems into small ones

For someone who does not know how to program, "create a food delivery application" means a lot. For someone who knows how to do that, “create a food delivery application” implies:

Food delivery application
→ List of restaurants
→ Pull data from database
→ Display on screen
→ Cart
→ Add item
→ Calculate total cost
→ Order
→ Place an order
→ Track its status

This technique is not about solving big problems all at once. Instead, it focuses on breaking complex problems into smaller, more manageable components before attempting to solve them. By addressing each part individually, the overall problem becomes easier to understand and solve.

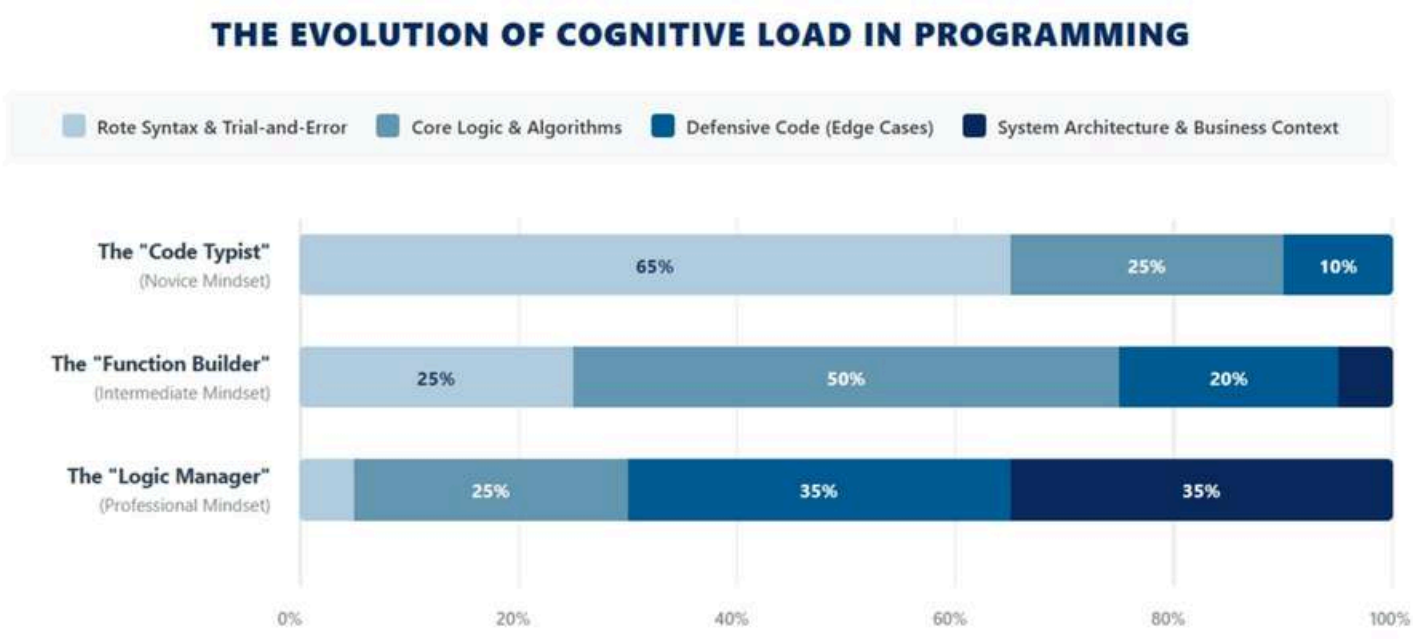

Figure 1: The reallocation of cognitive effort as developers transition from syntax execution to holistic systems thinking.

FUTURE

We have reviewed the five major approaches towards building an ideal programmer's mindset. But one important question remains open: would all of this become irrelevant in a future when AI is expected to substitute programmers?

The short answer is – YES. All this knowledge comprises the very CORE MENTAL MODEL of a programmer – a mindset which has been and will be the driver of every era of software development. The only difference is that from now on this mindset will be the absolute basic necessity to get into this industry.

The programmers who have acquired this mindset will immediately become leaders of this industry – the system architects, enterprise logics managers, lead developers and so on. The ones who haven't got this mindset simply won't survive. The juniors and interns who have based their job on coding and syntax memorization will not be needed anymore since these activities can be completely performed by AI-based agents.

