CONTENT

Note from our *Mentors*

Dr. Manpreet Singh
Principal CCET (Degree Wing)

Our mission at CCET is not only to produce engineering graduates but to produce engineering minds

Dr. Sunil K. Singh
Professor and HOD, CSE | Faculty Mentor

ACM CCET provides student a great opportunity to learn scientific and practical approach of computer science.

Dr. Sudhakar Kumar
Assistant Professor, CSE | Faculty Sponsor

Every person should be provided with an opportunity to learn and explore the field of computer science.

"The greatest achievement of technology is not how it changes life, but how it improves it."

ACM'S
VISION AND MISSION

VISION

Chandigarh College of Engineering and Technology aims to be a center of excellence for imparting technical education and serving the society with self-motivated and highly competent technocrats.

MISSION

1. To provide high quality and value based technical education.
2. To establish a center of excellence in emerging and cutting-edge technologies by encouraging research and consultancy in collaboration with industry and organizations of repute.
3. To foster a transformative learning environment for technocrats focused on inter-disciplinary knowledge; problem-solving; leadership, communication, and interpersonal skills.
4. To imbibe spirit of entrepreneurship and innovation for development of enterprising leaders for contributing to Nation progress and Humanity.

DEPARTMENT VISION AND MISSION

VISION

To produce self-motivated and globally competent technocrats equipped with computing, innovation, and human values for ever changing world and shape them towards serving the society.

MISSION

M1: To make the department a smart centre for learning, innovation and research, creativity, and entrepreneurship for the stakeholders (students/scholar, faculty, and staff).

M2: To inculcate a strong background in mathematical, theoretical, analytical, and practical knowledge in computer science and engineering.

M3: To promote interaction with institutions, industries and research organizations to enable them to develop as technocrats, entrepreneurs, and business leaders of the future.

M4: To provide a friendly environment while developing interpersonal skills to bring out technocrat's inherent talents for their all-round growth.

ASSOCIATION FOR COMPUTING MACHINERY AT CCET

ABOUT

The CCET ACM Student Chapter brings together the Association for Computing Machinery (ACM) and ACM-W, fostering a vibrant community of computing enthusiasts committed to innovation, learning, and inclusivity. Under the expert mentorship of Dr. Sunil K. Singh and Dr. Sudhakar Kumar, the chapter actively organizes technical workshops, coding competitions, hackathons, and outreach programs that encourage both skill development and collaboration. While ACM focuses on advancing computing as a science and profession, ACM-W works towards empowering and supporting women in computing, ensuring equal opportunities and representation. Together, they create a dynamic platform at CCET where students can explore emerging technologies, share knowledge, and grow as competent and responsible computing professionals.
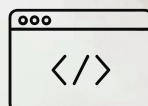
Student Speaker Program

Designing & Digital Art

Research and Development

Competitive Codong

Internship & Career Opportunity

CCET ACM STUDENT CHAPTER

ABOUT

ACM boosts up the potential and talent, supporting the overall development needs of the students to facilitate a structured path from education to employment. Our Chapter CASC focuses on all the aspects of growth and development towards computer technologies and various different elds. Overall, we at CCET ACM Student Chapter, through collaboration and engagement in a plethora of technical activities and projects, envision building a community of like-minded people who love to code, share their views, technical experiences, and have fun. We have been trying to encourage more women to join the computing eld, so we started an ACM-W Chapter to increase the morale of women. CASC launched an app which aimed at maintaining deco- rum of reading among CS members and sharing their ideas.
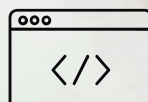
Student Speaker Program

Designing & Digital Art

Research and Development

Competitive Codong

Internship & Career Opportunity

CCET ACM-W STUDENT CHAPTER

ABOUT

The CCET ACM-W was founded in October 2021 with an aim to empower women in the field of computing and increase the global visibility of women in the field of research as well as development. We provide a platform for like-minded people so that they can grow together and contribute to the com- munity in a way that shapes a better world. Our chapter was founded to encourage students, especially women, to work in the field of computing. The chapter's main goal is to create even opportunities and a positive environment for students, where they can work to develop themselves profession- ally. We at the ACM Student chapter aim to build a globally visible platform where like-minded people can collaborate and develop in their field of interest.
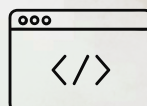

Student Speaker Program

Designing & Digital Art

Research and Development

Competitive Codong

Internship & Career Opportunity

ACHIEVEMENTS

Our team's recent publications showcase notable progress in diverse areas of Computer Science, including deep learning, security, and intelligent systems. These works have appeared in high-impact journals, conferences, and book chapters during the initial part of 2025.
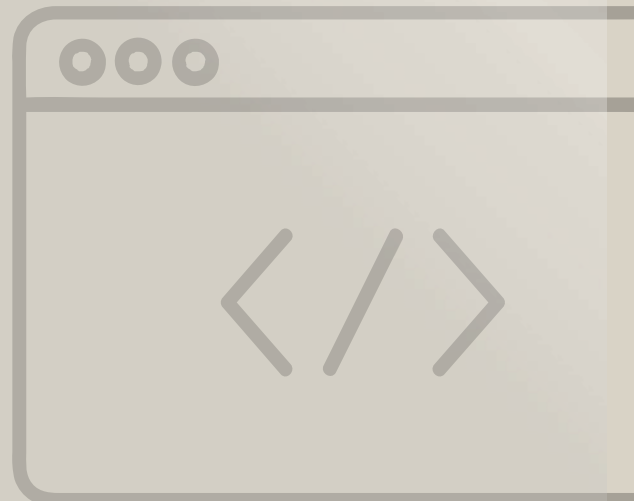
Journal Articles

- Advanced Web Traffic Modelling and Forecasting with a Hybrid Predictive Approach.
  June 2025
  Ujjwal Thakur, Sunil Kr Singh, Sudhakar, Kwok Tai Chui
- Cardiovascular Sound Classification Using Neural Architectures and Deep Learning for Advancing Cardiac Wellness.
  June 2025.
  Deepak Mahto, Sudhakar Kumar, Sunil Kr Singh, Bassma Saleh Alsulami
- Quantum-Resistant Cryptographic Primitives Using Modular Hash Learning Algorithms for Enhanced SCADA System Security.
  July 2025
  Sunil Kr Singh, Sudhakar Kumar, Manraj Singh, Brij B. Gupta

