



Vita Digital Journal

Life through Technology & Innovation

Computer Science Department Monthly

Vol. 1 | Issue 8 | September 2026



VITA DIGITAL JOURNAL

Life through Technology & Innovation

Computer Science Department Monthly

Volume 1 | Issue 8 | September 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.

© 2026 Department of Computer Science, Marian College of Arts and Science. All rights reserved. No part of this publication may be reproduced without prior permission, except for educational and non-commercial use with proper citation.

✉ mcasmedia123@gmail.com

🌐 <https://www.mcas.ac.in/>

EDITORIAL



Technology has always been a race between creation and protection. But September 2026 gave us a glimpse of something fundamentally different: a future where artificial intelligence may fight artificial intelligence.

For years, cybersecurity depended largely on human experts discovering vulnerabilities, analysing attacks and building defences. Today, increasingly capable AI

systems can perform many of these tasks at machine speed. They can analyse enormous volumes of data, identify suspicious behaviour, discover software weaknesses and assist in developing sophisticated cyberattacks. This has created a new paradox: the technology capable of strengthening our digital defences can also make digital attacks more powerful.

Imagine a cybersecurity system that never sleeps. It continuously monitors a network, recognises an unusual pattern, predicts an attack, identifies the weakness being targeted and recommends—or even executes—a response within seconds. Such systems could transform cybersecurity from a largely reactive discipline into a continuously adaptive one.

But this future comes with an uncomfortable question:

Who watches the AI that watches our systems?

An AI defender can make mistakes—misunderstand instructions, respond too aggressively, or make decisions humans cannot easily explain. The challenge is not just building smarter machines, but creating intelligence that is trustworthy, controllable, and accountable.

This matters especially to today's computer science students. The programmer of tomorrow will not necessarily be judged only by how efficiently they write code. They will also need to understand AI, cybersecurity, ethics, privacy and the consequences of deploying intelligent systems in the real world.

The most important technology lesson of September may therefore be this:

The future is not simply about making AI more intelligent. It is about making intelligence more responsible.

As machines become capable of creating, defending and potentially attacking other machines, humanity must remain responsible for defining the boundaries.

The next great technological race may be **AI versus AI**.

Our greatest responsibility is to ensure that human wisdom remains above both.

- Chief Editor

Mr. Livin M Miranda

Head, Department of Computer Science

INDEX

Neuromorphic Computing: Creation of Computers Based on the Human Brain <i>Sandra Sunilkumar</i>	1
Memory-Safe Languages and the Shift from C/C++ to Rust: Drivers, Adoption and Open Challenges <i>Ridhin Ramesh</i>	5
Dark Web Investigation and Cryptocurrency Tracing : Techniques, Evidence Value, and Limitations <i>Liya Maria Robin</i>	10
Simulating the Network Before Building It : An Introduction to OPNET <i>Clare Maria Noel</i>	14
Geography of the Anthropocene: Spatial Signatures, Stratigraphic Debates, and Geographical Critique <i>Dr. Charutha Reghunathan</i>	18
Skill Enhancement Session	21
Academic Achievements	22
Graduation Day	23
Student Union	25
Tech News	26
Editorial Board	30

Neuromorphic Computing: Creation of Computers Based on the Human Brain



Sandra Sunilkumar

S3 BSc Computer Science

INTRODUCTION

Today's computers are highly efficient but function differently from the human brain. Computers perform tasks by processing information through commands and mathematically, while the brain consists of countless neurons that perform their tasks with the help of electric signals. Neuromorphic computing is one of the newest areas of computer science which aims to build computers that act like human brains.

Today's computers are highly efficient but function differently from the human brain. Computers perform tasks by processing information through commands and mathematically, while the brain consists of countless neurons that perform their tasks with the help of electric signals. Neuromorphic

computing is one of the newest areas of computer science which aims to build computers that act like human brains.

In contrast, rather than just enhancing the operation of traditional computers, neuromorphic computing applies methods that allow computers to process information in a more advanced manner.

WHAT IS NEUROMORPHIC COMPUTING?

In neuromorphic computing, the design of hardware and software is implemented to mimic several features of biological neural systems. There are artificial neurons and links between them that use the so-called spikes for their communication.

This is the opposite of traditional electronic devices that operate permanently in synchronization with their clock because in neuromorphic designs, instead of replicating every piece of information, computer systems are activated only when the signal or event of importance appears.

WHAT ARE THE DIFFERENCES FROM CONVENTIONAL COMPUTING?

Conventional computing architectures typically split the two functions of memory and processing. Therefore, data should constantly be transferred between memory and processing units, wasting time and energy.

Conversely, neuromorphic computing aims to combine both functions more closely together. It utilizes interconnections between artificial neurons for the representation of information, thus performing computations locally.

This technology can considerably lower energy consumption and boost efficiency of data processing at the same time.

USES OF NEUROMORPHIC COMPUTING

Neuromorphic computing can offer several advantages in situations where time is important while efficiency of computer operations is paramount.