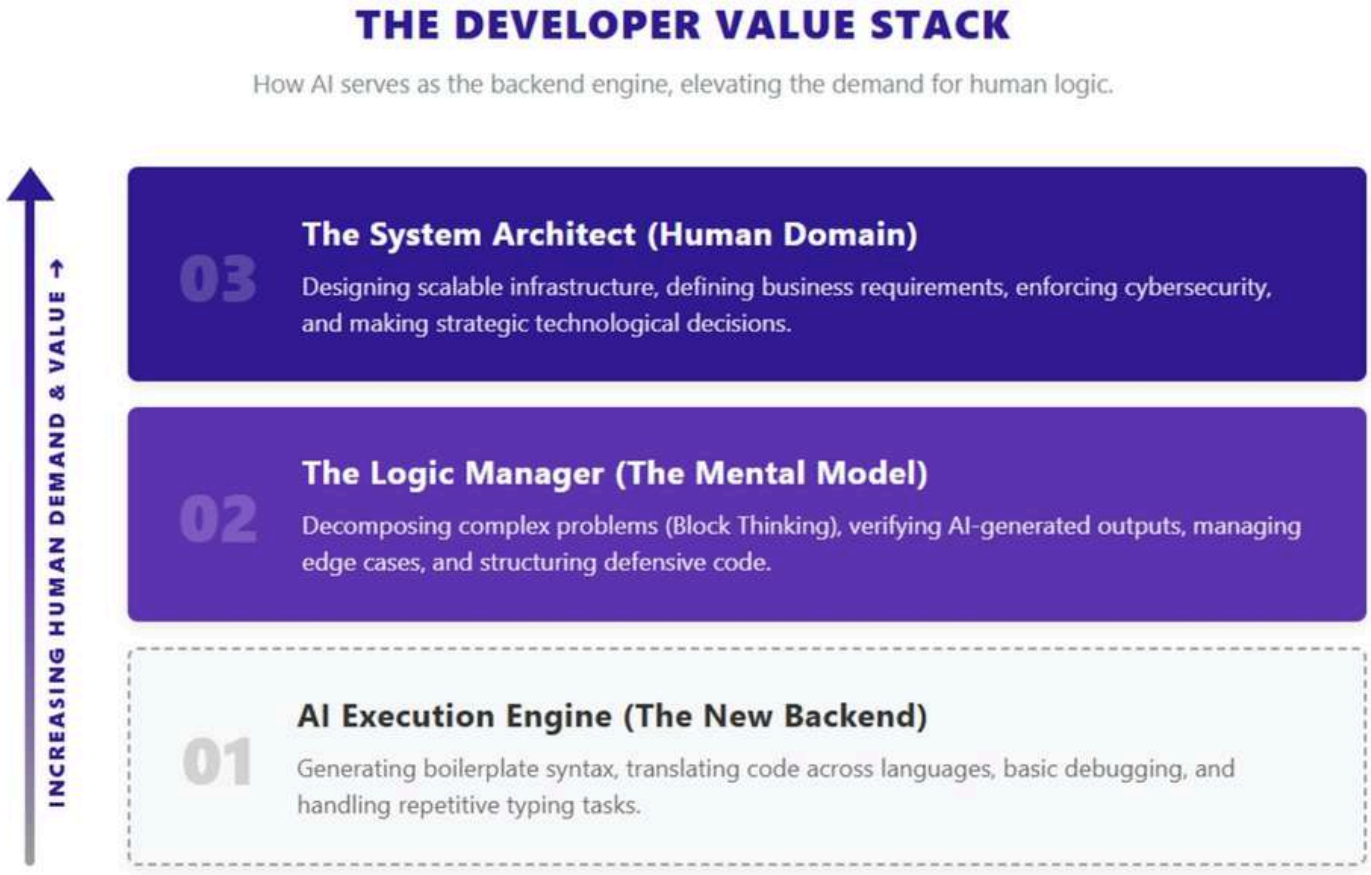

Figure 2: AI is not replacing the programmer; it is replacing the typist. The market demand has shifted upward, requiring humans to operate as architects and logic managers above the AI baseline.

CONCLUSION

The transformation of software development is not about the end of programming. It is about the end of human compilers. While artificial intelligence will definitely automate the "HOW" through syntax, boilerplates, and script automation, it will not be able to automate the

"WHAT": the breakdown of a problem, anticipation of edge cases, and architectural skills needed to build robust systems.

In an age where computer science students graduate from college into this brave new world, there is one thing that we must do: stop competing with machines when it comes to rote learning and memorization of syntax, and focus on logic.

REFERENCES

- ARTICLE Spraul, V. A. 2012. Think Like a Programmer: An Introduction to Creative Problem Solving. No Starch Press.

- Martin, R. C. 2008. Clean Code: A Handbook of Agile Software Craftsmanship. Prentice Hall.

