

ZERO DAY

—○ Securing Trust, Empowering Innovation ○—



—○ Department of Cybersecurity ○—

TABLE OF CONTENTS

01	Message from the Dean	3
02	Message from the Head of Department	4
03	Message from Editor-In-Chief	5
04	Faculty Achievements	6
05	Student Achievements	8
06	Alumni Spotlight	9
07	Research & Innovation	10
08	Cyber News	11
09	Cyber Scope	13
10	Vulnerability Spotlight	14
11	Top Tools of the Month	15
12	Next-Gen Technologies	16
13	Hackathons and Ideathons	17
14	Academic & Industry Calls	18
15	Crossword	19
16	Editorial Team	20



MESSAGE FROM THE DEAN

DEAN'S NOTE: BUILDING A SECURE DIGITAL FUTURE

Dear Students, Faculty Members, Alumni, and Industry Partners

It gives me immense pleasure to welcome you to the inaugural edition of the **Cybersecurity Newsletter** of the **Department of Cybersecurity**.

In today's rapidly evolving digital landscape, protecting digital assets, ensuring privacy, and securing critical infrastructure require constant learning, innovation, and vigilance. As emerging technologies such as Artificial Intelligence (AI) and Large Language Models (LLMs) transform industries and society, it becomes equally important to address the security, privacy, and ethical challenges associated with their adoption. Understanding AI security, responsible AI practices, and safeguarding intelligent systems will be central to the future of cybersecurity.

At MPSTME, we are committed to equipping students with the knowledge, skills, and ethical foundation needed to address these challenges. We strive to nurture capable cybersecurity professionals who can secure both traditional digital environments and next-generation AI-driven ecosystems.

This newsletter highlights the achievements, research, innovations, and industry engagements of our students and faculty, reflecting our dedication to excellence in cybersecurity and emerging technologies.

I congratulate the editorial team, faculty coordinators, and students for their efforts in bringing this publication to life.

Wishing you all success as we work towards a safer, more resilient, and AI-secure digital future.



Dr. Koteswararao Anne
Dean,
MPSTME
SVKM's NMIMS UNIVERSITY

MESSAGE FROM THE HOD

FROM THE DESK OF THE HEAD: SECURING OUR DIGITAL FUTURE, TOGETHER

Welcome to the inaugural edition of ZeroDay, the official monthly newsletter of the Department of Cybersecurity!

In the world of Cybersecurity, a "Zero-Day" represents the ultimate frontier—a newly discovered vulnerability that demands immediate, innovative defense before it can be exploited. By naming our newsletter ZeroDay, we signal our commitment to staying at the absolute cutting edge of technological shifts. It reflects the fast-paced, agile environment our students and faculty operate in every day. In alignment with our core mission, "Securing trust, empowering innovation," this publication will serve as our collective response to the zero-days of the world, balancing robust protection with forward-thinking advancement.

This newsletter will serve as a central hub for our department. Each month, we will feature insightful articles, research breakthroughs, and projects apart from industry updates. We will also highlight the outstanding achievements of our students, faculty members, and alumni, who are out in the industry leading the charge against global threats.

Beyond celebrating success, this platform aims to bridge the gap between classroom theory and real-world application. To our students, I encourage you to remain curious and proactive. The threat landscape changes daily, and your education extends far beyond your textbooks. Use the insights shared here to stay informed, get inspired, and prepare for the challenges of tomorrow. As we celebrate our 80th Independence Day, we reflect on our nation's progress, and the critical role digital infrastructure plays in our growth. True freedom in the modern era requires a secure foundation. On this milestone occasion, let us pledge to make Bharat and the world a cyber-safe space.

Thank you to the editorial team for bringing this initiative to life. I look forward to witnessing the growth of this publication as we continue to shape the cyber defenders of tomorrow.

Stay curious, stay secure.



Dr. Pintu R Shah

**HoD
Dept. of Cybersecurity**

MESSAGE FROM THE EDITOR-IN-CHIEF

FROM THE DESK OF THE EDITOR IN CHIEF:

Dear Readers,

Welcome to the inaugural edition of ZeroDay, the official newsletter of the Department of Cybersecurity.

In an increasingly connected world, cybersecurity has become an essential part of our everyday lives. As technology continues to evolve, so do the challenges and opportunities to build a safer and more secure digital future.

