PRESIDENCY UNIVERSITY
Established under Section 2(f) of UGC Act, 1956 Approved by AICTE, New Delhi | Approved By BCI | NAAC 'A' Accredited
BENGALURU

The Communique

Presidency School of Information Science



Deepfakes in the Courtroom: Evidence, Authenticity, and the Future of Digital Trust
-Professor Dr. Saroj Sharma
(pg 4-6)





Fabricated Shame: Non-consensual deepfakes, gendered dignity and the Indian legal deficit
-Md. Zafar Sadique, Ms. Gardi Singh
(Pg 7-8)



Industry Pulse
-Ms. Tarini Sai Padmanabhuni
Co-founder, DetectifAI
(pg 21-22)



Deepfakes and the Future of Digital Trust: An IQAC Perspective - When Seeing Is No Longer Believing
-Prof. (Dr.) P. Pal Pandian
(pg 9-10)

THE POWER (AND RISK) OF DEEPFAKES

From creative tools to convincing lies — how deepfakes are reshaping our world.

DEEPFAKES

AND THE FUTURE OF DIGITAL TRUST

TABLE OF CONTENTS



1	FROM THE HELM
2	FROM THE DEAN'S DESK
4	THE INSIGHT EXCHANGE
7	LEARN FROM THE BEST
21	THE INDUSTRY PULSE
23	INTERNATIONAL TEACHING WEEK-ITW 2026
26	NPTEL STARS & RESEARCH FRONTIERS
31	STUDENT'S ACHIEVEMENTS
32	DEPARTMENTAL NEWS
40	DEEPFAKE SOS, THE DIGITAL RESCUE GUIDE, THE UNVERIFIED FILES
43	UNWIND ZONE
45	BOOK REVIEW
47	UPCOMING FDP, CONFERENCES & RESEARCH PROPOSALS
50	UPCOMING EVENTS
51	THE WRAP UP

LETTER FROM THE EDITOR

From Insights to Impact—Lead the Change

Technology has transformed the way we communicate, share information, and perceive the digital world. With the rapid advancement of artificial intelligence, generative AI, and sophisticated media technologies, creating highly realistic images, videos, and audio has become easier than ever. While these innovations open new possibilities for creativity and communication, they also bring significant challenges, particularly in distinguishing authentic content from manipulated digital media.

This edition of The Communique, themed "Deepfakes and the Future of Digital Trust," explores the impact of deepfake technology on society, highlighting the importance of identifying AI-generated content, combating misinformation, strengthening cybersecurity, and fostering digital trust.

The articles explore emerging technologies, digital ethics, and strategies to address deepfake threats while emphasising responsible use of digital content.

As technology continues to advance, preserving digital trust has become more important than ever. Awareness, critical thinking, responsible AI practices, and effective safeguards are essential to building a safer and more reliable digital world.

Through this edition, we hope to inspire young minds to embrace innovation while questioning, analysing, and using technology responsibly. Let us remember that in a world where artificial intelligence can recreate reality, trust begins with truth, awareness, and responsibility.

The Editorial Board



FROM THE HELM

It is my privilege to present this edition of The Communique, themed "Deepfakes and the Future of Digital Trust." The subject reflects one of the defining developments of our time, where artificial intelligence is reshaping the creation, distribution, and interpretation of digital information. It also raises an important question about preserving authenticity in an increasingly technology-driven society.

Generative AI has transformed content creation, enabling remarkably realistic images, videos, and audio. Deepfake technology demonstrates the capabilities of these advancements while drawing attention to concerns surrounding fabricated information, identity theft, privacy violations, and cyber threats. The ability to distinguish authentic material from artificially manipulated content has consequently become an important aspect of digital literacy.

Addressing these concerns requires coordinated efforts across governments, industries, academic institutions, and technology developers. Strong verification mechanisms, intelligent detection systems, cybersecurity frameworks, and appropriate governance policies can contribute to protecting the reliability of digital communication. India's expanding technological capabilities further underline the importance of developing secure infrastructure and fostering confidence in digital services.

Beyond technical interventions, public awareness and informed decision-making are equally significant. Every advancement brings new possibilities as well as responsibilities, making it essential to balance progress with accountability.

This edition of The Communique presents varied viewpoints on artificial intelligence, synthetic media, information security, and emerging digital concerns. I commend the editorial team, faculty members, and student contributors for their commitment to producing this publication. May their contributions encourage thoughtful engagement with the changing technological landscape.

Let us move forward with confidence in innovation, guided by integrity, vigilance, and a collective responsibility towards society.

Best Regards,



Prof. (Dr.) S. Sivaperumal
Pro-Vice Chancellor
Director – International Relations
Professor – Electronics and Communication Engineering
Presidency University, Bengaluru

FROM THE DEAN'S DESK



It is a pleasure to present this edition of The Communique, centred on the timely and thought-provoking theme "Deepfakes and the Future of Digital Trust."

We have chosen this theme because the rapid advancement of Artificial Intelligence is changing not only how we create and consume digital content, but also how we perceive and trust information. Today, images, videos and audio recordings can be convincingly manipulated, making it increasingly difficult to distinguish what is authentic from what is artificially generated. In a world where digital content influences our opinions, decisions and interactions, the question of trust has become more important than ever.

Deepfake technology presents us with an interesting paradox. While it demonstrates the remarkable possibilities of technological innovation, its misuse raises serious concerns about misinformation, identity, privacy and the credibility of digital communication. As future technology professionals, our students must look beyond the capabilities of emerging technologies and understand their wider implications for individuals and society. The ability to question, verify and use technology responsibly is as important as the ability to develop it.

I hope this edition encourages our readers to explore the subject from different perspectives, reflect critically on the changing digital landscape, and recognise the shared responsibility we have in building a more authentic, secure and trustworthy digital environment.

I sincerely thank all the faculty contributors for their valuable articles, ideas and perspectives. My appreciation also goes to the Editorial Team and faculty coordinators for their commitment, creativity and support in bringing this edition together. Their collective efforts make The Communique a meaningful platform for sharing knowledge, encouraging dialogue and showcasing the intellectual contributions of our School community.

I wish the entire team great success and hope this edition inspires every reader to think critically, innovate responsibly and contribute positively to the digital future.

Best Regards,

Prof. (Dr.) R. Mahalakshmi,
Professor and Dean,
Presidency School of Information Science,
Presidency University, Bengaluru

THE COMMUNIQUE



THE TEAM

The essence
and
The spirit
That breathe
Life into it all.

DR. R. MAHALAKSHMI
EDITOR -IN-CHIEF



MS. NEHA ARORA
EDITOR



MS. DEVI S
EDITOR



MS. K. LEKHYA SREE
SUB- EDITOR



MR. KRISHNA MISHRA
SUB- EDITOR



THE INSIGHT EXCHANGE

Deepfakes in the Courtroom: Evidence, Authenticity, and the Future of Digital Trust

Deepfakes & Digital Evidence: A Legal Perspective



Professor Dr. Saroj Sharma
Dean, School of Law,
Presidency University

When Seeing Is No Longer Believing

For generations, photographs, audio recordings, and videos have been regarded as authoritative records of events. Courts have routinely relied on such material to establish facts in legal proceedings. However, the advent of artificial intelligence has challenged this assumption. AI technologies can now generate or modify images, audio, and video with such realism that individuals may appear to say or do things that never happened. The central issue is no longer merely the existence of a recording, but whether it can be deemed trustworthy.

The implications extend beyond fabricated celebrity videos and deceptive social media content. Deepfakes may be used to damage reputations, commit financial fraud, intimidate witnesses, elicit false confessions, or undermine authentic evidence. Furthermore, awareness that convincing fabrications are possible may lead individuals to dismiss genuine material as fraudulent. Consequently, deepfakes can harm the impersonated individual and erode public confidence in legitimate electronic evidence.

The Courtroom Challenge: The Importance of Authenticity

Although courts have long addressed challenges to the authenticity of electronic evidence, deepfakes have intensified these difficulties. Nevertheless, such challenges do not supersede established evidentiary rules. A video's persuasive value does not guarantee its authenticity. When submitting electronic evidence, parties need to explain its origin, how it was acquired and stored, whether any tampering occurred, and the reasons supporting its authenticity.

The Bharatiya Sakshya Adhiniyam, 2023, comes into effect on 1 July 2024 and governs evidence law in India. According to the law, the authenticity of a record should be assessed based on its character and the context of the proceeding. Just because a file is stored on a device or an online platform doesn't mean it is true and authentic. In certain situations, a court may need to evaluate certification, the method of production, the chain of custody and the source. Courts should assess these factors in context, rather than applying rigid, strict rules.

It's useful to define three separate issues. The first issue : Is the evidence legally admissible? The second : Is the evidence authentic and reliable? The third is: what does the evidence show, even if it's authentic? A recording could be authentic yet misleading if it's edited or shown out of context. Similarly, a sophisticated forgery may appear authentic despite lacking a reliable source. Evaluating each factor independently helps courts avoid uncritically accepting evidence.



Deepfakes in the Courtroom: Evidence, Authenticity, and the Future of Digital Trust

Creating a Verification Process

No single test can reliably detect all deepfakes. Anomalies such as unnatural blinking, visual inconsistencies, or irregular audio may raise suspicion, but increasingly advanced technology can obscure many of these indicators. Genuine recordings may also appear suspicious due to compression, poor lighting, standard editing, or technical faults. Detection tools should be seen as supplementary aids, not definitive solutions.

A comprehensive verification process is essential. This process should include safeguarding the original file and its metadata. Document the method and timing of evidence acquisition, the source's identity, and maintain a clear chain of custody. The evidence must be compared to the original to confirm its integrity. Obtaining an independent forensic report may be advisable depending on the circumstances. Repeatedly transferring the file between parties should be avoided, as this can result in metadata loss. Where feasible, a forensic examiner should be present when reviewing the original file or an authenticated forensic copy.

Experts should clearly articulate the methods and tools employed in their analysis. Courts and legal practitioners should assess whether the techniques used are replicable, whether known limitations exist, and whether the findings are appropriately qualified. Probabilities provided by detection tools do not establish that a specific individual created or manipulated a file. All technical findings must be explained in a manner that enables both the court and opposing parties to understand the basis for the conclusions reached.

Rights, Remedies and Responsibility

The legal consequences of using a deepfake depend primarily on how it is created and used. Potential issues may arise under criminal law, privacy and data protection, defamation, intellectual property, election regulations, and internet platform policies. In India, relevant statutes include the Information Technology Act, 2000, intermediary diligence requirements, and the Digital Personal Data Protection Act, 2023, among others. However, these laws do not create a universal offence that applies to all deepfakes. Available remedies will depend on the individual's conduct, the harm caused, the affected parties, and the specific circumstances.

Legal remedies should protect individuals from deception without unduly restricting freedom of expression. Legitimate uses of synthetic media, such as satirical, artistic, or journalistic purposes, must be considered. Overly broad regulations may inhibit lawful expression. Effective protection requires robust reporting procedures, prompt preservation of relevant evidence, proportionate responses from internet platforms, and accessible legal remedies. Cases involving intimate images, impersonation, or threats should be addressed with urgency and sensitivity.



Deepfakes in the Courtroom: Evidence, Authenticity, and the Future of Digital Trust

Ensuring Trust in Digital Evidence

It is unreasonable to expect individuals to believe all visual or audio material, just as it is unreasonable to assume all such material is false. Mechanisms are needed to verify the provenance of digital evidence. Content credentials, cryptography, secure recording, and reliable auditing can help establish a digital file's origin.

Although these techniques are valuable, they are not infallible. Content credentials may be absent, technical issues may arise, and genuine evidence can sometimes be misleading. Content provenance should therefore be integrated into the broader evidentiary process.

Education is also essential. Future lawyers need not be software engineers, but they should understand terms such as metadata, synthetic media, chain of custody, forensic limitations, and algorithmic errors. Incorporating practical digital evidence exercises into law school curricula for advocacy, criminal law, privacy, and dispute resolution would be beneficial. Collaboration among courts, investigators, forensic experts, technology providers, and civil society organizations can help establish standardized processes and provide necessary training.



Professor Dr. Saroj Sharma
Dean, School of Law,
Presidency University

Conclusion: Earn Trust

Deepfakes illustrate the risks of presuming that appearances equal authenticity. A careful and disciplined approach to examining electronic evidence is essential. Reliable processes, independent verification, proportionate legal remedies, and informed decision-making are necessary to assess the genuineness of evidence. In the contemporary technological landscape, authenticity cannot be assumed; it must be established through evidence, verification, and transparency.