- Wing, J. M. 2006. Computational thinking. Communications of the ACM.

- Fowler, M. 2024. Software Engineering in the Era of Generative AI. Retrieved from martinfowler.com

Teaching Machines to Read the Body : How Machine Learning Is Reshaping Medical Diagnosis

Goutham G Nair
S5 BSc Computer Science

INTRODUCTION

Walk into almost any hospital today and there is a good chance an algorithm is quietly looking over a doctor's shoulder. Machine learning, a branch of computer science that lets systems find patterns in data without being explicitly programmed for every rule, has moved from research labs into radiology suites, pathology departments, and primary care clinics. This shift matters because diagnosis, the process of figuring out what is wrong with a patient, is still one of the hardest parts of medicine. Symptoms overlap, images are subtle, and even experienced clinicians get tired or miss things. Machine learning will not replace doctors anytime soon, but it is already changing how fast and how accurately certain conditions get caught, which is exactly why it deserves a closer look.

HOW MEDICAL MACHINE LEARNING WORKS

At its core, medical machine learning takes large sets of labeled data, such as thousands of chest X-rays marked as healthy or diseased, and trains a model to recognize the statistical fingerprints of illness. Convolutional neural networks are especially good at this kind of image-based pattern recognition, while simpler methods like support vector machines and random forests are often used on structured data such as lab results or vital signs (Ahsan & Siddique, 2022). Once trained, these models can scan a new image or record in seconds and flag anything that looks suspicious.

APPLICATIONS IN HEALTHCARE

The clinical reach of this technology is already broad and continues to expand across multiple medical specialties. In radiology, deep learning systems help detect tumors, fractures, and signs of stroke, while also assisting clinicians in interpreting complex medical images more quickly and consistently. A large meta-analysis found their diagnostic accuracy in medical imaging to be comparable to that of trained clinicians across several disease areas, highlighting their value as decision-support tools in modern healthcare (Aggarwal et al., 2021). In cardiology, models trained on demographic and laboratory data have improved the early detection of heart disease risk, enabling physicians to identify high-risk patients before severe complications occur (Ahsan & Siddique, 2022). Hematology has also benefited: a French multicenter study showed that a machine learning model using routine laboratory parameters could predict subtypes of acute leukemia with strong accuracy, potentially speeding up a diagnosis that normally takes days and allowing treatment to begin sooner (Alcazer et al., 2024). Neurology is another growing frontier, where machine learning is being applied to identify early biomarkers of neurodegenerative diseases like Alzheimer's and ALS before symptoms become obvious. These advances could support earlier interventions, improve long-term patient outcomes, and contribute to the development of more personalized treatment strategies (Myszczynska et al., 2020).

ADVANTAGES OF MEDICAL MACHINE LEARNING

These tools bring real advantages. They do not get tired, they apply the same criteria to every case, and they can process far more data than a human ever could in the same amount of time. Rajkomar et al. (2019) point out that this consistency is particularly valuable in high-volume settings such as screening programs, where a small percentage improvement in accuracy can affect thousands of patients.

CHALLENGES AND LIMITATIONS

The limitations are just as important to understand. Many models are trained on data from specific hospitals or populations, so their accuracy can drop sharply when applied elsewhere, a problem often described as poor generalizability. There is also the well-known "black box" issue: deep learning systems can be difficult to interpret, making it hard for clinicians to know why a model reached a particular conclusion (Topol, 2019).

REGULATION AND FUTURE OUTLOOK

This lack of transparency is part of why regulation has become such a hot topic. In the United States, the Food and Drug Administration has authorized several hundred AI- and machine-learning-enabled medical devices, and that number keeps climbing every year as the agency works out how to evaluate software that can keep learning after it reaches the market (U.S. Food and Drug Administration, 2023).

Table 1

Common machine learning approaches in diagnostic medicine

Method	Typical Use	Data Type	Strength
Convolutional Neural Networks	Imaging (X-ray, MRI, CT)	Images	Pattern detection
Random Forests	Risk scoring, lab-based prediction	Tabular data	Handles many variables
Support Vector Machines	Disease classification	Tabular data	Works with small datasets
Recurrent Networks (LSTM)	Monitoring vitals over time	Time-series data	Captures trends

CONCLUSION

Machine learning has clearly earned its place in modern diagnostics. It speeds up image review, flags risk factors clinicians might overlook, and handles routine screening at a scale no human team could match. At the same time, questions about bias, interpretability, and regulatory oversight are far from settled, and no model should be trusted without a clinician checking its reasoning.