Conference Papers

- Application of Green IoT in Digital Oilfields for Achieving Sustainability in the OnG Industry. March 2025 Soumya Sharma, Sunil Kr Singh, Sudhakar Kumar, Tarun Vats
- Blockchain Based Election System Using Fingerprint Recognition.
- March 2025
- Uday Madan, Sunil Kr Singh, Sudhakar Kumar, Himanshu Setia
-

Book Chapters

- Advanced Tools and Technologies for Phishing Prevention.
  February 2025
  Kashish Preet Kaur, Sunil Kr Singh, Sudhakar Kumar, Sunil Kr Sharma
- Advanced Techniques and Best Practices for Phishing Detection.
  February 2025
  Ravina Mittal, Sunil Kr Singh, Sudhakar Kumar, Konstantinos Psannis
- Phishing Prevention Solutions and Mechanisms.
  February 2025
 Abhavya Muku, Sunil Kr Singh, Sudhakar Kumar, Vandana Sharma

EVENTS

GENERATIVE AI

Speaker:- Bhavya & Aanshi Bansal
Date: 22 August,2025
Number of attendees in the event:- 26

Event's Brief
The ACM CCET Student Speaker Event focused on the theme "Generative AI: Redefining Today". The session explored how generative AI is transforming technology and society, covering its core concepts along with real-world applications. Organized as part of ACM's initiative to engage students with emerging technologies, the event offered insightful discussions that highlighted both the opportunities and challenges of generative AI, leaving participants with a deeper understanding of its impact on the present and future.
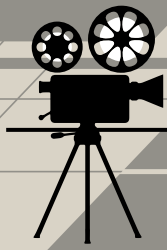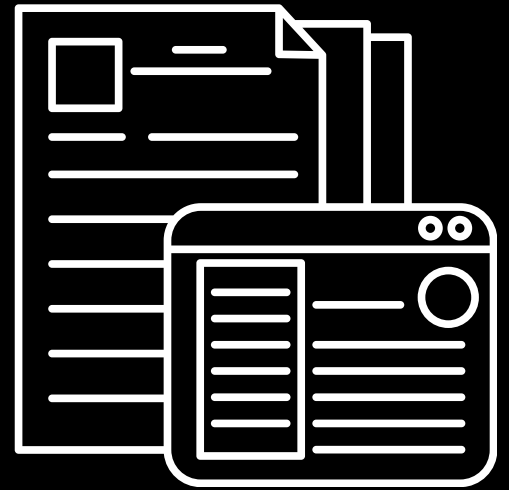
GLIMPSE OF THE EVENT

THE RISE OF CONFIDENTIAL AI: ENABLING PRIVACY-PRESERVING MACHINE LEARNING WITH TEES AND HOMOMORPHIC ENCRYPTION

Introduction to Confidential AI

Data protection has become as crucial as data processing at a time when data is the new oil. The need of data security has increased dramatically as artificial intelligence (AI) quickly permeates industries including healthcare, banking, national security, and customized digital services. Large datasets are used by traditional machine learning (ML) algorithms to identify trends and provide predictions, but these datasets frequently include proprietary, sensitive, or personally identifiable information. Exposure of sensitive data, even while it is being processed, can result in privacy breaches, intellectual property theft, or non-compliance with regulations such as the CCPA, GDPR, and HIPAA. This includes transactional history in banks and patient records in hospitals.

A paradigm known as Confidential AI makes it possible for machine learning models to work with private information without ever disclosing it. Confidential AI combines the advantages of secure hardware with state-of-the-art cryptography to enable the analysis of encrypted data while preserving total anonymity. In our highly regulated and privacy-conscious digital world, this idea is not only a luxury but a need [1].

Technologies Enabling Confidential AI

A number of innovative technologies that each focus on a distinct aspect of safe computing have come together to form Confidential AI. Trusted Execution Environments (TEEs) such as AMD Secure Encrypted Virtualization (SEV), ARM TrustZone, and Intel Software Guard Extensions (SGX) isolate certain memory areas within a CPU at the hardware level. These secure enclaves guarantee that the data and calculations within the enclave are safe even in the event that the operating system is corrupted [2].

Fully Homomorphic Encryption (FHE) is a groundbreaking method in the field of cryptography. Without first decrypting the data, FHE enables calculations to be done directly on encrypted data. This implies that during the ML lifespan, sensitive data never leaves its encrypted form [3]. For instance, without having access to any patient's raw data, a healthcare provider may utilize FHE to train an AI model using encrypted patient data from several institutions.

Multiple entities can collaboratively calculate a function over their inputs in parallel using Multi-Party Computation (MPC), which keeps the inputs secret from one another. It's especially helpful in cooperative settings, like bank consortiums looking to identify fraud trends without disclosing specific client information. As a complement, Differential Privacy adds controlled randomization to datasets, protecting individual inputs while guaranteeing statistical analysis [4].

Article

A pull quote is an impactful quote taken from the article. You can place the quote you want to highlight here.
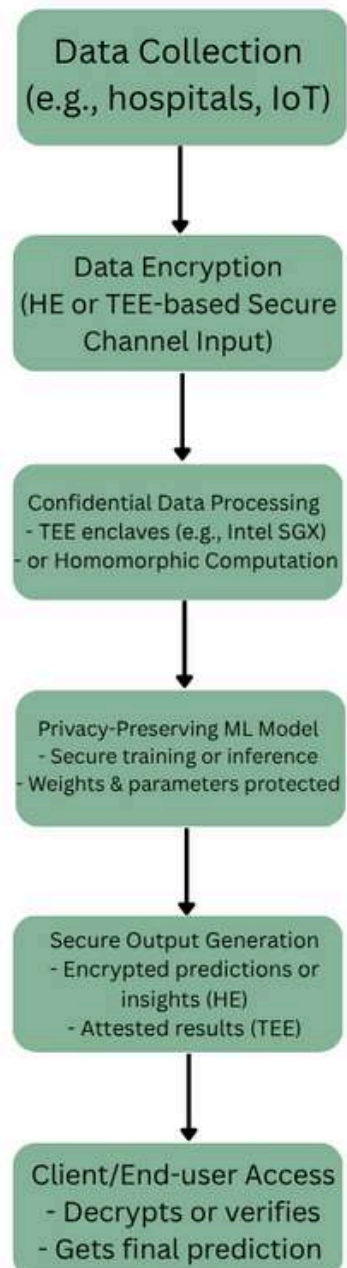
It's especially helpful in cooperative settings, like bank consortiums looking to identify fraud trends without disclosing specific client information. As a complement, Differential Privacy adds controlled randomization to datasets, protecting individual inputs while guaranteeing statistical analysis [4].