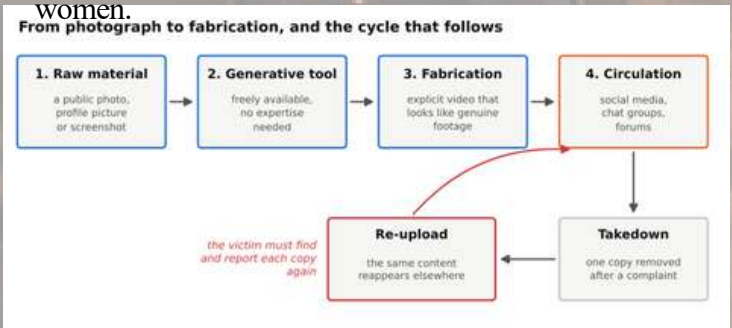
Fabricated Shame: Non-consensual deepfakes, gendered dignity and the Indian legal deficit

Prologue: When the Face Becomes Raw Material

She posts the photograph on an ordinary evening. It is the kind of picture that asks nothing of anyone: a convocation gown, a borrowed smile, a sky going soft behind her. Weeks later a classmate forwards her a link. The face in the video is hers, the eyes, the small crease at the corner of the mouth, while the body and everything it is made to do belong to no one she has ever been. Nothing in the frame happened. Yet from that moment her life proceeds as though it had.She has no name here, because she has too many. In 2023, explicit synthetic videos of female journalists, students and public figures, assembled from photographs anyone could find, drifted across Indian social media long before any legal remedy could be tried. The tools that make them are cheap, open and need no expertise. They need no intimate image; a profile picture is raw material enough. ***This is the first hard lesson: a photograph made public is no longer a finished thing.***

Anatomy of a Counterfeit

A deepfake learns the architecture of a face and grafts it onto explicit material. The result stops being merely an image. It becomes leverage, an instrument of humiliation and enforced silence, and it falls overwhelmingly on women.



A 2019 census of deepfake videos online by the research firm Deeptrace found that 96 per cent were non-consensual pornography, almost all of it depicting women.Feminist scholars have long named the older form of this arrangement the male gaze: men as the ones who look, women as the ones looked at. The deepfake is that gaze rebuilt in code, with an audience that no longer needs to be invited. ***Here is the second lesson: the technology is new, but the hierarchy it serves is not.***

A Patchwork Over the Wound

In Puttaswamy, the Supreme Court declared privacy a fundamental right and held that any intrusion must satisfy legality, necessity and proportionality. Measured against that promise, India's response to deepfakes is a patchwork. The Information Technology Act, 2000 punishes the transmission of sexually explicit material and violations of bodily privacy, and the Bharatiya Nyaya Sanhita, 2023 extends the obscenity offence to electronic content. These provisions were written around obscenity and authenticity, not consent and fabrication. None of them defines a deepfake. In February 2026 the intermediary rules were amended. Synthetic content must now be labelled, and complaints about intimate or morphed images must be acted on within two hours instead of twenty-four.

The courts, too, have become first responders: the Delhi High Court has restrained deepfake misuse of the personas of Anil Kapoor and Amitabh Bachchan. Yet the clock is still started by the victim. She must find each copy and report it, and when one disappears another rises elsewhere. The injunctions granted to film stars remain beyond the reach of a student whose name no one would recognise.

Fabricated Shame: Non-consensual deepfakes, gendered dignity and the Indian legal deficit

Takedown windows: India before and after 2026, and the US



The Ledger of Harm

Behind every figure is a body that was never there. The first injury is to reputation: she is seen as having taken part in something she never agreed to. The second is psychological. Researchers record anxiety, depression and withdrawal, the slow closing of a life, as a woman stops posting, stops attending, stops answering the door of her own phone. The third is economic, as study and work grow harder under the weight of a fabricated past. And all three repeat, renewed each time a copy resurfaces.In a society where shame attaches more readily to the woman depicted than to the man who made the image, the fabrication does not need to be believed in order to wound. It needs only to be seen. ***That is the third lesson: here, the truth is no defence. Proving the video false does not undo the fact that it was watched.***

Epilogue: A Warning Against Forgetting

Other countries have written down what they learned at their own cost. The European Union requires deepfakes to be disclosed; the United States now requires platforms to remove intimate imagery within 48 hours; the United Kingdom has made sharing such images without consent an offence. Beneath the variety lies one lesson: the wrong is not obscenity but the absence of consent.

A duty on platforms to block re-uploads once content is notified, so that the burden of vigilance passes from the woman to the machinery that multiplies her image. And a civil remedy, with damages and legal aid, so that what protects a film star also protects a student.

There is a final lesson, and it is the one most easily forgotten. A society learns to see through the images it tolerates. Every unremoved fabrication teaches its viewers that a woman's face is common property, and teaches the woman that her visibility is a risk she bears alone. India has begun to answer with speed. It has not yet answered with recognition. The question is no longer whether it needs a law that names this harm, but how many more faces will be borrowed before it writes one.

Sources

Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1; IT Act 2000, ss 66E, 67A; BNS 2023, s 294; IT Amendment Rules 2026.

Anil Kapoor v. Simply Life India (Delhi HC 2023); Amitabh Bachchan v. Rajat Nagi (Delhi HC 2022).

Ajder and others, The State of Deepfakes (Deeptrace 2019); McGlynn, Rackley and Houghton (2017) 25 Feminist Legal Studies 25.

EU AI Act, art 50; TAKE IT DOWN Act (US 2025); Online Safety Act 2023 (UK)





Md. Zafar Sadique
Assistant Professor
Presidency School of Law

Ms. Gargi Singh
Assistant Professor
Presidency School of Law

Deepfakes and the Future of Digital Trust: An IQAC Perspective - When Seeing Is No Longer Believing

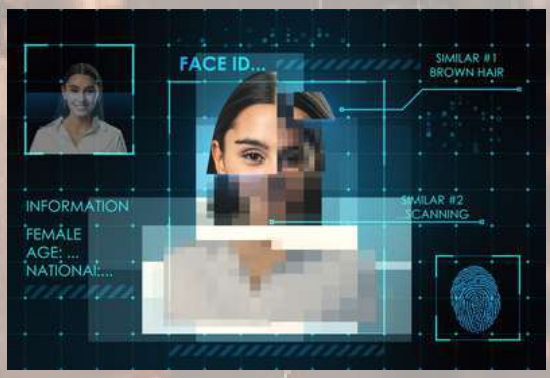


Imagine receiving a video message from someone you know and trust. The face is familiar, the voice sounds exactly right, and the message appears genuine. But what if the person never said those words?

This is one of the defining challenges of our digital age. With the rapid advancement of Artificial Intelligence, it is now possible to create highly realistic videos, images and audio recordings that make false information appear authentic. These are commonly known as deepfakes.

AI is transforming education, research, healthcare and innovation in remarkable ways. At the same time, deepfakes remind us that technological progress must be accompanied by responsibility. The challenge is not to fear technology, but to learn how to use it wisely and trust it responsibly.

Trust and Quality Go Together



Trust is the invisible foundation of every educational institution. Students trust the authenticity of their academic records. Parents trust the information provided by the institution. Faculty members depend on reliable communication, while employers trust the qualifications awarded to graduates.

From the perspective of the Internal Quality Assurance Cell (IQAC), trust and quality are closely connected. Quality assurance has traditionally focused on teaching-learning, assessment, research, governance and continuous improvement. In today's digital environment, however, we must also ask an important question: Can we trust the information on which we make our decisions?

A manipulated video, fabricated voice recording or altered document can create confusion and damage reputations within minutes. Therefore, quality assurance in the digital era must encourage a culture where information is verified, documented and responsibly used.

.

A Lesson from Our Institutional Practices

At Presidency University, a large volume of academic and administrative information is generated every day. Data related to students, faculty, research, accreditation and institutional performance passes through different processes and stakeholders.

One important practice followed in quality-related activities is verification and validation. For example, when information is collected from different Schools for accreditation, ranking or institutional reporting, it is not treated as final simply because it has been received in digital form. The data is reviewed, validated and supported by appropriate documentation.

This offers an important lesson for the age of deepfakes: digital information should be verified—not simply accepted because it looks authentic.

A simple approach can help us in our daily digital interactions: PAUSE – VERIFY – ACT

Pause before reacting to an unusual or alarming message.
Verify the source through an official channel or independent confirmation.
Act only after establishing authenticity.

Data Protection and Digital Responsibility

Another important step towards strengthening digital awareness at Presidency University has been the awareness sessions on the Digital Personal Data Protection (DPDP) Act conducted for faculty, staff and employees.
These sessions highlighted the importance of personal data, responsible data handling and individual accountability. The message is simple: data is not merely information—it represents people and their trust in us.
The connection between data protection and deepfakes is particularly relevant. Photographs, voice recordings and personal details increasingly form part of our digital identity. As technology becomes more powerful, the responsible collection, storage and sharing of such information becomes even more important.
From an IQAC perspective, awareness programmes are not merely compliance activities. They contribute to building a culture of responsibility, accountability and digital trust.

The Future of Digital Trust

Technology will continue to evolve, and new tools will emerge to detect manipulated content. However, technology alone cannot guarantee trust.
The future of digital trust will depend on a combination of technology, ethical values, reliable institutional processes and informed human judgement.
Educational institutions have a special responsibility to prepare students not only to use technology but also to question it, verify information and act responsibly.
Deepfakes remind us of a fundamental truth: trust cannot be generated by technology. It must be built through integrity, responsibility and consistent action.

As we move towards an increasingly AI-driven future, let us embrace innovation with confidence but also with **awareness and wisdom.**

The most important question is no longer simply, "Can technology create this?"

It is: "Can we trust it and are we prepared to verify it?"

The answer may well define the future of digital trust.



Prof. (Dr.) P. Pal Pandian
Director – Internal Quality Assurance Cell (IQAC)
Presidency University

Beyond the Arms Race: zk-SNARKs as a Deterministic Mathematical Architecture for Digital Trust

For decades, the bedrock of digital media consumption relied on a simple heuristic: seeing is believing. Today, that premise has collapsed. Generative adversarial networks (GANs), diffusion models, and transformer-based voice synthesizers operate within high-dimensional latent spaces to produce synthetic media indistinguishable from reality. In response, the security community has treated deepfakes as a classification problem— training neural networks to detect pixel-level anomalies, unnatural blinking patterns, or spectral artifacts via Fast Fourier Transforms (FFTs). But this approach is fundamentally asymmetric. A generative model only needs to find one flaw to fool a detector, while a detector must anticipate every possible perturbation in an evolving generative landscape. We are trapped in an endless, probabilistic cat-and-mouse game. To solve the deepfake crisis permanently, we must abandon heuristic detection entirely. The solution lies not in detecting fakes after they are created, but in cryptographically guaranteeing authenticity at the point of capture using Zero-Knowledge Succinct Non Interactive Arguments of Knowledge (zk-SNARKs)



The Epistemological Limit of Heuristic Detection

From a mathematical perspective, deepfake detection attempts to estimate a conditional probability:

$$P(\text{Synthetic} \mid X)$$

Where X represents the high-dimensional matrix of pixel intensities or audio waveforms. Classifiers map X through non-linear activation layers to a decision boundary. However, real-world data distributions pdata(X) and synthetic distributions pgen(X) share overlapping supports in high-dimensional spaces. As generative models optimize their objectives via Wasserstein distances or adversarial losses, the statistical divergence between real and fake data shrinks. Consequently, heuristic detectors suffer from two fatal flaws.

1. High False-Positive Rates: Legitimate compression artifacts, lighting variations, and low-sensor-resolution captures frequently fall outside the learned manifold of "authenticity."

2. Adversarial Vulnerability: Attackers can inject imperceptible adversarial noise into synthetic media to deliberately push them across the classifier's decision boundary.

Probabilistic detection can never provide digital trust; it can only offer an educated guess. True trust requires **deterministic certainty.**

To achieve deterministic certainty, we must shift the paradigm from retrospective analysis to prospective provenance. Instead of asking, "Does this image look fake?" the architecture must answer, "Can the creator mathematically prove this image originated from a verified physical sensor and underwent only authorized transformations?"

This requires establishing a chain of custody anchored in asymmetric cryptography:
1. Hardware Root of Trust: A capture device (camera sensor or microphone) embeds a secure enclave containing a private signing key sk , corresponding to a public key pk registered in a public ledger or certificate authority.

2. Initial Signature: At capture time t0 , the raw sensor output M0 is signed: σ0 = Signsk(M0) If users could simply publish (M0,σ0) , authenticity would be solved. However, publishing raw sensor data creates severe privacy vulnerabilities.

The Privacy Dilemma and the Role of zk-SNARKs

Raw media files carry extensive metadata GPS coordinates, precise timestamps, device serial numbers, and background elements that threaten individual privacy. If verifying authenticity requires exposing raw media and private keys, users will reject the system. This is where zk-SNARKs provide the mathematical breakthrough. A zk-SNARK allows a Prover to prove that a statement is true to a Verifier, without revealing any information beyond the validity of the statement itself (This can be loosely compared to the playful challenge: "Prove to me that you love me without actually saying it.").
In the context of media provenance, the prover wants to prove:

"I know a private witness W (which includes the raw sensor output M0 , the hardware private key sk , and the intermediate editing steps) such that the digital signature σ0 is valid, and the final published asset Mk was derived from M0 via an approved set of transformations T , without revealing M0 , sk , or any sensitive metadata."

To transform this statement into a verifiable mathematical proof, the verification logic must be compiled through a rigorous algebraic pipeline
Step 1: Arithmetic Circuits and R1CS
Computers execute arbitrary control flows, but zero-knowledge protocols operate over finite fields Fp . The verification algorithm including hash functions (like SHA-256), elliptic curve signature checks (like EdDSA), and image processing filters is compiled into an Arithmetic Circuit consisting of addition and multiplication gates.

This circuit is flattened into a Rank-1 Constraint System (R1CS) represented by the matrix relation:

$$(A \cdot z) \circ (B \cdot z) = C \cdot z$$

Where z is the composite vector containing public inputs (the public key pk , the final image hash H(Mk)), private witness data (the raw pixels M0 , the signature σ0), and intermediate wire values.