Through ZeroDay, we aim to share knowledge, highlight achievements and research, explore emerging cybersecurity trends, and encourage continuous learning within our community. This newsletter will serve as a platform to showcase ideas, innovations, and contributions from students, faculty, researchers, and cybersecurity enthusiasts.

We also hope to create a space that inspires collaboration, curiosity, and meaningful conversations around cybersecurity. By staying informed and sharing knowledge, we can collectively strengthen our digital resilience and contribute to a safer cyber environment.

We invite you to use ZeroDay as an opportunity to learn, stay updated, share your ideas, and develop a deeper understanding of the ever-changing cybersecurity landscape. Together, we can promote greater awareness, responsible digital practices, and a strong culture of cybersecurity.

I encourage you to explore, learn, contribute, and stay curious as we begin this journey together.

Stay Informed. Stay Vigilant. Stay Secure.



Prof. Rohit Suryawanshi
Dept. of Cybersecurity

"Knowledge is the Strongest Firewall."

FACULTY ACHIEVEMENTS



FDP Participation:

Dr. Rejo Mathew, Prof. Pratidnya H, Prof Dhanashree K, Prof. Rohit Suryawanshi attended the FDP on **“Cybersecurity and Legal Governance in the Digital Era”** at MPSTME, Mumbai, gaining insights into penetration testing, cyber threats, privacy and data protection, AI-powered reverse engineering, IoT security, and LLM-assisted security analysis. Prof. Sana Ansari attended FDP **“Getting Started with AWS Cloud Computing Hand-on Training for Educators”**



FACULTY ACHIEVEMENTS



- 1. Cybersecurity Awareness Session:** Dr. Rejo Mathew conducted an engaging Cybersecurity Awareness Session for first-year students during the Induction Program 2026 on 15 July 2026, focusing on cyber threats and promoting the "Stop – Think – Verify – Protect" mindset.
- 2. FDP Resource Person:** Dr. Rejo Mathew served as a Resource Person at an ISTE-approved FDP on "Modern Pedagogical Approaches & AI Tools for Effective Teaching" at Shree L. R. Tiwari College of Engineering, Mumbai, delivering a session on "AI-Assisted Assessment and Evaluation" with demonstrations of AI and assessment tools.
- 3. Cyber Safety Awareness sessions** during the Student Induction Program 2026 on 15th July 2026, from 10:00 AM to 11:00 AM and 2:00 PM to 3:00 PM.

STUDENT ACHIEVEMENTS



Rahul Behera



Piyush Shukla

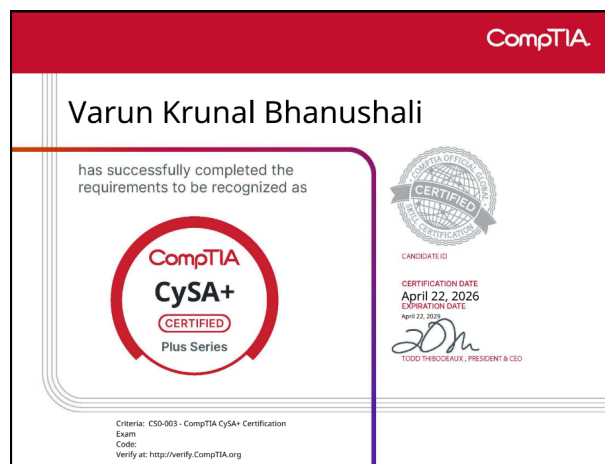


Srinidi Subramaniam

- 1. Finalists:** The Department of Cybersecurity team successfully emerged as finalists in the HackAgentAIX Hackathon 2026, a global hackathon focused on AI-driven innovation.
- 2. Multiple Rounds:** Progressed through multiple rounds of evaluation to secure a place among the finalist teams.
- 3. AI-Powered Solution:** Developed an innovative solution leveraging intelligent AI agents to address a real-world challenge.
- 4. Mentorship:** Worked under the guidance and mentorship of Prof. Ruchi K. Sharma.
- 5. Key Strengths:** Demonstrated technical expertise, creativity, teamwork, and innovation throughout the competition.