Architecture of a Privacy-Preserving AI Pipeline

Secure data intake, privacy-preserving model training, encrypted inference, and protected output creation are the general steps that make up a privacy-preserving AI pipeline. The technological stack being used—TEEs, FHE, MPC, or a hybrid model—determines the architecture that is used.

Raw data is ingested and fed into a secure enclave, which also houses the training or inference model, in a TEE-based pipeline. During computing, the enclave makes sure that no external system or process may access the data or model internals. For developers to implement such applications, cloud providers provide SDKs and APIs, such as AWS Nitro Enclaves and Azure Confidential Computing [5].

Data in a pipeline driven by FHE is encrypted all the way through. ML models that are fitted to FHE constraints or specifically developed circuits are frequently used to enable homomorphic operations in the AI model. The calculation produces an encrypted output that only the data owner can decrypt.

Data Collection
(e.g., hospitals, IoT)

↓

Data Encryption
(HE or TEE-based Secure Channel Input)

↓

Confidential Data Processing
- TEE enclaves (e.g., Intel SGX)
- or Homomorphic Computation

↓

Privacy-Preserving ML Model
- Secure training or inference
- Weights & parameters protected

↓

Secure Output Generation
- Encrypted predictions or insights (HE)
- Attested results (TEE)

↓

Client/End-user Access
- Decrypts or verifies
- Gets final prediction

MPC in conjunction with federated learning is another pipeline that prioritizes privacy. Every participant—such as a hospital server or smartphone—trains a local model using its own data and only exchanges encrypted model updates. MPC procedures combine these updates, but they never make the individual models public. Privacy-preserving systems like Google's GBoard and Apple's Siri are powered by this technology [6].

Challenges and Trade-offs

Confidential AI has a number of practical and technical obstacles in spite of its potential. Performance overhead is one significant drawback. For deep learning models in particular, FHE can be 100–1000× slower than normal compute, although being theoretically safe [3]. While recent hardware acceleration attempts are increasing viability, most FHE systems still cannot do real-time inference.

Despite their speed, TEEs are susceptible to side-channel attacks, such as Spectre and Meltdown, which are speculative execution defects. Furthermore, training big models without specialized memory handling is challenging because to the restricted memory of enclaves.

Another obstacle is the intricacy of development. Developers must be knowledgeable about low-level hardware security as well as cryptography technologies in order to implement confidential AI. When data is encrypted or concealed behind secure enclaves, debugging becomes intrinsically challenging.

Although tooling is becoming better, popular frameworks like PyTorch and TensorFlow are still catching up in terms of native support for calculations that protect privacy.Furthermore, a lack of standardization makes it difficult to integrate many systems and manufacturers. Confidential AI deployment in multi-cloud or hybrid systems is still difficult given the absence of standardized APIs or protocol standards.

Real-World Implementations

The development of Confidential AI is being spearheaded by a number of organizations. Libraries like PySyft for differential privacy and federated learning integration with PyTorch have been made available by the open-source group OpenMined. FHE libraries are offered by IBM HELib and Microsoft SEAL, and they are being used more and more in pilot corporate deployments and scholarly research [3].

A useful MPC framework for safe cross-organization data sharing is Google's Private Join and Compute. Without disclosing their own datasets, it enables two or more parties to calculate shared statistics [4].

Additionally, startups are inventing. Zama is developing deep learning APIs and compilers that are compatible with FHE. Secure AI collaboration solutions for national defense, healthcare, and finance are offered by Duality Technologies. A U.S. firm called Enveil focuses on encrypted search and analytics for both commercial and classified customers. Researchers are using these technologies to build cross-hospital AI models without transferring sensitive data, and banks are already working together on fraud detection [1][6].

Article

Conclusion

At the nexus of machine intelligence, privacy, and security, secret AI promises a future in which potent AI systems may function without ever jeopardizing the privacy of the data they depend on. Technologies like TEEs, FHE, and MPC will become more and more important in the AI development pipeline as public demand for data privacy and regulatory pressure increase. Although speed, standards, and developer accessibility issues still exist, there is no denying the momentum behind secret computing. Confidential AI is becoming more than just a theory thanks to increasing corporate use and scholarly advancements; it's a fundamental change in the way we create reliable, privacy-preserving artificial intelligence. In a digital world, by adopting these technologies, we can foster innovation without compromising the rights and standards of people and organizations.

References

[1] D. Evans, V. Kolesnikov, and M. Rosulek, "A Pragmatic Introduction to Secure Multi-Party Computation," Foundations and Trends® in Privacy and Security, vol. 2, no. 2–3, pp. 70–246, 2018.

[2] F. McKeen et al., "Innovative Instructions and Software Model for Isolated Execution," in Proc. of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy (HASP), 2013.

[3] M. Kim, Y. Song, and V. Shmatikov, "Secure and Scalable Machine Learning Using Homomorphic Encryption," in Proc. of the 26th USENIX Security Symposium, 2017.

[4] B. Corrigan-Gibbs and D. Boneh, "Private Data Analysis via Learning with Errors," in Theory of Cryptography Conference (TCC), 2015.

[5] Intel, "Intel® Software Guard Extensions (SGX) Developer Guide," 2024. [Online]. Available: https://software.intel.com/sgx

[6] Google AI Blog, "Federated Learning: Collaborative Machine Learning without Centralized Training Data," 2017. [Online]. Available: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

DHRUV BALI

POST-BREACH FORENSICS: LEVERAGING DIGITAL EVIDENCE FOR CYBERSECURITY RESILIENCE
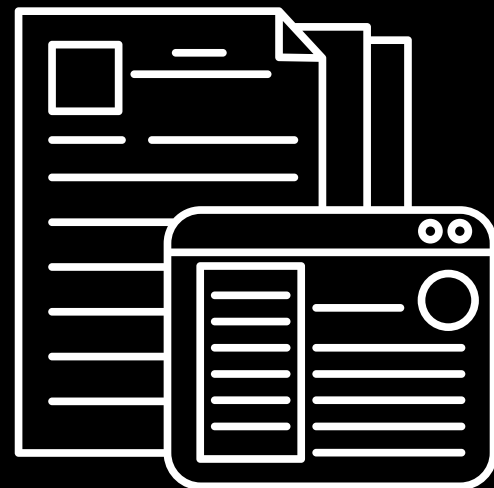
Introduction

In the hyperconnected digital world we live in, when it comes to cyberattacks, it's not a question of "if," but of "when." Despite their best efforts, no target is immune to sophisticated threats, such as ransomware moving laterally with perfect through the network to malicious insiders to advanced persistent threats (APTs). After a breach takes place, the most important step is the post-breach investigation. Digital forensics is crucial in this phase so companies can learn more about the scope and nature of the incident and its fallout, for the purposes of this post-breach context as well as better securing their environments moving forward.

