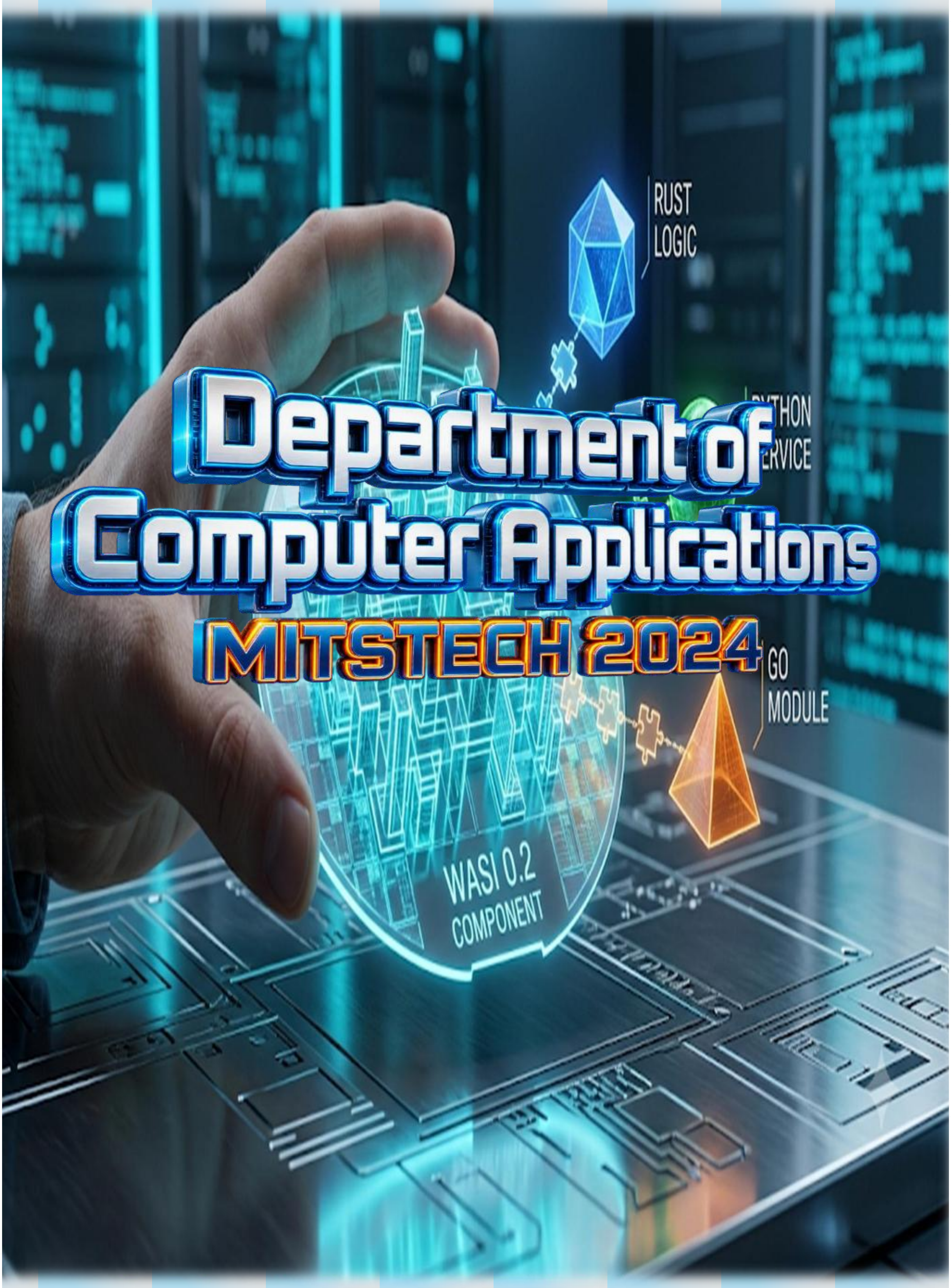
MITS MADANAPALLE

MADANAPALLE INSTITUTE OF TECHNOLOGY & SCIENCE

(UGC-AUTONOMOUS INSTITUTION)

Department of Computer Applications

MITSTECH 2024



MESSAGE FROM THE CORRESPONDENT

I feel exhilarated that the Department of Computer Applications of MITS is bringing out a magazine called MITSTECH from the year 2021. This Magazine brings out the intellectual brilliance in various new techniques introduced in Information Technology industry.

``HARD WORK, SINCERITY, DEDICATION AND ENTHUSIASTIC DEVOTION TO WORK WILL FETCH YOUR UNBOUND SUCCESS, MAY THE LORD SHOWER HIS BLESSINGS ON YOU``

I heartily congratulate the students and the staffs of MCA Department and Wish them a grand success.

Dr. N. Vijaya Bhaskar Choudary

Correspondent

MESSAGE FROM THE PRINCIPAL

Dr. C. Yuvaraj

Principal

I feel delighted about the magazine "MITSTECH" to be hosted by the Department of Computer Applications of MITS.

On this magnanimous occasion, I congratulate all the students and faculty members of department of Computer Applications for their great efforts and coordination in bringing out the magazine a great success.

MESSAGE FROM THE HEAD OF THE DEPARTMENT

Dr. N. Naveen Kumar

Head of the Department

MITSTECH is dedicated to addressing emerging topics and challenges in the field of technology. It aims to create awareness of new innovations, ideas, and technological advancements among students and readers.

I wish the readers of "MITSTECH" a rewarding and enriching reading experience. I sincerely appreciate your support and encourage you to share your valuable feedback and suggestions, which will help us further improve the quality and standards of our magazine.

ABOUT MITS

Madanapalle Institute of Technology & Science is established in 1998 in the picturesque and pleasant environs of Madanapalle and is ideally located on a sprawling 26.17 acre campus on Madanapalle - Anantapur Highway (NH-205) near Angallu, about 10km away from Madanapalle. MITS, originated under the auspices of Ratakonda Ranga Reddy Educational Academy under the proactive leadership of and Dr. N. VijayaBhaskar Choudary, Secretary & Correspondent and Sri. N. Krishna Kumar, Chairman of the Academy.

