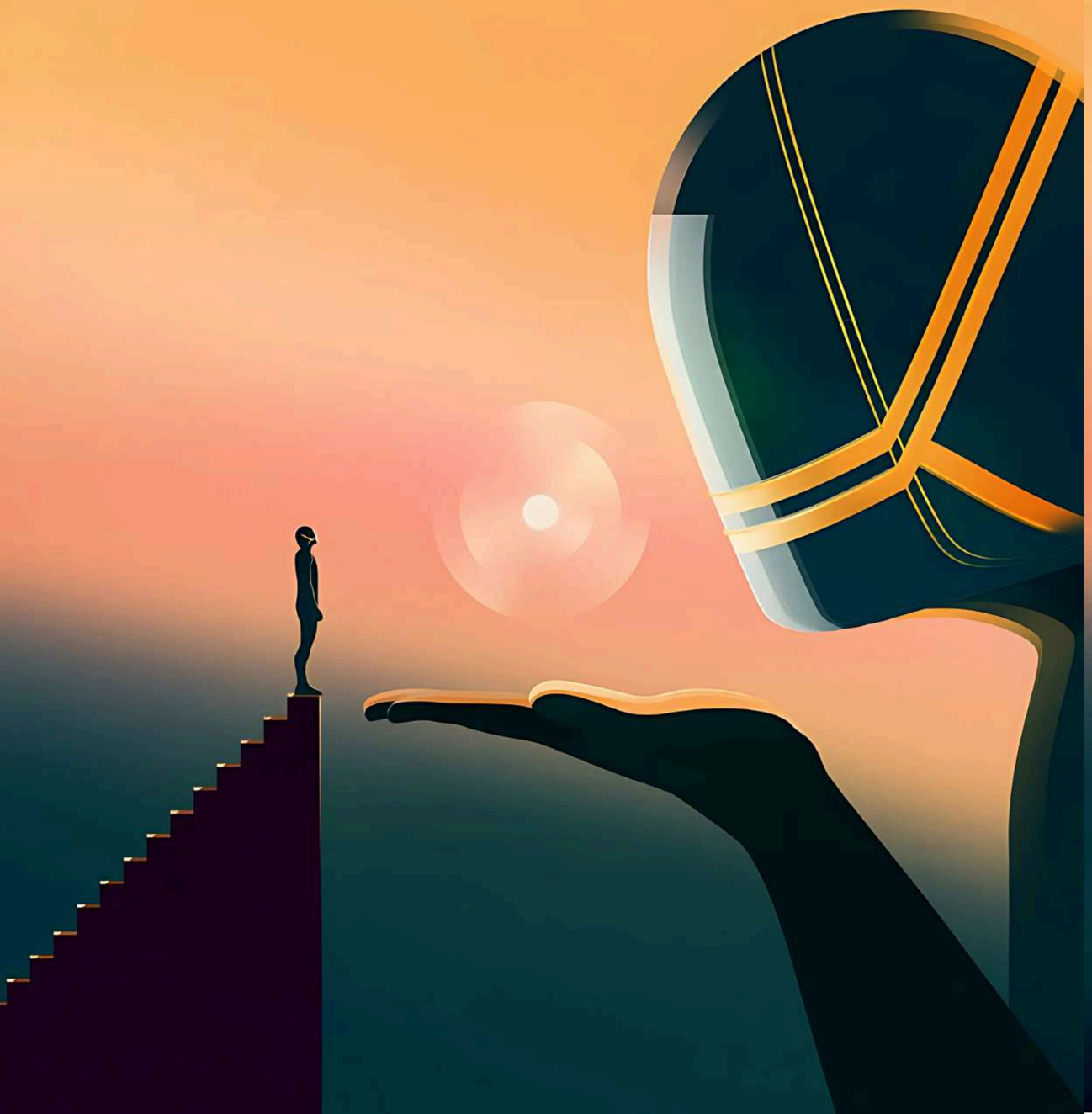
BITWISE VOL-6



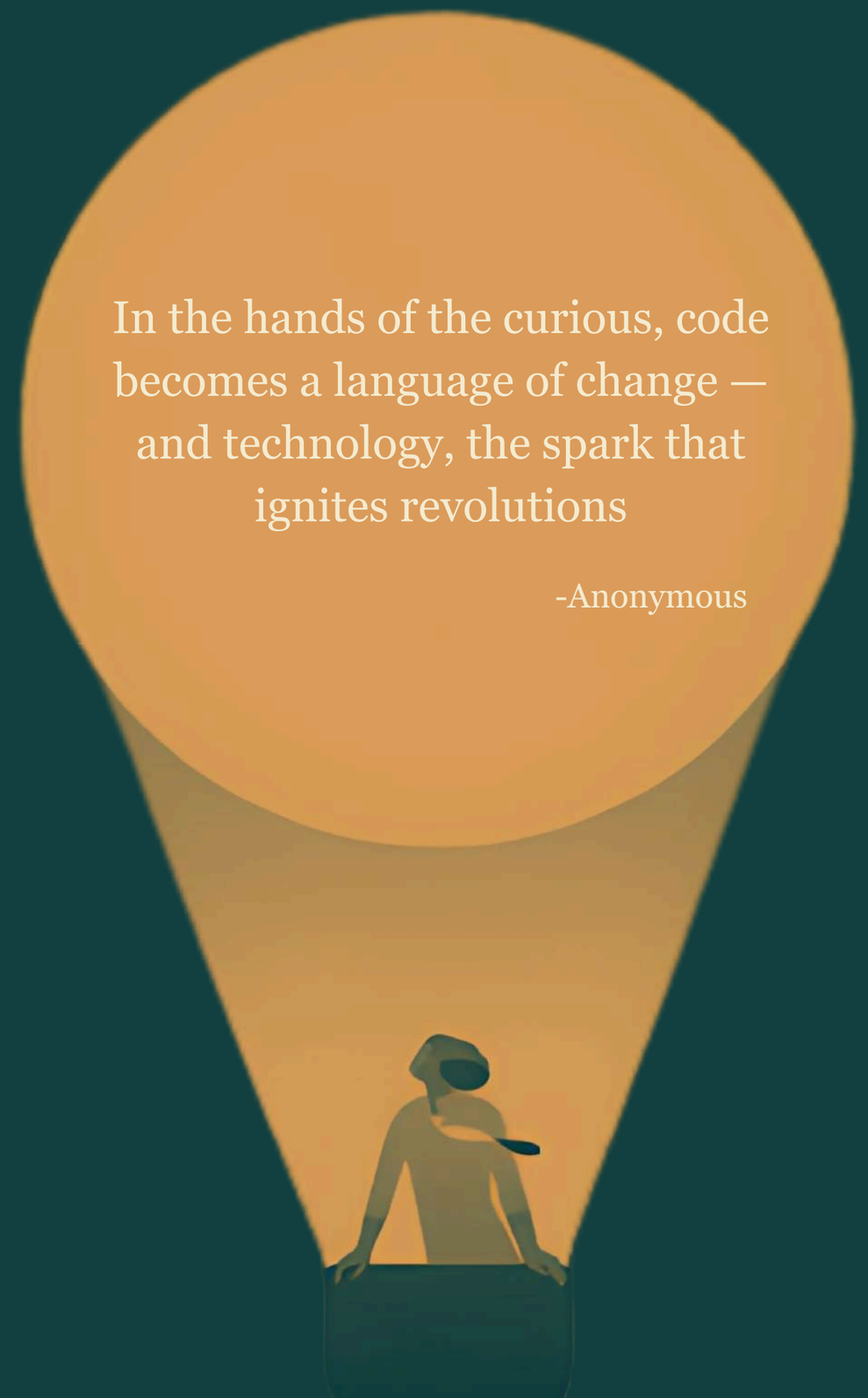
Ordinateur

The Computer Science Society

(2024 - 25)

In the hands of the curious, code becomes a language of change — and technology, the spark that ignites revolutions

-Anonymous



CONTENTS

01 WORDS OF ENCOURAGEMENT 03 - 06

02 LETTER FROM EDITORS 07 - 08

03 ANNUAL REPORT 09 - 12

04 ACHIEVEMENTS 13 - 14

05 ONE CLICK TOTAL CONTROL 15 - 18

06 THE NEW FACE OF CYBERCRIME 19 - 20

07 BEYOND INCOGNITO 21 - 24

08 FACTS AROUND THE WORLD 25 - 26

09 THE RISE OF DEEPFAKE CYBERTHREATS 27 - 30

10 THE FUTURE OF CYBERSECURITY 31 - 32

11 THE RISE OF QUANTUM COMPUTING 33 - 36

12 COMIC 37 - 38

13 INTERNET OF THINGS AND CYBERSECURITY 39 - 40

14 HUMAN IS A NEW HARDWARE 41 - 44

15 THE GREENTECH REVOLUTION 45 - 46

16 IAM: FOUNDATION OF CYBERSECURITY 47 - 50

17 AI IN CYBERSECURITY: FRIEND, FOE OR FRENEMY 51 - 52

18 CROSSWORD PUZZLE 53 - 54

19 FACULTY MEMBERS & BITWISE TEAM 55 - 57

WORDS *of* ENCOURAGEMENT

Prof. (Dr.) Rama (Principal)

Hansraj College has always been more than just an institution—it is a nurturing ground for academic excellence, intellectual growth, and holistic development. Our NAAC A++ accreditation and an impressive NIRF ranking of 12 stand as a testament to the dedication, hard work, and collective spirit of our students, faculty, and staff.

The Computer Science Society stands as a shining example of this commitment through its dedication to technological innovation, creative problem-solving, and collaborative learning.As Dr. APJ Abdul Kalam rightly said, *"Learning gives creativity, creativity leads to thinking, thinking provides knowledge, and knowledge makes you great."* The Computer Science Society truly embodies this spirit—encouraging students to think beyond boundaries, embrace new ideas, and bring their creative visions to life.

I would like to express my sincere gratitude to the faculty members whose mentorship and dedication play a vital role in shaping the future of our young technologists. Their commitment to fostering curiosity and critical thinking empowers students to achieve more.

A heartfelt appreciation also goes out to the student members whose passion, creativity, and relentless pursuit of knowledge have made this society a hub of innovation and excellence. The release of BITWISE is a reflection of your collective hard work, ingenuity, and dedication.

On behalf of Hansraj College, I extend my heartfelt congratulations and best wishes to the Computer Science Society, the faculty, and all its members for their remarkable efforts. May you continue to scale new heights of creativity, innovation, and academic excellence, making Hansraj College proud with your outstanding contributions to technology.

MESSAGE FROM TEACHER-IN-CHARGE

Prof. Baljeet Kaur

It is with great pleasure that I share this magazine, a reflection of the passion, creativity, and commitment of Computer Science students at Hansraj College. More than just an outline of ideas, it represents an enthrallment of curiosity and innovation. As you'll see, the students have explored technology well beyond the text.

In this age of rapidly evolving technology—where AI, automation, and cybersecurity are reshaping every field—education must go beyond knowledge. It must involve questioning, experimenting, and nurturing uniqueness. More than anything, we want our students to develop curiosity, adaptability, and problem-solving skills so they can explore, create, and make an impact. Watching them transition from learners to active participants in projects, ideas, and conversations has been truly inspiring.

This magazine showcases our students' creativity, critical thinking, and technological talent. Within its pages are insightful contributions—from trend analysis to unique ideas—that reflect a shifting technological landscape. These perspectives provoke thoughtful discussions on learning, innovation, and the future.

I hope this spirit of collaboration and forward-thinking inspires future technologists to embrace uncertainty and take bold steps. Sincere thanks to the students and faculty whose hard work brought this magazine to life. Your teamwork and determination are deeply valued. This same commitment is evident in our students' achievements in sports and extracurriculars, where their growth and dedication shine.

May this edition inspire, challenge, and motivate you to reflect on your own passions in technology. I hope it encourages you to dream big, think critically, and pursue excellence in our fast-changing digital world.

Happy reading!

Message from Senior Advisor

Dr. Harmeet Kaur

With great pride, I present the 6th edition of Bitwise, the annual publication of the Computer Science Department at Hansraj College for the academic year 2025–26. This edition reflects the dedication, creativity, and growth of our students and faculty. The year has been one of innovation, collaboration, and exploration. Our students embraced challenges, excelling not just academically but also through hackathons, workshops, and competitions. These experiences have cultivated an environment of creativity, curiosity, and problem-solving, where students have not only expanded their knowledge but also honed skills that transcend traditional classroom boundaries.