Looking ahead, the field seems to be moving toward hybrid systems where large language models help summarize patient histories alongside traditional prediction models, and where regulators are building frameworks flexible enough to handle software that keeps learning after approval. If that balance between innovation and accountability holds, machine learning will likely become less of a novelty and more of a quiet, dependable part of how medicine gets practiced.

REFERENCES

- Aggarwal, R., Sounderajah, V., Martin, G., Karthikesalingam, A., King, D. (2021). Diagnostic accuracy of deep learning in medical imaging: A systematic review and meta-analysis.

- Ahsan, M. M., & Siddique, Z. (2022). Machine learning-based heart disease diagnosis: A systematic literature review. Artificial Intelligence in Medicine.

- Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine.

- Myszczynska, M. A., Ojamies, P. N., Lacoste, A. M. B., Neil, D., Saffari, A., Mead, R., Hautbergue, G. M., Holbrook, J. D., &Ferraiuolo, L. (2020).

- Applications of machine learning to diagnosis and treatment of neurodegenerative diseases. Nature Reviews Neurology.

- Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. New England Journal of Medicine.

Quantum Computing : Bridging Theory and Real-World Application

Anantha Krishna A
S5 BSc Computer Science

INTRODUCTION

Quantum computing has moved from a purely theoretical curiosity to a field that engineers, physicists, and computer scientists are racing to build hardware for. Unlike the computers on our desks, which store information as bits that are either 0 or 1, quantum computers use qubits that can exist in a mix of both states at once. This single idea, borrowed from quantum mechanics, opens the door to solving certain problems far faster than any classical machine ever could. As industries from pharmaceuticals to finance start paying attention, it is worth understanding what quantum computing actually offers, where it still falls short, and why it matters right now.

FUNDAMENTAL PRINCIPLES OF QUANTUM COMPUTING

At the core of quantum computing sit two properties: superposition and entanglement. Superposition lets a qubit represent a combination of 0 and 1 simultaneously, so a system of just a few dozen qubits can represent an enormous number of possible states at the same time. Entanglement links qubits together so that measuring one instantly affects the state of another, even if they are physically separated. Together, these properties allow quantum algorithms to explore many solutions in parallel rather than checking them one at a time, which is how classical computers are forced to operate (Nielsen & Chuang, 2010).

DEMONSTRATING QUANTUM ADVANTAGE

The clearest demonstration of this advantage came in 2019, when a team at Google announced that their 53-qubit processor, Sycamore, completed a specific sampling task in about 200 seconds, a task the team estimated would take the fastest classical supercomputer thousands of years (Arute et al., 2019). IBM disputed the size of that gap, arguing that a classical machine could complete the same task in a few days rather than millennia, which highlights an important point: quantum advantage is often narrow and problem-specific rather than a blanket superiority over classical computing (Gibney, 2019). Even so, the experiment marked the first time a quantum processor had done something practically impossible for classical hardware, and it pushed the whole field into the mainstream conversation.

EMERGING APPLICATIONS

Real applications are starting to take shape, though most remain experimental. In chemistry and materials science, quantum simulations promise to model molecules far more accurately than classical approximations allow, which could speed up drug discovery and battery design. In logistics and finance, quantum optimization algorithms are being tested for routing and portfolio problems where the number of possible combinations grows too large for classical search. Cryptography is another area under close watch, since a sufficiently powerful quantum computer running Shor's algorithm could break the encryption schemes that currently protect online banking and communications.

PREPARING FOR THE QUANTUM ERA

This concern is not farfetched enough to ignore: in 2024 the National Institute of Standards and Technology finalized its first set of post-quantum cryptography standards, designed to keep data secure even after large-scale quantum machines arrive (National Institute of Standards and Technology.

CURRENT LIMITATIONS

The current stage of the technology is known as the Noisy Intermediate-Scale Quantum (NISQ) era, where quantum computers remain too error-prone for most large-scale applications. Qubits are highly sensitive to environmental disturbances, causing errors known as decoherence. Overcoming these errors through effective error correction remains one of the biggest challenges in quantum computing.

FUTURE OUTLOOK

Companies such as IBM and Google continue to publish roadmaps aiming for machines with thousands of qubits and built-in error correction within the next several years. Achieving these goals could enable quantum computers to tackle complex real-world problems in fields such as medicine, materials science, and cryptography. However, timelines in this area have historically slipped because of the significant technical challenges involved in building stable, large-scale quantum systems.