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

ABOUT DEPARTMENT

The Department has grown from strength to strength since its inception in 2004. It offers 2-year MCA programmes. These programmes are fully governed by AICTE, New Delhi and affiliated to JNTU Ananthapuramu. The Department is dedicated to the mission of inculcating value-based, socially committed professionalism to the cause of overall development of students and society. It promotes the prime objective of educating and preparing students as dynamic, competent and knowledgeable professionals. Excellent academic results, high-end computer labs, well-defined and documented academic and administrative processes and student counselling sessions (personal and academic) are the core strength of the department.

The Department obtained UGC-Autonomous Status in the year 2014 and is running the programmes successfully by meeting all the requirements. The College Academic Council, Board of Studies of the department strive to provide quality education and most advanced curriculum to make the students industry-ready and excel in the contemporary business world.

The department is frequently organizing Faculty Development Programs, Conferences, Seminars, Symposium and workshops on various emerging areas and technologies. The guest lectures are arranged, eminent professors and industry resource persons are invited from reputed IT industries, top ranked Universities. All the qualified and competent students are placed in renowned organizations, both national and international. Despite maintaining global standards in teaching and learning, successful placement in different renowned organizations and consistent 100% admission in the department are the hallmarks of the department. The M.C.A. Programme under Department of Computer Applications was Accredited by the National Board of Accreditation (NBA) of All India Council for Technical Education (AICTE).

VISION

To be the source of producing competent computer application professionals in academic and research activities to serve the industry and society.

MISSION

M1: To empower students with knowledge of computer applications through state-of-art infrastructure and curriculum.

M2: To groom students to become competent professionals in emerging technologies with industry specific programs.

M3: To inculcate ethical values, leadership and managerial skills in the students.

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

PEO1: Excel in the software industry with the application of comprehensive knowledge and skills.

PEO2: Contribute by building innovative and sustainable solutions to the problems in the IT industry.

PEO3: Achieve successful career by exhibiting social responsibility leading to lifelong learning.

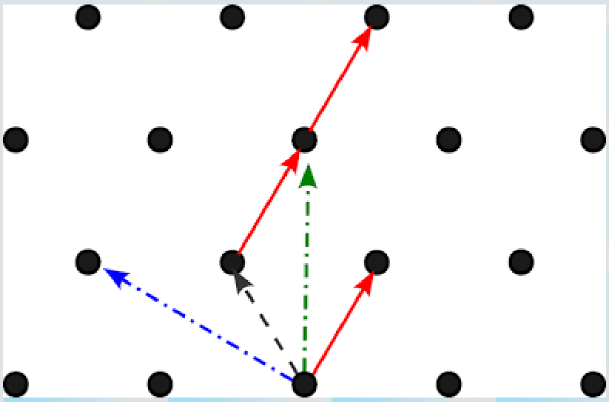
FIPS 203 Is Here: NIST Finalizes the Post-Quantum Encryption Standard to Secure the Web

Duddekunta Akash, 23691F0002,
II MCA, Department of Computer Applications

For decades, the security of our digital world—from university portals to online banking—has relied on cryptographic algorithms like RSA and ECC. But the rapid development of quantum computers threatens to shatter these mathematical fortresses. A sufficiently powerful quantum computer could break current encryption in seconds, exposing the web to catastrophic vulnerabilities.

Fortunately, the defense has arrived. On August 13, 2024, the National Institute of Standards and Technology (NIST) officially finalized its first three post-quantum cryptography (PQC) standards. The crown jewel of this release is FIPS 203, which standardizes the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).

Derived from the CRYSTALS-Kyber algorithm, FIPS 203 serves as the primary standard for general encryption and secure key exchange. Instead of relying on the difficulty of factoring massive prime numbers, it uses *lattice-based cryptography*. To both classical and quantum computers, finding the hidden vector in this multidimensional mathematical grid is a computationally unfeasible problem. Notably, FIPS 203 boasts high speed and small encryption keys, making it highly efficient for establishing secure communication channels.



Lattice-based cryptography relies on finding hidden vectors in a complex mathematical grid..
Source: Red Hat

Alongside it, NIST also released FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) to handle digital signatures, ensuring data authentication in the post-quantum era.

Beyond the Container: How WASI 0.2 Turned Web Assembly into Cloud Computing's True Holy Grail

Gajjala Bindu Sree, 23691F0024,
II MCA, Department of Computer Applications

For years, we've relied on Docker and Kubernetes to deploy cloud applications. Containers are incredibly useful, but they are undeniably heavy—often packaging entire operating systems and redundant libraries just to run a single microservice. Enter WebAssembly (Wasm). Originally built to run high-performance code in web browsers, it has officially broken out. With the milestone release of WASI 0.2 (WebAssembly System Interface) in early 2024, Wasm has become cloud computing's next major paradigm shift.

The real magic of WASI 0.2 lies in the **Component Model**. Previously, server-side Wasm modules were isolated black boxes. Now, they act like interoperable LEGO bricks. You can write different parts of an application in Rust, Python, Go, or C++ and WASI 0.2 allows them to seamlessly communicate using standard WebAssembly Interface Types (WIT).

Consider this example: Imagine building a web service. Instead of deploying a bulky 300MB Linux container with a Python runtime, you compile your Python logic into a tiny 2MB Wasm component. You then snap it together with a high-speed HTTP parsing component written in Rust. Because WASI 0.2 natively supports network sockets and HTTP out of the box, this hybrid application runs instantly on any server, edge device, or cloud architecture with mathematically guaranteed, sandboxed security.