In this edition, we proudly showcase the culmination of their hard work — their technical achievements, yes, but also their ingenuity, resilience, and thirst for knowledge. My heartfelt thanks to the editorial team and contributors who brought this magazine to life. Bitwise is more than a publication; it captures the dynamic spirit of our department and the exciting journey we're on together.

As you flip through these pages, I hope you find inspiration. The future of computer science holds endless possibilities — and you, our students, are key to shaping it. Keep innovating, collaborating, and pushing your limits. Here's to your continued success and a bright, ever-evolving future in technology!

Message from Bitwise Convener

Dr. Sunita Chand

Dear Readers,

It is my immense pleasure to welcome you to the latest edition of Bitwise Vol. 6, the voice of the Computer Science Department at Hansraj College. As the convener, I am thrilled to witness the passion and innovation of our students, faculty, and contributors come together to create this vibrant publication.

In the ever-evolving world of technology, this magazine serves as a platform to explore, discuss, and celebrate the ideas shaping our future. This issue dives into "cutting-edge advancements in Cyber security, AI, and the creative intersections of tech and society", reflecting the brilliance and curiosity of our community. Whether you're a coder, a thinker, or a tech enthusiast, there's something here for you. I extend my deepest gratitude to our talented team of writers, editors, and designers from the department, whose hard work has made this edition possible. A special thanks to our readers—your engagement fuels our drive to push boundaries and showcase the spirit of computer science at Hansraj.

As we move forward, let's continue to inspire and challenge each other in this dynamic field. I invite you to dive into these pages, share your feedback, and join us in this exciting journey of discovery.

Letter From Editors

It gives us great pleasure to present Bitwise 6.0, the sixth edition of the annual magazine of the Computer Science Department, Hansraj College. This edition is the result of months of effort, teamwork, and shared enthusiasm for all things technical, and we are thrilled to finally share it with you.

As the editorial heads, we aimed to put together a magazine that not only showcases our department's technical skills but also captures the ideas and interests of our students. In Bitwise 6.0, you'll find a variety of articles on cool topics and innovations in the tech world.We've got pieces on everything from artificial intelligence and cybersecurity to blockchain.

Through the editing process, we focused on keeping the quality high while encouraging students to share their curiosity about technology. We carefully reviewed each article to make sure they were clear, relevant, and original. What you'll read in this edition comes from thoughtful selection and teamwork. This journey was deeply fulfilling, but it wasn't without its difficulties. Working with contributors, sticking to deadlines, and keeping everything consistent took a lot of effort.Every challenge taught us something new and brought us closer together as a team. We're really proud of how this edition turbed out, and we hope it sparks knowledge and inspiration for you.

A big thank you to all our contributors for their hard work and dedication. We're also thankful to our faculty mentors for their guidance and support throughout this process.

Bitwise 6.0 is more than just a bunch of articles — it represents the passion and drive of our department. We hope you find this edition both informative and enjoyable. Thanks for joining us on this journey!

Kritiman Pathak
Thejas Suresh
Mehak Narang

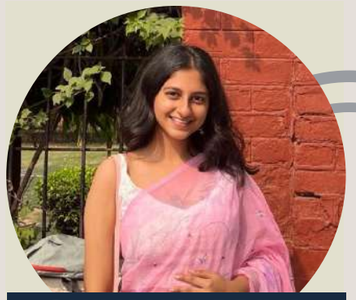
Editorial Heads

OFFICE BEARERS 2024-25

NETRESH SINGH
President

HARSHIT RAWAT
Vice President

YASHASVI MITTAL
General Secretary



SHIVANGI PRIYA
Treasurer

DIVYA BABBAR
Joint Secretary

DIYA JHANWAR
Joint Treasurer

ANNUAL REPORT
2024-25

Bitwise Ordinateur

This year was an eventful one for **Ordinateur**, the Computer Science Society of Hansraj College. Staying true to its goal of encouraging curiosity and learning among students, the society hosted a variety of activities that focused on practical learning, peer collaboration, and insights from the tech world. With constant support from the faculty and active participation from students, Ordinateur continued to be a space where ideas could grow and new skills could take shape.

The academic session started off with an **Arduino for Beginners Workshop** on **4th October 2024,** held in collaboration with the Departments of Physics & Electronics and the Institution's Innovation Council (IIC). Conducted in CS Labs 1 & 2, the session introduced 48 students to basic Arduino concepts, sensors, and actuators. The workshop was led by **Dr. Nishant Shankhwar** and **Mr. Suyash Kumar**, who helped students build a strong foundation in embedded systems.

On **6th November 2024**, the society organized **The Digital India Talk Show** in the Old Seminar Room. In collaboration with **NeGD, MeitY**, the session featured speakers like **Mr. Karan Tandon, Mr. Arshil Khan, Mr. Sanjay Patel, Mr. Mohammad Kaif,** and **Mr. Abhishek Kumar**, who spoke about **DigiLocker, ABC/NAD–APAAR, Cyber Laws, UMANG,** and more. The session ended with a quiz, making it both informative and engaging for attendees.

Following this, a **Gemini AI Workshop** was held on **7th–8th November 2024** in collaboration with Google Developer Group – Hansraj. The two-day event took place in Labs 1 & 5 and gave students the chance to work with **HTML**, **CSS, JavaScript**, and APIs to build Gemini-inspired web tools. The session was guided by **Rakshit Rabugotra, Deepanshu Saini, Parth Ratra**, and **Mayank Yadav,** who helped participants get hands-on experience in web development and AI.

In January, the society conducted **Techiza 2025,** a tech quiz competition on 30th January 2025. The quiz featured rounds on programming, AI, and space technology. **Moinak Roy, Divyansh Bansal,** and **Vishu,** all first-year students of BSc (H) Computer Science, secured the top spot.

To build stronger ties with former students, Alumni Connect was held on 16th February 2025 via Google Meet. Speakers included **Ms. Khushboo (DE Shaw)**, **Ms. Priyanka (YMSLI)**, and **Ms. Jyoti Srivastava (Fractal Analytics)**, who shared their experiences with placements, internships, and skill-building — offering valuable guidance to current students.

March brought the much-anticipated **Hans Innoverse 1.0 Hackathon,** conducted on **3rd March 2025** in partnership with IIC. Held in the Multipurpose Hall, the event saw over 900 registrations. Out of these, 12 teams made it to the final round and presented their working prototypes to a panel of 11 judges. **Malaai, Invincibles, Safespace** and **Pandas** were declared the top three teams. The event celebrated creativity, collaboration, and problem-solving.

Concurrently, from **1st March to 12th April 2025**, the society conducted a 4-day offline Workshop on **"HTML, CSS, and JavaScript"** at CS Lab 1. Held every Saturday and led by student resource person Netresh Singh (President, Ordinateur), the sessions introduced 21 participants to the basics of frontend development. From creating simple webpages to building a stylized login page and an expense tracker app, the workshop provided hands-on experience in designing interactive websites. Guided by Mr. Suyash Kumar and Dr. Vidhi Khanduja, the workshop created a supportive, collaborative environment that encouraged experimentation and sparked interest in web technologies.

The session wrapped up with **Cyber Awareness Week** on **27th March 2025,** held in collaboration with **C-DAC Noida under ISEA-III**. The event focused on topics like phishing and data breaches, and included demonstrations of tools like HaveIBeenPwned and VirusTotal. A quiz and a street play (Nukkad Natak) added an interactive and impactful touch to the discussions on cybersecurity.

On **5th March 2025**, the society hosted a **Generative AI Workshop** in collaboration with IQAC, Hansraj College. Guest speaker **Mr. Aditya Kumar** introduced participants to LLMs, Python-based AI development, and Gemini LLM. A hands-on session using **LangChain** allowed students to build their own chatbot. A quiz concluded the workshop, with winners receiving goodies and all participants earning certificates.

In Conclusion

The 2024–25 academic year was full of learning, discovery, and connection. Through workshops, talks, competitions, and community events, Ordinateur created opportunities for students to learn new skills, think creatively, and explore different sides of the tech world. As the society looks ahead, it remains committed to creating spaces where students can learn, grow, and support each other.

Achievements

1. ACADEMIC

Internships and Placements :

- **Vibhor Jain** & **Jyoti Singh** secured placement at **De Shaw & Co**.
- **Aishmanya Nishi** completed a paid internship with IISD and Carbon Minus India for the Global Sustainability Summit 2025 at Vigyan Bhawan. She was selected as one of six core team members and served as Social Media Head.
- **Thejas Suresh, Priyam Gupta, Shivangi Priya, Pranjal Shome, and Shruti Maurya** were selected for the prestigious Vice Chancellor's Internship Scheme (Part-Time) for the year 2024–25.
- **Yashasvi, Mayank, and Netresh Singh** were selected for the Hansraj College internship focused on maintaining and managing the official college website.
- **Mehak Narang** completed internships in Data Analytics at VerveBridge and NullClass, and in Python Development at CognoRise Infotech.
- **Vineet Kumar Kankerwal**, **Arya Agarwal**, **Ashish Kumar**, and **Sahil Gupta** have secured placement at Fractal Analytics.
- **Kanak** and **Ronak Seth** have secured placement at **United Airlines.**

Competitions:

- **Parth Ratra, Rahul Sharma, Pranay Rajvanshi, Kirti Rathi, Anishka Raghuwanshi, and Sakshi Dhariwal** – Team TrashCam **won** the **Smart India Hackathon 2024** and also won the cash prize for this under the Clean & Green Technology theme for PS1592.
- **Siya Chandna, Shruti Singh, Ritik Kumar Gupta, Shreya Sharma, and Bhumika Dahiya** – Team D-Core ranked among the Top 30 at Smart Delhi Ideathon 2025 for the problem statement "Achieving Zero Waste", with their project EcoBin, an AI-powered waste management app featuring gamification and a recyclables marketplace.
- **Parth Ratra, Nikhil Sain, Kirti Rathi, Anishka Raghuwanshi** – Team random.random ranked among the Top 137 teams nationwide and Top 27 on their PS at Amazon Smbhav Hackathon 2024, among over 1,00,000 participants.
- **Parth Ratra, Rahul Sharma, Pranay Rajvanshi, Kirti Rathi, Sakshi Dhariwal** – Team UrbanEco won at BuzzOnEarth India Hackathon 2024 (IIT Kanpur) for the Best Use of Intel AI Toolkit.
- **Parth Ratra, Rahul Sharma** – Team UrbanEco were Finalists at the Urban Innovation Challenge 2.0 with their urban sustainability proposal.
- **Parth Ratra, Rahul Sharma, Pranay Rajvanshi, Kirti Rathi, Anishka Raghuwanshi, Sakshi Dhariwal** – Team TrashCam secured 3rd position at the SIH Internal Hackathon 2024, Hansraj College.
- **Parth Ratra, Rahul Sharma, Pranay Rajvanshi, Harsh, Nikhil Sain** – Team part-time students ranked among the Top 30 at Smart Delhi Ideathon 2025 for the problem statement "Creating a Safer Delhi for Women."

Others:

- **Kanak, Subhajit Das, Krishan Kant, Sanchit Jain, Ashish Kumar Swarnkar and Thejas Suresh** Co-authored a research paper accepted for publication at the prestigious ICICV-2025 Conference, under the supervision of Prof. Baljeet Kaur.
- **Harshit Rawat and Netresh Singh** completed Industrial Training in CCNA Essentials (Aug–Oct 2024) from the Indian School of Ethical Hacking (ISOEH) in collaboration with Hansraj College. They achieved an O+ grade (90%+), gaining hands-on expertise in networking fundamentals, device configuration, subnetting, VLANs, and key protocols like TCP/IP, OSPF, and EIGRP.
- **Vibhor Jain** secured an All India Rank (AIR) 29 in GATE 2025 – Data Science & AI, and AIR 182 in GATE – Computer Science & IT.
- **Shruti Singh and Yogita** were Awarded the Reliance Foundation Undergraduate Scholarship for the academic years 2024–2027.
- **Gauri Tiwari, Aastha Garg, Yogita, Divyansh Chauhan, Aadarsh Sharma and Priyanshu Bhatt** were selected for the Dell Aspire Scholarship program under the Michael & Susan Dell Foundation for the academic years 2025–2028.
- **Vishu** won 3 science-themed games on National Science Day 2025
  organized by the CS, Botany, and Physics departments;
  activities included critical thinking, memory mapping,
  sensory challenges, general quizzes, and myth-busting.