Table 1

Classical Computing vs Quantum Computing

Feature	Classical Computer	Quantum Computer
Basic unit	Bit (0 or 1)	Qubit (0, 1, or both)
Processing style	Sequential, one state at a time	Parallel, many states at once
Error sensitivity	Very low	High, requires error correction
Best suited for	General everyday computing	Optimization, simulation, cryptography research
Current maturity	Mature, widely deployed	Early stage, NISQ era

CONCLUSION

Quantum computing is not about replacing the laptop or phone in front of you. It is about tackling a narrow but important class of problems, ranging from molecular simulation to cryptographic security, that classical machines handle poorly. The field has already produced striking milestones, but noisy qubits, short coherence times, and the difficulty of scaling error correction mean that fully fault-tolerant quantum computers are still likely years away. What happens between now and then matters just as much as the eventual destination. Researchers are refining algorithms, standards bodies are preparing encryption for a post-quantum world, and companies are steadily increasing qubit counts and stability through advances in hardware and error correction. As these improvements continue, quantum computing is expected to move gradually from laboratory research to practical applications across multiple industries. Whether or not a person ever uses a quantum computer directly, its influence on cybersecurity, medicine, materials science, and scientific research is likely to arrive sooner than many expect.

REFERENCES

- Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., ... Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor.

- Gibney, E. (2019). Google's 'quantum supremacy' shakes up the tech world.

- National Institute of Standards and Technology. (2024). NIST releases first 3 finalized post-quantum encryption standards. U.S. Department of Commerce.

- Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information (10th anniversary ed.). Cambridge University Press.

- Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum.

AI in Drug Design - Revolutionizing Biochemistry and Medicine

Dr. Jasmine Peter
Asst. Prof.,
Dept of Zoology

INTRODUCTION

The traditional process of finding a new drug takes 10 to 15 years and costs more than $2 billion. Most of the time is spent on trial and error, trying thousands of molecules in the lab until one is found that works. This is where Artificial Intelligence is turning the tide in biochemistry. AI in drug design is the use of machine learning and deep learning algorithms to predict the interactions of chemical compounds with biological targets such as proteins and enzymes. Instead of having to test every molecule physically, AI can screen millions of compounds on a computer in days. The main principle of biochemistry is "structure determines function". AI helps us predict structure and function much more rapidly. The Key Applications of AI in Drug Design are target identification, drug molecule generation, predicting drug properties and drug repurposing.

APPLICATIONS OF AI IN DRUG DESIGN

The key applications of AI in drug design include target identification, drug molecule generation, predicting drug properties, and drug repurposing.

AI analyzes genomic, proteomic, and biochemical data to identify the correct protein or enzyme target for a disease. During the COVID-19 pandemic, AI models helped identify the SARS-CoV-2 spike protein as a key drug target within weeks. AI can also design entirely new molecules using

models such as Generative Adversarial Networks (GANs). In addition, tools like AlphaFold2 predict three-dimensional protein structures, helping researchers determine where drug molecules should bind.

AI is also used to predict whether a molecule will be toxic, how well it will dissolve, and whether it can cross the blood-brain barrier. This process, known as ADMET prediction(Absorption,Distribution, Metabolism, Excretion, and Toxicity), significantly reduces the time required for laboratory testing. AI can also analyze approved drugs to identify new therapeutic uses, an approach that was widely used during the COVID-19 pandemic.

BENEFITS OF AI IN DRUG DESIGN

One of the greatest advantages of AI is its ability to make drug discovery faster and more cost-effective. AI can screen millions of chemical compounds in just a few days, whereas traditional laboratory methods can take years. It also improves accuracy by predicting how drug molecules interact with target proteins and by identifying potential toxicity and side effects at an early stage, reducing failures during clinical trials.

Furthermore, AI supports drug repurposing and personalized medicine by analyzing large biochemical and genomic datasets to identify new applications for existing drugs and develop treatments tailored to individual patients. Overall, AI accelerates drug discovery, lowers costs, and increases the chances of developing safe and effective medicines.

CHALLENGES AND LIMITATIONS

Despite its potential, AI in drug design faces several important challenges. High-quality biochemical, genomic, and clinical data are essential for accurate predictions, but such data are often incomplete or biased. Another limitation is the "black box" problem, where researchers cannot easily understand why an AI model selected a particular molecule.

Laboratory validation also remains essential because AI-generated

predictions must still be verified through experiments and clinical trials, which are both time-consuming and expensive. Other challenges include the high cost of AI tools, a shortage of skilled professionals, and ethical concerns related to data privacy. These factors highlight that AI complements rather than replaces traditional scientific research.