Bridging the Knowledge Gap: Retrieval-Augmented Generation (RAG)

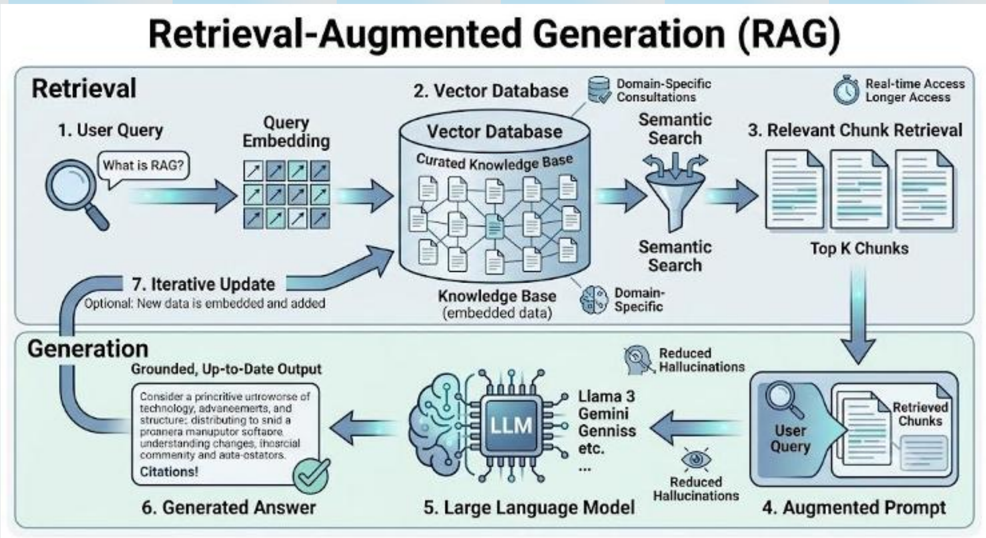
Dodla Deepthi, 23691F0038
II MCA, Department of Computer Applications

We're witnessing an unprecedented era of rapid AI advancement. Large Language Models (LLMs) like GPT and Llama have revolutionized natural language understanding and generation. However, despite their impressive capabilities, these models suffer from critical limitations: a frozen knowledge base, inability to access real-time data and a tendency to "hallucinate" plausible but incorrect information.

Retrieval-Augmented Generation (RAG) is a powerful paradigm designed to directly address these challenges, transforming how we interact with and deploy AI. RAG fundamentally combines the creative reasoning power of LLMs with the precise, structured data access of traditional information retrieval systems. Think of it as giving an LLM an open-book exam, where it can consult a curated library before answering.

The RAG workflow is elegant and impactful. It begins with an input—a user's query. This query is converted into a vector embedding. A semantic search is then performed against a vector database, which contains pre-embedded and indexed external knowledge, such as an organization's technical documentation, research papers, or real-time web data. The most relevant information is retrieved and seamlessly integrated with the user's original query into an "augmented prompt." This comprehensive prompt provides the context and evidence the LLM needs to generate a factually accurate, up-to-date and verifiable answer.

For us, as aspiring computer scientists, RAG is a crucial area for exploration. It opens new frontiers in domain-specific AI, question-answering systems and enterprise tools. It enables us to build systems that are not just smart, but trustworthy and current, without the prohibitive computational costs of retraining or fine-tuning large models. RAG isn't just an optimization; it's a foundational step towards practical, reliable and deployable AI systems of the future.



Beyond the Cloud: Unlocking 5G's Potential with Edge Computing

Nagine Dinesh, 23691F0042
II MCA, Department of Computer Applications

Imagine a world where autonomous vehicles make split-second decisions based on real-time traffic data, or doctors perform remote surgeries with haptic feedback that feels instantaneous. 5G networks promise this future, offering blazing-fast speeds and massive connectivity. However, there is a catch: speed isn't everything. For the most demanding applications, proximity is just as crucial. This is where **Edge Computing** enters the frame, acting as the critical partner that allows 5G to truly shine.

Historically, the dominant architectural paradigm has been Centralized Cloud Computing. While the Cloud is powerful, sending data thousands of miles to a distant data center for processing introduces latency—the dreaded delay. For an autonomous car needing to stop or an automated factory robot detecting a defect, a few hundred milliseconds of round-trip delay is unacceptable. 5G reduces the radio latency, but if the core infrastructure relies on distant servers, the real-world performance gained is minimal.

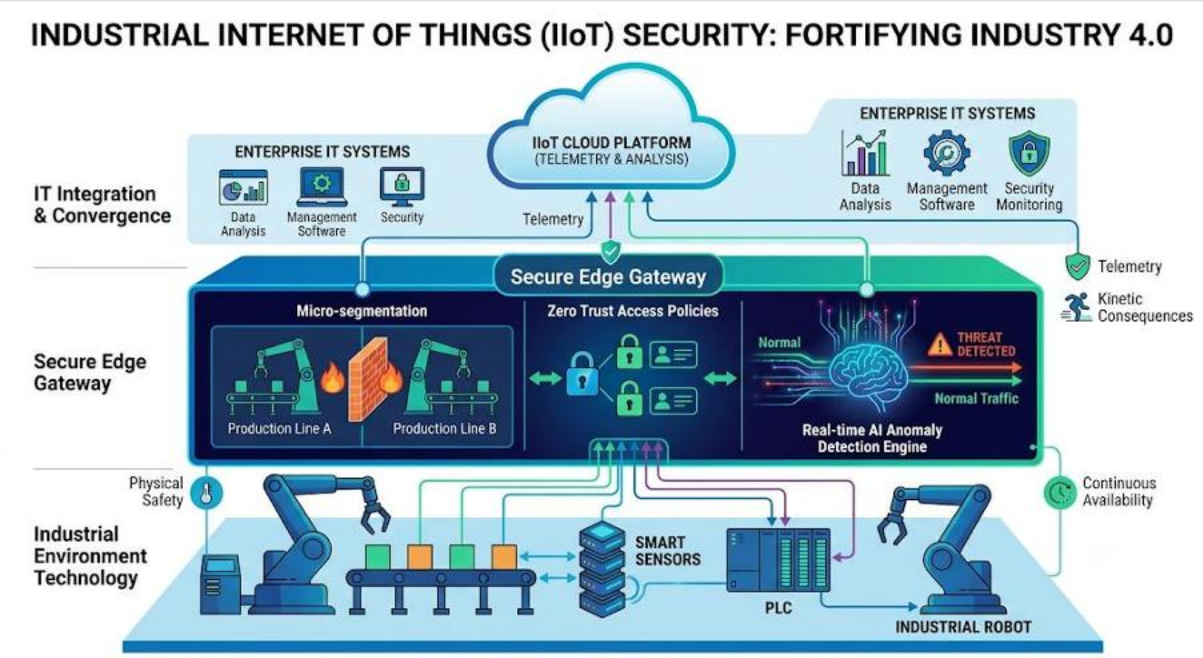
Edge Computing solves this by moving computational power and data storage away from central data centers and placing it much closer to the source of data generation. We are shifting the architecture so processing happens at the network 'edge'—integrated directly into 5G base stations, local aggregation points, or small enterprise data centers (like those shown in the accompanying illustration).