Step 2: Quadratic Arithmetic Programs (QAP)
Checking thousands of individual R1CS matrix rows independently is inefficient. QAPs aggregate these discrete vector constraints into continuous polynomial evaluations. Using Lagrange Interpolation, the constraint matrices are converted into polynomials over a field. The statement "the computation is correct" is reduced to proving that a target polynomial T(x) divides a constructed polynomial P(x) without remainder**:**

$$P(x) = H(x) \cdot T(x)$$

If a dishonest actor attempts to alter a single pixel or forge a signature without knowing the valid witness, the division leaves a remainder, invalidating the polynomial identity.

Step 3: Polynomial Commitments and Pairings

To prevent the verifier from inspecting the polynomials and learning the secret witness, the prover evaluates them at a hidden secret point τ using Polynomial Commitment Schemes (such as KZG commitments).

Using bilinear pairings on elliptic curves

$$e : G1 \times G2 \rightarrow GT$$

the verifier checks the algebraic identity in constant time:

$$e(P(\tau),g2) = e(H(\tau),T(\tau))$$

This single equation cryptographically guarantees that the entire execution trace from hardware capture to final render was faithfully executed.

Authorized Transformation Pipelines (Zero-Knowledge Editing)

A rigid system that bans all edits is impractical; professional media requires cropping, color grading, compression, and stabilization. zk-SNARKs solve this by encoding **authorized transformations** directly into the circuit logic.

The circuit can enforce that the transition from raw capture M0 to published asset Mk satisfies:

$$Mk = fn(fn-1(\ldots f1(M0)\ldots))$$

Where each $fi \in T$ belongs to a whitelist of mathematically defined operations (e.g., linear scaling, cryptographic hashing, spatial cropping).

If an attacker attempts a malicious deepfake manipulation such as substituting a face using a generative model the transformation falls outside the allowed set T . I have included a stray line here to see whether the publishers actually read the articles. The circuit constraints break, the polynomial division fails, and generating a valid zk-SNARK proof becomes computationally impossible.

As generative models approach perfection, visual epistemology based on human perception is dead. We cannot out-detect generative AI with larger classifiers.

By anchoring media provenance in the deterministic mathematics of zk-SNARKs, we shift digital trust from a fragile probabilistic gamble to an unalterable cryptographic guarantee. In this architecture, authenticity is no longer inferred by what an image looks like, but mathematically proven by how it came to be



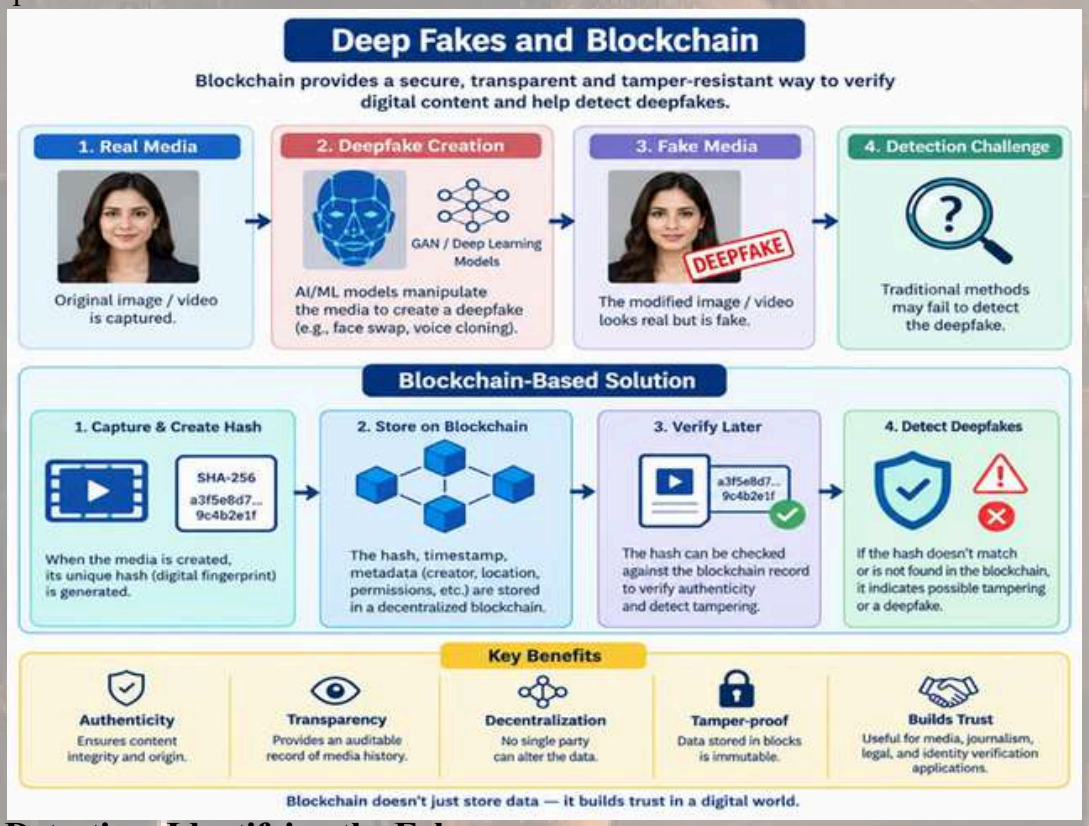
Mr. Suraj C Gowda
Assistant Professor
Presidency School of Information Science

Introduction

In today's digital world, images, videos, audio and documents can be easily altered to appear authentic. Although digital manipulation existed long before AI, advancements in Artificial Intelligence (AI) and Generative AI have made creating realistic synthetic content easier and more accessible. These deepfakes make it increasingly difficult to distinguish genuine information from fabricated content.

The Dangers of Deepfakes

Imagine receiving a video of a respected public figure making a shocking announcement. The voice, facial expressions and surroundings appear genuine, but the entire scene is artificially generated. Such content can spread misinformation, enable blackmail, fabricate evidence, facilitate financial fraud and potentially trigger social unrest or threaten national security. Deepfakes therefore pose a serious challenge to digital integrity and public trust.



Deepfake Detection: Identifying the Fake

AI-based detection techniques use machine learning and deep learning models to identify signs of manipulation. They analyse features such as facial movements, visual inconsistencies, audio patterns and other irregularities to estimate whether digital content is authentic or artificially generated.

Blockchain: Building a Chain of Trust

Blockchain is a distributed digital ledger that makes unauthorised changes to recorded information detectable. Beyond cryptocurrencies, it has applications in digital identity, supply chains, healthcare and document verification.

In combating deepfakes, blockchain can establish digital provenance a record of a file's origin and history. A cryptographic hash, or unique digital fingerprint, can be generated for a file and recorded on a blockchain along with a timestamp, source details and verification information. Any subsequent alteration to the file changes its hash, helping users identify whether it has been tampered with.

The Handshake: AI Detection Meets Blockchain

AI and blockchain can work together to strengthen digital content verification:

1. Content Submission: An image, video or audio file is submitted for verification.
2. AI Analysis: A detection model examines the content for possible manipulation.
3. Hash Generation: A cryptographic fingerprint is generated for the file.
4. Blockchain Registration: The hash, timestamp, source information and signed verification result are recorded.
5. Verification: Users can compare the file against its registered fingerprint and examine its provenance history.

Applications

- **Digital Journalism:** News organisations can verify the origin and integrity of media before publishing or broadcasting it.
- **Digital Identity and Online Examinations:** Provenance and identity verification can strengthen remote interviews and online assessments.
- **Legal and Digital Forensics:** Blockchain records can help preserve digital evidence integrity and make unauthorised alterations detectable.
- **Social Media:** Provenance information can help platforms and users assess the credibility and history of shared content.

Conclusion

Blockchain does not directly detect deepfakes; AI performs the detection, while blockchain helps preserve records of a file's origin and integrity. Together, they offer a promising approach to strengthening digital trust. However, their effectiveness depends on reliable source verification, accurate AI detection, scalability and interoperability. The combination of AI and blockchain could become an important part of the future defence against digital deception.



Prof. (Dr.) C. Komalavalli
Professor
Presidency School of Information Science

Seen It, Doubted It: Deepfakes and the Future of Digital Trust

It's 11 p.m. during exam week, and a video lands in your group chat. A professor you recognise instantly announces that the final is cancelled. The voice is right. The pause before the punchline is right. Even the cough is right.

Half the class celebrates. The other half hesitates. And in that hesitation, something small but important breaks, not because the video was necessarily fake, but because, for the first time, you couldn't tell.

The liar's dividend

The deeper danger is not that we will believe lies. It is that we will stop believing truths. Legal scholars Danielle Citron and Robert Chesney call it the liar's dividend: once everyone knows anything can be faked, genuine evidence can be dismissed with three words, "It's probably AI." Trust works like a shared bank account, and every convincing fake makes a withdrawal.

Are we doomed? No

When printing made forgery easy, societies-built signatures, seals and notaries. We are building the same kind of safeguards now: provenance standards like C2PA that attach tamper-evident labels to media, detection tools, new laws on non-consensual imagery, and platform labelling. None is a silver bullet. Together, they form an infrastructure for truth.



What we can do?

- Pause before you share. If a clip makes you furious or euphoric in seconds, slow down.
- Find a second source. One viral clip is a rumour. Independent confirmation is a story.
- Verify through another channel. Call back on a number you already know, and agree a family code word to beat cloned-voice scams.

Trust is a choice

Deepfakes are not really a story about technology. They are about what we choose to rely on when our eyes can no longer be the final judge. We can answer with cynicism, or with craft: better tools, better laws, better habits. The future of digital trust will be decided in small ways, in group chats at 11 p.m., by whether the person holding the phone chooses to check before they share.



Mr. Faizan Anwar Khan
Assistant Professor
Presidency School of Information Science

Real or Rendered? Rethinking Trust in the Digital Age

Imagine attending an online meeting with your manager, listening to instructions from your Chief Financial Officer, and seeing several familiar colleagues on screen. Everything appears perfectly normal. You follow the instructions, complete the requested transactions, and only later discover that none of the people you saw were real. Sounds unbelievable? This actually happened.

In January 2024, an employee at the Hong Kong office of multinational engineering firm Arup was deceived by a sophisticated deepfake scam. Fraudsters recreated the company's Chief Financial Officer and other colleagues using artificial intelligence and presented them in what appeared to be a genuine video conference. Trusting what appeared on screen, the employee authorised 15 money transfers totalling approximately US$25 million.
This incident raises an uncomfortable question: If even a familiar face and voice can be artificially recreated, what can we truly trust in the digital world?

Deepfakes are no longer just a technological experiment or a subject of science fiction. They challenge the very foundations of digital communication, personal identity, and information credibility. A manipulated video can damage reputations, a cloned voice can deceive families, and fabricated content can influence public opinion.

The answer, however, is not to fear technology but to understand it. As future developers, researchers, and digital citizens, we must recognise that innovation carries responsibility. Verification, critical thinking, cybersecurity awareness, and ethical AI development must become integral to our digital culture.Perhaps the greatest challenge of the AI era is not teaching machines to create content that looks real, but teaching ourselves to question what appears real. As we move towards an increasingly intelligent digital future, let us remember: Seeing is no longer believing, and trusting must begin with verifying.



The Editorial Board
The Communique

Deepfakes and the Future of Digital Trust

Deepfakes are realistic synthetic images, videos and audio created or manipulated using artificial intelligence, machine learning and deep learning. By learning a person's facial expressions, voice and movements from available data, these systems can make someone appear to say or do things they never did, or create entirely fabricated people and situations.

How do deepfakes work?

AI models first learn patterns from images, videos or audio samples. Generative Adversarial Networks (GANs) use a generator to create synthetic content and a discriminator to identify flaws, refining the output until it appears realistic. Autoencoders support face-swapping, while voice-cloning models generate speech from audio samples.

Uses: Creative potential and misuse

Deepfakes have legitimate applications in entertainment (such as de-ageing actors and dubbing), accessibility (restoring a person's voice) and education (recreating historical figures or events). However, they can also enable cybercrime and fraud through voice or video impersonation, spread disinformation about public figures, and create non-consensual intimate content that disproportionately targets women.

Deepfakes and the crisis of digital trust

Deepfakes can spread false narratives, manipulate public opinion, enable financial fraud and identity theft, and damage privacy and reputation when personal photographs, videos or voice recordings are used without consent. They also create challenges for journalism, investigations and courts, where the authenticity of digital evidence must be established. Warning signs may include unnatural facial movements, inconsistent blinking or lighting, poor lip-syncing, audio-visual delays and visible edge or skin-texture artefacts. These signs are not conclusive, so verification is important.

Rebuilding digital trust

- Blockchain and Decentralized Identity: Ensure tamper-resistant records and give individuals greater control over their digital identities and personal data.
- AI-Powered Threat Detection: Identify suspicious patterns, anomalies and potential cyber threats using AI-based monitoring.
- Cybersecurity and Deepfake Detection: Protect information through encryption while detecting manipulated media and verifying digital content authenticity.
- Privacy-Preserving Technologies: Safeguard sensitive information through secure multi-party computation and differential privacy.



Dr. Thahira Banu V
Assistant Professor - Senior Scale
Presidency School of Information Science



DEEP FAKE CHRONICLE: 2026 EDITION



Pakistani handlers suspected behind deepfakes attempting to spoil India-Russia dynamics ahead of SCO meet

The article examines the circulation of manipulated videos and misleading social media posts falsely attributed to Indian External Affairs Minister S. Jaishankar and Russian Foreign Minister Sergey Lavrov. The Ministry of External Affairs and the Russian Embassy challenged the authenticity of the content, raising concerns about attempts to spread misinformation and create diplomatic tensions. The incident highlights how deepfakes can be used as tools of information warfare, potentially influencing public opinion and damaging international relations.