FUTURE PROSPECTS

The future of drug discovery lies in collaboration between AI systems and biochemists. AI will analyze vast amounts of data and generate predictions, while biochemists will validate findings through laboratory research. This partnership is expected to accelerate the development of treatments for cancer, Alzheimer's disease, and rare genetic disorders. Companies such as DeepMind, Insilico Medicine, and Atomwise are already using AI to develop promising drug candidates for clinical trials.

CONCLUSION

AI is not replacing biochemists but becoming one of the most powerful tools in modern drug discovery. By combining biochemical expertise with the speed and analytical capabilities of AI, researchers can develop safer, more effective, and more affordable medicines in less time. As AI technology continues to advance, it is expected to play a major role in discovering treatments for diseases that remain incurable today.

REFERENCE

- Jumper, J., et al.(2021). Highly accurate protein structure prediction with AlphaFold. Nature.
- Vamathevan, J., et al.(2019). Applications of machine learning in drug discovery and development. Nature Reviews Drug Discovery.
- Zhavoronkov, A., et al.(2019). Deep learning enables rapid identification of potent DDR1 kinase inhibitors. Nature Biotechnology.
- Chen, H., Engkvist, O., Wang, Y., Olivecrona, M., & Blaschke, T. (2018). The rise of deep learning in drug discovery. Drug Discovery Today.

Edge Computing and Artificial Intelligence : Concepts, Architectures, and Strategic Challenges

Ms. Rini Amado

Asst. Prof.,
Dept of Computer Science

ABSTRACT

Deployment of large-scale foundational Artificial Intelligence (AI) models has resulted in economic disruption yet exposed several strategic challenges including issues such as legal data jurisdiction, latency, network dependency, and geographic constraints. The existing hyper-scaler public cloud infrastructures by their nature operate in centralized fashion involving traversing of physical borders and requiring high latency roundtrips, posing security threats and operational challenges. This research article provides an overview of the concept and architecture of edge computing and artificial intelligence architectures that are designed to serve mission-critical low-latency applications. We define the technical requirements in terms of data sovereignty, operational autonomy, and hardware independence at edge locations. Analyzing the contemporary orchestration solutions based on hybrid architectures, federated edge sites, and hardware-based trusted execution environments allows us to provide a solid reference architecture for maintaining localized real-time inference while preserving state-of-the-art computational performance.

INTRODUCTION

The prevalence of Artificial Intelligence (AI) and Large Language Models (LLMs) has made

computation a crucial element of operational autonomy. Due to the fact that today's deep learning architectures depend extensively on the processing of high frequency streaming data, the location of physical networks in which the data transits, resides and makes inferences becomes a controversial issue. When organizations deal with telemetry data or proprietary data on infrastructure affected by wide area network latency and legal jurisdiction outside the country, they are inadvertently making their architectural borders porous and infringing upon reliability requirements. Edge AI architecture solves the aforementioned problems. An edge AI architecture offers isolated execution environment, operational setup and governance that ensures the processing of data completely stays within a specified local network or peripheral device border . It is important to note that due to the increasing dependence of AI on distributed real time pipelines, creation of edge architectures is not only about storage borders, but also about hardware, model compression and inference lifecycle.

THEORETICAL APPROACH TO EDGE AI

According to the definition, Edge AI implies that the entity or organization is capable of processing AI algorithms on peripheral computing devices, such as gateways, local servers, and embedded systems, without constant reliance on centralized cloud computing data centers . Architectural independence is reached through the solution of three major issues:

Data Proximity: The guarantee that all live sensor streams, local corpora, and user metadata are processed locally and not subject to any WAN constraints and external operation monitoring.

Operational Independence: The guarantee that local edge nodes perform inference and local maintenance independently, so that the central cloud shutdowns or other network failures do not affect local processes.

Algorithmic Efficiency: Reduction of latency overheads by adhering to the principles of model quantization (INT8/FP16) and knowledge distillation.

IMPLEMENTATIONS IN ARCHITECTURE

The implementation of an Edge AI paradigm involves moving away from traditional encryption-less, centralized computing towards a zero-trust, peripheral architecture.

A. Confidential Computing Using Trusted Execution Environment

In order to ensure safety in the inference and training stages, trusted execution environments based on hardware are necessary. These can include ARM TrustZone, AMD SEV, or Intel TDX. Security micro-architectures such as TEEs will help to encrypt data stored in memory lines. This way, neither local system administrators nor host software of the edge will be able to access model parameters or datasets.