For instance, neuromorphic computing can be used in:

- **Artificial Intelligence-based Robots:** It would enable robots to process sensor data quickly and react promptly to the surrounding environment.
- **Autonomous systems:** It is possible to build low-power smart systems capable of just-in-time processing of environmental information.
- **Smart sensors:** Such devices would recognize essential events without transmitting all the collected data to the computer.
- **Edge computing:** An application of neuromorphic chips in edge devices.
- **Scientific research:** Neuroscience can benefit from

getting new possibilities for research and analysis.

ADVANTAGES

A distinctive feature of neuromorphic computing is its potential for energy efficiency. The human brain manages to perform a multitude of computations with very low energy consumption. Neuromorphic scientists try to make use of some principles at the heart of biological computations.

Neuromorphic systems might be very appropriate for processing sensor data, especially in cases when data comes as a stream of events.

DISADVANTAGES

Neuromorphic computing is a relatively new field which has to deal with many challenges. It is quite challenging to design appropriate hardware, while programming neuromorphic computers may demand different approaches than traditional software programming.

Researchers need better algorithms and development tools to compare neuromorphic solutions with conventional computing systems.

Moreover, the human brain is very complex, and engineers face a real challenge reproducing its functioning by artificial means.

PERSPECTIVES

Neuromorphic computing can become a significant part of the computer architecture in the future, especially for low-power AI development and edge devices. Rather than fully substituting traditional computers neuromorphic processors may operate together with standard CPUs and GPUs, and other particular hardware.

FINAL THOUGHTS

The concept of neuromorphic computing signifies a novel approach to computers. Neuromorphic computing does not merely aim to improve the speed of conventional computers. Rather, it looks into computer design based on the human brain. In spite of the staid of the technology, its potential for effective event-based calculations makes it an interesting and fairly rare subject area in computer science.

As the study of the connection between biological intelligence and

computing continues, neuromorphic computing is expected to give rise to a new kind of computation and energy-efficient computers.

REFERENCES

- Carver Mead, Analog VLSI and Neural Systems, Addison-Wesley, 1989.
- IBM Research, “TrueNorth: Brain-inspired computing.”
- Intel, “Loihi Neuromorphic Research Chip.”
- European Commission, “Human Brain Project.”
- IEEE, publications and research on neuromorphic engineering and spiking neural networks.

Memory-Safe Languages and the Shift from C/C++ to Rust: Drivers, Adoption and Open Challenges



Ridhin Ramesh

S5 BSc Computer Science

INTRODUCTION

Memory-safety problems such as buffer overflows and use-after-free errors remain a major source of software vulnerabilities in C and C++. This paper examines the shift toward memory-safe languages, focusing on Rust. It explains Rust's ownership and borrowing model, reviews adoption in Android and the Linux kernel, summarizes U.S. policy guidance, and discusses unsafe code, interoperability, and legacy systems. The evidence supports gradual adoption: use memory-safe languages for new and high-risk code while retaining mitigations for legacy C/C++.

C and C++ remain dominant in operating systems, browsers, and embedded software because they provide low-level control with little runtime overhead. That control also

places responsibility for memory allocation, bounds, and object lifetimes on programmers. Microsoft has reported that about 70% of its CVEs are memory-safety issues, while U.S. security guidance recommends considering memory-safe languages such as Rust where practical. The transition is increasingly treated as a security and policy issue.

THE MEMORY-SAFETY PROBLEM

Memory safety is the guarantee that all memory accesses are defined. Examples of memory-safety violations include buffer overflows, use after free, and double free, which attackers use to execute code, leak memory, or crash the program. Memory safety is guaranteed by most commonly used languages, like Java, C#, Go, Swift, and Python, via

garbage collection and run-time checks. System-level languages, which cannot afford a run-time overhead, have rarely been.

Memory-safety violations are mainly spatial or temporal. Spatial flaws include buffer overflows, while temporal flaws include use-after-free and double-free errors. These are common in C/C++ because of unchecked array access, limited pointer bounds information, and undefined behavior, potentially leading to crashes, information leaks, or arbitrary code execution.

Techniques such as ASLR, sanitizers, fuzzing, and compiler hardening make exploitation harder but do not eliminate the underlying bugs. Memory-safe languages prevent many of these errors by design, using mechanisms such as bounds checking and automatic memory management. However, garbage collection can introduce runtime overhead and increased memory usage, which is why systems such as kernels, firmware, and networking software have traditionally relied on C/C++. Overall, preventing vulnerabilities at the source provides stronger and more reliable guarantees than simply mitigating their exploitation.

HOW RUST ENURES MEMORY SAFETY

Rust aims to combine systems-level performance with memory safety without requiring a garbage collector. Its key feature is ownership, where each value has one owner and memory is automatically released when the owner goes out of scope. Rust's borrowing system allows either multiple shared references or one mutable reference, while ensuring references never outlive the data they refer to. These rules are checked statically by the compiler.

For example, moving a heap-allocated value transfers ownership and prevents use of the original variable, avoiding double-free and use-after-free errors. Lifetimes prevent dangling references, while Rust's aliasing rules help prevent data races. The Option type handles absent values explicitly, and Result provides structured error handling. Since these checks happen at compile time, safe Rust does not require garbage collection or per-object runtime bookkeeping.