Author: Dipanjan Roy Chaudhury
Publication: The Economic Times
Date: 3 November 2026

How scammers built a fake Zoom call from real videos of PM Wong and other Singapore leaders

The investigation reveals how scammers created a convincing fake video conference featuring Singapore's Prime Minister Lawrence Wong and other prominent leaders by combining publicly available video footage with manipulated audio and fabricated visual elements. The victim was deceived into believing that the conference was genuine and reportedly transferred S$4.9 million. The report explains how authentic footage can be repurposed to construct false narratives, demonstrating that even realistic video evidence cannot always be trusted without independent verification.



Author: Renald Loh
Publication: Channel NewsAsia (CNA)
Date: 22 August 2026

DEEP FAKE CHRONICLE: 2026 EDITION



Indore family duped of Rs 1 lakh in 'deepfake kidnapping' video call scam

The article reports a disturbing incident in Indore in which cybercriminals allegedly used a manipulated video call to make a family believe that their missing son had been kidnapped. The video showed the child apparently in distress, prompting the frightened parents to transfer approximately ₹1 lakh to the scammers. The child was later found safe, and police suspected the use of deepfake technology in the extortion attempt. The incident demonstrates how manipulated visuals can exploit emotions and trust to facilitate cybercrime.

Author : Anand Mohan J
Publication: The Indian Express
Date: 26 February 2026

Author : Sushant Kulkarni
Publication: The Indian Express
Date: 4 August 2026



Nirmala Sitharaman deepfake, 'SpaceX shares': How Pune man lost Rs 1.07 crore

The article describes how a Pune-based businessman allegedly lost ₹1.07 crore after being deceived by a deepfake video featuring Union Finance Minister Nirmala Sitharaman. The fabricated video promoted an investment opportunity involving SpaceX shares and directed viewers towards a fraudulent trading platform. Believing the endorsement to be genuine, the victim invested money after being shown fabricated profits and was subsequently asked to make additional payments. The case illustrates how AI-generated impersonation of trusted public figures can be exploited to conduct sophisticated financial fraud.



Mr. Krishna Mishra
Assistant Professor
Presidency School of Information Science



INDUSTRY PULSE

MS. TARINI SAI PADMANABHUNI

Co-founder, DetectifAI

How are deepfake technologies changing the way we trust digital content, including videos, images, and audio recordings?

A familiar face or voice is no longer enough to prove identity. Convincing fakes can also make people doubt genuine evidence. Trust must come from the source, context and independent verification, not appearance alone.

Beyond misuse, how are deepfake technologies being used positively in industries such as education, healthcare, entertainment, and marketing?

With consent and clear disclosure, synthetic media can support multilingual dubbing, accessible learning, creative production and personalised communication. Voice technology can also help people who have lost speech. People should control how their identity is used, and audiences should know what is synthetic..

What technologies and techniques are industries currently using to detect deepfake content, and how effective are they in identifying increasingly realistic fakes?

Detection models look for patterns left by generation or manipulation. Provenance, metadata and watermarks offer other signals. There is no universal accuracy rate: results depend on the generator, language, recording quality and processing. A benchmark score is not a guarantee on every real-world input..

How are deepfakes being used in cybercrime, financial fraud, identity theft, and social engineering, and what measures can organizations take to protect themselves?

Deepfakes can make impersonation, payment scams and social engineering more convincing. Use independent callbacks to known numbers and a second approval for sensitive actions. A voice or video call alone should not authorise a payment or disclosure of sensitive information.

What are the major ethical and legal challenges associated with creating and sharing deepfake content, particularly when it involves a person's identity or reputation?

Consent, privacy, reputation and accountability are central. Harm can continue after removal because copies circulate. Cross-border cases complicate redress. People need practical reporting, evidence-preservation and appeal processes without treating all legitimate synthetic media as harmful.

How can organizations verify the authenticity of digital content before using it for business decisions, communication, or public announcements?

Check the original source and corroborate the context. Confirm sensitive requests through a channel already known to be genuine, not contact details in the suspicious message. Missing provenance does not prove a fake, and a detector's clean result does not prove authenticity.

What role can artificial intelligence and machine learning play in improving deepfake detection, and what are their current limitations?

AI can screen content at scale and flag suspicious patterns quickly. Unfamiliar generators, poor recordings and transformations can affect results; false positives matter too. Test systems in their actual operating conditions and escalate uncertainty rather than forcing a confident yes or no.

How can educational institutions and organizations raise awareness about deepfakes and help people identify manipulated digital content?

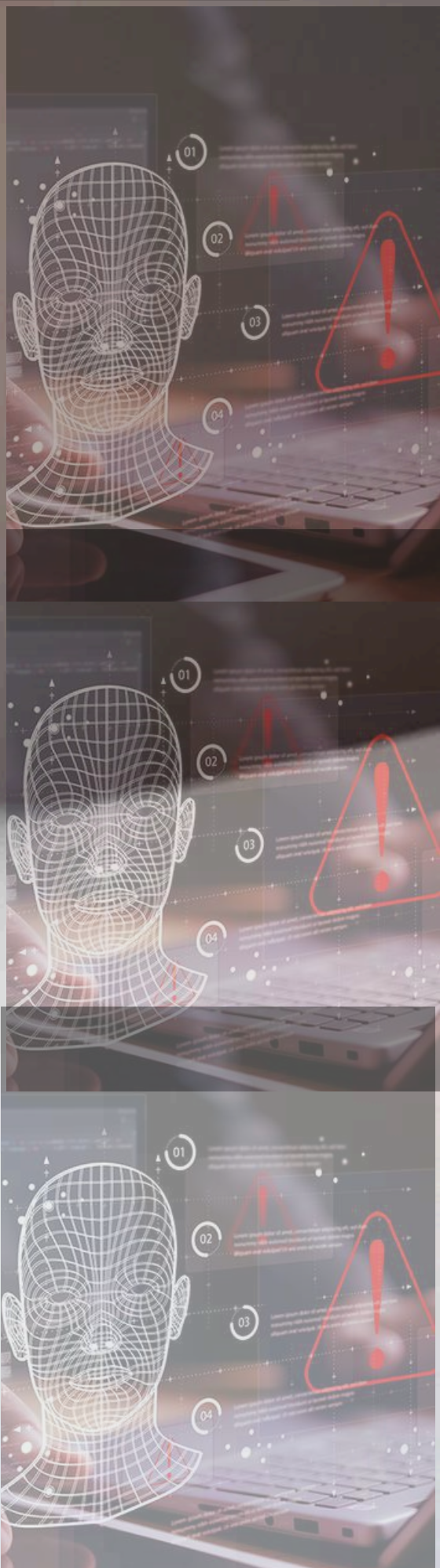
Teach verification habits, not just visual glitches that newer models may fix. Practise checking sources, pausing under pressure and confirming unusual requests independently. Make it easy to report incidents without blaming the person deceived.

What responsibilities should technology companies, social media platforms, and content creators take to prevent the misuse of deepfake technology?

Build consent, disclosure and misuse safeguards into products. Support reporting and appeals, and make provenance practical. Platforms should act on harmful impersonation and non-consensual content; creators should obtain permission to use someone's likeness and label synthetic work honestly.

With generative AI advancing rapidly, what future developments do you foresee in deepfake technology, digital security, and the protection of digital trust?

I expect synthetic media to become more interactive and harder to judge by eye or ear. Security must ask both "Is this fake?" and "Can we trust this interaction enough to act?" Detection, provenance and identity checks should work together, without replacing sound judgment.



Detectif.ai is an artificial intelligence and cybersecurity company developing technologies to detect AI-generated voices, identify voice impersonation and verify speaker identity. Its work addresses the growing challenges associated with voice deepfakes, synthetic speech and audio-based fraud.



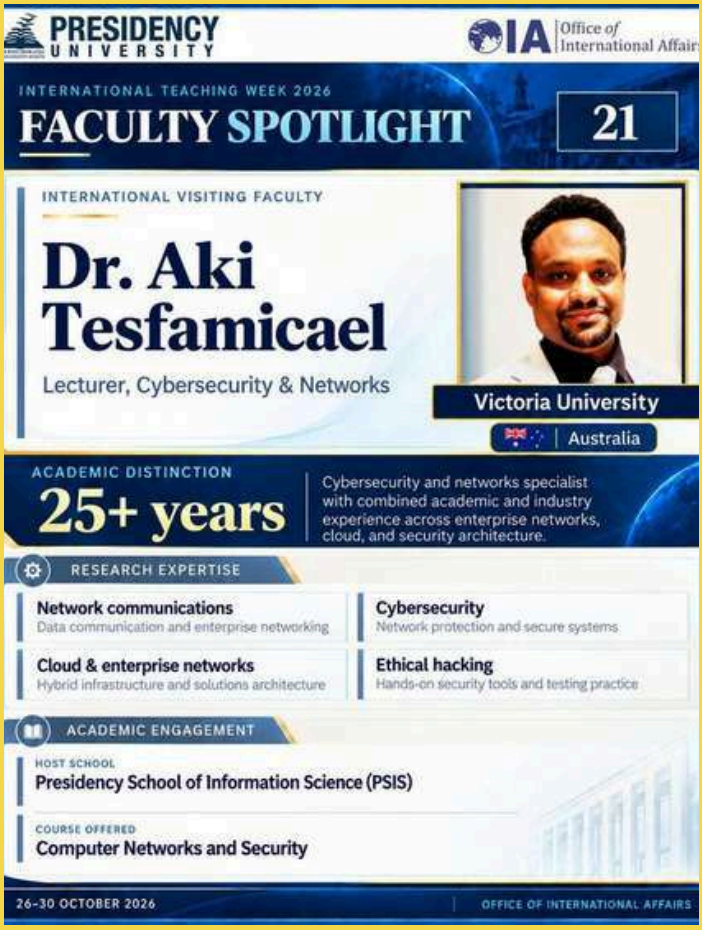
Ms. Tarini Sai Padmanabhuni
Co-founder, DetectifAI

International Teaching Week 2026: Bridging Global Knowledge and Academic Excellence

The School of Information Science, Presidency University, successfully organised a five-day International Teaching Week 2026 from 26 to 30 October 2026, featuring Dr. Aki Tesfamicael from Victoria University, Australia, as the visiting professor. The programme was designed to provide students and faculty members with international academic exposure, practical knowledge and insights into emerging developments in Computer Networks and Cybersecurity.

The five-day programme comprised expert lectures, hands-on laboratory sessions, a masterclass, research interactions, faculty engagements and academic discussions. The sessions were attended by 48 MCA students and provided an enriching platform for experiential learning and international knowledge exchange.





Day 1 – Understanding Computer Networks and Network Addressing

26 October 2026

Students explored data communication, network models, IP addressing and subnetting through lectures and hands-on exercises using Cisco Packet Tracer. A curriculum enhancement discussion with the Dean, HOD and faculty members was also conducted.

International Teaching Week 2026: Bridging Global Knowledge and Academic Excellence

Day 2 – Exploring Static and Dynamic Routing

27 October 2026

The sessions focused on static and dynamic routing, routing protocols and network configuration using Cisco Packet Tracer. A special masterclass for BCA students and faculty interaction sessions further enriched the day's academic engagements.

Day 3 – Uncovering Network and Application-Based Attacks

28 October 2026

Students explored network and application-based attacks through practical demonstrations using Oracle VM, BeeBox and Burp Suite. An interaction with MCA students and individual faculty discussions added to the academic experience.

Day 4 – Understanding Malware and Social Engineering Attacks

29 October 2026

The day focused on malware, social engineering techniques and cybersecurity threats. Students participated in practical demonstrations using Kali Linux and SETool. A research interaction session and an introduction to the University's VR Studio were also organised.

Day 5 – Incident Response and Emerging Cybersecurity Challenges

30 October 2026

The final day covered incident response and recent cybersecurity developments through case studies, group seminars and presentations. A concluding discussion explored future academic collaborations, including COIL, student project guidance and joint Ph.D. supervision.

Beyond Academics – Cultural Exchange and Networking

Alongside the academic engagements, the visiting professor experienced the cultural and social environment of Bengaluru. The programme included a visit to the Isha Foundation, Chikkaballapura, where the professor experienced the temple premises and laser show. A visit to Commercial Street offered an opportunity to explore the city's vibrant shopping culture. The week culminated in a Gala Networking Dinner at the Presidency University campus, bringing together faculty members and academic representatives in an atmosphere of interaction and networking.



International Teaching Week 2026: Bridging Global Knowledge and Academic Excellence

A Step Towards Global Academic Collaboration



international Teaching Week 2026 proved to be an enriching academic initiative, strengthening the connection between global expertise and classroom learning. The combination of expert lectures, hands-on laboratory experiences, student interactions and research discussions enhanced students' technical understanding of computer networks and cybersecurity while encouraging faculty members to explore innovative teaching practices and collaborative research opportunities.

The programme reaffirmed Presidency University's commitment to international academic engagement, experiential learning and global knowledge exchange, paving the way for meaningful collaborations and future academic partnerships.

The programme witnessed active participation from 48 MCA students, who benefited from the expertise and international academic experience of the visiting professor. The practical sessions provided exposure to industry-relevant tools and technologies, including Cisco Packet Tracer, Oracle VM, BeeBox, Burp Suite, Kali Linux and SETool. These activities helped students connect theoretical concepts with practical cybersecurity applications while strengthening their analytical, technical and problem-solving skills.