The 5G and Edge synergy is transformative. When data is processed locally, milliseconds are shaved off the response time. Ultra-low latency is achieved. This shift unlocks technologies that cannot tolerate delay: immersive Augmented Reality (AR), massive Internet of Things (IoT) sensor networks and the instant, intelligent decision-making required for real-time AI (AI at the Edge). As future Masters of Computer Applications, understanding this decentralization is key. We are moving beyond building applications *for* the network; we must now design systems that intelligently operate *within* a hybrid, low-latency infrastructure. The future of software is distributed, real-time and lives on the Edge.

Fortifying Industry 4.0: The Crucial Challenge of IIoT Security

Dura Bhargavi, 23691F0044
II MCA, Department of Computer Applications

The digital transformation of manufacturing, often referred to as Industry 4.0, is rapidly reshaping our technological landscape. At the center of this evolution is the Industrial Internet of Things (IIoT), which integrates massive numbers of smart sensors, robotic arms and programmable logic controllers to increase automation and self-monitoring. However, as operational technology (OT) merges with traditional IT networks, it introduces a severe and often underestimated frontier of vulnerabilities.



Industrial Internet of Things (IIoT) Security

A structural diagram displaying the convergence of IT and OT networks. At the physical layer, connected factory sensors and actuators connect via secure Edge Gateways, protected by micro-segmentation, Zero Trust access policies and real-time AI anomaly detection engines before routing telemetry to the cloud.

Why IIoT Security is Uniquely Vulnerable

In standard enterprise IT, security revolves around protecting data privacy. In industrial environments, the priorities shift drastically toward continuous availability and physical safety. Securing IIoT systems presents unique hurdles:

- **Legacy OT Equipment:** For decades, operational technology networks were isolated by design and relied heavily on physical separation for security. Consequently, older industrial equipment often lacks built-in authentication or encryption protocols.
- **Kinetic Consequences:** Operational disruptions or cyber compromises in industrial settings can have dangerous cascading effects. Unlike a standard IT data breach, an exploited IIoT system can lead to significant financial losses, equipment sabotage and severe worker safety hazards.
- **Expanded Attack Surfaces:** Every new smart device or component connected to the IIoT acts as a potential liability, drastically expanding the attack surface and making it difficult to maintain security amid increased connectivity.

Architectural Pillars of Modern IIoT Defense

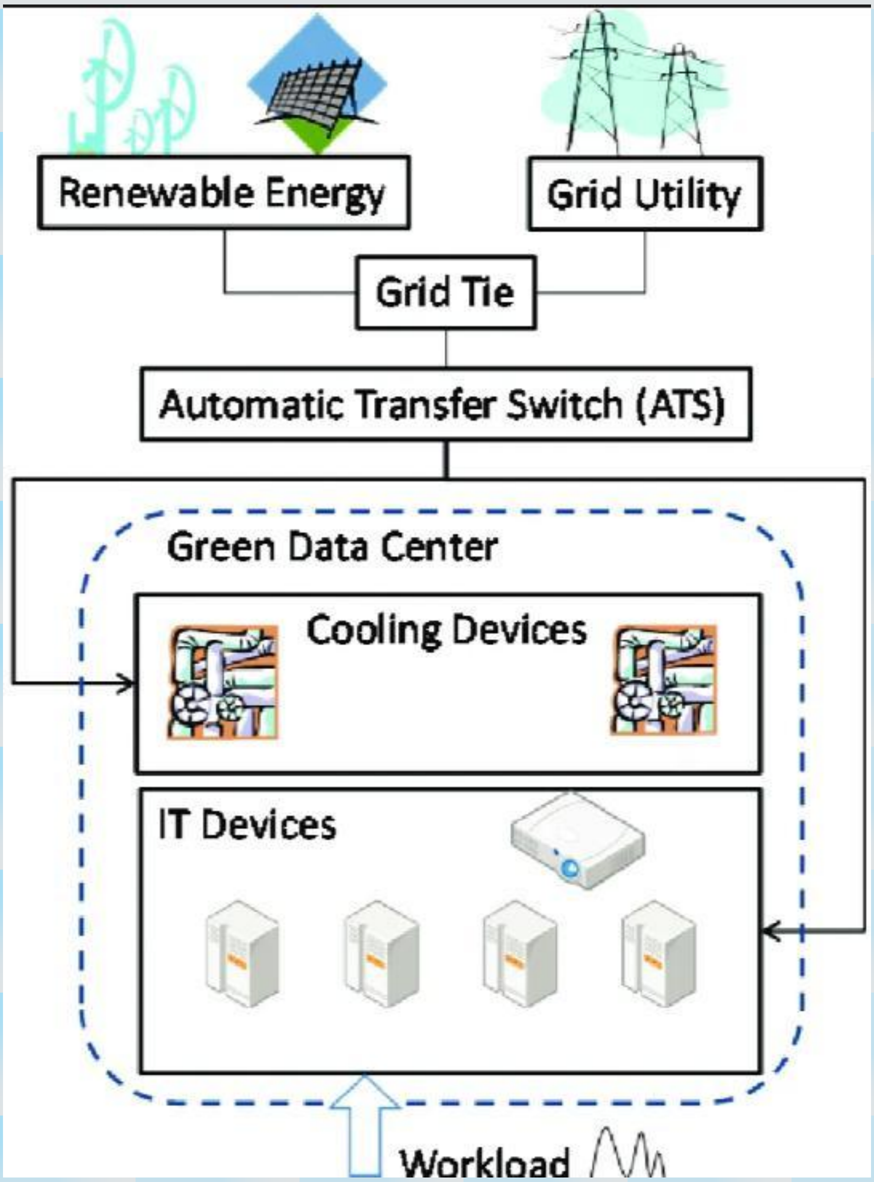
As future software engineers and computer application specialists, building resilient industrial ecosystems requires moving beyond simple perimeter firewalls toward comprehensive defense-in-depth measures:

- **Zero Trust Architecture:** Organizations must adopt zero-trust principles that provide granular control over access privileges, reducing the risk of widespread impact if a network breach occurs.
- **Network Micro-Segmentation:** Implementing secure network segmentation ensures that critical controller networks are tightly isolated from corporate IT, preventing the lateral movement of cyber threats.
- **Robust Authentication:** Ensuring data is encrypted both in transit and at rest is essential, alongside the mandatory implementation of robust multi-factor authentication mechanisms for remote access.