2. CO- CURRICULAR

- **Saloni Kaushik** represented Hansraj College as a member of Oorja, the western dance team, at the 100 Plus Competition featuring 100+ colleges across Delhi-NCR, where the team secured 60 positions and ranked as the No. 1 team in the Delhi dance circuit. She also won 2nd prize in the solo dance competition at Uphoria'25, Bennett University's annual cultural fest.

ONE CLICK TOTAL CONTROL

Written by:
Divyanshu Rangad (II)
Shivangi Priya (II)

WHAT HAPPENED TO UBER?

The Security Breach That Shouldn't Have Happened

Imagine riding home late at night, trusting the Uber app to keep you safe. Now, picture a hacker gaining full control over Uber's systems—tracking rides, accessing payment details, and manipulating driver accounts. This is exactly what happened in 2022.

Using **MFA (Multi-Factor Authentication)** fatigue attacks, the hacker bombarded an employee with authentication requests until they finally approved one. That single mistake granted access to Uber's security tools, financial records, and customer data.

With **Zero Trust Architecture (ZTA)**—where every request is verified continuously—this attack could have been stopped before it started.

What is Zero Trust Architecture?

Imagine a high-security facility where every door and access point requires verification—no open pathways, no assumptions of trust. That's ZTA—"Never Trust, Always Verify." The outdated "castle-and-moat" model, where the perimeter is secured but the interior is trusted, is obsolete. Modern threats require a dynamic, adaptive approach.

The End of Blind Trust

A simple password once granted full network access. Today, cybercriminals use phishing, ransomware, and insider threats to bypass defenses. Zero Trust assumes all access requests may be malicious, even inside the network.

Core Principle of Zero Trust

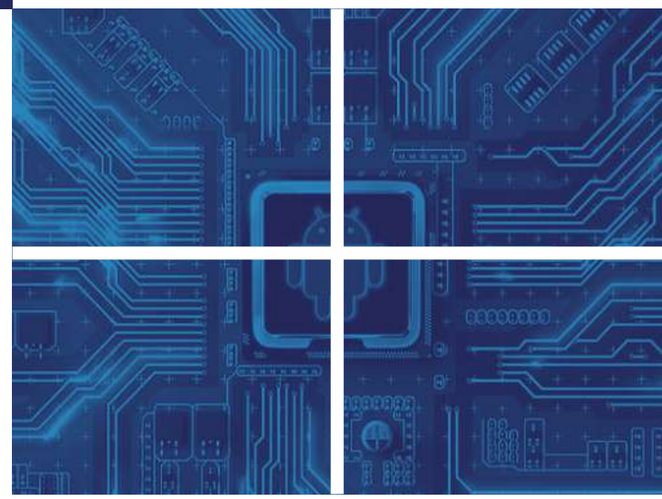
Verify Continuously – Multi-factor authentication (MFA), biometrics, and AI-driven risk analysis ensure strict identity verification.

Least Privilege Access – Users and devices get only necessary access—no blanket permissions.

Micro-Segmentation – Networks are divided into isolated segments, preventing lateral movement.

Real-Time Monitoring – AI-driven analytics detect anomalies and flag threats before escalation.

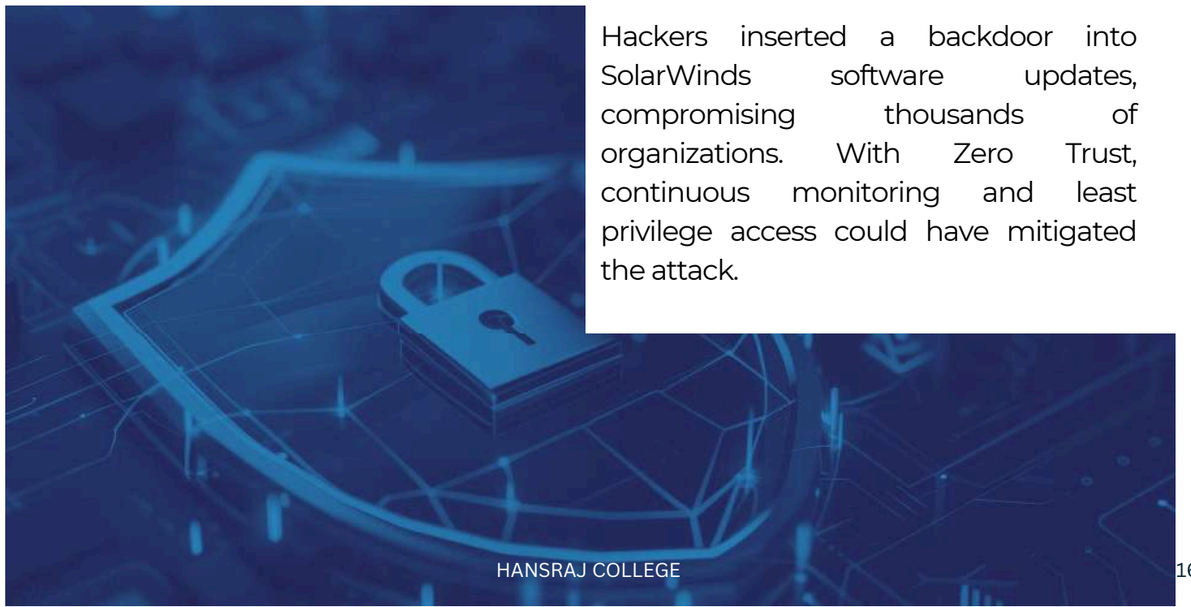
Encryption Everywhere – Data is encrypted at all times, ensuring security even if intercepted.



Why Zero Trust Matters: Real-World Cases

SolarWinds Breach (2020) - "The Trojan Inside the Castle"

Hackers inserted a backdoor into SolarWinds software updates, compromising thousands of organizations. With Zero Trust, continuous monitoring and least privilege access could have mitigated the attack.



Google's Operation Aurora (2009) - "When Google Stopped Trusting Itself"

A cyber-espionage attack led Google to develop **BeyondCorp**, one of the first Zero Trust models, proving perimeter security is insufficient.

Target Data Breach (2013) - "The HVAC Hack That Froze Target"

Hackers exploited a third-party HVAC vendor's access to steal 40 million credit card records. Zero Trust's strict access controls could have prevented lateral movement.

Why ZTA is Essential

Imagine using public Wi-Fi at a café. Without Zero Trust, an attacker could exploit vulnerabilities and access your company's data. With ZTA, each request is independently validated, blocking unauthorized access—even with stolen credentials.

1. Rising Cyber Threats
Cyberattacks are more sophisticated than ever. Zero Trust reduces risks by verifying all activities.

2. The Remote Work Shift
With global remote work, Zero Trust ensures secure access anywhere.

3. Cloud and IoT Expansion
Cloud computing and IoT create more attack points. ZTA enforces security policies across all platforms.

Challenges of Implementing Zero Trust

- **Complexity and Cost** – Organizations must overhaul security, adopt new tech, and train staff.
- **Performance Issues** – Continuous verification can slow systems if not optimized.
- **Resistance to Change** – Frequent authentication may frustrate employees, but security must come first.
- **Legacy Systems** – Older infrastructures may require updates or replacements.

How to Implement Zero Trust

Secure Critical Assets – Protect sensitive data, apps, and devices with strong controls.
Strengthen Identity and Access Management (IAM) – Use MFA,biometrics, and AI-driven risk assessments.
Apply Least Privilege Access – Grant users and devices only necessary access.
Adopt Micro-Segmentation – Isolate networks to contain breaches.
Deploy Continuous Monitoring – Use AI and machine learning to detect threats in real-time.

The Future of Cybersecurity

Cyber threats evolve, and defenses must adapt. Zero Trust isn't optional—it's essential. Whether a large enterprise or an individual, embracing ZTA ensures data security everywhere. Cybersecurity isn't about building higher walls—it's about verifying every request, securing interactions, and staying ahead of attackers. Ready for the future? It starts with Zero Trust.

THE NEW FACE OF CYBERCRIME

- YOGITA (I)

We live in a time when technology, especially artificial intelligence, makes life incredibly easy. Whether it's browsing the internet, doing online shopping, or finishing work in minutes—everything feels just a click away. But this convenience also comes with hidden dangers.

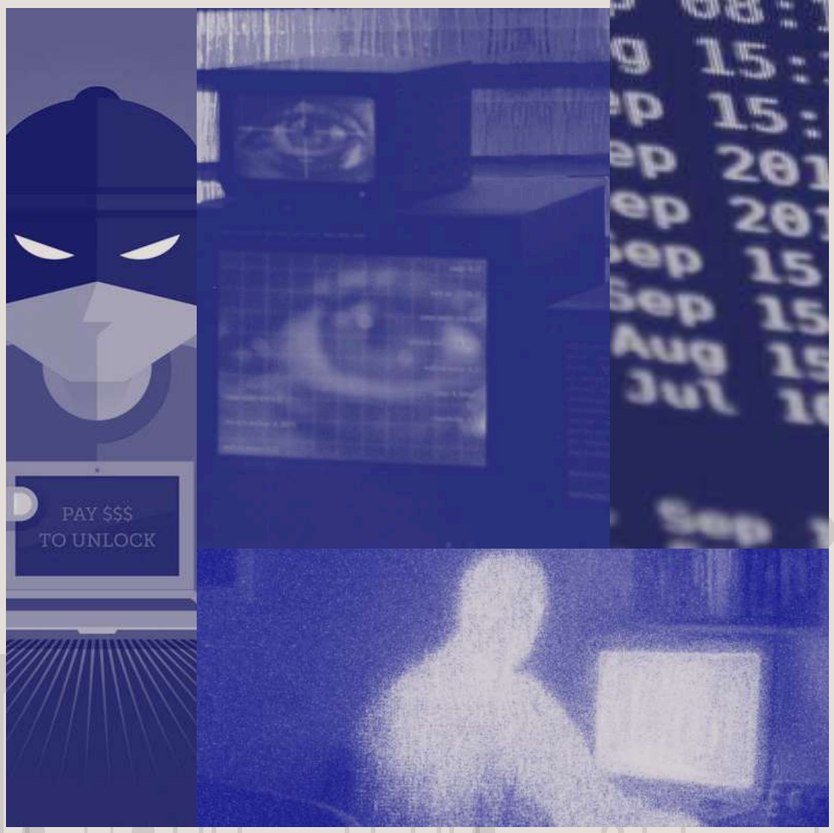
One of the biggest threats in today's digital world is ***ransomware****—a type of malicious software that locks you out of your own files and demands money to get them back. It's a growing problem that can affect anyone: students, working professionals, small businesses, even schools.*

SCAM ALERT

What Exactly Is Ransomware?

It usually starts with something innocent—an email that looks real, a free download, or even a link from social media. Once you click on it, ransomware secretly installs on your device. It then **encrypts your files**, making them impossible to open unless you pay a ransom, usually in cryptocurrency.

But even after paying, there's no promise you'll get your data back. Ransomware spreads quickly and can crash not just your system but also connected devices, backups, and cloud storage. For businesses, this can lead to huge financial losses and damage to their reputation. For individuals, it could mean losing precious memories and important documents forever.



Why It's So Dangerous ?

The damage caused by ransomware goes far beyond losing files. People have lost personal photos, videos, and important data. Companies have faced massive bills for recovery, legal issues, and even had to shut down.

And the worst part? All of it can start with just **one wrong click**.

How to Protect Yourself

The good news is that you can protect yourself by taking a few smart steps:

1. **Back Up Your Data**: Regularly save your files in a secure cloud or an external hard drive that's not always connected. If ransomware hits, you can restore your files without paying anything.
2. **Keep Everything Updated**: Old software often has security gaps. Update your apps and system regularly to stay safe.
3. **Be Careful with Emails and Links**: Most ransomware enters through phishing emails. Don't click on links or download attachments from unknown senders.
4. **Use Strong Passwords**: Simple passwords are easy to hack. Use long, unique passwords and a password manager to keep them safe.
5. **Turn On Multi-Factor Authentication (MFA)**: This adds an extra layer of protection to your accounts Even if someone knows your password, they can't log in without a second code sent to your phone.