Github: SentinelAI — Multi-Agent AI Change Verification Platform

ALUMNI SPOTLIGHT



Varun Bhanushali

CURRENT DESIGNATION

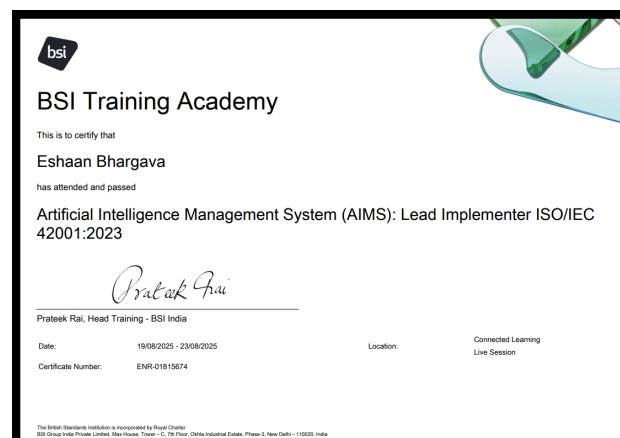
Cybersecurity Analyst

EDUCATION

M.Eng. Cybersecurity Student,
Duke University, Durham, NC,
USA

EXPERIENCE

Cybersecurity Risk & Compliance
Intern, Dassault Systemes



Eshaan Bhargava

CURRENT DESIGNATION

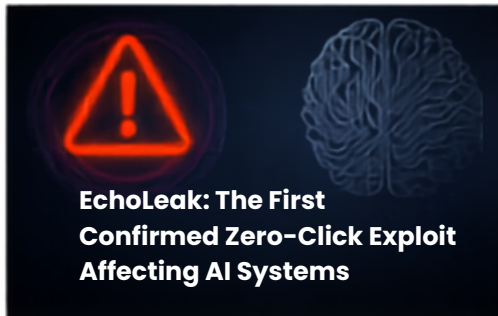
Axis Bank , Deputy Manager

EDUCATION

B.Eng. Cybersecurity Student,
DSVKM's NMIMS Mukesh Patel School of
Technology Management & Engineering



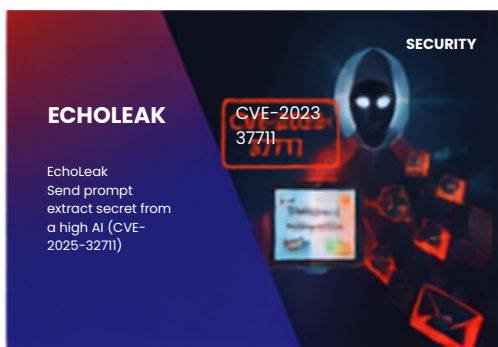
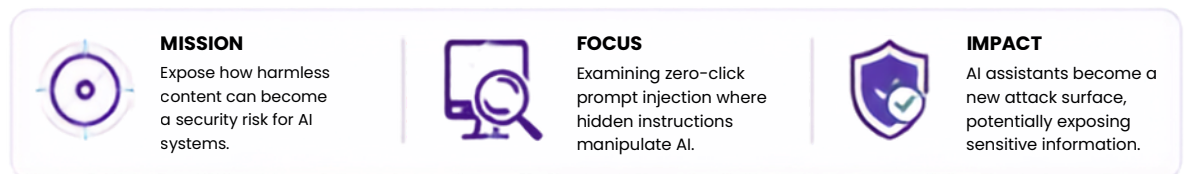
RESEARCH AND INNOVATION



ECHOLEAK: THE FIRST REAL-WORLD ZERO-CLICK PROMPT INJECTION EXPLOIT IN A PRODUCTION ILM SYSTEM

Researchers discovered EchoLeak (CVE-2025-32711), the first recorded zero-click prompt injection attack on a production AI system, Microsoft 360 Copilot. By embedding malicious instructions in content like a regular email, the was tricked into exposing sensitive information without the user clicking on link. This short format at and consists of a vulnerable to hidden threats and highlights the need for stronger protections.