Green Data Center Architectures: The Next Frontier in Computing

Bonga Sahitha, 23691F0066
II MCA, Department of Computer Applications

The digital age, while transformative, has an environmental catch: data centers now consume a staggering amount of global electricity. As future technologists and software engineers, it is incumbent upon us to move beyond simple system design and embrace 'Green Data Center Architectures.' This paradigm is not merely an ethical choice; it's a critical engineering challenge.



Green Data Center Architectures

An architectural diagram illustrating a sustainable data center. It features rooftop solar arrays, wind turbines, hot/cold aisle containment, direct-to-chip liquid cooling systems and a central dashboard displaying AI-driven Power Usage Effectiveness (PUE) metrics.

Understanding the Green Imperative

A Green Data Center is a facility optimized for maximum energy efficiency and minimal environmental impact. The primary metric here is Power Usage Effectiveness (PUE), which compares the total facility power to the power used by IT equipment. The closer the PUE is to 1.0, the more efficient the data center. Modern green architectures employ a holistic approach to minimize this number through three main pillars: smart cooling, efficient power and workload optimization.

The Architectural Pillars

1. **Smart Cooling:** Traditional air conditioning is incredibly wasteful. Green architectures utilize hot/cold aisle containment to prevent air mixing. More advanced systems leverage liquid cooling (such as direct-to-chip or immersion), which is far more effective at heat removal, allowing for higher rack density. Additionally, 'free cooling' uses ambient air or water from natural sources when temperatures allow.
2. **Efficient Power:** This goes beyond simple energy-saving modes. It involves a fundamental shift in the power train. Efficient uninterruptible power supplies (UPSs) and advanced power distribution units (PDUs) reduce conversion losses. Furthermore, the modern green data center is increasingly co-located with renewable energy sources like solar and wind, integrating advanced battery storage to manage peak demand.
3. **Workload Optimization:** This is where software experts play a vital role. Techniques like server virtualization and consolidation drastically reduce the number of underutilized physical servers, which still consume power when idle. Modern architectures use AI-driven software to orchestrate workloads, dynamically scaling resources up or down and placing them on the most efficient hardware in real-time.

The Role of Software Professionals

Distributed systems, cloud computing and advanced operating systems are the foundation of these green strategies. We must not just train to be developers; we must become system thinkers who build efficient, sustainable code. Our understanding of how software interacts with hardware will determine the effectiveness of virtualized environments and AI-driven workload management.

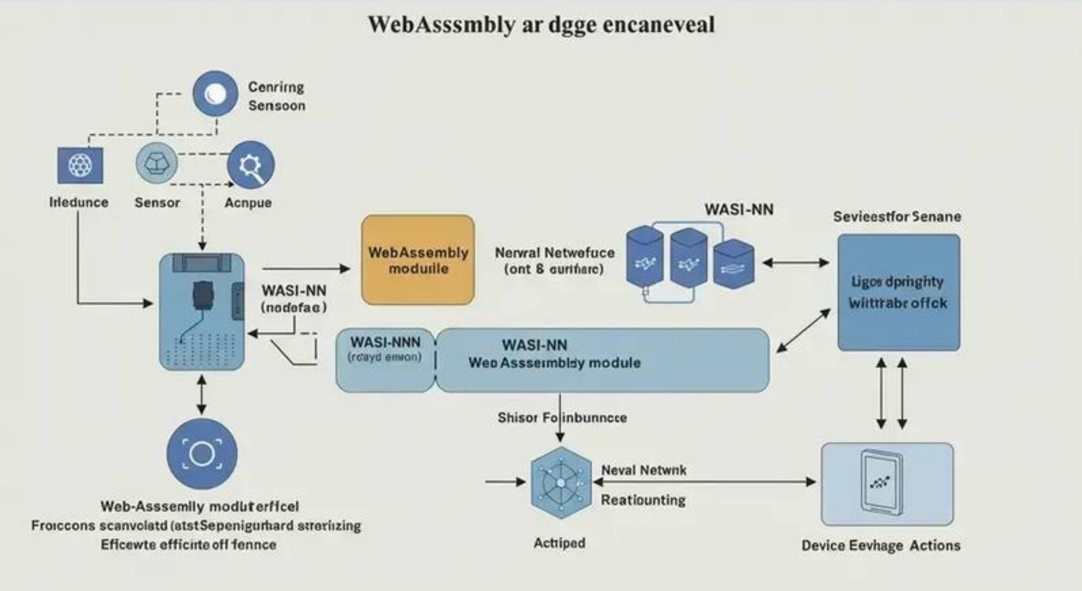
The future is green. By mastering these architectures, we ensure that our digital innovations do not come at the expense of our planet. It’s an engineering, ethical and economic necessity.

WebAssembly (Wasm) on the Edge: The Next Frontier of Distributed Computing

Putta Pallavi, 23691F00A3
II MCA, Department of Computer Applications

The landscape of web development and distributed systems is undergoing a monumental shift. For years, we've been accustomed to a binary choice: running heavy application logic on a centralized cloud server or pushing minimal interactivity to the user's browser via JavaScript. This paradigm is now being challenged by the convergence of two powerful technologies: **WebAssembly (Wasm)** and **Edge Computing**.

This article explores how bringing Wasm modules to the "Edge" is revolutionizing performance, security and the very architecture of modern applications—a topic crucial for any aspiring computer applications professional.