After the dust settles, how an organization responds in the aftermath of an attack can either help or hinder a full recovery. Forensics not only reveals what happened, but more importantly, how we can stop it happening again, which is why it's a key component of long-term security resilience. As regulation tightens and reputations are on the line, post-breach forensics in real time is a critical business function. This paper discusses the post-breach forensic investigation process, available tools, the associated challenges, and the emerging concept of forensic readiness in a cyber-resilient organization.

Understanding Post-Breach Forensics

Post-breach forensics the process of investigating and analyzing after an information security incident as to the reason behind the breach, what compromised, and who was responsible. This method is necessary not just to control the harm but also to develop better defenses in the future. It's a combination of technical, legal and procedural aspects that must be carefully managed, harmonizing IT, legal and compliance functions.

Post-breach forensics does not aim just to gather and analyze evidence; the objective is to fully narrate the story of an attack, from initial compromise to its ultimate impact. This story enables decision-makers, from management to regulators, to decide how to manage risk, liability and potential reporting needs.

Stages of a Post-Breach Forensic Investigation

1. Preparation and Triage: The forensic process is initially started with setup and triage. This includes setting the forensic team up, setting investigation goals, and outlining affected systems. When such assets are prioritized over others, the investigation can be directed where the business is most at risk. Triage can also include quarantining harmed systems in order to protect them from continued destruction and also to protect volatile evidence.

A pull quote is an impactful quote taken from the article. You can place the quote you want to highlight here.

2. Evidence Execution: After the scope of an investigation is set, the second step is evidence execution. This includes logs, network traffic, system RAM, and disk images. Similarly, evidence needs to be gathered using traceable tools. The process, if documented, can help to ensure that any data collected can be entered into evidence in court without argument [1].

3.Preservation and Documentation: The preservation of digital evidence is of utmost importance. Forensics Detectives use software to produce bit-by-bit images of affected drives and copy volatile memory such as with FTK Imager or dd. Each and every step in the forensics work must be documented with meticulous notes that prove the authenticity and integrity of the evidence.

4. Analysis and Reporting: This phase is the meat of the forensic investigation. This means looking for evidence to piece together attacker activity (timeline), consider the available points of entry, and evaluate the exfiltrated data. Analysts connect the logs, examine malware samples and map the network paths to piece together the entire attack. The full report should contain results, IOCs, and actionable recommendations.

Key Tools in Digital Forensics

1. Disk and Memory Imaging Tools: EnCase and FTK are widely used to image and analyze data forensically. They offer keyword searching, file retrieval and metadata scraping. Volatility is widely used to analyze RAM images in order to detect malwares or rootkits that are running in memory [2].

2. Network Analysis Tools: People use Wireshark to collect evidence on most of the items in those lists (e.g., they view a packet capture of "suspicious" activity like packets to/from unknown IP space and data exiting the organization). This kind of analysis is important in order to build knowledge about attacker tactics and their movement through the network.

3. Log Analysis: With centralized logging tools like Splunk or the ELK stack, analysts can collect and search logs from devices, servers and applications. This is important for pattern analysis and identifying which suspicious events are related over time.

4. Open-Source and Low-Cost Tools: These are powerful open-source tools such as Autopsy, which is capable of disk image analysis, file carving, and hash comparison. It is equipped with a GUI for user-friendly operation, which is convenient for smaller groups or academic scenarios.

Article

Comparison of Key Forensic Tools

Tool	Type	Primary Functions	Common Use Case
EnCase	Disk Imaging & Analysis	Keyword search, file recovery, metadata analysis	Detailed investigation of hard drives and file systems
FTK	Forensic Toolkit	Data carving, email analysis, registry examination	Comprehensive system investigations, including email and file timelines
Volatility	Memory Forensics	RAM analysis, malware detection, process scanning	Rootkit detection and memory-based malware investigation
Wireshark	Network Analysis	Packet capture, protocol analysis, network traffic inspection	Identifying data exfiltration or command-and-control (C2) communications
Splunk	Log Analysis	Log aggregation, search, and correlation	Security event analysis across large infrastructures
Autopsy	Open-source Disk Forensics	File carving, hash analysis, user activity review	Budget-friendly disk image analysis for small teams or training

Challenges in Post-Breach Forensics

1. Encrypted Stealth: Cyber-attackers obfuscate both communication and payloads to bury malware actions deep, deep, inside the mess. They also use evasion techniques which include packing, polymorphism etc.

2. Anti-forensic Methods: Attackers use anti forensics techniques including log wiping, time stomping (changing timestamps), and deleting registry keys to obstruct forensic reconstruction. In addition, the attackers will also mislead authorities with behaviors that will muddy the waters further [3].

3. Cloud and Distributed Environments: Due to the wide adoption of cloud computing, data is commonly fragmented across different regions and managed by 3rd-party servers. This clouds the collection of evidence, worse in institutions that have no physical access to infrastructure.

4. Lack of skills and resources: Forensic investigation needs specific abilities and tools. Most companies can't even hire or keep good analysts, much less have some on the bench for when the incidents start piling up.

Future Trends in Digital Forensics

1. AI and Machine Learning: AI is being harnessed for quick analysis of large data sets to recognize attack patterns. Machine learning has the potential to spot anomalies and automate some elements of the investigation.

2. Cloud Forensics: As yet more of your infrastructure moves to the cloud, the forensic tools evolve. For cloud native forensics you need to gather information from an API, VMs as well as cloud storage services to track how the adversary moved.

3. Blockchain & Cryptocurrency Forensics: With the increase of cryptocurrency related crimes, forensic professionals have had to put in the time to trace blockchain transactions and smart contracts, in effect exposing unlawful activities and identifying the flow of money.

4. IoT Forensics: With the rise of Internet of Things (IoT) devices come new forms of evidence. Such traditional computer forensic methodology must evolve in response to the logs on the devices, firmware analysis, and the new data formats.