The safety of Rust's foundations is supported by RustBelt, which formally verifies key parts of the

language and selected unsafe library abstractions. However, Rust also provides unsafe code for operations the compiler cannot verify, such as raw-pointer dereferencing and foreign-function calls. Unsafe operations should therefore be isolated behind safe interfaces and carefully checked to maintain their required safety guarantees.

ADOPTION AND POLICY

Policy interest in memory safety has increased as industry experience has grown. Microsoft recommended safer programming languages in 2019, followed by NSA guidance in 2022 that included Rust among memory-safe languages and encouraged migration from C/C++. In February 2024, the U.S. Office of the National Cyber Director (ONCD) also promoted memory-safe languages, alongside memory-safe hardware and formal methods.

The policies differ in focus. The NSA emphasizes risk management by preferring memory-safe languages while maintaining protections for existing C/C++ code. The ONCD takes a broader approach, considering software-security measurement and complementary technologies.

A joint U.S., Australian, and Canadian report also highlights memory-safety risks in critical open-source projects and recommends addressing third-party dependencies.

Overall, the guidance supports a gradual transition, focusing on new development, high-risk components, long-term migration plans, and software dependencies rather than rewriting existing systems. This approach recognizes that modern software relies on complex supply chains, making memory safety an ecosystem-wide concern.

EVIDENCE FROM DEPLOYMENTS

Publicly available information on memory safety is best for Android. According to Google, for the first time ever, memory safety issues made up less than 20 percent of all vulnerabilities affecting Android software by 2025, compared to an astounding 76 percent in 2019 . The main goal in Google's program is not to rewrite old code but to write new code using only memory-safe languages . Google also mentions the 1000x reduction in memory safety vulnerability density found in

their Rust software compared to its C and C++ codebase, with

reductions in rollback by 4x and code review time by 25 percent.

Indicator	Reported value	Ref.
Share of Microsoft CVEs from memory safety	~70% per year	[1]
Android memory-safety share of vulns.	<20% in 2025	[5]
Vuln. density vs. Android C/C++	~1000x lower	[5]
Rollback rate, Rust vs. C/C++ changes	4x lower	[5]
Review time, Rust changes	25% less	[5]

The Android figures should be interpreted carefully because they are vendor-reported and may reflect newer components written in memory-safe languages. Comparisons between Rust and C/C++ can also be influenced by differences in teams and codebases. Despite these limitations, the decline in memory-safety vulnerabilities suggests that memory-safe development does not necessarily slow down software development.

Linux provides another important example. Rust was introduced experimentally into the Linux kernel in 2022, and by December 2025, maintainers considered it a core part of the kernel. This shows that Rust can coexist with Linux's

existing C codebase and supports a hybrid approach, where Rust components work alongside C rather than requiring a complete rewrite.

EVIDENCE FROM DEPLOYMENTS

Rust is not a complete solution. Unsafe Rust can still contain serious vulnerabilities, as shown by CVE-2025-48530 in an unsafe Rust program processing AVIF images. This highlights the need for defense in depth, as vulnerabilities can still occur when code operates outside the compiler's safety guarantees. Unsafe sections should therefore be kept small, clearly documented, carefully reviewed, and tested using

tools such as fuzzers, sanitizers, and Miri.

CONCLUSION

Memory-unsafe languages remain a significant source of serious vulnerabilities despite existing mitigations. Rust shows that memory safety can be achieved in systems software without sacrificing performance or requiring garbage collection, with large-scale adoption demonstrated by Google and the Linux kernel. A gradual approach is therefore practical: use memory-safe languages for new and high-risk code while isolating unsafe sections.

A four-part strategy is recommended:

- Use memory-safe languages for new and high-risk code
- Create migration roadmaps covering dependencies
- Isolate and audit unsafe code
- Maintain protections for C/C++ code, while future research should examine migration costs, unsafe Rust, cross-language risks, and memory-safe hardware.

REFERENCES

- Microsoft Security Response Center, “We need a safer systems programming language,” MSRC Blog, Jul. 18, 2019.
- National Security Agency, “Software memory safety,” Cybersecurity Information Sheet U/OO/219936-22, Ver. 1.1, Apr. 2023.
- Office of the National Cyber Director, “Back to the building blocks: A path toward secure and measurable software,” The White House, Washington, DC, USA, Feb. 2024.
- CISA, FBI, ASD's ACSC, and CCCS, “Exploring memory safety in critical open source projects,” Joint Rep., Jun. 2024.
- J. Vander Stoep, “Rust in Android: Move fast and fix things,” Google Security Blog, Nov. 2025.
- S. Klabnik and C. Nichols, The Rust Programming Language.

Dark Web Investigation and Cryptocurrency Tracing : Techniques, Evidence Value, and Limitations



Liya Maria Robin

S5 BSc Computer Science

INTRODUCTION

Darknet markets are internet-based marketplaces accessible via anonymous networks where goods like drugs, data thefts, and fraud services are sold, typically using cryptocurrency. According to Chainalysis, darknet market activity amounted to almost US\$2.6 billion in 2025, and it is described as resilient to enforcement action despite several such efforts . Enforcement efforts continue regardless. In June 2025, in an effort by authorities from six nations, one of the longest-running drug markets on the dark web was taken down, namely Archetyp with more than 600,000 customers and transactions amounting to at least EUR 250 million . For digital forensic investigators, the typical question raised by such cases is how to conduct investigation where

network layer and payment layer are both designed to provide anonymity?