Final Thought: Be Smart, Stay Safe

Technology brings us comfort, but also risk. Ransomware is a reminder that every click matters. By staying alert and following some basic safety steps, you can enjoy the perks of technology—without falling into its traps.

So next time you're about to click, pause and think: is it really safe?

BEYOND INCOGNITO

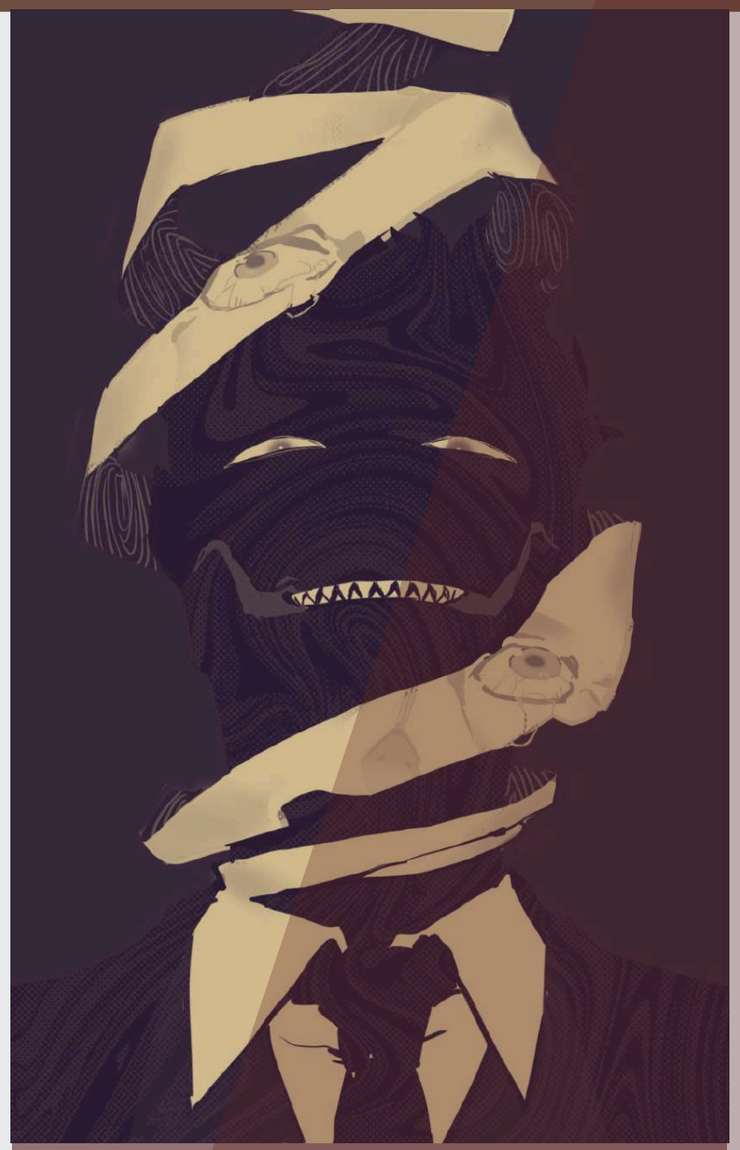
Chronicles Of The Dark Web

VISHU (I)

(Warning: Read at your own risk)

Cybersecurity — a buzzword, right? — protecting data, avoiding threats, staying safe and all. That's it but what if I tell you there's much more..... A whole different side of the internet with which the netizens are unaware. But what is it? Well, that's not the domain I have been asked to write about, but who says we can't shift from learning about our protection to satisfying our curiosity?

Let's switch to Dark Mode !



USE AT YOUR OWN RISK

2.5 M+ Visitors

Tor Access

Introduction to the Dark Web

Welcome to the **Dark Web**, a hidden part of the internet that is not indexed by search engines like Google and cannot be accessed by our regular browsers, no matter what (and yeah, no incognito tabs can help you with it). It operates using encrypted networks such as **Tor (The Onion Router)** and allows users to stay anonymous. No doubt, it plays a crucial role in secure communication for journalists and activists, but it is also a hotspot for cybercriminal activities.

If asked my opinion, I would say the best way to protect ourselves from cybercriminal activities is by understanding these activities in depth — because awareness is the best defense !

Common Cyber Crimes on the Dark Web

1. Digital Black Market

One can imagine the Dark Web as **Amazon**, but of illegal products, drugs, counterfeit passports and hacking tools. Cybercriminals also sell stolen credit card details, hacked social media accounts, and leaked databases containing personal information. This increases identity theft, financial fraud, and corporate espionage.

2. Ransomware-as-a-Service (RaaS)

Ransomware is a malicious virus that locks a person's files and asks for money to unlock them. On the Dark Web, there are **Ransomware-as-a-Service (RaaS)** websites where even people with no computer skills can rent these viruses and use them to attack others.

3. Drug & Weapon Trafficking

Anonymous transactions on the Dark Web make it a hub for **illegal drug sales and firearms trading**. Cryptocurrencies like **Bitcoin and Monero** are used to facilitate transactions without revealing buyers' and sellers' identities (one of the reasons why it is dangerous).

4. Hiring Hitmen & Other Criminal Services

There are many reports of **hitmen-for-hire services** being offered on the Dark Web. It claims to offer professional killers who can be hired to target anyone — for a price. However, many of these are **scams**, where individuals pay large sums of money, only to be cheated by fake assassins.

5. Child Exploitation & Human Trafficking

Imagine spells like Sectumsempra and Crucio getting real in the Muggle world — but in the most horrifying way possible, seems terrible, right? The Dark Web hides some of the most

heartbreaking crimes, where innocent lives are exploited and distributed to the users accessing the web.

Impact of Dark Web Cybercrimes

Dark Web cyber crimes have many consequences that affect individuals, businesses, and even entire countries. People and companies lose billions due to online scams, stolen data, and harmful software like ransomware. Privacy is also at risk, as leaked personal information can lead to identity theft and blackmail. On a larger scale, cybercriminals use the Dark Web to sell weapons and plan attacks, creating serious threats to national security.

As these crimes continue to rise, people are losing trust in digital transactions and online platforms, making the internet a less safe place for everyone.

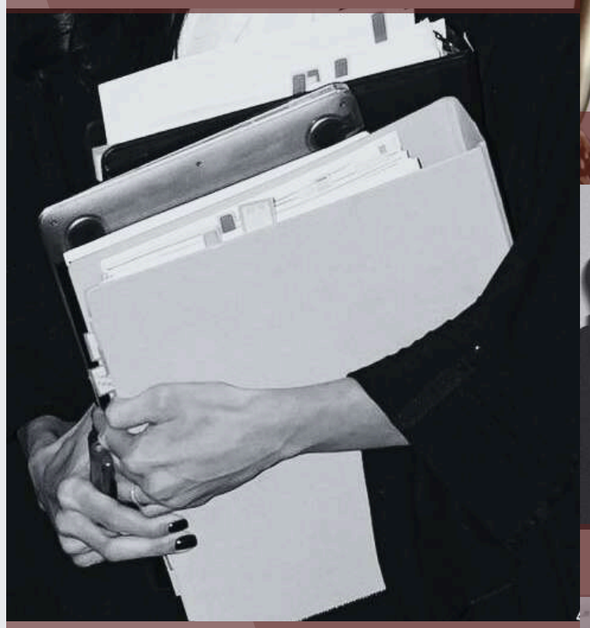
How Law Enforcement Fights Dark Web Crimes

Even though the Dark Web hides identities, law enforcement has still managed to catch major criminals. They do this by secretly joining Dark Web groups, using AI to track cryptocurrency transactions, and working together with global agencies like the FBI, Interpol, and Europol to stop cybercrime networks

Some major Dark Web takedowns include:

- **Silk Road (2013)** – Silk Road was one of the most infamous Dark Web marketplaces. It was a hub for illegal drug transactions. It was shut down by the FBI, and its founder, Ross Ulbricht, was arrested.
- **AlphaBay (2017)** – AlphaBay was another massive Dark Web market. It was seized by authorities, leading to a major crackdown on illegal online trade.

DATA



HUMAN TRAFFICKING

HUMAN TRAFFICKING

DATA

Conclusion

The Dark Web may sound interesting, but it comes with its own dangers. From illegal marketplaces to cybercriminal services, it is a place where stolen data, drugs, weapons, and even human lives are traded. But should we fear it, or should we learn from it?

This raises an important question: How can we protect ourselves from these ever-growing cyber threats? Well, you can find the answers in the later articles of the magazine (as I have already reached the word limit).

(Fun Fact: 10% of the readers' search history may look like "How to download Tor on PC?")

— Anonymous

Wait, turning the light mode back!

FACTS

Cybercrime is a Major Threat

Humans Are the Weakest Link

Ransome every 11 SECONDS

A business falls victim to a ransomware attack every 11 seconds, costing billions globally.

Think before you click

Typing isnt PRIVATE

Using AI and video footage, researchers have developed a way to detect what you're typing just by analyzing your shoulder movements —making it possible to steal passwords without screen access!

AI Hacks in Minutes

Headphones CAN SPY

A malware called Speake(a)r can reprogram the audio jacks on your computer and turn your headphones into a recording device, allowing hackers to spy on you without a mic being plugged in!

Printers got RICKROLLED

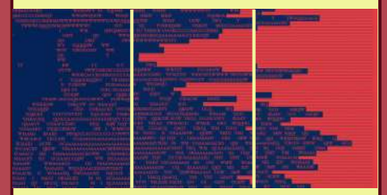
A hacker named Stackoverflowin hacked 150,000+ printers worldwide and made them print Rick Astley's "Never Gonna Give You Up" lyrics. He did it to warn people about insecure printers, but he also Rickrolled the entire world at once!

Dark Web MARKET

Stolen credit card details, login credentials, and personal data are frequently sold on the dark web for as little as $1.

First computer VIRUS

It was created in 1982 and was called *Elk Cloner*. It spread through floppy disks and displayed a playful poem on infected screens.



Fake CHARGING STATIONS

Hackers can create fake USB charging stations in airports or cafes — once you plug in your phone, they can install malware or steal data through a technique called "juice jacking."

Clock's Ticking, Hack's Coming

One hacker, ONE NATION

In 2007, Estonia faced a massive cyberattack, allegedly by Russia. The entire nation's banks, media, and government services were shut down for weeks. This led to NATO creating its first cyber defense unit.

Files in DNA

Researchers have successfully stored and retrieved digital files using synthetic DNA, making biological storage the future of data archiving .

Young hacker, MAJOR BREACH

In 1999, a 15-year-old hacker named Jonathan James infiltrated NASA's systems,

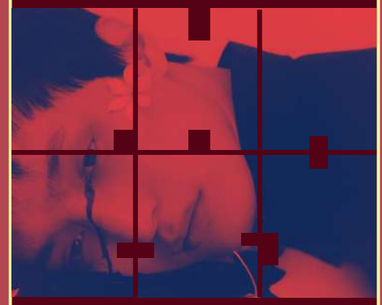
downloading software worth $1.7 million — NASA had to shut down its network for three weeks.

Teenagers Hacked Twitter

Smart BUT SNEAKY

Many smart TVs come with built-in microphones, cameras, and voice recognition features, allowing them to listen to voice commands. However, some manufacturers have been caught secretly recording conversations, tracking viewing habits, and even sending data to third parties without user consent.

Dark Side OF SCIENCE



There are reports of underground human experimentation discussions on the *dark web*, including "People being sold to secretive labs for unethical experiments", "Involuntary surgeries performed on kidnapped individuals". One particularly eerie case involved an alleged "Zombie Drug Experiment", where individuals were forcibly injected with unknown chemicals to observe their mental and physical deterioration.

DDoS = Digital Flood

THE RISE OF DEEPFAKE CYBER THREATS:

ARE WE READY FOR THE ILLUSION?

- Unnati (I)

Imagine getting a video call from your boss, urgently asking you to transfer money for an important business deal. Everything seems normal —their face, voice, and mannerisms are exactly as you know them. But what if I told you that the person on the screen **isn't real?**

No, this isn't the plot of a sci-fi thriller—it's happening right now. Welcome to the **dangerous world of deepfake cyber threats**, where artificial intelligence (AI) is being used to create highly realistic fake videos, audios, and images that can fool even the smartest people.