Conclusion

Post-attack forensics is a cornerstone of today's cybersecurity. It supports organizations in conducting a complete investigation of an incident, preserving important evidence and building better future defenses. Although it is always difficult and stressful, Trimming the fat is something that can be done right if you follow proven frameworks and use the right resources. In a world where digital reliance is growing and threat landscapes are changing, being prepared for a breach is not just an IT issue, it is a business critical. Enterprises need to spend more than reacting to incident, they must invest in forensic readiness. This involves educating teams, implementing strong tooling, and matching the regulatory expectations. With increasing threat size and complexity, forensic intelligence will be the cornerstone of resilient, trustworthy and secure digital intelligence ecosystems.

References

[1]https://www.sans.org/white-papers/introduction-digital-forensics/

[2]https://www.guidancesoftware.com/products/encase-forensic

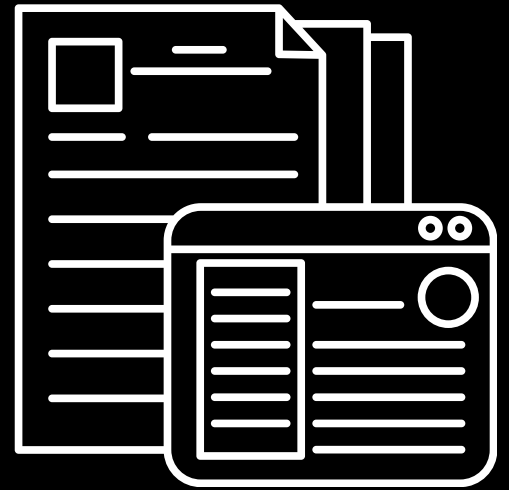[3]https://www.ncsc.gov.uk/guidance/anti-forensics-techniques

[4]https://iapp.org/news/a/international-data-transfers-gdpr-and-cross-border-forensics/

BHUMIKA BIJLWAN

INTRODUCTION TO QUANTUM COMPUTING

Introduction

An advanced section of computer science called quantum computing makes use of the unique rules of quantum physics to carry out computations. Quantum computers use qubits, which can be 0, 1, or both at once (thanks to superposition), in comparison with classical computers, which process data using bits (either 0 or 1). These computers can execute complex calculations far more quickly than conventional systems because they can also use interaction for linking qubits. This article provides a simple to read introduction for quantum computing, outlining its fundamental ideas, operation, distinctions from classical computing, and practical uses.

Rise of Quantum Computing

Ever wonder how scientists secure huge information transmissions or represent molecules? Classical computers are excellent at everyday activities like playing games or browsing the internet, but they start to struggle with more difficult issues like understanding complex encryption or implementing quantum physics. Quantum computing can help with it. Quantum mechanics, a similar knowledge that explains atoms and subatomic particles, is the foundation of this new computing method. Quantum computers use qubits, which can be in multiple states simultaneously, in place of regular bits (0 or 1), giving them ability when solving particular kinds of problems.

In addition to the efforts of technology companies like Google, IBM, and Microsoft, India's National Quantum Mission (2023–2031) is a significant step in the direction of quantum research [4].

Current Research and Projects (2022–2024)

Between 2022 and 2024, quantum computing research advanced rapidly across government, industry, and academia. In 2022, IBM introduced its 433-qubit Osprey processor and announced plans for systems exceeding 1000 qubits [1]. Google continued to advance quantum computing by focusing on quantum error correction, scalability, and practical applications beyond its original quantum supremacy demonstration [2]. Microsoft's Azure Quantum cloud platform supports multiple backends and hybrid quantum-classical workflows [3]. Researchers have also explored quantum advantage in machine learning and the development of noise-resilient quantum circuits [4]. In India, the National Quantum Mission, launched in 2023, aims to establish four specialized research centers for quantum computing, metrology, sensing, and communication [5]. Together, these collaborative efforts are laying the foundation for accessible, practical, and secure quantum computing.

> A pull quote is an impactful quote taken from the article. You can place the quote you want to highlight here.

Difference Between Classical and Quantum Computers

There are several significant differences between quantum and classical computers. The bit, which can be either 0 or 1, is the fundamental unit of data in classical computing. On the other hand, qubits which, according to the principle of superposition, can be 0, 1, or both simultaneously are used in quantum computing. Quantum computers use quantum gates like the Hadamard gate or CNOT gate, which operate on qubits and enable complex quantum operations like superposition and entanglement, whereas classical computers use Boolean logic gates (like AND, OR, NOT) to manipulate bits. Even with multi-core processors, classical computers can only process one computation path at a time, which limits their parallelism. However, quantum computers are capable of large parallel processing by using superposition to explore multiple possibilities simultaneously. When it comes to solving complex problems, such as converting large numbers, analysing molecules, or searching databases, quantum computers are capable of beating classical ones by an exponential margin. Real-world uses for classical computers include word processing, spreadsheets, and web browsing. Although they are still in their early years, quantum computers are being developed for complex uses like financial modelling, drug discovery, cryptography, and AI optimization.

Qubits: The core of quantum computing is a qubit, or quantum bit. A qubit can hold a 0, 1, or a combination of both, just like a bit can hold a 0 or 1. Similar to a spinning coin, it could show heads, tails, or both until you catch it. Small particles like electrons or photons are used to create qubits, which require strict control (often at very low temperatures).

Superposition: A qubit can exist in more than one state at once because of superposition. For example, a qubit in superposition can simultaneously be 70% 0 and 30% 1, whereas a classical bit can only be either 0 or 1. This means that 2^{10} (i.e., 1024) combinations can be stored simultaneously in a quantum computer with only 10 qubits.

Entanglement: The process known as entanglement, in which two qubits become connected, sounds magical. No matter how far apart they are, if one qubit changes, the other one responds right away. Because of this characteristic, qubits can be coordinated by quantum computers in ways that are not possible with classical systems. It also makes secure communication and quantum teleportation possible.
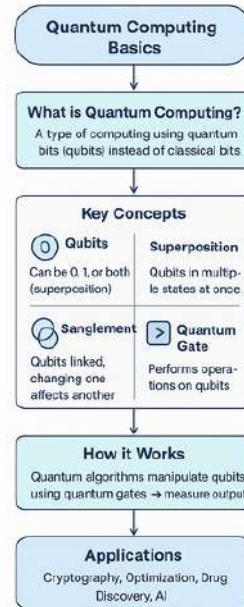
Quantum Gates: Quantum computers use quantum gates to carry out operations, just like classical computers do with logic gates (AND, OR, NOT). These consist of: Superposition is created by the Hadamard Gate (H). Pauli-X Gate: Functions similarly to a NOT gate. Qubits are entangled by the CNOT gate.To solve issues, these gates are placed in quantum circuits.