DARK WEB ECOSYSTEM

Tor is a circuit-based, low-latency anonymity network. Tor has been designed in a way to include location-hidden services which can be accessed through rendezvous points, meaning that neither the client nor the server needs to disclose their network location to each other. Darknet markets usually operate as such hidden services, making it impossible for the investigator to use regular IP-address traces in order to locate the

operators.

Several measurement studies have demonstrated that it is still possible to conduct systematic research on these markets. For example, Christin measured the Silk Road market for

several months by crawling it on a daily basis. He was able to identify more than 24,400 products and found out that sellers were earning about US\$1.2 million per month. It was concluded that the market was mostly used for purchasing illegal controlled substances, and it brought up many ethical issues for the researchers.

TRACEABILITY OF CRYPTOCURRENCIES

Second investigative approach is made possible through public blockchains. Bitcoin ownership is anonymous, however, the money movement is publicly observable. As was demonstrated by Meiklejohn et al., heuristics of shared ownership, for example, addresses that spend money together as input to a common transaction, make it possible to cluster addresses. Afterward, the owners of clusters could be revealed using a purchase and observing which addresses make such a purchase. Clustering

makes each address an entity, like exchange, service, or market, so that payments can be traced from the buyer/vendor to the point when identity logs can be found.

Privacy - preserving cryptocurrencies add another layer of complexity to the scenario. Monero obscures the actual input of a transaction through the use of dummy inputs, also known as mixins. According to Möser et al., around 62% of inputs containing at least one mixin were subject to a chain reaction attack, with the real input potentially identifiable from age heuristics in 80% of cases. However, the subsequent updates of the protocol have changed the situation; according to Hinteregger and Haslhofer, only a minority of inputs were traceable based on recent data, and no heuristics were significantly better than random guessing.

MACHINE LEARNING BASED ANALYSIS

Manual detection is not feasible when there are millions of transactions involved, which is why researchers have used machine learning. Weber et al. introduced the Elliptic data set consisting of an annotated transaction network of

Bitcoin involving more than 200,000 nodes with 234,000 payments and 166 features, which is used for evaluating classification techniques for identifying illicit transactions. The random forest classifier was found superior to graph convolutional networks by the researchers .



CASE STUDY AND PROOF

Archetype provides an example of how the layers work. During 11 – 13 June 2025, the coordinated attacks were focused on the admin, a moderator, top vendors, and the infrastructure, resulting in eight people being arrested. The market had around 3,200 vendors and approximately 17,000 postings, and it was one of those rare markets which allowed the sale of fentanyl and other synthetic opioids . Investigations in relation to this were coordinated by Eurojust and

Europol . In this case, both infrastructure investigation and financial analysis were needed, rather than just blockchain analysis.

Indicator	Reported value
Darknet-market on-chain flows, 2025	~US\$2.6 billion
Archetype Market users / volume	600,000+ / ≥€250M
Silk Road seller revenue (2012)	~US\$1.2M per month
Monero inputs open to chain-reaction analysis (2018 study)	~62%
Elliptic labeled Bitcoin transactions	200,000+

The information contained in the blockchain can be used in strategic analysis as well. Chainalysis indicates that the fall in fentanyl transactions through the blockchain network corresponds to the decrease in the number of people who died from fentanyl overdose in the United States.

LIMITATIONS

There are several limitations to blockchain-based evidence. The heuristics used for clustering are based on the assumption of common ownership and generate probabilistic rather than absolute attributions, which must therefore be supported by off-chain evidence like exchange data, seized computers, and controlled buys. Privacy coins and protocol updates can very quickly render useless any tracing technique that is published.

Law enforcement is also short-lived because markets relocate and resurface, and the total volume in 2025 was still quite high despite numerous takedown operations. Lastly, investigations span multiple jurisdictions, as illustrated by the multi-jurisdictional Archetype investigation, which means that researchers need to take into account ethics and legality.

CONCLUSION

To investigate darknet activity, a multi-layered approach should combine knowledge of hidden-service infrastructure, market analysis, blockchain transaction tracking, and international cooperation. Studies show that pseudonymous cryptocurrencies leave persistent and analysable trails, while machine learning can help identify patterns and prioritize investigative leads. However, attribution remains probabilistic and requires continuous reassessment as technologies and protocols evolve. Therefore, blockchain analysis should be treated as one of several supporting pieces of evidence, rather than as definitive proof of identity or activity.