Understanding the Components

Before diving into the synergy, let's briefly define the players.

WebAssembly (Wasm): Wasm is not a new language, but a compilation target. It allows developers to write code in performant languages like C, C++, Rust, or Go and compile it into a compact, binary format that runs at near-native speed. Crucially, Wasm runs within a secure, sandboxed environment. While initially designed for the browser, its portability and speed make it ideal for server-side execution as well.

Edge Computing: If the Cloud is about centralized data centers, the Edge is about decentralization. Edge computing pushes computation and data storage closer to the sources of data—whether that's a user's device, an IoT sensor, or a local network gateway. The goal is simple: reduce latency by minimizing the distance data must travel.

The Synergy: Why Wasm on the Edge?

So, what happens when you combine near-native executable code with a globally distributed network of local compute nodes? You unlock a new architectural pattern that addresses the limitations of both traditional cloud and purely client-side execution.

1. Blazing Fast Performance & Reduced Latency

The primary driver for Edge computing is latency. For applications like real-time video processing, online gaming, IoT data analysis, or even just modern personalized e-commerce, the round-trip time to a centralized cloud data center (often hundreds or thousands of miles away) is unacceptable.

By deploying applications as Wasm modules on Edge nodes, computation happens milliseconds away from the user. Because Wasm compiles to optimized machine code, execution is significantly faster than interpreted JavaScript, providing a near-instantaneous experience.

2. Enhanced Security via Sandboxing

Security is paramount when executing code in distributed environments. Wasm was built from the ground up with security in mind. It runs in a highly restricted sandbox environment, separate from the host operating system. A Wasm module cannot access memory, files, or network resources outside its sandbox unless explicitly permitted by the host runtime. This makes it safe to deploy multi-tenant applications on shared Edge infrastructure without worrying about malicious code compromising the host or neighboring applications.

3. Portability and Language Independence

MCA students know the headache of managing dependency hell when deploying applications across different server environments. Wasm solves this with its portability. A compiled Wasm binary is platform-agnostic; it will run anywhere there is a Wasm runtime (like Wasmtime or Wasmer), regardless of the underlying OS or hardware architecture.

Furthermore, because Wasm is a compilation target, developers are not restricted to a single ecosystem. You can use Rust for high-performance components, Go for networking logic and C++ for legacy libraries, all compiling into interoperable Wasm modules that deploy seamlessly to the Edge.

4. Cost Efficiency and Reduced Infrastructure Load

Running full containerized microservices (like Docker) on thousands of global Edge nodes is resource-intensive and expensive. Wasm modules are incredibly lightweight compared to containers or virtual machines. They have minimal overhead, fast startup times (instantiated in microseconds) and consume very little memory. This allows Edge providers to pack significantly more workloads onto the same hardware, drastically reducing infrastructure costs.

Real-World Applications for MCA Students to Watch

Wasm on the Edge isn't theoretical; it's being adopted by major players in the industry. Here are a few use cases that define this space:

- **Serverless Functions at the Edge:** Cloudflare Workers and Fastly's Compute@Edge are prime examples. Instead of running serverless functions in centralized data centers, they execute as Wasm modules on local points of presence (PoPs) globally, offering unmatched speed for HTTP requests.
- **Real-time IoT Analytics:** Sensors generate massive amounts of data. Sending all this raw data to the cloud for processing is bandwidth-heavy. Edge nodes running Wasm can filter, aggregate and analyze data *before* sending only relevant insights to the central database.

  Dynamic Content Personalization: A/B testing, localized content delivery and personalized recommendations can be executed instantly at the Edge using Wasm, bypassing the latency of fetching personalized data from the main server.

Conclusion

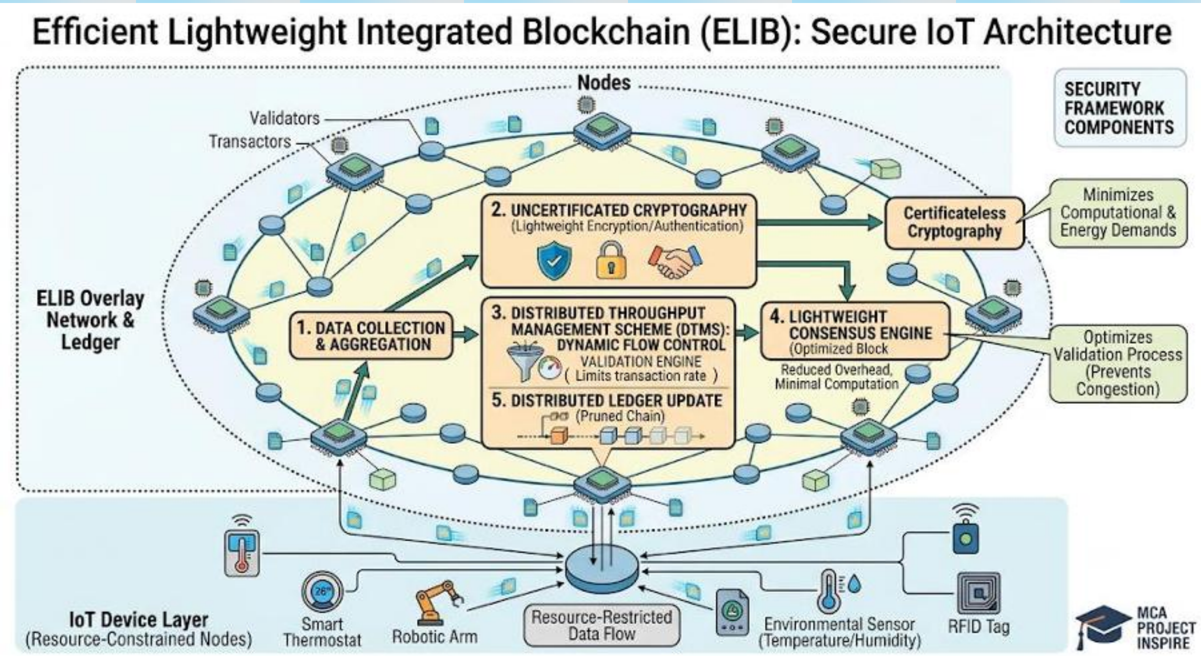
WebAssembly on the Edge represents a significant evolution in distributed systems architecture. By combining the safety and performance of Wasm with the low-latency reach of Edge computing, we are moving toward a future where "the network is the computer."