How Quantum Computers Work

Qubits are manipulated by specially made quantum circuits in quantum computers. First, the qubits are initialized in a known state, usually all set to 0. The qubits are then subjected to a sequence of quantum gates to modify their states. These gates enable the system to process multiple solutions simultaneously by introducing superposition, entanglement, and other quantum effects. Quantum computers evaluate multiple paths in parallel, in contrast to classical computers that only follow one path through an issue. After the gate's operations, the last stage is measurement, which generates the result by breaking each qubit's quantum state into a classical value (either 0 or 1). Quantum systems are very sensitive, though. To avoid decoherence which is the loss of quantum behaviour brought on by external interference. They must be maintained in extremely cold conditions close to absolute zero. To maintain the stability of their quantum processors, businesses such as Google and IBM employ enormous refrigerators known as dilution refrigerators. In such environments, high-precision lasers and microwaves are used to control qubits composed of trapped ions or superconducting materials. Despite their early development, today's quantum computers can already solve specific problems that would take thousands of years for classical computers to solve.

Introduction to Quantum Computing

How Quantum Computers Work

Some of the real-world application of Quantum computing are:

Cryptography: By rapidly factoring big numbers (using Shor's algorithm), quantum computers can decode traditional encryption algorithms like RSA [5]. They also contribute to the development of quantum-safe encryption at the same time.

Drug Discovery & Chemistry: In ways that classical computers cannot, quantum computers are able to recreate molecules and chemical reactions. This could result in new disease treatments or a quicker development of vaccines.

Finance: As compared to traditional tools, they can analyse large financial datasets for risk optimisation, stock prediction, and fraud detection far more quickly.

Article

Artificial Intelligence: AI model training can be sped up with Quantum Machine Learning (QML). Google and IBM, for example are currently testing hybrid quantum-classical models [1],[2].

Optimization Problems: For supply chains, airlines, and logistics, quantum computers can assist in real-time route, network, or resource optimisation.

Conclusion

Instead of being science fiction, quantum computing is quickly becoming a reality. The potential is huge, even though there are lots of challenges to overcome. Quantum computers have the potential to transform everything from data security to drug discovery by solving issues that are currently unsolvable by classical machines. Quantum computers are still in their early stages, despite their potential. Today, widespread use suffers by challenges like error correction, qubit instability, decoherence, and high production costs. But progress is being sped up by international efforts from major tech companies like Google, IBM, and Microsoft as well as government programs like India's National Quantum Mission. In addition to developing quantum hardware, these partnerships are enabling researchers and students to access cloud-based tools like Qiskit and Azure Quantum. The goal of quantum computing is to solve issues that were previously believed to be difficult, not just to create faster machines. As a result, it is among the most fascinating areas of science and technology at the moment.

References

[1] IBM, "Qiskit Documentation," [Online]. Available: https://qiskit.org.

[2] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Google AI Blog, Oct. 23, 2019. [Online]. Available: https://research.google/pubs/quantum-supremacy-using-a-programmable-superconducting-processor/.

[3] Microsoft, "Azure Quantum," [Online]. Available: https://azure.microsoft.com/en-us/products/quantum.

[4] Ministry of Electronics and Information Technology (MeitY), "National Quantum Mission (India) – Press Release," Press Information Bureau, 2023. [Online]. Available: https://pib.gov.in/PressReleasePage.aspx?PRID=2111953.

[5] C. Bernhardt, Quantum Computing for Everyone, MIT Press, 2019. [Online]. Available: https://mitpress.mit.edu/books/quantum-computing-everyone.

KHUSHI

ZERO TRUST NETWORK ACCESS: REIMAGINING SECURITY IN A PERIMETER LESS WORLD
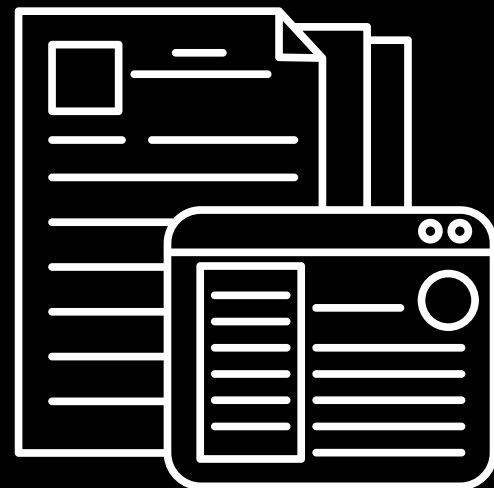
Introduction

The enterprise security landscape is undergoing fundamental transformation. Historically, network defense was grounded in the idea of a hardened perimeter trusted users and devices operated within, while unknown actors were kept out of the network. Technologies such as firewalls and Virtual Private Networks (VPNs) were sufficient when applications were hosted in central data centers and employees worked exclusively from office networks.

However, with the rise of remote work, bring-your-own-device (BYOD) culture, cloud-native applications, and hybrid infrastructure, traditional perimeter-based security has become obsolete and ineffective. Zero Trust Network Access (ZTNA) has emerged as a modern security model that replaces implicit trust with continuous verification, providing identity-aware, context-sensitive, and application-level access control [1].

The Shift to Zero Trust

ZTNA is grounded in the Zero Trust philosophy: "Never trust, always verify." Unlike conventional models that grant broad network access after a single authentication, the ZTNA enforces access control on a per-application basis, ensuring that users and devices are authenticated and authorized continuously throughout the session.

ZTNA replaces static credentials and internal trust assumptions with dynamic policies based on identity, location, device posture, time, and risk factors. This architecture is particularly vital for distributed enterprises, where users access sensitive data from multiple networks and platforms.

Core Principles of ZTNA

ZTNA implementations vary by vendor but consistently follow certain foundational principles.

- Application-Specific Access: Users are granted access to only the applications they need, not the entire network. This limits the lateral movement and reduces the attack surface [2].

- Microsegmentation: Each connection is isolated, and access to one service does not imply access to other services. If a breach occurs, its spread is contained immediately.