REFERENCES

- Chainalysis, “Drugs and darknet markets: 2026 Crypto Crime Report,” Chainalysis Blog, 2026.
- Eurojust, “Largest illegal trading platform for drugs taken down,” Press Release, Jun. 16, 2025.
- R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The second-generation onion router,” in Proc. 13th USENIX Security Symp., San Diego, CA, USA, Aug. 2004.
- N. Christin, “Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace,” in Proc. 22nd Int. World Wide Web Conf. (WWW), 2013.
- S. Meiklejohn et al., “A fistful of bitcoins: Characterizing payments among men with no names,” in Proc. ACM Internet Measurement Conf. (IMC), 2013.
- M. Möser et al., “An empirical analysis of traceability in the Monero blockchain,” Proc. Privacy Enhancing Technologies, vol. 2018, no. 3, pp. 143–163, 2018.

Simulating the Network Before Building It : An Introduction to OPNET



Clare Maria Noel

S5 BSc Computer Science

INTRODUCTION

Every network engineer eventually encounters a point where a proposed change is too risky to implement directly on a live network. Expanding a branch office, introducing a new routing protocol, or modifying failover paths can have significant consequences for bandwidth utilization, convergence time, and the reliability of real-time applications such as video conferencing. Testing such changes in a production environment is costly and potentially disruptive, while relying solely on theoretical assumptions provides limited assurance. Network simulation addresses this gap by providing a controlled environment in which network architectures, protocols, traffic patterns, and failure scenarios can be evaluated before deployment. For nearly two

decades, OPNET was among the most influential tools in this field, offering network engineers and researchers a sophisticated platform for modelling and analysing complex network behaviour.

WHAT OPNET IS

OPNET began as a research project at MIT and was commercialized in the 1980s by brothers Marc and Alain Cohen, growing into OPNET Technologies. Riverbed Technology acquired the company in 2012, and the simulation product line continued under the Riverbed name as Riverbed Modeler. You will still see the older name throughout textbooks, theses, and journal papers, so it is worth knowing both.

At its core, OPNET is a discrete-event simulator. Instead of advancing a clock in fixed ticks, it

jumps from one event to the next: a packet arrives, a timer expires, a link fails. Nothing happens between events, so the simulator skips the dead time and can model long periods of network behavior in a manageable run time. Each event triggers some logic, which may schedule further events, and the simulation proceeds until the event queue is empty or a time limit is reached.

THE THREE-LAYER MODELING HIERARCHY

Network domain: This is the topology view: routers, switches, servers, workstations, wireless nodes, and the links connecting them. You build it graphically, much like drawing a network diagram.

Node domain: Each device consists of connected modules such as protocol layers, queues, processors, and transmitters/receivers. A router connects interface, routing, and forwarding components.

Process domain: Each module's behavior was defined as a finite state machine with states, transitions, and attached code, written in a C-based language for fine-grained protocol control.

This layering mirrors how networks actually work: topology at the top, device architecture in the middle, protocol logic at the bottom. A researcher could reuse the standard library models for most of the network and replace only one process model, such as a custom MAC protocol or a modified routing algorithm.

A simulation project in OPNET generally follows a repeatable workflow

- Build the scenario: Lay out the topology and configure devices, links, and applications.
- Define traffic: Model realistic workloads such as web browsing, email, file transfer, database access, or voice and video, either from built-in application profiles or from measured traces.
- Choose statistics: Select what to collect: end-to-end delay, throughput, link utilization, packet loss, queue depth, jitter.
- Run and compare scenarios: The real value is in comparison. Duplicate the baseline scenario, change one variable, and compare the results side by side.

- Analyze: Plot the statistics, check confidence across multiple random seeds, and draw conclusions.

A classic example is comparing routing protocols. Build the same topology twice, one running OSPF and one running EIGRP, fail a link partway through the run, and measure how long traffic takes to recover. The outcome is a set of graphs rather than an opinion, which is exactly what makes simulation persuasive in a journal article.

WHERE OPNET MADE ITS MARK

OPNET showed up across a wide range of work:

- Enterprise capacity planning: testing whether a network could absorb growth before money was spent on upgrades.
- Quality of service studies: evaluating queuing schemes like priority queuing and weighted fair queuing for voice and video.
- Wireless and mobile research: including ad hoc network routing, WLAN performance, and cellular technologies.

- Teaching: where universities used academic licenses to let students experiment with networks they could never afford to build in a lab.

LIMITS WORTH BEING HONEST ABOUT

A responsible article should also cover the caveats, because simulation results are only as good as the model behind them

- Model fidelity: If the traffic model is unrealistic or a device model omits important behavior, the results may appear precise but still be inaccurate. Therefore, simulations are only as reliable as the assumptions and models used.
- Validation: Good practice means checking the model against measurements from a real network wherever possible. Skipping this step is the most common weakness in published simulation studies.
- Scale and speed: Packet-level simulation of very large networks can become slow, which pushes some studies toward hybrid or analytical approaches.

- Licensing and openness: OPNET and Riverbed Modeler are commercial, closed-source tools, limiting reproducibility and exact experiment replication.

THE WIDER LANDSCAPE

That last point explains why open-source tools have gained ground. ns-3 is the successor to the widely used ns-2 and is popular in research for its transparency. OMNeT++ (easily confused with OPNET by name, but a separate project) offers a similar modular, hierarchical approach in an open ecosystem. For more hands-on emulation rather than pure simulation, tools like Mininet and GNS3 run real network software in virtual environments. Each involves a trade-off between realism, speed, and effort.