Once a fun party trick or meme material, deepfake technology is now being misused for fraud, blackmail, and political manipulation And if you think you're too smart to be tricked, well—so did the CEO who lost $35 million to a deepfake scam.

Let's break down how deepfakes work, how criminals are using them, and—most

importantly—how to avoid becoming the next victim of an AI-generated scam.

What Are Deepfakes and How Do They Work?

Deepfakes are created using **"advanced AI technology"** that learns to play real voices, facial expressions, and movements. Think of it like Photoshop on steroids but instead of just editing pictures, it manipulates entire videos and voices to make anyone appear to say or do something they never actually did.

The most common tool used for this is called **"Generative Adversarial Networks (GANs)"** which teaches AI to create ultra-realistic fake media. The more data it has, the more convincing the deepfake becomes. So, yes—those countless selfies and videos you post online? They're basically free training material for AI scammers.

Deepfake Cyber Threats: More Than Just Fake Videos

Most people think deepfakes are just funny celebrity videos or Instagram filters gone wild, but they're now being used for ***"serious cybercrimes"***

1. Financial Fraud & CEO Impersonation

In 2020, a finance employee received a call from his CEO instructing him to transfer $35 million to an urgent business partner. The voice was perfect. The mannerisms were spot on.

What could go wrong?

just one tiny problem—the real CEO was on vacation , The call was a deepfake, and the company lost millions.

This new type of scam is called *"Business Email Compromise 2.0"*, where deepfake audio and video make scams nearly impossible to detect.

2. Identity Theft & Blackmail

Ever posted a selfie video online? Congratulations, you've given scammers the perfect material to create a fake version of you.

Deepfake criminals can take just a few minutes of your footage and generate a convincing fake video of you saying something outrageous.

Imagine waking up to a message:

"Send $10,000 or this video of you robbing a bank goes viral."

Now you're in a panic, even though the closest thing you've ever robbed is your roommate's snacks. This blackmail scam is real and has already targeted high-profile individuals.

3. Fake News & Political Manipulation

In 2018, a deepfake of Barack Obama went viral, showing him saying things he never actually said *"It was just a test to prove how easily deepfakes could be used to "spread false information"*.

Now imagine an election where deepfakes are used to create fake speeches, fake confessions, or even fake crimes. Scary, right?
As deepfake technology improves, it could be used to spread lies, create conflicts, or manipulate public opinion—turning *"fake news"* into something far more dangerous.

4. AI-Powered Phishing Scams

Regular phishing emails: *"Dear Customer, click this link to claim your $1,000 prize!"*
Deepfake phishing scams: A video message from your 'bank manager' personally asking you to verify your account details.

How Can We Detect and Defend Against Deepfakes?

Deepfakes are scary, but you don't have to live in fear. Here's how you can outsmart the AI scammers:

- ***Educate Yourself and Your Team***

Deepfake scams are new, and many people don't know how to spot them, Companies should train employees just like they do for phishing emails. If an urgent video call or voice message seems suspicious, double-check through another method before acting. Your CEO probably isn't asking for a secret money transfer via WhatsApp.

- ***Look for Flaws***

Even though deepfakes are realistic, they still have flaws. Common giveaways include:
- weird eye blinking or unnatural facial movements
- Lips that don't perfectly match speech
- Glitches or distortions in the video
- A voice that sounds slightly robotic or off

If something feels off , trust your instincts.

- ***Use Deepfake Detection Tools***

Tech companies are building AI tools to catch deepfakes before they fool you.

Some useful
ones include:
- Microsoft's Video Authenticator
- Deepware Scanner
- AI-Powered Forensics

- ***Use Multi-Factor Authentication (MFA)***

If a scammer plays your boss's face or voice, they still won't have access to secondary security codes needed to verify their identity.

- ***Push for Stronger Cyber Laws***

Governments are finally catching on to deepfake dangers, but stronger laws are needed to hold scammers accountable.
If you see fake content being spread, report it—because today it's someone else, but tomorrow it could be you.

The Future of Deepfake Cybersecurity: Can We Stay Ahead?

As AI gets smarter, deepfakes will become even harder to detect. We're entering a digital era where we can't trust everything we see or hear. But don't panic—cybersecurity experts are already developing better AI-driven detection tools and security systems to fight back.
Until then, stay skeptical, double-check before you believe, and remember—just because it looks real, doesn't mean it is.
So next time you get an unexpected video message, take a deep breath and ask yourself: ***"Is this real, or just another digital illusion?"***
Stay safe, stay smart, and don't believe everything you see.

THE FUTURE OF CYBERSECURITY

Written by:
Gauri Tiwari (I)

Emerging Threats Solution

What is Cybersecurity ?

In today's fast-moving digital world, technology keeps advancing faster than ever before. But with every advancement comes a new set of threats. As AI, cloud computing, and IoT reshape our lives, cybercriminals, hackers, data breaches, and malicious attacks can compromise personal information, disrupt businesses, and even threaten national security. This is where cybersecurity steps in. It is the shield that protects our digital world, ensuring that our information remains safe, and our systems stay secure.

AI Powered Cyberattacks:

AI is changing the game, hackers use AI to automate attacks, crack passwords, and create realistic phishing scams—fake messages or websites that trick people into revealing personal data. AI can spot security flaws and exploit them before companies notice.

Rise of Quantum Computing Threats:

Quantum computers can process complex calculations at unimaginable speeds. While this is exciting for innovation, it poses a serious cybersecurity threat. Today's encryption methods, which protect banking and government data, could be cracked by a powerful quantum computer.

Expanding IoT Vulnerabilities:

From smart assistants to fitness trackers, IoT devices are everywhere. They've made life more connected than ever, but with convenience comes risk. Each device is a potential entry point for hackers, and many lack strong protections.

Advanced Ransomware Tactics:

Ransomware attacks are evolving fast. Hackers now steal sensitive data before locking it and threaten to leak it if ransoms aren't paid.

Solutions & Innovations in Cybersecurity

AI and Machine Learning in Cyber Defense:

Cybersecurity experts are turning to AI and machine learning. These technologies analyze huge amounts of data in real time, detect suspicious activity, and predict attacks before they happen, making defenses smarter and faster.

The Adoption of Zero Trust Architecture:

Traditional security models aren't enough anymore. Zero Trust Architecture (ZTA) is based on a simple rule: "Never trust, always verify." It treats every access request as a potential threat and requires continuous authentication.

Advancements in Encryption and Quantum-Safe Security:

Modern encryption protects our banking, messages, and transactions. But with quantum computing, even the strongest encryption could soon be broken. To prepare, researchers are creating quantum-safe encryption that can withstand future computing power.

Strengthening IoT Security:

IoT devices often lack built-in protection. Weak passwords, old software, and unsecured networks make IoT devices easy targets for hackers.

Enhancing Cybersecurity Awareness & Training:

Technology alone can't stop cyber threats. Many attacks succeed because people aren't informed. Employees clicking malicious links or using weak passwords can open the door to serious breaches.

What Should We Conclude?

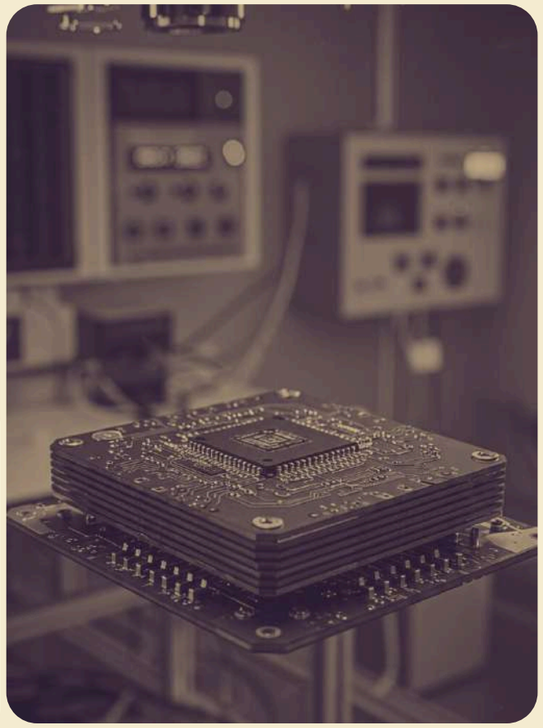
The future of digital security isn't just about technology—it's about awareness and action. As cyber threats grow, no one is entirely safe. Hackers exploit weaknesses through AI, ransomware, and smart device breaches. That's why simple but important steps like strong passwords, two-factor authentication, and cautious online behavior must be taken. Beyond personal safety, businesses and governments must invest in stronger defenses and education. Staying informed and alert is the key to a secure digital future.

THE RISE OF QUANTUM COMPUTING

Written By: TULIP DUGTAL (I)

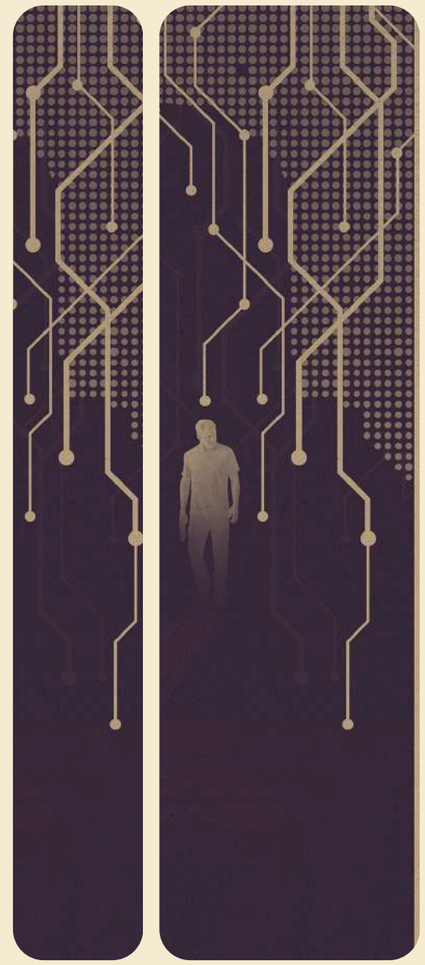
Over the past two decades, computing technology has advanced at an unprecedented pace. However, as traditional computers reach their limits in solving highly complex problems, a new frontier is emerging —quantum computing. This revolutionary technology has the potential to transform industries, from cryptography and artificial intelligence to pharmaceuticals and logistics. Recognizing its immense possibilities, governments and tech giants worldwide are investing billions into its development. Quantum computing is no longer just a theoretical concept; it is gradually becoming a reality.

Unlike classical computers that use bits (0s and 1s) to process information, quantum computers operate with quantum bits (qubits), which leverage two fundamental principles of quantum mechanics: superposition and entanglement. Superposition allows qubits to exist in multiple states simultaneously, enabling quantum computers to process vast amounts of data at once. Entanglement creates strong correlations between qubits, allowing for incredibly fast and efficient computations.



The power of quantum computing lies in its ability to solve problems beyond the reach of classical computers. Some key areas where it is expected to have a significant impact include:

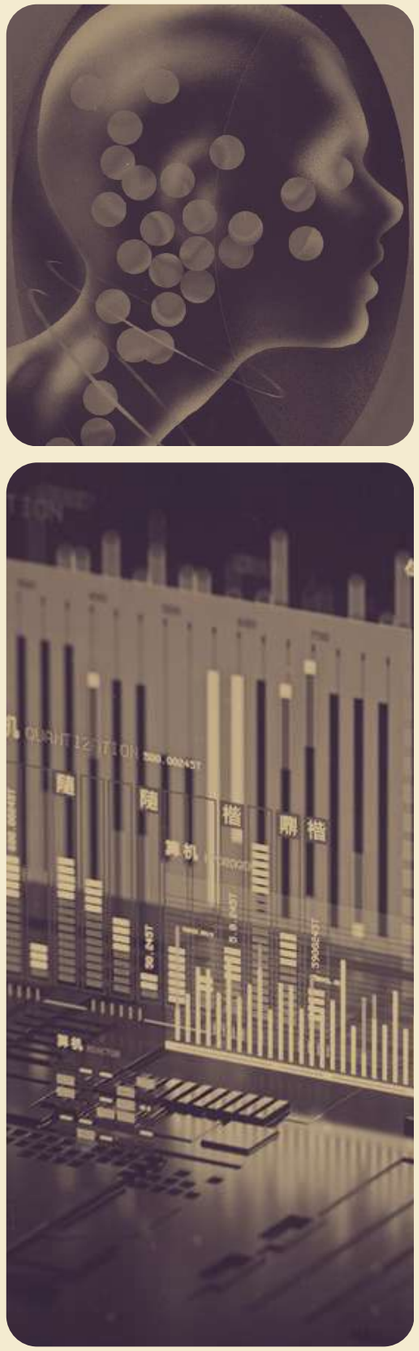
- ***Cryptography*** : Quantum computers could break current encryption methods, necessitating the development of quantum-resistant cryptographic protocols.
- ***Drug Discovery & Material Science*** : Quantum simulations can model molecular interactions with extraordinary accuracy, speeding up drug discovery and the development of new materials.
- ***Optimization Problems*** : Industries like manufacturing, finance, and logistics can use quantum algorithms to optimize supply chains, risk assessments, and routing efficiency.
- ***Artificial Intelligence*** : Quantum computing can enhance machine learning models by processing massive datasets and solving optimization problems at unprecedented speeds.