B. Federated Learning Across Distributed Edge Nodes

Where there is no possibility of combining data across the central server due to privacy or bandwidth limitations, federated learning architecture across edge nodes is implemented. With this approach, global model parameters are distributed in a secure way to local edge nodes. Training is conducted locally on the data available at the local node and only the gradients updates are uploaded to the aggregator using cryptography-based aggregation processes.

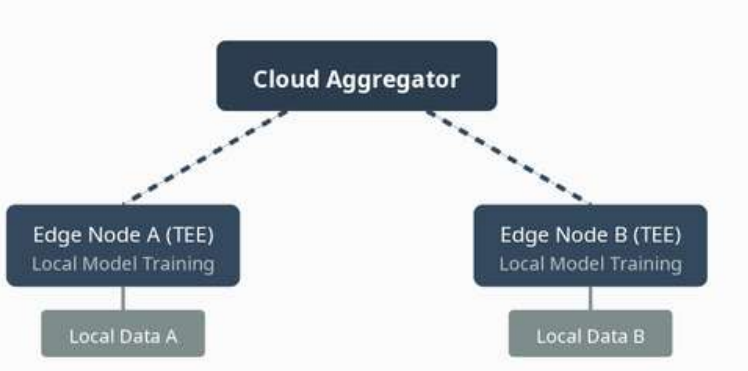

Fig. 1. Architectural schematic illustrating federated edge node topology with hardware TEE isolation and localized storage boundaries.

EXPERIMENTAL ASSESSMENT AND TRADING

The move towards localized edge computing comes with observable trade-offs with respect to processing latencies, power usage, and memory footprint of the hardware. Experiments to assess the variations on these benchmarks were performed in three main testbeds: Public Cloud, Hybrid Edge-Cloud, and Pure Local Edge Hardware.

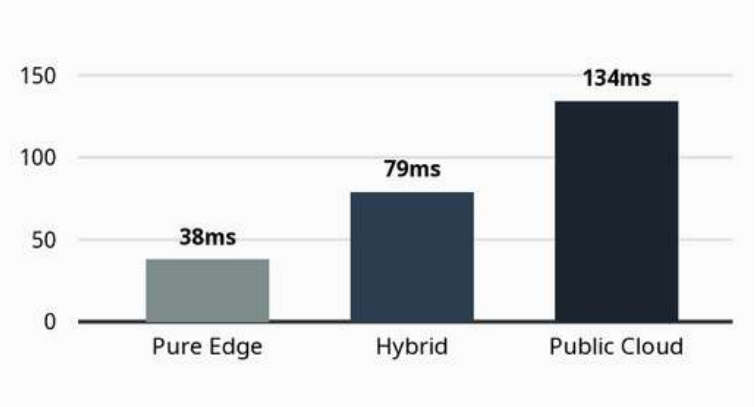

Fig. 2. Comparative API and inference latency (ms) across different architectural runtime environments.

Empirically observed data suggest that purely local edge setups have lower latencies (38ms) and therefore avoid any wide-area networking latencies. Meanwhile, cloud setups (134ms) have substantial latencies in transmission, while the hybrid setup finds an optimal middle ground (79ms).

Architecture	Latency	Autonomy	Bandwidth
Public Cloud	134ms	Low	High
Hybrid Cloud	79ms	Medium	Moderate
Pure Edge	38ms	Full	Minimal

CONCLUSION

Edge AI architectures are shifting from their specific use case to being a basic foundation of real-time intelligent applications. With the help of memory protection at the hardware level, local model quantization, and federated learning techniques, companies can successfully avoid the risks associated with central cloud architecture. The benefits of reduced latency discussed above confirm the necessity of edge deployment.

REFERENCES

- E. Albaroudi and M. A. Hatamleh, "Empowering data sovereignty through artificial intelligence: A framework for sustainable smart energy systems"
- S. Anasuri, "Confidential computing using trusted execution environments," Int. J. Artif. Intell., Big Data, Cloud Comput. Mobile Security, vol. 4, no. 2.
- S. Coleman, "A comprehensive evaluation of privacy-preserving mechanisms in cloud-based big data analytics: Challenges and future research directions"
- V. S. S. A. I. A. Daliparthi, "Digital sovereignty for collaborative AI engineering: A survey"
- L. Heim et al., "Governing through the cloud: The intermediary role of compute providers in AI regulation"

DEEKSHARAMBH 2026

Marian College of Arts & Science marked the beginning of the new academic year with "Deeksharambh 2026", the Academic Year Inauguration, held on 1 July 2026 at the MCAS Auditorium. The programme was inaugurated by Prof. Josukutty C. A., Director, UGC-MMTTC (HRDC), University of Kerala.