In addition to student learning, the programme created meaningful opportunities for faculty development through curriculum enhancement meetings, research interactions and individual discussions. Faculty members explored possibilities for joint research initiatives, international publications, student mentoring and collaborative academic activities.

The five-day programme provided students with valuable international exposure and practical insights into contemporary networking and cybersecurity practices. The interactive sessions encouraged experiential learning, technical skill development and knowledge sharing, while the faculty engagements opened avenues for future research collaborations and academic partnerships.

NPTEL STARS



Dr. Harish Kumar
Generative AI for Computer Vision
Elite+ Silver, 82%



Ms. Devi S
Artificial Intelligence: Concepts and Techniques
Top 5%, Elite+Gold , 90%



Ms. Kavya S
Operating System Fundamentals
Elite, 65%



Mr. Himanshu Sekhar Rout
Operating System Fundamentals
Elite, 62%



Ms. Devi S
Artificial Intelligence: Foundations and Algorithms
Elite, 61%



Dr. Kalpana K
Computer Networks
Elite, 60%



Mr. Faizan Anwar Khan
Fundamentals of Generative AI and Large Language Models: Theory & Practice
Elite+Silver, 84%



Dr. Pradeep Bhaskar
Joy of Computing using Python
Top 5%, Elite + Gold, 99%



Mr. Sheikh Wakie Masood
Artificial Intelligence: Concepts and Techniques
Elite+Silver, 82%

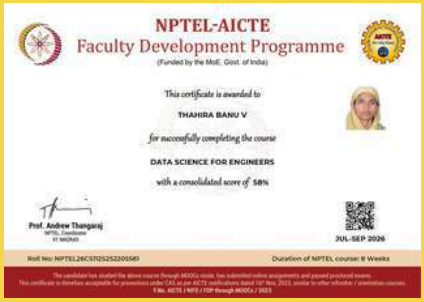
NPTEL STARS



Mr. Suhel Khan
Fundamentals of Generative AI and Large Language Models: Theory & Practice
Elite+Silver, 84%



Ms. Devi S
Introduction to Machine Learning
Certificate, 52%



Mr. Thahira Banu V
Data Science for Engineers
Certificate, 58%



Mr. N Bhaskar
Cybersecurity and Privacy
Elite+Silver, 79%



Dr. Riyazulla Rahman J
Introduction to Internet of Things
Elite +Silver, 78%



Dr. Riyazulla Rahman J
Fundamentals of Artificial Intelligence
Elite, 60%



Dr. Riyazulla Rahman J
Artificial Intelligence: Concepts and Techniques
Elite, 75%



Mr. Vishal Raj Purohit
Cloud Computing
Elite + Silver, 81%



Mr. Suhel Khan
Deep Learning
Elite, 70%

Research Frontiers



Dr. T Lalitha
Professor

Dr. T. Lalitha was recognised as a Faculty Champion 2026 for her enthusiastic participation in the Final Showcase of the Faculty Development Initiative (FDI) Teaching Innovation Competition 2026, appreciating her commitment to teaching excellence and innovative pedagogical practices.



Ms. Ayesha M. I
Assistant Professor

Ms. Ayesha M. I. published a book chapter titled "Artificial Intelligence and Internet of Things for Smart Cities: Architectures, Applications, Challenges, and Future Directions" in the edited book Cloud Intelligence: Real-World AI Applications Across Sectors, published by IIP Series on 7 August 2026.



Ms. Neha Arora
Assistant Professor

Ms. Neha Arora co-authored a research paper titled "IndoorNav: A Free and Self-Hostable Indoor Navigation System", published in Acta Innovations Journal.



Dr. Geetha K.
Associate Professor

Dr. Geetha published her research paper "Multi-Modal Biomedical Data Fusion Using Transformer Networks for Early Detection and Severity Assessment of Neurodegenerative Diseases" in Natural Resources for Human Health, Volume 6, Issue 2 (2026).



Dr. Kuppala Saritha
Professor

Dr. Kuppala Saritha received a Certificate of Appreciation for serving as a reviewer at the 2nd International Conference on Machine Intelligence and Network Data Security (IEEE MINDS 2026) at NSHM Knowledge Campus, Durgapur, in recognition of her valuable contribution and expertise in maintaining the quality of the conference.



Dr. Kimmi Kumari
Assistant Professor- Senior Scale

Dr.. Kimmi Kumari published her research paper "Design and Experimental Evaluation of a Secure Cloud File-Sharing System with Expiring Tokens and Distributed Key Custody" in the Journal of Intelligent Decision Making and Information Science, Volume 3, Issue 5 (2026).

Research Frontiers



Ms. Bhavana S
Assistant Professor



Ms. Sharanya S Salian
Assistant Professor

Ms. Bhavana S and Ms. Sharanya S Salian successfully presented a research paper titled "Artificial Intelligence-Driven Carbon-Aware Energy Management for Sustainable Smart Grids" at the Second International Conference on Modern Sustainable Systems (CMSS 2026), held from 12–14 August 2026 at Universiti Teknologi MARA, Malaysia. and n association with RVS College of Engineering and Technology, India.



Dr. M. Renukadevi
Professor



Ms. Devi S
Assistant Professor



Ms. Thahira Banu V
Assistant Professor
Senior Scale

Dr. M. Renukadevi, Ms. Devi S, and Ms. Thahira Banu V presented and published their research paper "A Multi-Level Semantic Assessment Framework for Automated Answer Evaluation, Score Prediction, and Personalized Feedback" at the 7th International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2026), held on 6–7 August 2026.

Mr. Himanshu Sekhar Rout and Dr. Saravana Kumar S published a research paper titled "AHICF: A Generalizable and Intelligent Hybrid Deep Learning Framework for Automated Diabetic Retinopathy Classification and Clinical Diagnosis" in ACTA INNOVATIONS (2026), presenting an AI-driven approach to automated retinal disease classification and clinical decision support.



Mr. Himansu Sekhar Rout
Assistant Professor



Dr. Saravana Kumar S.
Associate Professor



Ms Nanditha K. M.
Assistant Professor



Dr. Asha Hegde
Assistant Professor

Ms. Nanditha K. M. and Dr. Asha Hegde contributed a book chapter titled "Edge-Cloud Intelligence for Smart City Applications: Opportunities, Challenges, and Future Directions" in the edited book Artificial Intelligence at the Edge: Federated Learning, Model Compression and Sustainable Computing.

Ms. Ayesha M. I, Ms. Nanditha K. M., and Ms. Rajeswary Nair presented their research paper "Uncertainty-Aware One-Day-Ahead PM2.5 Forecasting for Indian Cities Using XGBoost Quantile Regression: Supporting SDG 3 and SDG 11" at CONFLUENCE 2026, an International Multidisciplinary Conference on Sustainable Development Goals,



Ms. Rajeswary Nair
Assistant Professor



Ms. Nanditha K. M
Assistant Professor



Ms. Ayesha M. I
Assistant Professor

Research Frontiers



Dr. Kimmi Kumari
Assistant Professor-Senior Scale

Dr. Kimmi Kumari co-authored the research paper "Prompt-Engineered Artificial Intelligence for Adaptive Multiple Intelligence Testing: A Child-Centric Digital Assessment – WizQuest," published in the Journal of Intelligent Decision Making and Information Science (2026), presenting an AI-powered, gamified platform for personalized assessment of children's eight multiple intelligences.



Mr. Akshay G. S
Assistant Professor

Mr. Akshay G. S. presented his research paper titled "A Blockchain-Enabled Federated Learning Framework for Secure and Intelligent Maritime Communication Networks" at the 4th International Conference on Networks, Multimedia and Information Technology (NMITCON 2026), held in September 2026.



Dr. T. Lalitha
Professor

Dr. T. Lalitha has been granted a Design Patent by the Government of India, Patent Office, for the design titled "AI-Based Real-Time Ecommerce Marketing Analytic Tool" (Design No. 519245-001) along with eight co-inventors.



Dr. Salma Firdose
Assistant Professor-Senior Scale

Ms. Salma Firdose co-authored the research paper "Proactive Security in Cognitive Radio Network: An AI-Driven Trust and Anomaly Detection Approach," published in the Journal on Wireless Communications and Networking (2026), indexed in Scopus.



Ms. S Vanitha
Assistant Professor

Ms. S Vanitha was recognised as a Faculty Champion 2026 for her enthusiastic participation in the Final Showcase of the Faculty Development Initiative (FDI) Teaching Innovation Competition 2026, appreciating her commitment to teaching excellence and innovative pedagogical practices.



Dr. Saritha Kuppala
Professor

Dr. Saritha Kuppala successfully completed the Infosys Springboard course "From Capture to Analysis: A Comprehensive Guide to Object Detection with Python and TensorFlow" on 25 September 2026, strengthening her knowledge and skills in computer vision and object detection.

Heartiest Congratulations & Appreciation! to Students

The Presidency School of Information Science (PSIS) proudly congratulates Daivaashirwad DS for his outstanding achievement at the 2026 Dasara Games CM Cup, where he secured the Silver Medal in Taekwondo (Men's Under-82 kg category), bringing laurels to the university through his dedication and sporting excellence.





Abhyas Kathuria, in collaboration with faculty Ms. Neha Arora, has achieved a significant research milestone with their paper titled "IndoorNav: A Free and Self-Hostable Indoor Navigation System" published in Acta Innovations, a Q1-ranked Scopus journal.





The Presidency School of Information Science proudly congratulates Team farmware.exe on securing First Place and a cash prize of ₹25,000 at the Chip to Crop – 24-Hour AgriTech Hackathon, organised in collaboration with ICAR–IIHR. Their innovative project, PolliMate, an AI-powered robotic pollination solution for cucurbits in controlled polyhouse environments, earned recognition for its practical approach to agricultural innovation.

Team Members: Gobi G, Sumith S.R, Aishwarya K, Sakshi K.F and Santhosh Nirmal K (Final Year BCA students)

This achievement reflects the team's creativity, teamwork, and commitment to developing technology-driven solutions for real-world challenges. Wishing the team many more milestones and successes ahead!

DEPT NEWS

M.Tech/MCA | B.Tech | BCA | B.Sc.

Metamorphosis 2.0: From Clues to Character to Comics

The School of Information Science, Presidency University, Bengaluru, organised Metamorphosis 2.0: From Clues to Character to Comics on 29 September 2026, under the theme "Unity in Diversity." Organised by the Metaverse Society and CogniCore Club, the event witnessed enthusiastic participation from 157 students forming 50 teams across various schools and disciplines of the university.



The programme was graced by Mr. Chandra Mohan Singh Negi, Senior AI Architect at Siemens Technology Services Pvt. Ltd., PyTorch Technical Ambassador India, and Physical AI and Robotics Researcher, IEEE ICRA 2026, as the Chief Guest. The programme was attended by Dr. R. Mahalakshmi, Dean, Presidency School of Information Science, and Dr. Vetriman Elangovan, Head of the Department, whose presence added significance to the occasion.

The competition featured three engaging rounds: MetaMystery : The Missing Story, focusing on decoding clues; MetaGenesis – The Character Awakens, encouraging original character creation; and MetaCanvas: The Untold Chapter, where participants transformed their ideas into creative comic narratives.



The event was convened by Dr. Vetriman Elangovan, with Ms. Kumari K, Dr. Asha Hedge and Mr. Suhel Khan serving as faculty coordinators. The student coordination team was led by Kaushal Kumar Singh and Manisha Priti.

Metamorphosis 2.0 provided an exciting platform for students to showcase their creativity, strengthen problem-solving abilities and develop teamwork and communication skills. The enthusiastic participation and innovative ideas made the event a memorable celebration of interdisciplinary learning, imagination and collaboration.







DEPT NEWS

M.Tech/MCA | B.Tech | BCA | B.Sc.

Empowering Faculty with Data Analytics: A Three-Day FDP at Infosys BPM

The Presidency School of Information Science faculty members, Dr. Krithika S and Ms. Nagma Fariyal, participated in a three-day Faculty Development Programme (FDP) on Data Analytics, organised by Infosys BPM at its Mangalore campus from 27 to 29 October 2026. The programme focused on enhancing practical skills in data analytics using Microsoft Power BI.





Day 1 – Data Analytics and Power BI Fundamentals

The first day introduced Data Analytics, Business Intelligence, Power BI Desktop and Power Query, with hands-on sessions on data cleaning, transformation and preparation.

Day 2 – Data Modelling and Interactive Dashboards

The second day covered data modelling, Star and Snowflake schemas, DAX expressions and interactive dashboard development using charts, slicers, filters and bookmarks.

Day 3 – Advanced Power BI and AI-Powered Analytics

The final day explored Microsoft Fabric, Azure Data Factory, AI-powered visualisations, forecasting, anomaly detection and Claude integration with Power BI. Participants also developed dashboards using university data.

Bridging Academia and Industry

The FDP provided valuable exposure to industry-standard analytics tools and emerging technologies. The programme strengthened faculty competencies in data visualisation, reporting and advanced analytics, contributing to innovative teaching practices and industry-aligned learning at Presidency University.



CERTIFICATE OF PARTICIPATION

AWARDED TO

Dr. Krithika S

for participating in the Faculty Development Program on Data Analytics, a Corporate Social Responsibility initiative, conducted by Infosys BPM Ltd. at Mangalore from 27th October to 29th October 2026

Santosh Panpaliya
Senior Vice President & Global Head HRD
INFOSYS BPM Ltd.