- Continuous Authentication: ZTNA continuously validates user credentials, device posture, and behavioral context. If anomalies are detected mid-session (e.g., sudden location changes or suspicious activity), access can be revoked.

- Contextual Risk Evaluation: Access decisions are based not only on identity but also on real-time contextual information, such as device security status, IP reputation, geolocation, and access time.

- Obfuscation of Network Infrastructure: Internal applications and IP addresses are never directly exposed. They are hidden behind secure access brokers and are accessible only via pre-authenticated tunnels [3].

A pull quote is an impactful quote taken from the article. You can place the quote you want to highlight here.

ZTNA vs VPN: A Modern Security Contrast

Feature	VPN	ZTNA
Access Granularity	Full network	Per application
Authentication	One-time	Continuous
Visibility	Basic logging	Fine-grained, real-time
Device Posture Checks	Rare	Mandatory
Lateral Movement	Unrestricted	Prevented
Performance	May degrade	Optimized
Scalability	Limited	High
Cloud Compatibility	Poor	Native

ZTNA Architecture and Deployment

ZTNA consists of three primary components.

1. Client Device or Agent: Installed on the user device or accessed via browser (agentless), it communicates identity and device posture information.
2. ZTNA Controller: A policy engine that verifies identity, evaluates risk, and enforces rules.

ZTNA Gateway/Broker: Acts as a reverse proxy or intermediary to route approved traffic to internal resources.

There are two major deployment models.

- Agent-based ZTNA offers deeper device-level telemetry but requires software installation on the device.
- Agentless ZTNA enables quick deployment and is useful for third-party or unmanaged devices.

ZTNA integrates with identity providers (IdPs), Multi-Factor Authentication (MFA), endpoint detection and response (EDR), and Security Information and Event Management (SIEM) platforms for complete access visibility and control [5].
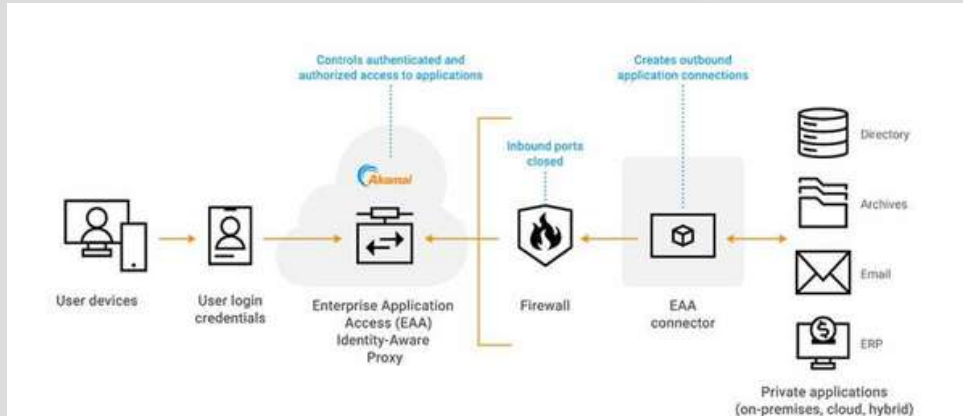
Types of ZTNA

ZTNA implementations can be categorized into three models depending on the focus:

- User-Centric ZTNA
- This approach focuses on securing user access to applications by verifying identity and device compliance before permitting any connection. The user is granted access through a direct, secure channel that bypasses the broader internet, reducing exposure to external threats.
- Workload-Centric ZTNA
- In this model, ZTNA is used to safeguard application workloads—both during development and in production. By restricting lateral movement within the infrastructure, ZTNA helps prevent unauthorized access and minimizes the risk of data breaches. This ensures secure communication between application components and services.
- Device-Centric ZTNA
- With the rise of bring-your-own-device (BYOD) practices, endpoint security has become a significant concern. ZTNA frameworks can enforce continuous monitoring and protection of data in transit to and from devices, ensuring that only trusted endpoints interact with corporate resources.

Each model can be blended to meet the unique security requirements of modern hybrid environments.

Security and Business Benefits

ZTNA offers multiple advantages over traditional security frameworks.

- Reduced Attack Surface: Applications remain invisible to unauthorized users, eliminating exposure to reconnaissance and brute-force attempts.
- Enhanced User Experience: Seamless access to apps without manual VPN toggling; traffic routes directly via optimized, encrypted paths.
- Operational Efficiency: Centralized management of policies and access; easier provisioning and deprovisioning of users.
- Cloud-Native Compatibility: Ideal for securing SaaS, multi-cloud, and hybrid workloads.

Regulatory Compliance: Fine-grained access logs and policies support GDPR, HIPAA, and other compliance requirements.

Challenges and Considerations

Despite its advantages, ZTNA adoption is not without challenges.

- Initial deployment complexity: Integration with legacy systems and identity platforms requires significant planning.
- Vendor Lock-In Risks: Certain solutions need specialized infrastructure or bundle proprietary agents.

- Visibility Gaps: Poorly designed ZTNA solutions can lead to blind spots in monitoring or incomplete policy enforcement.

To succeed, organizations must carefully choose vendors, ensure policy consistency, and maintain visibility of their environments.

Conclusion

Zero Trust Network Access represents a significant breakthrough in how organizations deal with cybersecurity in the context of cloud migration, remote working, and increased cyberattacks. By removing implicit trust and imposing granular context-aware access, the ZTNA offers a scalable, secure, and easy-to-use solution to safeguard contemporary digital assets.

With increasing sophistication in cyberattacks and growing distribution of infrastructure, ZTNA will increasingly become a standard security architecture for enterprises globally.

References

[1] Kindervag, J. (2010). "No More Chewy Centers: Introducing the Zero Trust Model of Information Security." Forrester Research.

[2] NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology (NIST).

[3] Google Cloud Platform. (2022). "BeyondCorp: A New Approach to Enterprise Security." BeyondCorp Zero Trust Enterprise Security | Google Cloud

[4] Gartner. (2023). Market Guide for Zero Trust Network Access.