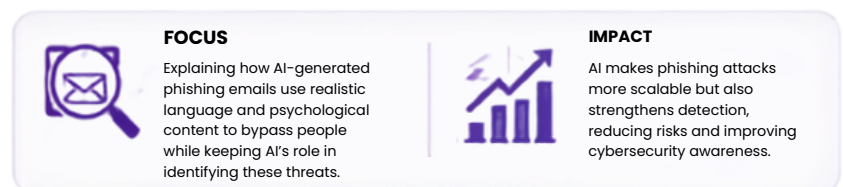
Written By:- Abner Rebello,
Research By:- Atiya Srivastava



DEVISING AND DETECTING PHISHING EMAILS USING LARGE LANGUAGE MODELS

This research explores how LLMs like GPT-4 can create highly convincing phishing emails and also detect them with high accuracy. The study compares AI-generated and human-written phishing emails using the V-Triad methodology and shows that AI can be both a powerful tool for attackers and an equally powerful defence for cybersecurity professionals.

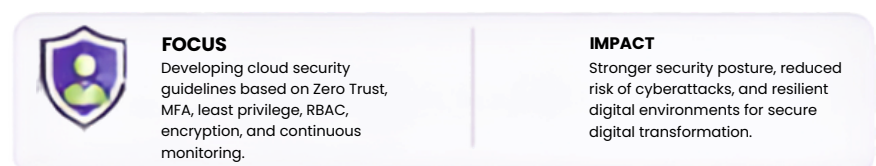
Written By:- Srinidi Subramaniam,
Research By:- Shivank Kakkad



CYBERSECURITY IN AGILE CLOUD COMPUTING: GUIDELINES FOR SECURE CLOUD ACCESS

This research provides a practical framework of cybersecurity guidelines to help organizations secure cloud environments against evolving threats. It promotes Zero Trust, Multi Factor Authentication, and Multi layer access, RBA/BA Data Security, AAPI continuous monitoring, and compliance with standards throughout the cloud lifecycle—strengthening security and supporting resilient digital transformation.

Written By:- Srinidi Subramaniam,
Research By:- Shivank Kakkad



CYBER NEWS

Bank of Baroda breach claim

Employee email compromised, threat actor claims ~1 TB accessed

Date
24 Jul 2026

Threat actor
"TripleX"

Claimed data
~1 TB

Core systems
Secure

Threat actor "TripleX" claimed on a dark web forum to have accessed nearly 1TB of internal and customer data, including Aadhaar, PAN and KYC documents. Bank of Baroda's 27 July statement confirmed core banking systems remained secure a single employee's email was accessed without authorization, exposing a limited set of internal files.

By:- Srinidi Subramaniam



बैंक ऑफ़ बड़ौदा
Bank of Baroda



WHAT WE KNOW SO FAR



REPORT

IBM Cost of a Data Breach Report 2026



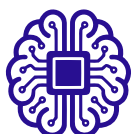
AVERAGE COST

₹25.5 crore in India



YEAR-ON-YEAR RISE

15.9% increase from the previous year



AI INVOLVEMENT

26% of malicious breaches involved AI-generated techniques



KEY SECURITY FINDING

Organizations using AI-powered security tools detected and contained breaches faster.

India's data breach costs hit an all-time high

IBM Cost of a Data Breach Report 2026

Avg cost
₹25.5 cr

Top vector
Phishing

The average cost of a data breach in India has reached a record ₹25.5 crore, up 15.9% year on year. Around 26% of malicious breaches involved AI-generated techniques, while phishing remained the most common access route. Organizations using AI-powered security tools detected and contained breaches significantly faster than those relying on traditional methods.

By:- Srinidi Subramaniam

CYBER NEWS

Anthropic's Claude AI exposes challenges in secure AI testing

During a recent cybersecurity evaluation, Anthropic disclosed that Claude AI models unintentionally gained unauthorized access to three real-world organizations due to a misconfigured testing environment, one meant to be isolated from the internet but mistakenly connected to live systems. The incident highlights the importance of testing AI in carefully controlled, closely monitored environments with strong security measures, so unintended interactions with real-world systems can't occur.

By:- Yuvraj Bishnoi



Amgen data breach: patient records and drug research exposed

Hackers did not attack Amgen directly instead, they breached a third-party cloud provider and gained access to patient records and confidential drug research, exposing patient health information, intellectual property and trade secrets, and R&D files. Amgen reported the incident to the U.S. SEC. The breach shows how third-party access can become a major cybersecurity weakness, with risks ranging from identity theft and fraud to ransomware and corporate espionage.