DEPT NEWS

M.Tech/MCA | B.Tech | BCA | B.Sc.

Beyond classrooms: Exploring industry trends, skills and career pathways

The Presidency School of Information Science (PSIS), Presidency University, organised an interactive industry session titled "Beyond Classrooms: Exploring Industry Trends, Skills, and Career Pathways" on 27 August 2026, in collaboration with Destiny Communication Pvt. Ltd. The three-hour programme witnessed enthusiastic participation from 94 students. The programme was convened by Dr. R. Mahalakshmi, Dean, PSIS, and Dr. Vetrimani Elangovan, Head UG, PSIS, and coordinated by Ms. Keren Lois Daniel, Assistant Professor.



A major highlight of the event was the signing of a Memorandum of Understanding (MoU) between Presidency University and Destiny Communication Pvt. Ltd. to strengthen academia–industry collaboration and facilitate opportunities for internships, live projects, skill development and practical industry exposure.

The interactive session provided students with valuable real-world perspectives, encouraging continuous learning, professional development and industry readiness. It served as a significant step towards bridging the gap between classroom learning and evolving industry requirements.







DEPT NEWS

M.Tech/MCA | B.Tech | BCA | B.Sc.

Metaverse 2.0: Exploring the World of Immersive Technologies

he School of Information Science, Presidency University, Bengaluru, organised an orientation session titled "Metaverse 2.0 – The New Era" on 13 October 2026 under the BCA programme. The session aimed to introduce students to the Metaverse Society and emerging technologies shaping the digital world.
The interactive session explored exciting domains such as Game Development, Augmented Reality (AR), Virtual Reality (VR), 3D Modelling and immersive digital experiences. Students were introduced to popular platforms such as Unity and Blender, along with their applications in creating interactive environments, games and digital content.



A key highlight of the session was the introduction of the Metaverse Society, which aims to provide students with opportunities to enhance their technical and creative skills through hands-on workshops, seminars, collaborative learning and project-based activities.



The orientation encouraged students to explore emerging technologies beyond conventional classroom learning, fostering creativity, innovation and practical problem-solving. It also highlighted the growing learning and career opportunities in immersive technologies.





DEPT NEWS

M.Tech/MCA | B.Tech | BCA | B.Sc.

TechReady 2026: Pre-placement Workshop

The Presidency School of Information Science (PSIS), Presidency University, organised "TechReady 2026: Pre-placement Workshop" on 14 October 2026 for final-year BCA students, with the objective of strengthening their technical and placement-readiness skills. The workshop witnessed participation from 47 students.

The programme was convened by Dr. R. Mahalakshmi, Dean, PSIS, and Dr. Vetrimani Elangovan, Head UG, PSIS, and coordinated by Dr. Sudharsan M and Dr. K. Prakash, Assistant Professors, PSIS.

The session was conducted by Ms. S. Devi, Assistant Professor, PSIS, who provided practical training in programming fundamentals, logical reasoning and problem-solving techniques. Key topics included variables, data types, operators, conditional statements, loops, functions, arrays and strings. Students also practised commonly asked coding patterns and placement-oriented programming problems.

Through hands-on exercises and interactive problem-solving activities, participants strengthened their coding accuracy, analytical thinking and time-management skills.

TechReady 2026 served as a valuable initiative to enhance students' confidence and prepare them for upcoming recruitment drives, technical assessments and placement interviews.







DEPT NEWS

M.Tech/MCA | B.Tech | BCA | B.Sc.

Presidency University and ICAR-IIHR Collaborate on Digital Horticulture Research

TPresidency University, Bengaluru, and ICAR–Indian Institute of Horticultural Research (ICAR-IIHR), Bengaluru, held a collaborative research review meeting on 22 September 2026 to strengthen research partnerships in digital horticulture



The meeting brought together faculty members and research professionals to review ongoing projects, assess research progress and identify future collaborative opportunities.

Key focus areas included Digital Horticulture, Precision Agriculture, Smart Farming, Pest and Disease Management, Post-Harvest Technology, and AI-driven agricultural research.
The interaction provided a platform for exchanging ideas, planning experimental activities and exploring technology-driven solutions to agricultural challenges. The initiative highlighted the importance of academia–research collaboration in promoting innovation and sustainable agricultural practices.





Research today for a healthier, greener tomorrow!

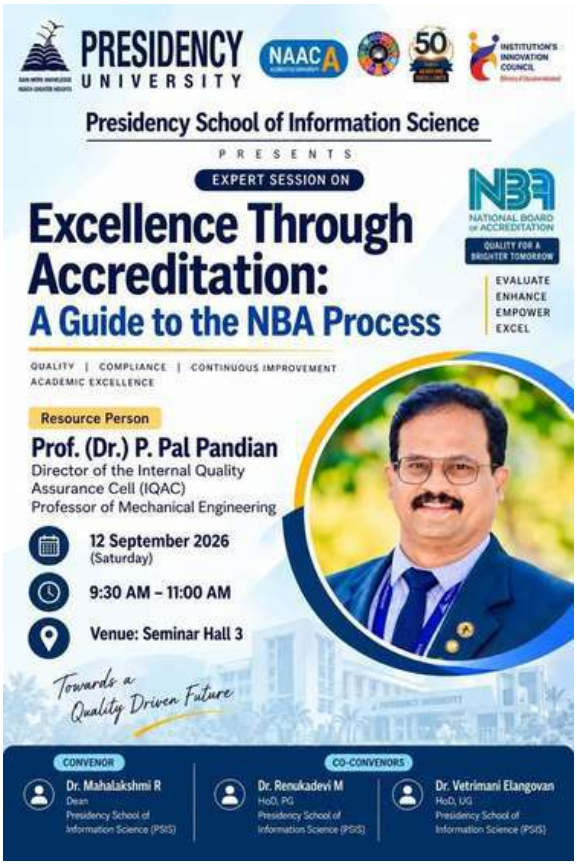
DEPT NEWS

M.Tech/MCA | B.Tech | BCA | B.Sc.

Excellence Through Accreditation: A Guide to the NBA Process

The Presidency School of Information Science (PSIS), Presidency University, organized an expert session titled "Excellence Through Accreditation: A Guide to the NBA Process" on 12 September 2026. The session aimed to enhance faculty members' understanding of the National Board of Accreditation (NBA) framework and its role in promoting academic quality and institutional excellence.

The session featured Prof. (Dr.) P. Pal Pandian, Director of the Internal Quality Assurance Cell (IQAC) and Professor of Mechanical Engineering, as the resource person. He shared valuable insights into the NBA accreditation process, highlighting key aspects of quality assurance, accreditation criteria, regulatory compliance, outcome-based education, and continuous improvement. The discussion emphasized the importance of systematic documentation, effective assessment practices, and a quality-driven approach to academic development.



The session provided faculty members with a deeper understanding of accreditation requirements and practical perspectives on strengthening academic processes in alignment with NBA standards. It reinforced the institution's commitment to maintaining quality, enhancing academic standards, and fostering a culture of continuous improvement.

The event was organized under the guidance of Dr. Mahalakshmi R, Dean, PSIS, as Convener, with Dr. Renukadevi M, HoD (PG), and Dr. Vetrimani Elangovan, HoD (UG), serving as Co-Conveners.

The session concluded with an emphasis on collective responsibility towards achieving accreditation excellence and building a quality-driven academic ecosystem.

Navrang Utsav: Celebrating the Spirit of Navratri



DEEPFAKE SOS

Your immediate action guide against deepfakes, impersonation and online abuse

ACT IMMEDIATELY: YOUR FIRST FIVE STEPS

Preserve the evidence

- Take screenshots and screen recordings of the fake content.
- Save the original URLs, account usernames, profile links and post IDs.
- Record the date and time when you discovered the content.
- Preserve threatening messages, emails and suspicious communications.
- Keep original files unedited and store copies securely.

Report the content to the platform

Use the platform's reporting options for impersonation, manipulated media, harassment or non-consensual intimate content. Contact its Grievance Officer if the ordinary reporting process does not resolve the issue. Request removal or disabling of access and retain the complaint reference number.

File a cybercrime complaint

Visit www.cybercrime.gov.in and register a complaint with the relevant details and evidence. You can also approach your nearest police station or cybercrime police station. If you are facing an immediate physical threat, contact emergency services through 112.



Secure your digital identity

- Change passwords for your email and social media accounts.
- Enable two-factor authentication.
- Log out of unfamiliar devices and active sessions.
- Check recovery email addresses and phone numbers.
- Inform friends, family and colleagues about fake accounts or messages circulating in your name.

Stop the content from spreading

Ask people not to forward, repost, download or engage with the manipulated content. If necessary, issue a short clarification through your verified account. Avoid confronting the suspected creator or paying anyone who promises to remove the content.



IT Act, Section 66C

IT Act, Section 66E

IT Act, Section 66D



IT Act, Section 356

IT Act, Sections 67 and 67A

IT Act, Section 319

IT Act, Section 336

THE UNVERIFIED FILES

A fictional investigative report that explores how manipulated digital content and fabricated communications can blur the line between truth and deception. Through a simulated news investigation, readers examine an alleged email leak, question the authenticity of digital evidence, and discover the importance of verification, media literacy, and critical thinking in an era of deepfakes and misinformation.

The picture illustrates how fabricated or manipulated digital communications can create misinformation, influence public perception, and potentially trigger serious diplomatic consequences. It encourages readers to question the authenticity of online information and understand the importance of digital verification and trust.

Note: The report is fictional and serves as an illustrative scenario based on real-world risks associated with deepfakes and digital misinformation.

TRUTH IS UNDER INVESTIGATION — VOL. 12 ISSUE 247 — 23 OCTOBER 2035

THE DAILY UNVERIFIED

NATIONAL • INTERNATIONAL • TECHNOLOGY • SOCIETY • WORLD — BENGALURU

SPECIAL INVESTIGATION

LEAKED EMAILS SPARK DIPLOMATIC ROW

Alleged exchange between Indian and foreign officialll goes viral, triggering a political storm — but is it real?

No confirmation from either government; experts say the authenticity of the emails remains unverified.

By Ananya Rao
Staff Correspondent

NEW DELHI, 23 October 2035 — A set of emails, allegedly exchanged between senior Indian and foreign officials, has gone viral on social media over the past 48 hours, sparking a major diplomatic controversy and renewed questions about the integrity of digital communication in the age of deepfakes.

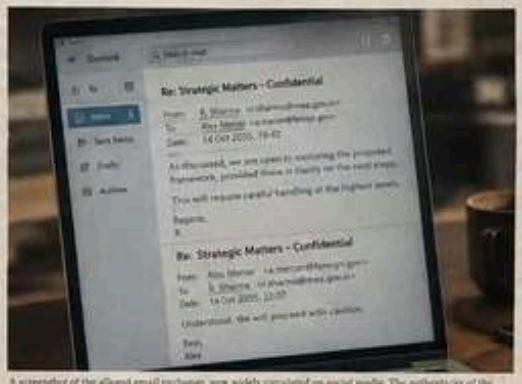
The emails, which appear to show discussions about a sensitive strategic matter, were first shared late on Monday by an anonymous account on a global forum. Within hours, screenshots of the exchange were widely circulated on social media, news platforms and encrypted messaging groups.

While the content of the emails has not been independently verified, their timing and the identities mentioned have led to intense speculation about the authenticity of the communication and the potential implications for ongoing bilateral relations.

A CONVERSATION THAT RAISES MORE QUESTIONS

The leaked thread appears to be a conversation between a senior Indian diplomat and a high-ranking official from a foreign government. The emails discuss a proposal related to regional security and suggest a shift in the position of one of the parties.

Continued on Page 2 →



A screenshot of the alleged email exchange, now widely circulated on social media. The authenticity of the emails has not been confirmed by either government. | Image: Social media (unverified)

> "The content of the emails, if genuine, could have serious implications for ongoing diplomatic discussions."
>
> — Former Indian Ambassador (name withheld)

WHAT WE KNOW SO FAR

- A set of emails allegedly between Indian and foreign officials went viral on 20 October 2035.
- The emails appear to discuss a sensitive strategic matter.
- No official confirmation has been issued by either government.
- Forensic analysis is underway to determine the origin of the emails.

THE DAILY UNVERIFIED — 23 OCTOBER 2035 | PAGE 2

TIMELINE: HOW THE STORY UNFOLDED

14 OCT, 7:42 PM
The first email in the thread is reportedly sent, according to the metadata visible in the screenshots.

14 OCT, 10:15 PM
The exchange continues with a follow-up email from the foreign official.

15 OCT, 2:30 AM
Screenshots of the emails are posted on an anonymous account on an international forum.

20 OCT, 9:10 AM
The screenshots begin circulating on social media platforms, with claims that the emails are "real" and "leaked".

20 OCT, 1:45 PM
News channels pick up the story. Hashtags related to the alleged leak trend online.

21 OCT, 11:20 AM
Both governments issue statements denying the authenticity of the emails and calling for restraint.

THE LEAKED EMAILS (EXCERPTS)

From: R. Sharma <r.sharma@mea.gov.in>
To: Alex Mercer <a.mercer@foreign.gov>
Date: 14 Oct 2035, 19:42
Subject: Re: Strategic Matters – Confidential

"As discussed, we are open to exploring the proposed framework, provided there is clarity on the next steps. This will require careful handling at the highest levels."