[5] Palo Alto Networks. (2024). "ZTNA Explained: Understanding the Framework." Zero Trust Network Access 2.0 - Palo Alto Networks

HARSHITA SHARMA

FUN FACTS
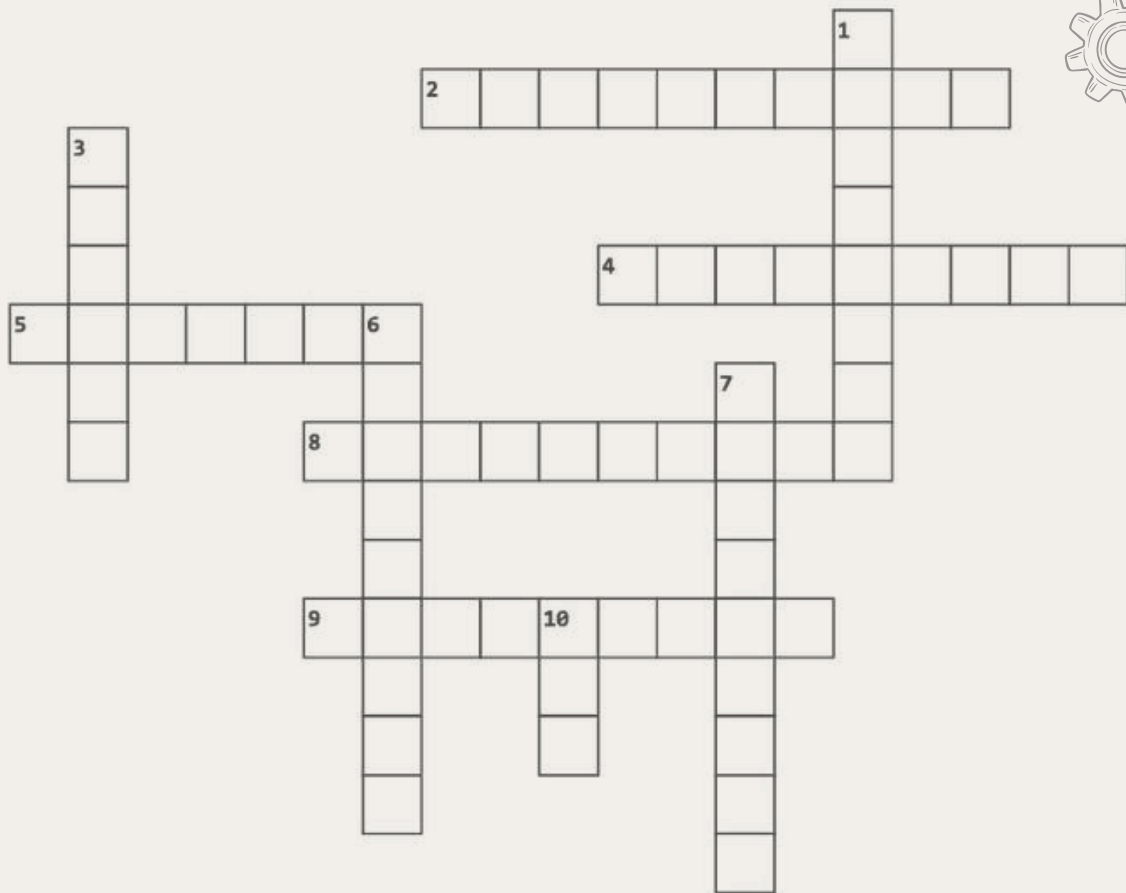
CLUES

ACROSS

2. Data Structures and __ are a major focus of ACM.
4. ACM has members in over 100 different __
5. ACM's online library of research and articles is called the __ library.
8. Many students join ACM to prepare for job __ .
9. ACM often organizes short/long timed contests

DOWN

- 1. College level communities of ACM.
- 3. In our college ACM is mainly known as __ club.
- 6. From C to python, ACM helps students master these.
- 7. ACM thrives on this method where seniors guide juniors.
- 10. Founded in 1947, this is world's first major computing society.

ACROSS: 2. Algorithms, 4. Countries, 5. Digital, 8. Interviews, 9. Hackathon
DOWN: 1. Chapters, 3. Coding, 6. Languages, 7. Mentoring, 10. ACM

CREDITS

Editorial Mentor Board

Dr. Sunil K. Singh
(Mentor)
Professor and HoD
Department of CSE

Dr. Sudhakar Kumar
(co-mentor)
Professor
Department of CSE

Sahil Garg
CASC Student
Chairperson
(2024-2025)

Ayushi
CASC-W Student
Chairperson
(2024-2025)

Jaiveer Singh
CASC Student
Chairperson
(2025-2026)

Ritika Kalia
CASC-W Student
Chairperson
(2025-2026)

Lead Editors

Aarushi
2023

Aanshi Bansal
2023

Content Editors

Eshmeet Singh Bhachu
2023

Vanshika Singla
2023

Feature Editors

Agamjot
2023

Khushi
2023

Bhavya
2023

Anshika Goyal
2024

Tanvi
2024

Shiven
2024

Aayush
2024

CASC Board

Jaiveer Singh
Chairperson

Satvik Pathak
Vice-Chairperson

Sanatan
Secretary

Shivam Vats
Membership Chair

Dhruv Bali
Treasurer

Abhay
Webmaster

Aarushi
Design Head

Kritin
External Member Head

Vanshika Singla
Editorial Head

Sahil Kumar
Social Media Manager

Maanit
PR Head

Aditya
Event Manager

Japjot
Domain Director(Web & DevOps)

Hitesh
Domain Director
(Competitive Programming)

Anshul
Domain Director
(Android)

Jasvir
Marketing Head

Jasjeet
Domain Director
(AI & Ml)

CASC-W Board

Ritika Kalia
Chairperson

Samriti Sharma
Vice-Chairperson

Simar Atwal
Secretary

Mehak Negi
Membership Chair

Khushi
Treasurer

Bhavya
Webmaster

Eshmeet Singh Bachu
Design Head

Ravina Mittal
Executive Member Head

Aanshi Bansal
Editorial Head

Bhumika Bijlwan
Social Media Manager

Harshita
PR Head

Sargun
Event Manager

Shreya
Domain Director(Web & DevOps)

Hitesh
Domain Director
(Competitive Programming)

Anshul
Domain Director
(Android)

Anshika Goyal
Marketing Head

Jasjeet
Domain Director
(AI & Ml)

Scientists explore the mysteries of what exists,
while engineers bring to life what once
only existed in dreams.

✉ - acmccet@gmail.com

⧉ - /acmccet

🌐 - https://ccet.acm.org

▶ - CCET ACM Student Chapter

f - /acmccet

in - ccet-acm-student-chapter

CCET, Degree Wing | Department of CSE | Sec-26 Chandigarh
Contact Us - www.ccet.ac.in