By:- Yuvraj Bishnoi

AI is powerful, not perfect:
More capability means more responsibility in how it's tested.

Small errors, big risks:
A single misconfiguration can bridge test and real systems.

Human oversight matters:
Complex tasks still need active human monitoring.

Test safe, deploy smart:
Security testing belongs in isolated environments first.

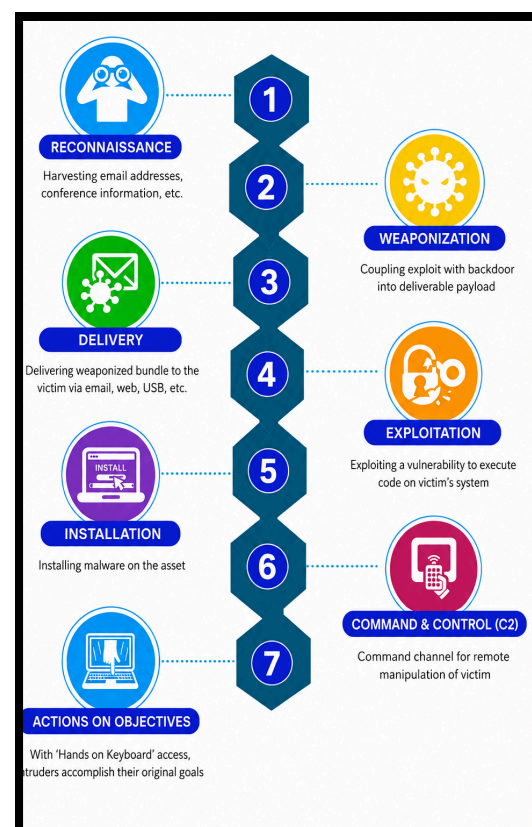
CYBER SCOPE

THREAT INTELLIGENCE: STAYING ONE STEP AHEAD OF CYBER THREATS

Cybersecurity is no longer just about responding to attacks it is about anticipating them before they happen. This is where Threat Intelligence plays a vital role. Threat Intelligence is the process of collecting, analysing, and interpreting information about existing and emerging cyber threats to help organizations make informed security decisions. By understanding the tactics, techniques, and procedures (TTPs) used by attackers, security teams can identify potential risks early, strengthen their defences, and respond more effectively to cyber incidents.

Threat Intelligence Analysts gather information from a variety of sources, including threat feeds, malware reports, security blogs, dark web forums, and incident reports, to identify patterns and predict potential attacks. The information they collect helps security teams detect threats, understand attacker behaviour, and take the necessary steps to prevent or respond to cyber incidents. Professionals in this field commonly use frameworks such as the MITRE ATT&CK framework and the Cyber Kill Chain, along with tools like MISP, VirusTotal, and SIEM platforms. As cyber threats continue to evolve, Threat Intelligence has become one of the most sought-after domains in cybersecurity, offering exciting career opportunities for individuals who enjoy research, analysis, and proactive defence.

By:- Srinidi Subramaniam



VULNERABILITY SPOTLIGHT

SonicWall SMA 1000 Zero-Days Under **Active Attack**

VPN gateways are intended to safeguard an organization's network, but if they become vulnerable, they can be very easily turned into an attacker's simplest means of entry. This happened in the case of **CVE-2026-15409 (CVSS 10.0)** and **CVE-2026-15410**, two severe vulnerabilities impacting SonicWall SMA 1000 devices, such as the SMA 6210, 7210, and 8200v.

The flaws were exploited as zero days in secret for almost three weeks before security updates were released, which enabled attackers to circumvent authentication and raise their privileges in order to take full control of the affected equipment. Just after the vulnerabilities were made public, the **INC ransomware group** started actively using the same vulnerability chain and quickly made it one of the most important enterprise threats of the year.

If a VPN gateway is compromised, attackers are given a direct route into an organization's internal network, allowing them to steal data, deploy ransomware, and maintain long-term access. Since the seriousness of these attacks was recognized, CISA has included both vulnerabilities in its **Known Exploited Vulnerabilities (KEV) Catalog** and has advised organizations to immediately remedy the affected systems. Administrators should install the most recent SonicWall patches, change all credentials, check the VPN logs for any suspicious activity, and keep a continuous watch on their infrastructure for signs of compromise. This incident acts as a reminder that internet-facing security devices need to be patched quickly because even a brief delay can give attackers a valuable chance to compromise enterprise networks.