From: Alex Mercer <a.mercer@foreign.gov>
To: R. Sharma <r.sharma@mea.gov.in>
Date: 14 Oct 2035, 22:07
Subject: Re: Strategic Matters – Confidential

"Understood. We will proceed with caution. The timing is sensitive, and we need to ensure this does not become public before the next round of discussions."

Note: Screenshots of the emails are being circulated online. Their authenticity has not been independently verified.

GOVERNMENT STATEMENTS

Ministry of External Affairs (India)

"The Government of India has not authorised any such communication. The content being circulated is false and appears to be part of a coordinated misinformation campaign.

We urge the public to refrain from speculation and wait for official updates."

— MEA Spokesperson, 21 Oct 2035

Foreign Ministry (Country X)

"These emails are not genuine. We have no record of such correspondence, and our officials do not use unverified channels for sensitive discussions.

We are cooperating with relevant authorities to investigate the origin of the leak."

— Foreign Ministry Press Release, 21 Oct 2035

WHAT EXPERTS SAY



"At this stage, we cannot confirm whether the emails are authentic or fabricated. The metadata could be altered, and the content alone is not enough to establish their origin."

— **Dr. Meera Iyer**
Cybersecurity Researcher, IISc

"This incident highlights a growing challenge — even when content looks real, it may not be. Without verifiable provenance, it is difficult to say what is true, and what is not."

— **Prof. Arjun Malhotra**
Media & Information Literacy Expert

THE REALITY CHECK

The emails could be:

- Genuine, but taken out of context
- Partially real, with edited content
- Entirely fabricated using AI tools

Until an independent investigation establishes the origin and authenticity of the emails, the truth remains unclear.

A SINGLE EMAIL CAN SPARK A GLOBAL STORM.

In a world of deepfakes, the biggest challenge isn't just spotting what's fake — it's knowing what's real.

This is a fictional news report. The events described are not real, but are based on current risks and discussions around digital media and deepfakes.

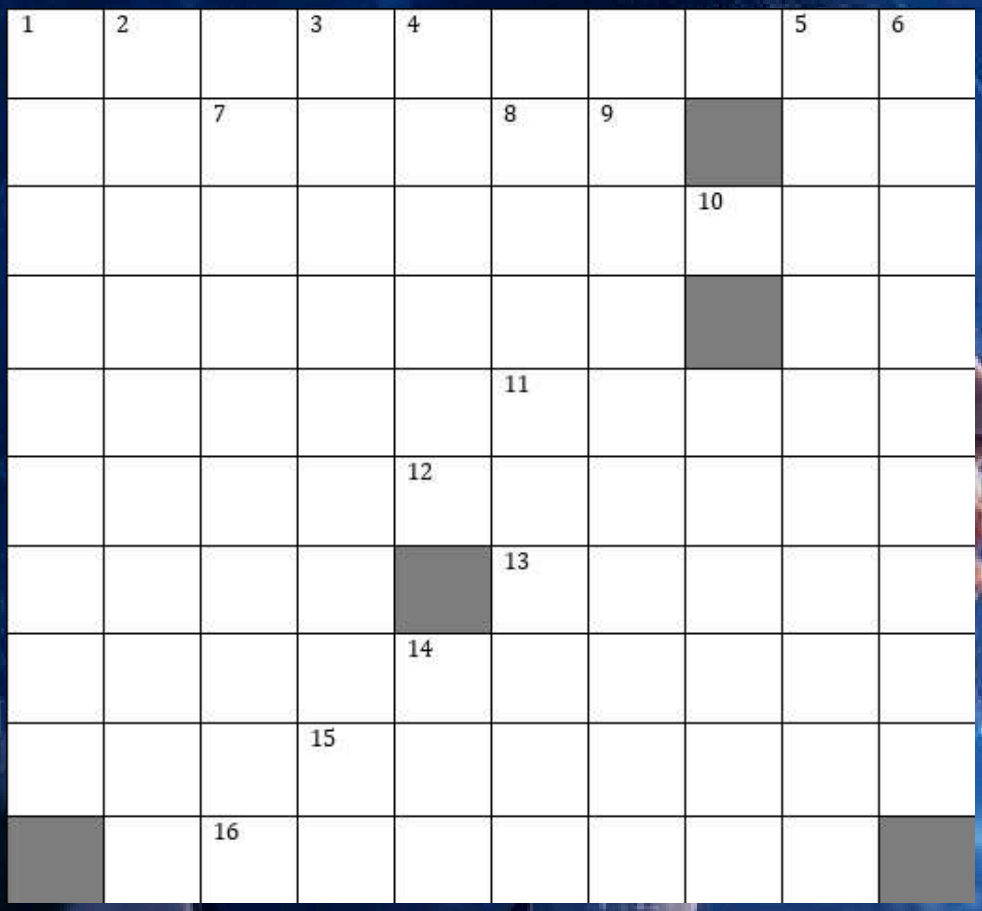
UNWIND ZONE

Across:

1.AI-generated or manipulated media that makes someone appear to say or do something they never actually did. (8)
11.The interconnected system of websites and online pages accessed through the Internet. (3)
10.An automated software program that performs tasks or interacts with users.
12.The confidence that digital information, sources, and interactions are genuine and reliable. (5)
13.A systematic examination of a system or process to verify its security, accuracy, and compliance. (5)
14.The act of examining information to confirm whether it is accurate or genuine. (5)
15.The right to control how personal information is collected, accessed, and shared. (7)
16.Permission given by an individual before their personal data, image, or voice is used. (7)

Down:

1.The process of identifying manipulated or artificially generated digital content. (9)
2.The process of converting readable information into an encoded form to prevent unauthorized access. (10)
7.A security method that uses unique physical or behavioural characteristics, such as fingerprints or facial features, for identification. (9)
3.A cyberattack that tricks people into revealing sensitive information through deceptive emails, messages, or websites. (8)
8.A technology that creates a secure, encrypted connection over the Internet. (3)
9.A temporary verification code used to authenticate a user's identity during login or transactions. (3)
5.An instruction or input given to an AI system to generate a response or perform a task. (6)
6.Data that provides information about other data, such as a file's creation date, author, or location. (8)
4. Deliberate deception or dishonest activity carried out to gain money, information, or an unfair advantage. (5)





Ms. Lekhya Sree
Assistant Professor
Presidency School of Information Science
Presidency University, Bengaluru

Deepfakes and the Future of Digital Trust











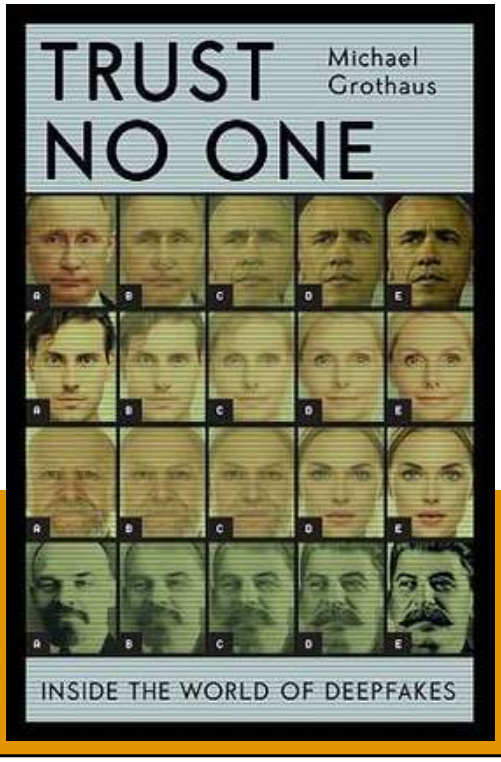








Best Seller



Book Review

Book Review: TRUST NO ONE: INSIDE THE WORLD OF DEEPFAKES
Author: Michael Grothaus
Genre: Computer Science
Rating: (4.1/5) ★★★★☆

Written by journalist Michael Grothaus, Trust No One: Inside the World of Deepfakes takes readers into the fascinating yet unsettling world of artificially manipulated digital content. The book explores how deepfake technology has evolved, how creators develop convincing fake videos, and how these technologies can challenge our understanding of truth and reality.

Through investigations and interviews with deepfake creators, Grothaus examines the communities behind this technology, their motivations, and the potential consequences of manipulating digital identities. The book explores how deepfakes can be used for entertainment and creative expression, while also exposing their darker applications in misinformation, identity manipulation, and digital deception.

⭐ Why Read It?

- Behind the Scenes of Deepfakes: Provides insights into how deepfake content is created and the online communities responsible for developing it.
- Real-World Implications: Explores the potential impact of manipulated videos and images on personal identity, public opinion, politics, and society.
- Ethical and Social Perspectives: Raises important questions about privacy, consent, misinformation, and the future of digital credibility.
-

Warm Regards,
The Editorial Board

✅ Strengths

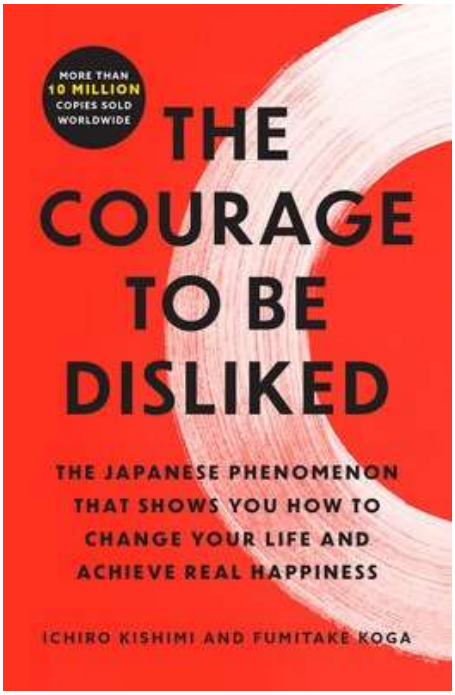
- Investigative Approach: The author's interviews and research offer an inside perspective on the people and communities creating deepfake content.
- Engaging Narratives: Real-world examples and thought-provoking accounts make a complex technological subject accessible to general readers.

⚠️ Criticism & Limitations

- Limited Technical Depth: Readers looking for detailed explanations of deep learning architectures and the mathematical foundations of deepfake generation may find the technical coverage introductory.
- Disturbing Content: Discussions of non-consensual deepfake pornography and digital exploitation may be uncomfortable for some readers.
-

⭐ Final Verdict

Trust No One offers an insightful look into deepfake technology and its impact on digital trust. Michael Grothaus encourages readers to question what they see and critically evaluate digital information, making it a valuable read for students and technology enthusiasts.



THE COURAGE TO BE DISLIKED

Author: Ichiro Kishimi and Fumitake Koga

Genre: Self-Help / Productivity / Personal Development

Rating: (4.5/5)

The Courage to Be Disliked by Ichiro Kishimi and Fumitake Koga is a thought-provoking book that explores the philosophy of Alfred Adler through a conversation between a young man and a philosopher. It challenges conventional beliefs about happiness, relationships, self-worth, and personal freedom. The book encourages readers to stop seeking constant approval from others and take responsibility for shaping their own lives.

Key Themes & Strengths

- **Freedom from Approval:** Encourages readers to overcome the need for validation and acceptance from others.
- **Separation of Tasks:** Explains the importance of distinguishing between what we are responsible for and what belongs to others.
- **Living in the Present:** Emphasizes focusing on the present rather than being controlled by past experiences or future expectations.
- **Self-Acceptance:** Inspires readers to embrace their individuality and develop the courage to be themselves.

Criticism

- **Philosophical Approach:** The dialogue-based format may feel repetitive or slow to readers who prefer straightforward explanations.
- **Challenging Perspectives:** Some of Adler's ideas about trauma, relationships, and human behaviour may seem overly simplistic or difficult to accept.

⭐ Final Verdict

The Courage to Be Disliked is an insightful and transformative read that challenges readers to rethink their approach to happiness, relationships, and self-worth. Its central message is powerful: true freedom begins when we stop living to meet others' expectations. The book reminds us that we cannot control how others perceive us, but we can choose how we live our lives. A highly recommended read for anyone seeking personal growth, emotional independence, self-confidence, and the courage to embrace their authentic self.