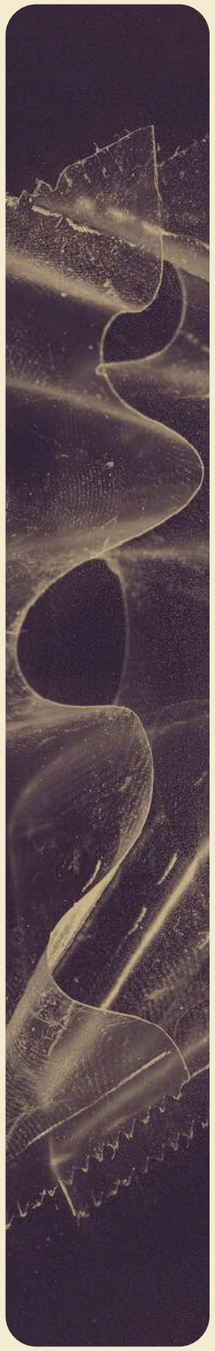


- ***Financial Modelling*** : It improves risk analysis, portfolio optimization, and fraud detection by simulating complex economic scenarios faster than classical systems.
- ***Cybersecurity*** : It poses risks to current encryption but enables unbreakable quantum-safe security through quantum key distribution (QKD).

Several leading technology companies, including Google, IBM, Microsoft, and Intel, are at the forefront of quantum computing research. In 2019, Google's Sycamore processor demonstrated quantum supremacy by performing a computation in minutes that would take classical supercomputers thousands of years. Meanwhile, IBM is making quantum computing more accessible through cloud-based services, allowing researchers and developers to experiment with real quantum processors.

Governments worldwide, including those of the U.S., China, and the European Union, are pouring resources into national quantum initiatives, recognizing the technology's strategic importance. India has also launched the National Quantum Mission, investing in quantum research to stay competitive in this rapidly evolving field.





AS RESEARCH PROGRESSES,

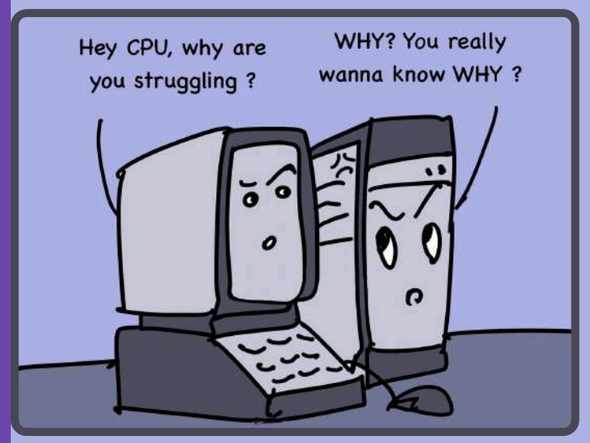
the question is no longer if quantum computing will revolutionize the tech industry, but when. The technology is advancing rapidly, and within the next few decades, we may witness quantum computers solving real-world problems that were previously thought to be impossible.

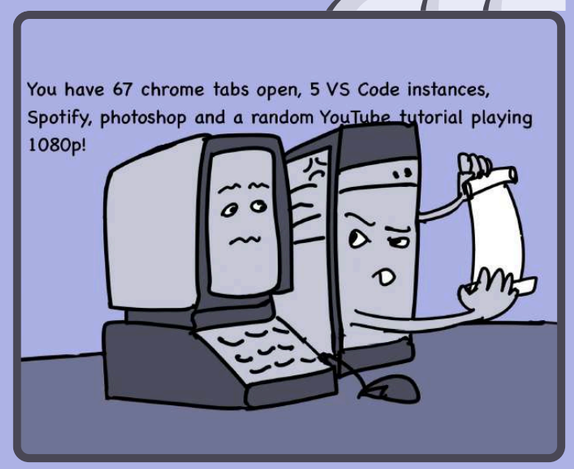
Having attended few seminars on quantum computing, I have observed firsthand how this field is gaining attention among researchers, students, and industries alike. The excitement surrounding it is justified—it has the potential to reshape our world in ways we are only beginning to understand. Whether it's revolutionizing medicine, breaking encryption, or enhancing AI, quantum computing is poised to be a defining technology of the future.

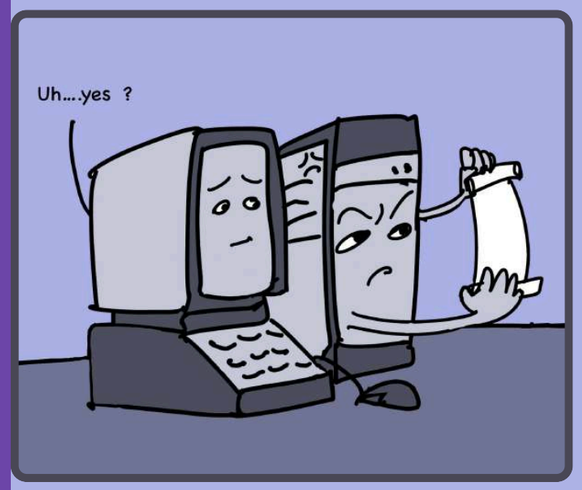
Despite its promise, quantum computing faces several challenges. Qubits are highly unstable and require extremely low temperatures to function properly. Quantum decoherence and error rates remain significant obstacles, but scientists are actively working on solutions like quantum error correction and hybrid quantum-classical computing to improve reliability.

CPU OVERLOAD:

The Digital Breakdown

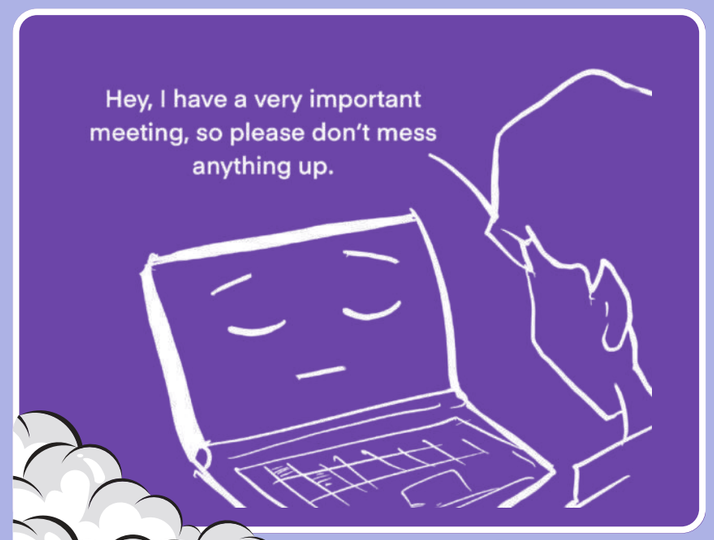


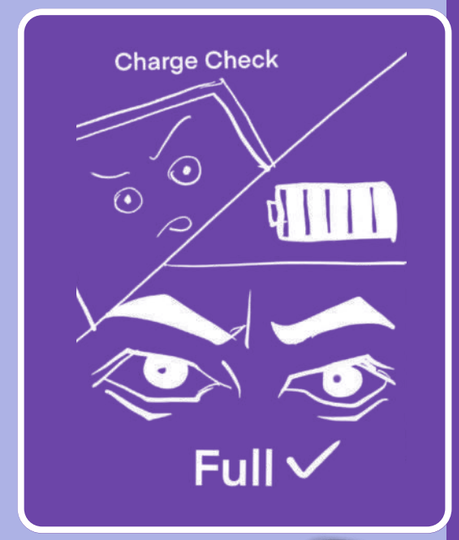


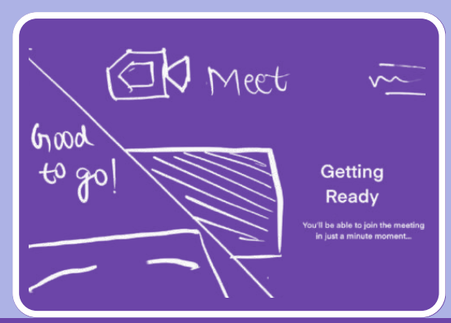


THE ULTIMATE BETRAYAL:

When Your Laptop Has Other Plans







INTERNET OF THINGS & CYBERSECURITY

SHRUTI SINGH (I)

Imagine waking up with half of your work already done.. The smell of fresh coffee from kitchen, your smartwatch monitoring your health in real-time, and your car warns you about potential traffic jams before you leave the house. Sounds like a scene from a futuristic movie, right? Nope, it's the magic of the ***Internet of Things (IoT)***, a technology that's transforming our every day lives. But, with great convenience comes great risk and a crucial question arises: H***ow secure is it?***

You might be wondering, what is this IoT??
In simple terms, ***IoT is the network of every day objects***—like smartwatches, refrigerators, and cars ...that are connected to the internet and can talk to each other. Think of it as giving every day objects a voice. Not literally, of course, but enabling them with small sensors and internet connections through which they talk to each other and the user. These devices collect and share data, helping us make better decisions and create a seamless, interconnected world.
IoT is improving the way we live, work, and interact with technology. But here's the catch: every connected device is a potential doorway for cybercriminals.

How IoT is Changing Our Daily Lives (and the Risks That Come With it)?

We often don't realize how much IoT is already a part of our routine. It's making life easier and more efficient while also opening new doors for cyber threats.
Imagine you're about to reach home from work, and with a tap on your phone, you switch on the lights, and start your favourite playlist ,so everything's perfect when you enter. Smart home devices like Amazon Alexa make daily life easy and more convenient. But what happens if a hacker gains access to your smart lock or security camera?

We're sharing a lot of information with all these connected devices. And that raises some big questions about ***privacy and security***. Who's watching? Who's listening? And how in the hell are we supposed to secure our data?

Balancing the benefits of IoT with cybersecurity measures is essential to ensure safety in this connected world. We need to have open conversations about privacy, security, and ethics. ***Raising user awareness*** about the best security practices like two-factor authentication, complex passwords, etc. Plus, we need to make sure that everyone has access to these technologies, along with the knowledge and tools to protect themselves.

In a nutshell, IoT is a revolution that's already reshaping our world in ways we never imagined. But as we integrate more smart devices into our lives, we must also be aware of the cyber risks that come with them. As these challenges rise, the future of IoT is bright, and its impact will only continue to grow.

So, the next time IoT helps you, take a moment to appreciate the incredible technology working behind the scenes but also make sure it's secure. Because in the world of IoT, convenience should never come at the cost of security.

Siya Chandna (I)

> *"Hackers no longer need to break into your system — they just need to break into your mind."*

HUMAN IS A NEW HARDWARE

Rewiring minds in the age of cybercrime

We've invested years bolstering our digital security — firewalls, antivirus, multi-factor authentication. But what if the weak point isn't your router, but **you**? Yes, you, reading this article on your screen right now. Cybercrime operators have figured out that the most susceptible "hardware" is not a server or a laptop — it's the human brain.

Welcome to the age of humans as new hardware. Now, as technology becomes more intuitive, so do cybercrooks. And their newest tool isn't malicious software or ransomware — it's **you**.