Following the Academic Year Inauguration, the college organized a three-day Student Induction Programme for the newly admitted students.

WORLD CUP-THEMED FOOTBALL TOURNAMENT

Football fever swept across the campus as students competed in a World Cup-themed tournament held from 13–15 July 2026. Representing iconic football nations, participants displayed remarkable skill, determination, and sportsmanship throughout the event.








TECH NEWS

EX-ANTE COMPETITION RULES FOR CLOUD SERVICES SEES PUSHBACK FROM 60% STAKEHOLDERS: CUTS STUDY

A recent study conducted by the Consumer Unity & Trust Society (CUTS International) found that nearly 60% of stakeholders oppose the introduction of ex-ante competition rules for cloud services. The survey gathered views from technology companies, industry experts, business organizations, legal professionals, and policymakers to understand opinions on regulating India's rapidly growing cloud computing sector. Most stakeholders believe introducing preventive regulations before any anti-competitive behavior occurs could discourage investment, increase compliance costs, and reduce the flexibility needed for innovation.

Cloud computing has become a critical part of the digital economy by providing businesses and governments with on-demand access to computing power, data storage, networking, and software over the internet. Major providers such as Amazon Web Services (AWS) Microsoft Azure, and Google Cloud have made cloud technology widely accessible. Due to their strong market presence, some policymakers have proposed ex-ante competition rules to prevent dominant companies from engaging in practices that could limit competition or create barriers for smaller providers.

The study recommends strengthening current regulations while promoting interoperability and data portability instead of introducing broad preventive rules. It concludes that a balanced regulatory approach is essential to protect competition while supporting innovation and the continued growth of the cloud computing ecosystem.

Source : ***The Indian Express***

YOUR CLAUDE AI CHATS MAY BE SEARCHABLE ON GOOGLE: HERE'S HOW TO KEEP THEM PRIVATE

A recent privacy concern involving Claude AI, the artificial intelligence chatbot developed by Anthropic, revealed that some users' shared conversations could appear in Google Search results. This happened because Claude allows users to generate public share links for their conversations. If these links are indexed by search engines such as Google, the conversations can become visible to anyone searching for related topics. Although chats are not public by default, users may unintentionally expose personal or sensitive information by sharing accessible links.

The issue has raised important questions about privacy and the handling of AI-generated conversations. Many users assume their chats with AI assistants remain private, but a shared conversation functions like a publicly accessible webpage and can be indexed unless restricted. As a result, anyone using relevant search terms may be able to find and read the shared conversation.

To protect user privacy, experts recommend avoiding the sharing of conversations containing personal information, financial details, passwords, or confidential business data. Users should carefully review their privacy settings and delete public links that are no longer needed. The incident also highlights the need for AI companies to strengthen privacy controls, provide clearer warnings when users create public links, and make it easier to manage or remove shared content. As AI becomes increasingly integrated into everyday life, maintaining strong privacy protections and educating users about safe sharing practices will remain essential.

Source : ***The Indian Express***

APPLE BRIEFLY TOPS $5 TRILLION MARKET VALUE, BECOMING SECOND COMPANY TO HIT MILESTONE

Apple briefly became the second company in history to reach a market valuation of over $5 trillion during intraday trading, marking a significant milestone in global financial markets. A company's market value, or market capitalization, is calculated by multiplying its current share price by the total number of outstanding shares. During trading, Apple's stock price rose high enough to push its market capitalization above the $5 trillion mark before later falling slightly below that level by the end of the session. Although the milestone was temporary, it highlights the company's strong financial performance and continued confidence from investors around the world. Nvidia was the first company to achieve a $5 trillion market valuation, making Apple the second member of this exclusive group.

Apple's remarkable rise in market value has been driven by strong demand for its products and services, including the iPhone, Mac, iPad, Apple Watch, and subscription-based services such as iCloud, Apple Music, and the App Store. Investors have also appreciated Apple's consistent profitability, massive cash reserves, regular share buyback programs, and stable long-term business strategy. Unlike several other major technology companies that have spent hundreds of billions of dollars on artificial intelligence infrastructure, Apple has taken a more measured approach by focusing on integrating AI features into its existing ecosystem while maintaining healthy cash flow and profitability. This strategy has reassured investors who are concerned about the rising costs of the global AI race.

Reaching a market value of $5 trillion demonstrates Apple's enormous influence on the global technology industry and financial markets. The achievement reflects the company's ability to maintain customer loyalty, generate consistent revenue, and adapt to changing technological trends.

Source : ***The Indian Express***

EDITORIAL BOARD