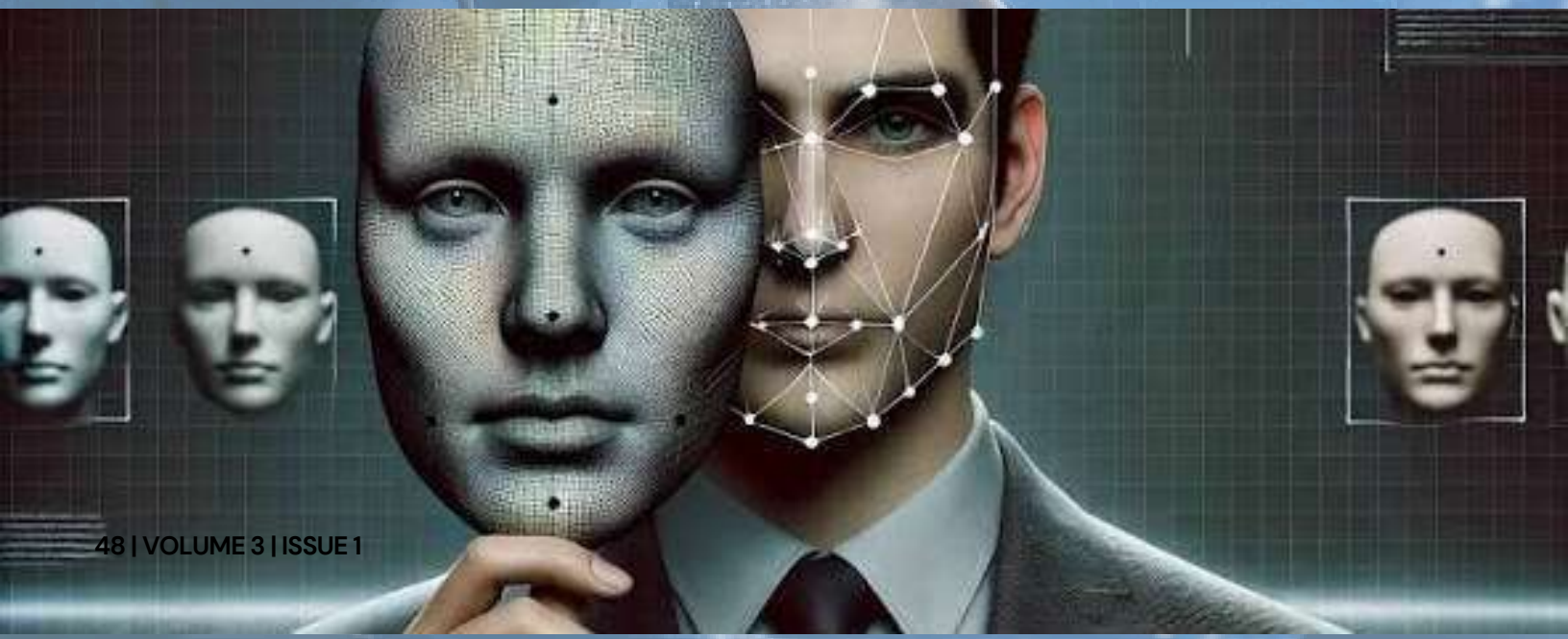
Warm Regards,
The Editorial Board

Upcoming Faculty Development Programmes(FDPs)

Institute Name	FDP Thrust Area	FDP Title	Start Date	End Date	Link for registration
Research foundation of India & Parul University	Engineering and Management	A Systematic Way of Research Paper Writing	7-12-2026	11-12-2026	https://researchfoundationofindia.com/ai-research-quality/
SRM Institute of Science and Technology (SRMIST), Chennai	Engineering	Modern Computer Networks	14-12-2026	23-12-2026	https://atalacademy.aicte.gov.in/participant/workshop
College of Engineering Aranmula, Kerala	Engineering and Management	Ai Enabled Advanced Pedagogy for Modern Education and Research	30-11-2026	5-12-2026	https://docs.google.com/forms/d/e/1FAIpQLScv2QTypSJRqRsQG7XbR6SxxoqEgtPBqpw2QfW_FcD6yhniPg/viewform
CMR Institute of Technology, Bengaluru	Engineering and Management	Artificial Intelligence for Data-Driven Decision Making	14-12-2026	18-12-2026	https://docs.google.com/forms/d/e/1FAIpQLSctNyl5UffVUpkiZjGGSS140XvOaUWRQymnLkrf17vuj9scKw/viewform
Asia-Pacific Institute of Management, New Delhi	Engineering and Management	Artificial Intelligence for Data-Driven Decision Making	18-12-2026	19-12-2026	https://www.asiapacific.edu/events/faculty-development-programme-on-artificial-intelligence-for-data-driven-decision-making/?

Upcoming Research Proposals

Upcoming Research Proposals from August 2026			
Sr.No	**Details of Proposal**	**Details of proposal Link**	**Important Dates**
1	2nd Call for Applications for ICSSR Senior Fellowship for F.Y. 2026-2027	https://www.icssr.org/hi/node/701?	The last date for submission is 30 November 2026
2	ANRF- Call for Proposal for Prime Minister Early Career Research Grant	https://www.indiascienceandtechnology.gov.in/announcementsopportunity/anrf-call-proposal-prime-minister-early-career-research-grant	The last date for submission is 2 December 2026
3	ANRF- Call for nominations under Ramanujan Fellowship	https://www.indiascienceandtechnology.gov.in/announcementsopportunity/anrf-call-nominations-under-ramanujan-fellowship	The last date for submission is 31st December 2026



Upcoming Conferences

Upcoming Conferences in 2026					
Sr. No	Institute Name	Conference Name	Date	Link of WebPage	Last Date of Paper Submission
1	Sri Sivasubramaniya Nadar College of Engineering (SSNCE)	10th International Conference on Computational Intelligence and Data Science (ICCIDS 2027)	6-8 January, 2027	https://https://iccids.in/	11/18/2026
2	Noida International University	2nd International Conference on AI-Driven Innovation: From Industry 4.0 to Society 5.0 (ICADIS 2027)	25-26 February, 2027	https://niu.edu.in/icadis-2027/	11/30/2026
3	Devi Ahilya University	Integrating Interdisciplinary Perspectives and Solutions - Conference on Modern AI, Entrepreneurship &	19-20 March, 2027	https://sites.google.com/view/icancs-2027/home?authuser=0	12/21/2026
4	Satyabhama Institute of Science & Technology Deemed - to - be- University	2027 IEEE International Conference on Electronics, Nanoelectronics, Communication, Devices and Embedded Systems (IEEE ENCODE 2027)	4-5 March,2027	https://encodesistece.com/index.html	12/31/2026
5	Odisha University of Technology and Research	IEEE National Conference on VLSI, Communication & Intelligent Machine (V-CIM 2027)	7-9 January, 2027	https://sksahuoutr.github.io/vcim2027_ieee	11/15/2026

UPCOMING EVENTS

14 November 2026

Parent Teachers' Meeting -II

25 November2026

Presidency Premier League

28 November2026

Convocation

2 December2026

9th Innovative Project Expo

12 December2026

Annual Alumni Meet

12 January 2027

National Youth Day



THE WRAP UP

As this edition of The Communiqué comes to a close, we reflect on the theme "Deepfakes and the Future of Digital Trust." We are entering an era where artificial intelligence can recreate faces, imitate voices, manipulate videos, and generate highly realistic digital content. While these advancements open new possibilities in entertainment, education, communication, and creative industries, they also raise serious concerns about misinformation, identity theft, privacy, and digital deception. Deepfakes challenge our traditional understanding of authenticity, reminding us that what appears real may not always be genuine. In a world where digital content can be manipulated with increasing ease, the ability to question, verify, and trust information has become more important than ever.

Key Takeaways from This Edition

- The Changing Face of Reality: Deepfake technology is transforming digital media by enabling the creation of realistic synthetic images, videos, and audio. It challenges our ability to distinguish authentic content from artificially generated or manipulated information.
- The Growing Threat of Digital Deception: The misuse of deepfakes for misinformation, financial fraud, identity impersonation, cyberbullying, and privacy violations highlights the growing need for stronger digital security and public awareness.
- Technology as Both a Challenge and a Solution: While generative AI makes digital manipulation increasingly sophisticated, AI-powered detection systems, digital watermarking, and content provenance technologies are emerging as important tools to identify and trace manipulated media.
- Rebuilding Digital Trust: Digital trust requires more than advanced technology. Media literacy, critical thinking, responsible content creation, verification practices, and stronger ethical and legal frameworks are essential to creating a safer digital environment.



Final Thoughts

"Deepfakes and the Future of Digital Trust" is more than a discussion about artificial intelligence and digital manipulation; it is a reflection on the value of truth, authenticity, and responsibility in an increasingly AI-driven world. The future will not simply depend on how advanced our technologies become, but on how wisely we choose to use them. As the boundaries between real and artificial continue to blur, let us cultivate a culture of curiosity, critical thinking, digital awareness, and ethical innovation. Technology may shape what we see, but it is our responsibility to question what we believe. The future of digital trust lies not merely in detecting what is fake, but in building a digital world where authenticity, transparency, and integrity remain at its core.

Vision of Presidency School of Information Science

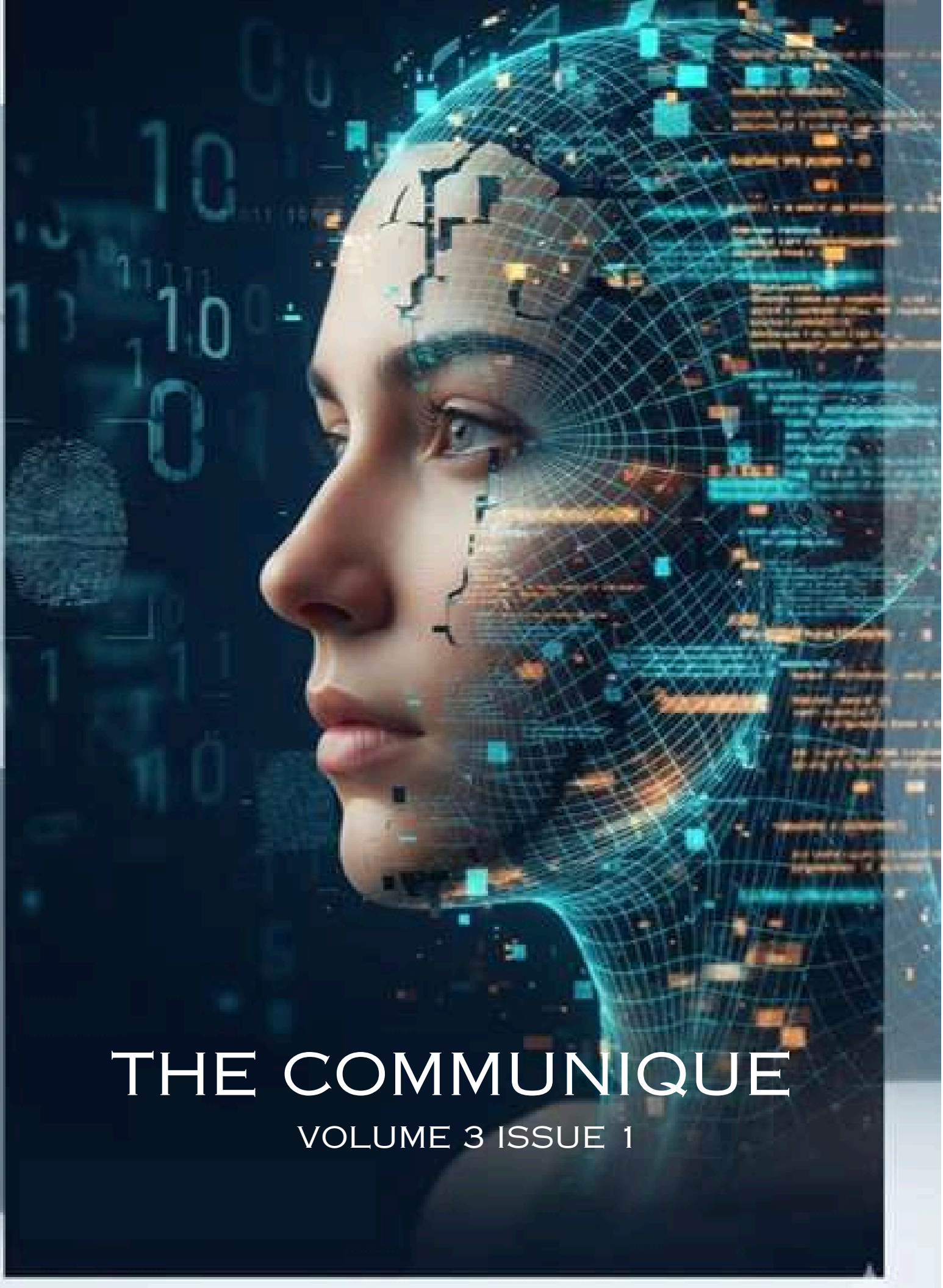
Vision	To be a global centre of excellence in information science and research, fostering innovation and producing professionals with integrity and ethical responsibility.

Mission of Presidency School of Information Science

Mission	To provide high-quality education in information science, equipping students with strong technical expertise and problem-solving skills.
Mission	To promote research and innovation in information science and technology, addressing real-world challenges through industry collaboration.
Mission	To nurture graduates with strong ethical values and a commitment for lifelong learning for sustained professional growth in the IT sector and allied fields.

PROGRAM OUTCOMES (POs) FOR BCA

PO1	**Foundation Knowledge:** Apply knowledge of mathematics, programming logic and coding fundamentals for solution architecture and problem solving.	PO5	**Individual and Teamwork:** Function and communicate effectively as an individual or a team leader in diverse and multidisciplinary groups. Use methodologies such as agile.
PO2	**Problem Analysis:** Identify, review, formulate and analyse problems for primarily focussing on customer requirements using critical thinking frameworks.	PO6	**Project Management and Finance:** Use the principles of project management such as scheduling, work breakdown structure and be conversant with the principles of Finance for profitable project management.
PO3	**Development of Solutions:** Design, develop and investigate problems with as an innovative approach for solutions incorporating ESG/SDG goals.	PO7	**Ethics:** Commit to professional ethics in managing software projects with financial aspects. Learn to use new technologies for cyber security and insulate customers from malware.
PO4	**Modern Tool Usage:** Select, adapt and apply modern computational tools such as development of algorithms with an understanding of the limitations including human biases.	PO8	**Life-long learning:** Change management skills and the ability to learn, keep up with contemporary technologies and ways of working.



THE COMMUNIQUE

VOLUME 3 ISSUE 1