These are the times when firewalls are standing high, passwords have become more robust, and virtual safes are protected — yet cyberthieves have found a new entry point: **us.**

Join us in the new era of cyber deception, where your instincts can be turned against you, your habits picked apart, and your emotions manipulated — without you even realizing it.

Techniques of Deception Used by Cybercriminals

Here's what's new: Modern attackers are becoming experts in psychological manipulation to get past digital defenses:

Emotional Intelligence

Attackers are skillful manipulators of the human mind. They take advantage of:

- **Fear:** "Your account has been hacked."
- **Urgency:** "Confirm now or lose account access."
- **Greed:** "You've won an award!"
- **Curiosity:** "See who's looking for you."

By leveraging your emotions, attackers circumvent reason — and
you click before you think.

Synthetic Identities & Manufactured Realities

With the advent of deepfake technology, AI voice cloning, and synthetic personalities, it's easy to impersonate real individuals these days. Suppose a video call from your "boss" or a voicemail from your "bank," delivering apparently genuine directions — but all fake.

Hyper-Realistic Phishing

Forget the screamingly obvious typo-ridden fake emails. Current phishing attacks closely impersonate trusted sources with unsettling accuracy, incorporating personal data scoured from your online presence — social media, search history, even GPS data. The attacks feel right, sound believable, and extremely realistic.

Vishing: The Voice That Deceives

Voice phishing is taking off quickly. Disguising themselves as a tech support specialist, HR manager, or government official, scammers employ verbal trickery to steal personal information. The voice is convincing, the tale seems pressing — and your data evaporates.

Cybercrime

HOW TO STRENGTHEN HUMAN CYBER DEFENSES

It is time we create our mental firewall. Here's how:

- ***Question Before You Trust***

Wait before you click. Check the source. Be cautious — not paranoid, but vigilant.

- ***Take Your Password Hygiene to the Next Level***

Strong, distinct passwords. Turn on multi-factor authentication. Password managers — don't use birthdays or pet names.

- ***Know, Share, and Thrive***

Cybersecurity is a team sport. Talk about scams with fellow students, parents, and coworkers. Share digital awareness, particularly with those who are least tech-savvy

- ***Click with Caution***

Always double-check links. Hover to preview. Avoid shortened or unusual URLs.

- ***Treat Your Personal Data Like Gold***

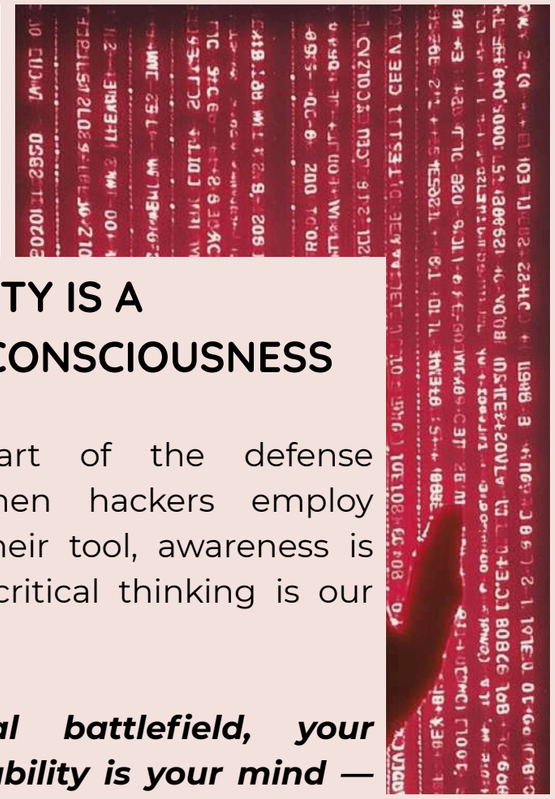
Avoid oversharing on the internet. What you put out there can power targeted assaults — even something as innocuous as a casual photo or remark.

- ***Report Suspicious Behavior Immediately***

Don't wait to report anything that's "off." It might keep it from spreading.

Why Traditional Cybersecurity Isn't Enough Anymore?

You can't put antivirus on human instinct.
Technical defenses are not sufficient to detect socially engineered threats. Firewalls cannot alert you to a plausible lie. Biometric scanners cannot shut out emotional coercion. Protecting systems today amounts to protecting ***human perception*** *— and for that, we need a psychological realignment of what we think of as security.*

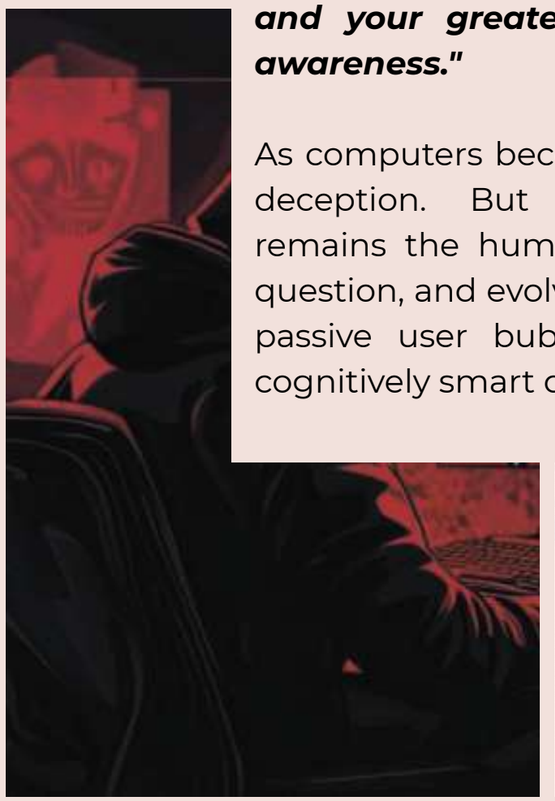


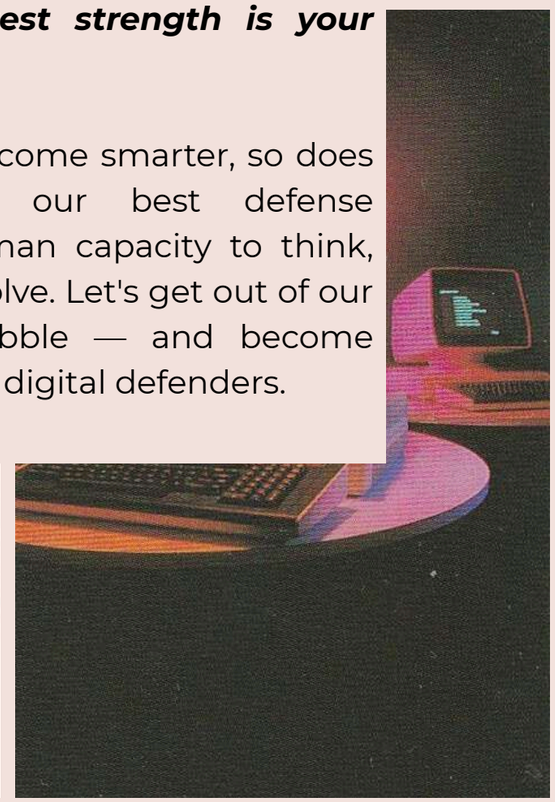
CYBERSECURITY IS A COLLECTIVE CONSCIOUSNESS

We are all part of the defense mechanism. When hackers employ psychology as their tool, awareness is our shield, and critical thinking is our firewall.

"In the digital battlefield, your greatest vulnerability is your mind — and your greatest strength is your awareness."

As computers become smarter, so does deception. But our best defense remains the human capacity to think, question, and evolve. Let's get out of our passive user bubble — and become cognitively smart digital defenders.





THE GREEN TECH REVOLUTION

Written by
-Shreya Sharma (I)

It was one of those slow, lazy mornings. I was coiled up on the settee, scrolling through my phone, half-asleep, when a caption caught my eye: “AI-Powered Solar Farms Are Outperforming Traditional Ones by 20%.” I stopped. AI and solar energy? Together? My curiosity was instantly sparked. I couldn’t help but wonder: Is this the future of green technology, or just another over promised trend?

A quick Google search later, I found a case study about a solar ranch in Spain. Apparently, AI programs were being used to adjust the angle of solar panels in real-time, making the most of energy based on weather and sunlight. It sounded like something from a sci-fi movie—except it wasn’t fiction. It was real, and it was happening right now.

The Green Tech Problem

Let’s be honest: the earth is in trouble. Climate change isn’t some far-off threat anymore—it’s here, and it’s critical.

From wildfires to floods, the signs are everywhere. But in the middle of all this, there’s a bit of hope. Green technology, powered by artificial intelligence, is becoming a big player in the fight for a sustainable future.

But here’s the catch: Can we really trust AI to save the earth? Or are we just swapping one problem for another? AI itself uses a lot of energy. Training a single AI model can produce as much pollution as five cars over their lifetimes. So, how do we fix this?

AI Meets Sustainability: A Perfect Pair?

The answer lies in how we use AI. When done right, AI has the power to change green technology for the better.

Smart Energy Management

Imagine a world where your home’s energy use is optimized in real-time. AI can adjust heating and cooling, and even sync with renewable energy sources. Google has cut energy use in its data centers by up to 40% using AI.

Precision Farming

From drones checking crop health to systems predicting the best planting time, AI is helping farmers use fewer resources and grow more. It’s good for the earth—and for business.

Climate Models and Disaster Prediction

AI can forecast hurricanes and wildfires more accurately, giving people more time to prepare. It’s like a crystal ball for the planet.

Recycling and Waste Management

AI-powered robots can sort trash more efficiently than humans. Companies like AMP Robotics are transforming recycling.

The Dark Side of AI in Green Tech

AI’s energy demand is a concern. But researchers are working on eco-friendly solutions—like energy-efficient models and data centers powered by renewables.

What Can You Do?

You don’t need to be a tech expert to contribute.

Support AI-Driven Green Projects

Choose products that use AI for sustainability.

Push for Responsible AI

Demand transparency and clean energy for AI systems.

Reduce Your Own Carbon Footprint

Small choices—like using public transport—still matter.

The Future is Green (and Smart)

As I closed my laptop that night, I felt hopeful. AI isn’t a magic fix—but it’s a powerful partner. So next time you hear about AI in green tech, don’t brush it off. It might just be the key to saving the earth.

IAM : FOUNDATION OF CYBERSECURITY

Written by-
Prince Thakur (I)

Have you ever wondered how our college, university or organization ensures that only authorized users access their sensitive data?
In today's digital-first world, organizations face the growing challenge of safeguarding their sensitive data and systems from unauthorized access. Whether it's cloud applications, corporate networks, or employee devices, ensuring the right people have access to the right resources is critical. Therefore, to enhance the security of our data and resources, we need something called as the Identity and Access Management (IAM).

WHAT IS IAM ?

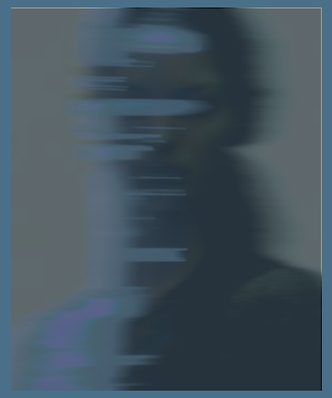
Identity and Access Management (IAM) refers to the processes, policies, and technologies that allow organizations to manage digital identities and control access to critical resources. At its core, IAM ensures that only the right individuals can access certain systems and data, based on their identity and roles within the organization. IAM systems manage how employees, customers, and other users authenticate their identity and what actions they can perform once authenticated. It provides mechanisms for user authentication, authorization, and auditing, making it a foundational aspect of modern cybersecurity.

Key Concepts in IAM

To help you understand IAM better, let's break down some of the key concepts:

- **Identity:** An identity is a digital representation of a person or entity within a system. It typically includes information like usernames, roles, and attributes, such as the person's job title or department. These identities are linked to specific access permissions.
- **Authentication:** Authentication is the first line of defense, through which the identity of a user is confirmed or verified. This can involve multiple methods, such as passwords, security tokens, or biometric data (like fingerprints or face recognition).
- **Authorization:** Once a user's identity is confirmed through authentication, authorization determines what that person can do within the system. For example, a student might be allowed to view his/her marksheets but not edit them. Authorization is often based on roles or specific permissions tied to an individual's identity.
- **Roles and Groups:** Instead of assigning permissions to individual users, IAM systems often use roles or groups to simplify access management. A role is a set of permissions that applies to users with similar job functions. For example, all teachers in the Computer Science Department may have access to the records of Computer Science students but not to the records of Commerce or Arts students.
- **Single Sign-On (SSO):** Single Sign-On allows users to access multiple applications or systems with one set of credentials. It eliminates the need for multiple logins, improving user experience and security by reducing the number of passwords users need to remember.