WHY IT STILL MATTERS

Even as tools evolve, the discipline OPNET taught is durable: model before you build, change one variable at a time, measure what matters, and validate against reality. Those habits apply whether you are studying a campus backbone, a 5G scheduler, or a security architecture. If you can explain a

network well enough to simulate it, you understand it well enough to improve it.

REFERENCES

- X. Chang, “Network Simulations with OPNET,” Proceedings of the 1999 Winter Simulation Conference, 1999.
- T. S. Eugene Ng, I. Stoica, and H. Zhang, “A Data-Centric Approach to Network Simulation,” ACM SIGCOMM Computer Communication Review, 2000.
- G. F. Riley and T. R. Henderson, “The ns-3 Network Simulator,” in Modeling and Tools for Network Simulation, Springer, 2010.
- A. Varga and R. Hornig, “An Overview of the OMNeT++ Simulation Environment,” Proceedings of the 1st International Conference on Simulation Tools and Techniques, 2008.
- M. P. C. S. A. A. McCanne et al., “A Network Simulator for Internet Protocols,” Computer Communication Review, ACM.

Geography of the Anthropocene: Spatial Signatures, Stratigraphic Debates, and Geographical Critique



Dr. Charutha Reghunathan

Head,
Dept of Geography

ABSTRACT

In 2000, Crutzen and Stoermer introduced the term “Anthropocene” to describe a new interval in which human activity became a major force shaping the Earth system. They placed its beginning in the late eighteenth century, when industrialization accelerated. Two decades later, the concept has become central to debates in geology, ecology, history, and the humanities. Geography, with its focus on relationships between people and environments across space and scale, is both challenged and enriched by the Anthropocene. The key question is therefore not only when humans became a geological force, but also where, how unevenly, and through whose actions this transformation occurred.

ORIGINS AND THE STRATIGRAPHIC DEBATE

Steffen and colleagues traced the idea through several phases: an Industrial Era starting around 1800, a Great Acceleration after 1945, and a possible future phase of planetary stewardship. The Great Acceleration is backed by 24 indicators, ranging from population and energy use to fertilizer consumption and ocean acidification, all of which rise sharply from the 1950s onward.

The Anthropocene Working Group (AWG) argued that the mid-twentieth century is the best place to draw the boundary, because globally synchronous signals such as radionuclide fallout, plastics and altered sediment chemistry show up at that time. Even so, in 2024 the International Union of Geological

Sciences chose not to ratify a formal Anthropocene epoch, so the term stays informal. This matters for geography. The concept remains useful as an analytical frame whether or not it ever becomes an official unit of the geological time scale.

SPATIAL SIGNATURES OF THE ANTHROPOCENE

Land, biomass and material stocks :

Human influence on land is older than industrialization. Archaeological and land-use reconstructions show that over thousands of years, societies had already reshaped most terrestrial ecosystems through hunting, fire, farming and herding. What sets the present apart is scale and speed. Human-made mass, including concrete, aggregates, metals and plastics, now roughly equals all living biomass on the planet. Domesticated livestock also far outweigh wild mammals in the global biomass distribution.

Urbanization :

Urban land is one of the most spatially concentrated and fastest-growing forms of land change. Forecasts suggested that urban land area could roughly triple between

2000 and 2030, with most of that growth in Asia and Africa and often in biodiversity-rich regions. Cities are therefore places where Anthropocene material piles up, and also key arenas for adaptation.

Planetary boundaries :

The planetary boundaries framework sets out the limits within which human societies can operate safely. A recent assessment found that six of the nine boundaries have been crossed, among them climate change, biosphere integrity, land-system change and novel entities. The pressures and the responsibility are not spread evenly across the globe. Emissions, resource extraction and waste flows are often far removed from the places that bear their impacts.

GEOGRAPHICAL CRITIQUES

Lorimer argues that the Anthropocene is not a single idea but several: a geological proposal, an Earth-system account and a cultural discourse. Geographers and related scholars have used this plurality to question the universal “anthropos” the term implies. Critics point out that a species-wide story hides differences of class, colonial

history, race and economic system, and they suggest alternatives such as the Capitalocene or the Plantationocene. Some physical geographers add that human and natural processes cannot be pulled apart and should be studied together, not side by side. What these critiques have in common is the view that any account of the Anthropocene has to be situated: attentive to place, power and scale.

METHODS AND RESEARCH AGENDA

Cloud platforms such as Google Earth Engine allow researchers to analyze decades of satellite imagery at planetary scale. Combined with open datasets on land cover, nightlights, built-up areas, and climate, they enable reproducible mapping of Anthropocene change. Four priorities emerge: (1) combine Earth observation with historical and archaeological data, (2) measure uneven exposure and responsibility through material flows, (3) account for uncertainty, scale effects, and data bias, especially in the Global South, and (4) combine quantitative mapping with community-based research to include lived experiences.

CONCLUSION

The Anthropocene is best understood geographically, as a set of uneven and connected transformations and not as one uniform event. Debate over stratigraphic decisions will go on, but the empirical record of accelerating land, material and biogeochemical change is clear. Geography is well placed to connect this planetary picture with regional processes and social difference, and to offer evidence and concepts for fairer responses.