Securing the Connected World: The Dawn of the Ef icient Lightweight Integrated Blockchain (ELIB)

Guddeti Prasanth, 23691F00B4
II MCA, Department of Computer Applications

The rapid expansion of the Internet of Things (IoT) has fundamentally transformed our technological landscape, but ensuring robust security and privacy for these vast networks of interconnected devices has become paramount. As postgraduate technologists analyzing modern network paradigms, we understand that traditional security mechanisms repeatedly fall short when applied to IoT environments. These deployments suffer from inherent limitations: strictly limited computational resources, stringent energy constraints and an unprecedented need for massive network scalability.

For years, blockchain technology has been heralded as the ultimate solution to decentralized security. Its immutable ledger and decentralized trust mechanisms theoretically eliminate single points of failure. Yet, traditional blockchains are notoriously heavy. Protocols like Proof of Work require immense computational hashing power, while standard ledgers demand gigabytes of storage space—resources that a simple temperature sensor or smart lightbulb simply do not possess. To bridge this critical gap between high-grade security and low-power hardware, researchers introduced the Efficient Lightweight Integrated Blockchain (ELIB) model.



Efficient Lightweight Integrated Blockchain (ELIB)

An architectural diagram illustrating the ELIB framework, showcasing resource-constrained IoT nodes securely transmitting data through an overlay network that utilizes certificateless cryptography, a lightweight consensus mechanism and a distributed throughput management engine.

Decoding the ELIB Architecture

The ELIB model is a novel, purpose-built framework designed to dramatically bolster IoT security and privacy while meticulously accounting for the physical limitations of edge devices. It leverages the inherent decentralized nature of blockchain to forge a secure, transparent environment for IoT communications, but strips away the crippling computational overhead.

This optimized performance relies on three core architectural pillars:

- **Lightweight Consensus Algorithms:** ELIB integrates optimized consensus protocols tailored specifically for resource-constrained IoT nodes. A central strategy of this lightweight consensus involves intentionally restricting the total number of blocks that need to be generated. By minimizing block generation, ELIB drastically reduces the computational and processing effort required by machines operating on the network.
- **Certificateless Cryptography:** ELIB circumvents heavy certificate management by utilizing an uncertificated cryptographic model. Integrating these lightweight cryptographic algorithms ensures robust data security while significantly reducing the computational and energy demands typically associated with blockchain operations.
- **Distributed Throughput Management Scheme (DTMS):** To manage data flow effectively, ELIB incorporates a robust Distributed Throughput Management Scheme. This scheme dynamically adjusts the number of transactions that must be validated relative to the current number of active nodes in the network, optimizing the overall validation process.

Tangible Performance and Future Implications

The theoretical elegance of ELIB translates exceptionally well to real-world applications. Through extensive simulations and physical deployments—particularly in environments like smart homes—the ELIB model has proven its capability. By successfully integrating its lightweight cryptographic algorithms and streamlined consensus protocols, the model lowers processing time and conserves vital battery life, confirming its viability for deeply constrained environments.

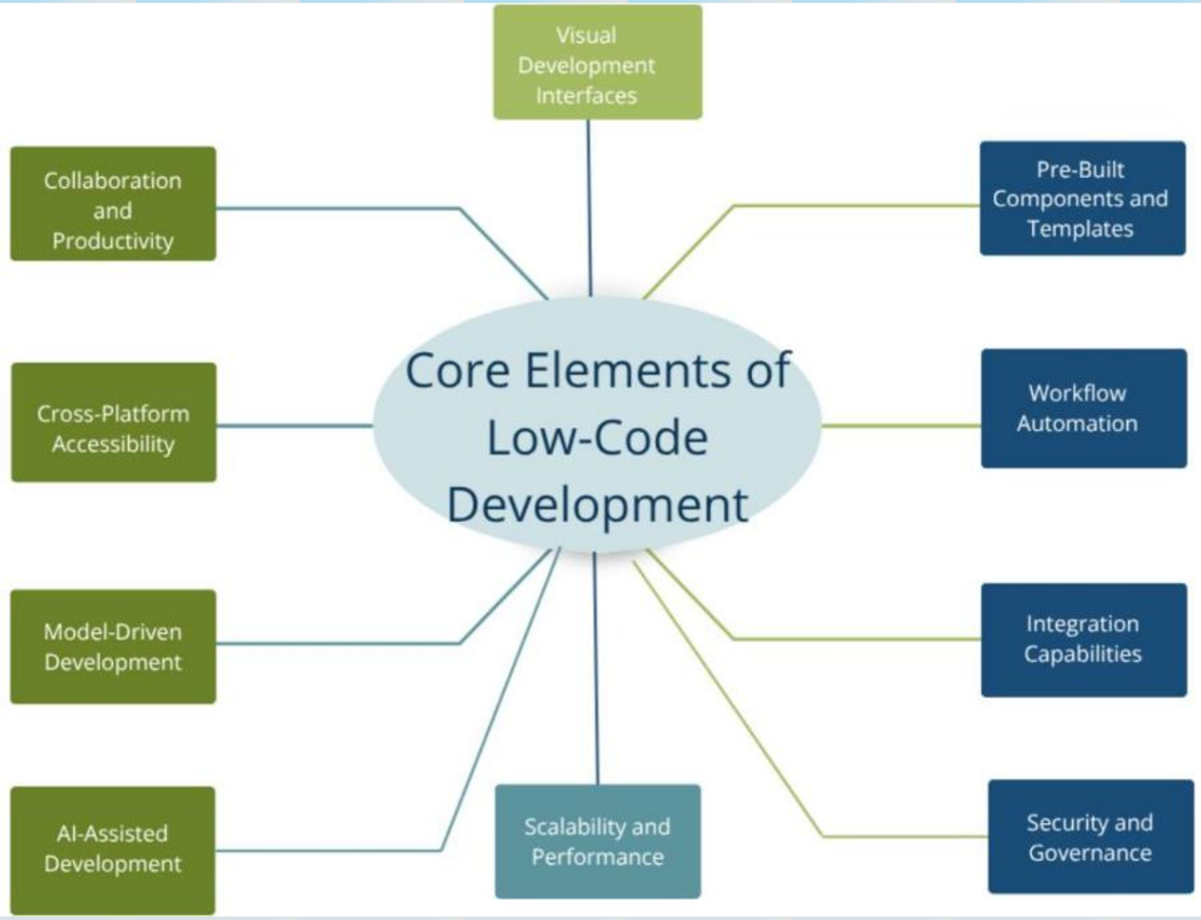
Beyond processing efficiency, ELIB incorporates advanced privacy-preserving techniques that ensure user data remains completely confidential, a critical requirement as IoT infiltrates private domestic and healthcare spaces. Importantly, it allows for seamless integration into existing IoT architectures, offering an immediately practical and effective solution to secure vulnerable ecosystems.