- **Multi-Factor Authentication (MFA):** MFA enhances the security by requiring users to present two or more verification factors to gain access to a system or resource (e.g., password + a one-time code sent to their phone, just as being used by the Student Portal of our University). It drastically reduces the risk of unauthorized access even if one factor (like a password) is compromised.



- **Access Control:** Access control mechanisms define how users are granted permissions to access resources. This could be based on roles (Role-Based Access Control or RBAC) or user attributes (Attribute-Based Access Control or ABAC).

Some Examples of IAM in Today's World

1. Multi-Factor Authentication (MFA) in Banking

- Banks like HDFC and SBI use IAM to authenticate users logging into their net banking accounts.
- They implement Multi-Factor Authentication (MFA), requiring passwords, OTPs, or biometric authentication (fingerprints, Face ID) for secure access.

2. Single Sign-On (SSO) for Corporate Employees

- Companies like Google, Microsoft, and AWS use IAM systems to allow employees to log in once and access multiple applications (Gmail, Drive, Slack) without needing multiple passwords.

- This increases security while reducing password fatigue.

3. Role-Based Access Control (RBAC) in Government Systems

- Government agencies use IAM to restrict access based on job roles. For example, in India's DigiLocker, only authorized government officials can access certain citizen documents.

4. Cloud IAM for Developers and IT Teams

AWS IAM, Google Cloud IAM, and Azure Active Directory help organizations control access to cloud resources.
Developers and IT admins are assigned permissions based on roles, preventing unauthorized access to sensitive data.

5. IAM in Social Media Platforms

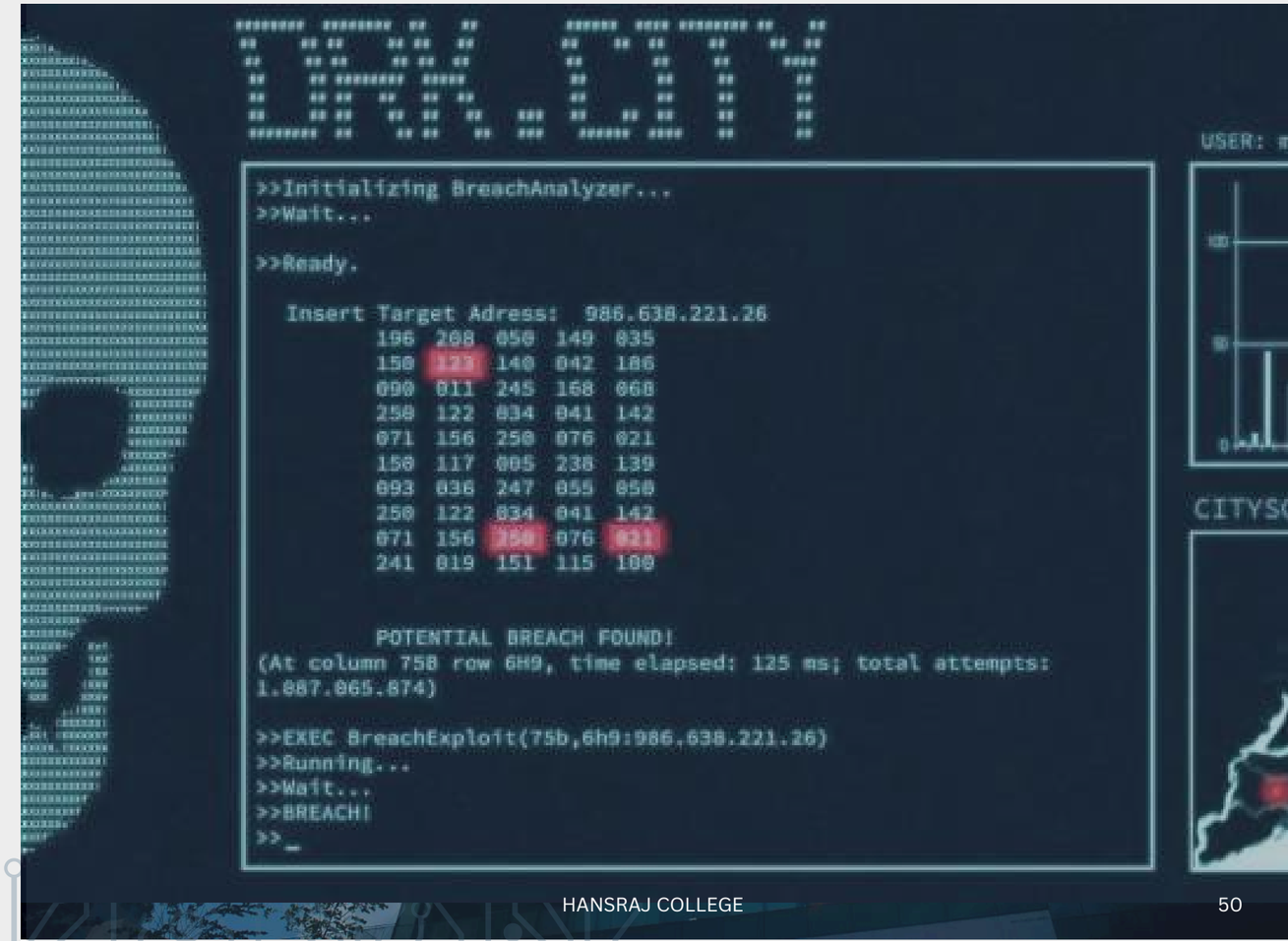
- Facebook, Instagram, and LinkedIn use IAM to manage user logins, detect unauthorized access, and enforce two-step verification when needed.
- They also allow users to control app permissions when logging in via third-party apps.

6. Customer IAM (CIAM) in E-commerce

- Amazon and Flipkart use IAM to manage customer accounts securely, ensuring only verified users can place orders and store payment details.

7. Zero Trust Security in Remote Work

- Many companies use Zero Trust IAM models, ensuring every user and device is authenticated before accessing internal systems, reducing cyberattack risks.



Written By-
MOINAK ROY (I)

AI IN CYBERSECURITY

FRIEND,FOE OR FRENEMY

THE PAST: Simplicity and Chaos Collide

Ah, the good ol' days—when "1234" and "password" were considered high-security measures and firewalls felt more like wooden fences in a hurricane. Cybersecurity was just a cat-and-mouse game between hackers and defenders, glorified on green-and-black terminals in hacker movies. And AI? That was still stuck in a sci-fi daydream, with early machine learning models about as reliable as a fortune cookie predicting a cyberattack.

THE PRESENT

AI Flexes Its Digital Muscles

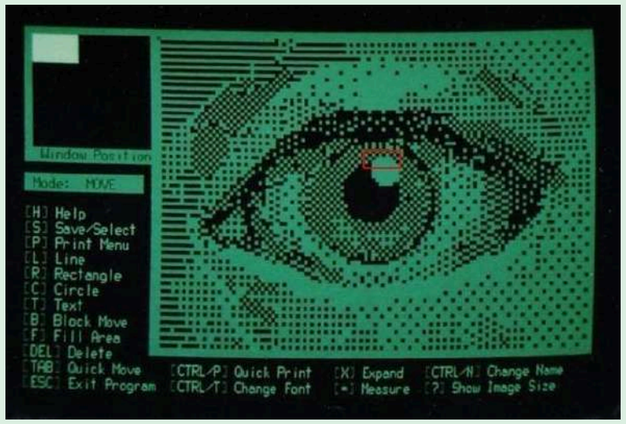
Fast forward to today, AI has moved from the sidelines to center stage, transforming cybersecurity from a reactive game into a proactive battleground.

1. Real-Time Threat Detection

Modern AI tools like Darktrace and CrowdStrike can now analyze massive data streams in real time, sniffing out malicious behavior before it becomes a headline. AI's ability to learn patterns and predict anomalies makes it our digital knight in shining armor. But here's the twist—if AI can detect threats, what stops another AI from becoming the threat?

2. Automated Cyber Response

Today's Security Information and Event Management (SIEM) systems don't wait for IT to intervene. AI now auto-shuts threats in milliseconds Think of it as a digital bouncer—minus the ego, but with zero tolerance. Yes, even the "pretty stranger on Valentine's Day" phishing scam won't make it past these defenses. (Sigh... loneliness wins again.)



3. AI vs. AI – A Cyber Battle Royale

Just as defenders use AI, so do cybercriminals. Adaptive malware powered by AI evolves to bypass security —creating an AI vs. AI warzone. It's like watching two supercomputers play chess, except the board is your personal data and Google search history. (Yes, the aunties still want your exam marks too.)

THE FUTURE

Rise of the Digital Guardians

So what's next? Salvation—or simulation?

1. Hyper-Intelligent Defenses:
Tomorrow's AI may predict and repair security flaws before hackers even know they exist. Imagine systems that heal themselves like digital Wolverine.

2. Cyber Bodyguards:
Future AI agents could negotiate with attackers in real time or launch counterattacks. They may act as your 24/7 digital protector, faster than any human team.

3. AI-Powered Ethical Hacking:
AI won't just defend—it'll attack systems ethically to expose vulnerabilities before the bad guys do. Ethical hacking just got a serious upgrade.

4.Neural Interfaces and Thought Security:

As brain-computer interfaces emerge, AI will need to defend not just your data, but your thoughts. Mind-hacking? It could become the new identity theft.

Caution and Optimism

AI is reshaping cybersecurity with speed and sophistication never seen before. But with great power comes great potential for chaos. Should you worry? Maybe a bit. But in the meantime, use strong passwords, skip shady emails from "Lonely Priya, 10 km away," and keep an eye on your smart fridge—because who knows what it's thinking.

Stay smart. Stay secure. And may your firewalls be ever impenetrable.

STAY ALERT.
STAY SAFE.

CROSS WORD

ACROSS

2. A structure used to store multiple elements in Python (5 letters)
4. The Brain of computer (3 letters)
7. A high-level programming language known for it's simplicity (6 letters)
8. A loop that never ends (8 letters)
9. the main memory of computer (3 letters)
10. The process of finding and fixing errors in a program (9 letters)

DOWN

1. A collection of related web pages (7 letters)
3. A type of error that occurs when a program runs (7 letters)
5. A form of cyber-attack that tricks users into giving sensitive information (8 letters)
6. The language that web browsers understand (4 letters)
9. A network device that forwards data packets (6 letters)

FACULTY MEMBERS

MR. SANJAY BATRA
Associate Professor
M.C.A.

DR. HARMEET KAUR
Associate Professor
M.C.A. | Ph.D.

PROF. BALJEET KAUR
Professor
M.C.A. | Ph.D.

PROF. MANOJ KUMAR
Professor
M.C.A. | Ph.D.

DR. VIDHI KHANDUJA
Assistant Professor
B.Tech | M.E | Ph.D.

MR. SUYASH KUMAR
Assistant Professor
B.Tech | M.Tech | Ph.D.(P)

DR. SUNITA CHAND
Assistant Professor
M.C.A. | M.Phil | M.Tech | Ph.D.

DR. RICHA VERMA
Assistant Professor
M.Sc. | Ph.D.

DR. DHEERAJ KUMAR
Assistant Professor
MSc | Ph.D.

BITWISE TEAM

YASHASVI MITTAL
Student Coordinator

RUPESH KUMAR
Chief Designer

AKSHAJ VERMA
Chief Designer

THEJAS SURESH
Chief Editor

MEHAK NARANG
Chief Editor

KRITIMAN PATHAK
Chief Editor

GAURI TIWARI
Editor

MOINAK ROY
Editor

SHREYA SHARMA
Editor

BITWISE TEAM

SHRUTI SINGH
Editor

TULIP DUGTAL
Editor

UNNATI CHAUDHARY
Editor

YOGITA
Editor

AISHMANYA NISHI
Designer

BHUMIKA DAHIYA
Designer

JANSHEEN
Designer

SIYA CHANDNA
Designer