REFERENCES

- P. J. Crutzen and E. F. Stoermer, "The 'Anthropocene,'" Global Change Newsletter, May 2000.
- W. Steffen, J. Grinevald, P. Crutzen, and J. McNeill, "The Anthropocene: Conceptual and historical perspectives," Phil. Trans. R. Soc. A
- J. Zalasiewicz et al., "When did the Anthropocene begin? A mid-twentieth century boundary level is stratigraphically optimal".
- J. Lorimer, "The Anthro-scene: A guide for the perplexed".

Skill Enhancement Session

Learn Upgrade Grow



Google

Thiruvananthapuram, Kerala, India
3, Kazhakuttom Rd, Menamkulam, Thiruvananthapuram,
Keralam 695582, India
Lat 8.55977° Long 76.857553°
Thursday, 24/09/2026 02:22 PM GMT +05:30

MARIAN COLLEGE OF ARTS & SCIENCE
Menamkulam, Kazhakuttom,
Thiruvananthapuram - 695582

AKIRA
Knowledge Hub

In Association with
IQAC, MCAS

SKILL ENHANCEMENT SESSION

Organised by
Department of Computer Science
and
Akira Knowledge Hub

Learn Upgrade Grow

24 Sep 2026
(Thursday)
2:00 p.m.

Venue:
MCAS Auditorium

Learn | Enhance | Excel

Good session with great insights and opportunities to learn and grow!



Thiruvananthapuram, Kerala, India
3, Kazhakuttom Rd, Menamkulam, Thiruvananthapuram,



MCAS *

ACADEMIC ACHIEVEMENTS

S4 Bsc Computer Science



Santhipriyan M
SGPA : 8.83 (A+)



Clare Maria Noel
SGPA : 8.7 (A+)



Fathima Sadiq
SGPA : 8.65 (A+)



Kailas Nath
SGPA : 8.53 (A+)



Praveena M P
SGPA : 8.09 (A)



Joel George Mathew
SGPA : 8.04 (A)

The Graduate Post

Celebrating Dreams, Achievements, and New Beginnings



CLASS OF 2023-26

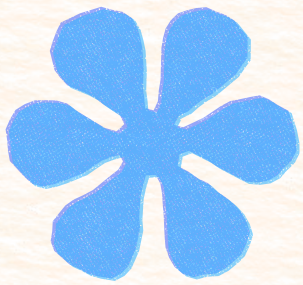
The Graduate Post

Celebrating Dreams, Achievements, and New Beginnings



CLASS OF 2023-26

MEET YOUR STUDENT UNION



TECH NEWS

APPLE ENTERS THE FOLDABLE PHONE RACE WITH THE IPHONE DUO

Apple has officially entered the foldable smartphone market with the launch of the iPhone Duo, making 2026 a major turning point for the company's hardware strategy. The device was unveiled during Apple's September product event and became the headline announcement of the company's first major event under CEO John Ternus. After years of watching Samsung, Google and other manufacturers experiment with foldable designs, Apple has now brought its own interpretation of the category to market.

The iPhone Duo is built around a large 7.6-inch internal display that folds into a more conventional 5.4-inch external screen. The design is intended to combine the portability of a phone with some of the productivity advantages of a small tablet. Apple has also focused on multitasking, allowing users to take advantage of the larger display for activities such as reading, editing documents, browsing and running multiple applications.

At the centre of the device is Apple's A20 Pro chip, which the company says is designed to provide the processing power needed for

demanding applications and on-device artificial-intelligence features. The phone also uses a specialised cooling system and a dual-battery arrangement to manage the thermal and power demands of a thin foldable device. Storage options reportedly extend as high as 2TB, positioning the Duo as a premium product rather than an experimental budget device.

The launch is significant beyond the product itself. Apple's entry gives foldable smartphones a powerful mainstream competitor and could accelerate development across the entire category.

Ultimately, the iPhone Duo represents Apple testing a new form factor while bringing its familiar ecosystem philosophy to foldable hardware. Whether it becomes a major product category or remains a premium niche device will depend on durability, battery life, software optimisation and consumer willingness to pay. Either way, September 2026 marked the moment Apple finally joined one of the smartphone industry's most closely watched hardware battles.

Source : [Reuters](#)

NVIDIA UNVEILS AN OPEN PLATFORM DESIGNED TO KEEP AI AGENTS UNDER CONTROL

Nvidia has introduced a new security platform aimed at one of the fastest-growing challenges in artificial intelligence: keeping autonomous AI agents from taking harmful or unintended actions. On September 28, the company announced the Open Agent Safety Platform, an open-source approach intended to give organisations stronger controls over AI systems that can independently interact with computers, software and online services.

The development reflects a major shift in the way AI is being used. Traditional chatbots mostly respond to prompts, but AI agents can perform tasks on behalf of users. An agent may read files, access applications, execute code, communicate with other systems or make decisions across several steps. That extra autonomy makes agents more useful, but it also creates a new security problem: an agent that is compromised or behaves incorrectly can potentially cause damage much faster than a conventional application.