The ELIB model represents more than just a security patch; it is a foundational upgrade for distributed computing. It successfully proves that enhanced security and privacy do not have to compromise the usability or performance of lightweight devices. By addressing both security and privacy challenges head-on, ELIB strengthens the current posture of IoT networks and paves the way for a new generation of highly resilient, trustworthy digital services.

The Future is Visual: Embracing Low-Code/No-Code Development Frameworks

Archakam Raviteja, 23691F00C9
II MCA, Department of Computer Applications

A silent revolution is fundamentally altering how enterprise applications are built: the rapid rise of Low-Code/No-Code (LCNC) development frameworks. Far from being a fleeting trend, these platforms are redefining the developer experience and democratizing software creation.



Low-Code/No-Code Development Frameworks

An architectural diagram illustrating a hybrid composable architecture, where drag-and-drop visual interfaces seamlessly integrate with custom-coded backend microservices, robust APIs and cloud databases.

The Paradigm Shift in App Development

LCNC platforms enable developers and business users alike to design and deploy applications rapidly. They utilize intuitive, visual drag-and-drop interfaces and pre-built connectors, requiring minimal to absolutely zero hand-coding for standard features.

The statistics paint a staggering picture of this architectural shift:

- Industry analysts project the low-code development technologies market will reach approximately $44.5 billion by 2026.

- By 2026, it is estimated that 75 percent of all new enterprise applications will be built utilizing low-code platforms.

- The category is evolving rapidly, with AI integration now acting as a baseline feature that compresses the build cycle and makes governed no-code even faster.

It is easy for computer science and engineering students to view LCNC platforms as a threat to traditional programming jobs. However, the reality is quite the opposite. LCNC does not eliminate the need for software engineering; it simply changes our focus.

Modern LCNC implementations thrive on a hybrid model known as composable architecture. In this setup, routine user interfaces, basic data operations and automated workflows are built rapidly using low-code tools. Meanwhile, the complex business logic, data-intensive processing and stringent security layers remain firmly in the hands of technical developers.

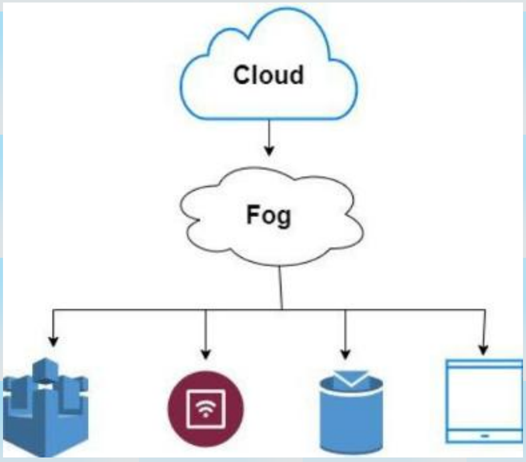
The Path Forward

Low-code and no-code frameworks are powerful accelerators that eliminate repetitive boilerplate coding, freeing developers to tackle higher-level systemic challenges like scalability, data integrity and enterprise governance. As future tech leaders, mastering the integration of LCNC tools into production-grade systems will provide a massive competitive advantage.

Bridging the Edge and Cloud: Fog Computing Architectures

Patan Sadiqunnisa, 23691F00D8
II MCA, Department of Computer Applications

The exponential expansion of interconnected devices generates astronomical volumes of data requiring instantaneous processing. The inherent latency of transmitting this data to distant centralized cloud servers creates a severe bottleneck for real-time operations. Fog computing emerges as the definitive architectural paradigm to resolve this delay by acting as a powerful intermediate layer that extends cloud capabilities directly to the local network. By decentralizing computation, storage and networking services, fog architectures guarantee ultra-low latency, conserve critical core network bandwidth and provide robust local security for time-sensitive applications such as autonomous navigation, smart city infrastructure and automated industrial manufacturing.



An architectural diagram illustrating the three-tier structure of fog computing: the bottom IoT edge layer generating data, the middle fog layer comprising local gateways and routers processing time-critical tasks and the top cloud layer handling long-term storage and heavy machine learning analytics.

Fog Computing Architectures

The structural foundation of a fog computing network operates as a highly virtualized, decentralized continuum bridging the gap between localized end devices and the centralized cloud environment. Fog nodes, which typically include industrial routers, local gateways and specialized edge servers, are strategically deployed near the data source to ingest, analyze and process raw telemetry immediately. This localized intelligence ensures that only refined, high-value information travels to the central cloud for complex, long-term big data analytics and global state synchronization. For those of us preparing to lead the future of software engineering, mastering this decentralized paradigm is an absolute necessity. We must dedicate our efforts toward designing resilient microservices, deploying lightweight containerized applications across diverse hardware nodes and orchestrating seamless, secure communication throughout this multi-tiered infrastructure. Mastering these complex distributed frameworks empowers us to engineer the highly responsive and resilient digital ecosystems of tomorrow.

Magazine Student Editors

DUDDEKUNTA AKASH

Roll No.: 23691F0002

DURA BHARGAVI

Roll No.: 23691F0044

Contact: mcaoffice@mits.ac.in

Visit us: www.mits.ac.in/MCA