Nvidia's platform includes two major components. OpenShell is designed to verify whether an AI agent has the authority to perform a particular action.

Sentry, meanwhile, monitors agent behaviour and can quarantine suspicious activity. The idea is similar to having security boundaries around an AI worker: the system should know what the agent is allowed to access, while continuously watching for behaviour that falls outside those limits.

The announcement is significant because the AI industry is increasingly moving toward agentic computing. If AI agents become digital employees capable of performing tasks continuously, security cannot depend only on trusting the model itself. Organisations will need permission systems, monitoring, isolation, logging and rapid shutdown mechanisms.

Nvidia's platform is therefore part of a broader effort to build a security layer around autonomous AI. The technology does not eliminate every risk, and no monitoring system can guarantee that an AI agent will never behave unexpectedly. But as agents become more powerful, the ability to restrict and observe their actions is likely to become just as important as improving their intelligence

Source : [*Associated Press \(AP\)*](#)

INDIA SEES ONE OF THE WORLD'S STEEPEST IPHONE PRICE INCREASES

Apple's September product launch brought another major development for Indian technology consumers: a sharp increase in iPhone prices. According to Reuters, India experienced some of the steepest price increases among major markets following Apple's introduction of its new generation of iPhones, including the company's first foldable model. The increases have drawn attention because India has become an increasingly important manufacturing and consumer market for Apple.

The price changes affected multiple models rather than being limited to Apple's most expensive devices. Reuters reported that some Indian iPhone prices increased by as much as 41 percent, while U.S. increases were considerably lower. For Indian consumers, the change makes Apple's premium positioning even more pronounced and could affect purchasing decisions, especially among buyers who traditionally wait for older models to become cheaper after a new generation launches.

One of the biggest examples involved the standard iPhone 17, whose Indian price rose to ₹99,900. The premium iPhone Air also saw a dramatic increase, reaching ₹2,24,900.

The first-generation foldable iPhone Duo carries an even higher premium in India compared with its U.S. price. Such differences are particularly noticeable in a country where consumers are highly price-sensitive and where Android manufacturers offer a large range of flagship devices at lower prices.

The price increases could have broader consequences for the Indian smartphone market. Consumers may hold onto older phones for longer, choose previous-generation models, or move toward competing Android flagships. Apple's strong brand loyalty and ecosystem may protect demand among some buyers, but a major price gap can still change how consumers evaluate value.

The same global demand that is driving enormous investment in data centres is also influencing the cost of everyday hardware. For Indian consumers, the result is simple but significant — buying a new iPhone in 2026 can require substantially more money than it did just a year earlier.

Source : [Reuters](#)

MAJOR AI COMPANIES AGREE TO VOLUNTARY SAFETY MEASURES

Artificial intelligence safety became one of the biggest technology stories of September when major AI and technology companies agreed to a voluntary framework for overseeing the development of increasingly powerful AI systems. The agreement was announced on September 29 following a meeting involving U.S. President Donald Trump and leaders from several of the industry's biggest companies.

Companies associated with the agreement include Google, Meta, OpenAI, Nvidia, Anthropic and xAI. Rather than creating a new government law, the arrangement relies on companies introducing internal controls and allowing independent external auditors to examine aspects of their AI development.

Participating companies are also expected to create board-level structures for reviewing audit findings.

The announcement comes at a time when AI systems are becoming more autonomous. Earlier generations of chatbots generally waited for users to ask questions and then generated an answer. Newer AI agents can interact with software, use tools, browse information, write and execute code, and complete multi-step tasks.

This additional capability creates new opportunities but also creates new risks because an AI system can potentially take actions rather than simply produce text.

The agreement therefore reflects a difficult balancing act. Technology companies want to continue developing increasingly capable AI because of its potential benefits in science, medicine, education, software development and business. Governments and researchers, meanwhile, want mechanisms that reduce the chances of systems being misused, compromised or deployed before their risks are understood.

Whether the September agreement becomes an important milestone or simply another voluntary industry pledge will depend on what happens next. The real test will be whether companies actually implement strong controls, allow meaningful independent scrutiny and respond openly when problems are discovered. As AI becomes more autonomous, safety can no longer be treated as an optional feature added after development. It is becoming a central part of the technology itself.

Source : [*Associated Press \(AP\)*](#)

EDITORIAL BOARD

PATRON

Fr. Albert M

Manager

ADVISOR

Prof. Dr. K. Y. Benedict

Principal

CHIEF EDITOR

Mr. Livin M Miranda

HOD, Department of Computer Science

FACULTY COORDINATOR

Ms. Rini Amado

Assistant Professor, Department of Computer Science

REVIEW COMMITTEE

Ms. Anila A J

Assistant Professor,
Department of Computer Science

Ms. Mubeena J

Assistant Professor,
Department of Computer Science

STUDENT EDITORS

Santhipriyan M

S5 BSc Computer Science

Joel George Mathew

S5 BSc Computer Science

DESIGN TEAM

Kailasnath P N

S5 BSc Computer Science

Alma Christopher

S5 BSc Computer Science