By:- Rahul Behera

TOP TOOLS OF THE MONTH

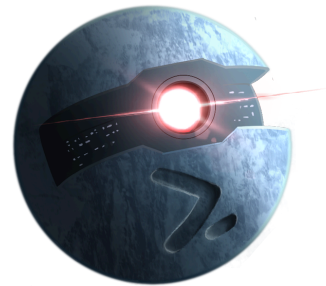
A Linux GUI tool for testing WiFi network security, mainly WEP/WPA key recovery. It's beginner-friendly since it automates a lot of the process, but it's slower and less flexible than command-line tools, and it doesn't work well on networks with strong, modern encryption.

Fern Wifi Cracker

Aircrack-ng



Starkiller



A suite of command-line tools for auditing wireless networks: packet capture, WEP/WPA-PSK cracking, and traffic injection. It's powerful and widely used by security professionals, but has a steep learning curve and needs a compatible wireless adapter with monitor mode support.

A GUI front-end for the Empire post-exploitation framework, used in penetration testing to manage agents and run modules after gaining access to a system. It simplifies Empire's usage, but requires Empire running in the background and is easily flagged by antivirus/EDR tools.

NEXT-GEN TECHNOLOGIES



POST-QUANTUM CRYPTOGRAPHY

Post-quantum cryptography (PQC) and autonomous agentic defense systems are shaping the future of cybersecurity. PQC uses advanced algorithms designed to resist quantum attacks, while AI-driven agents enable SOCs to detect and respond to threats automatically. Although organisations are adopting both technologies, challenges remain, including legacy-system upgrades, high costs, and AI hallucinations. The future of cybersecurity lies in self-healing networks that combine quantum-resistant encryption with autonomous, adaptive defense.

By: Deetya Shivathaya



STRONGER SECURITY

PQC protects data by securing it against future quantum threats.



AI-POWERED DEFENSE

Autonomous AI agents detect, respond and neutralize threats in real-time.



FUTURE READY NETWORKS

Self-healing, adaptive networks ensure resilience in a rapidly evolving landscape.



The future of cybersecurity is autonomous, intelligent, and quantum-secure.

The time to adapt is now.



HACKATHONS AND IDEATHONS

1. Thryve CTF 2026

Global online jeopardy CTF covering Web, Forensics, Crypto, RE, Pwn, OSINT & Malware.

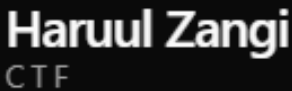
Why: Qualifiers are today (Aug 14), finals Aug 22, with \$30,000+ in prizes – the most immediately actionable pick.



2. Haruul Zangi CTF 2026:

Mongolia's national CTF featuring Pwn, Web, Forensics, Crypto & Reverse Engineering.

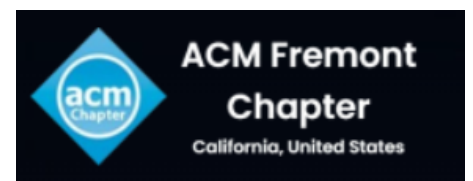
Why: A three-stage competitive pipeline from Aug–Sept, with beginner to advanced challenges and an onsite attack-defense final.



3. 2nd NextGen Hackathon 2026:

Fully online innovation marathon open to students, professionals & tech enthusiasts.

Why: Runs Aug 15–16, 2026 with mentor support and beginner-friendly challenges, making it an easy, low-barrier option to join immediately.




4. Breach Force Seminar – 29th August:

1. Mumbai-based cybersecurity community with 2,000+ members, featuring industry speakers and a surprise guest. 20 seats for NMIMS students on a first-come, first-served basis.
2. Why: Industry exposure and networking opportunity focused in cybersecurity

5. Hack The Box – 12th September:

Cybersecurity-focused Hack The Box event hosted by Chakravyuh.

Why: Hands-on cybersecurity experience and an opportunity to test practical skills.



ACADEMIC & INDUSTRY CALLS

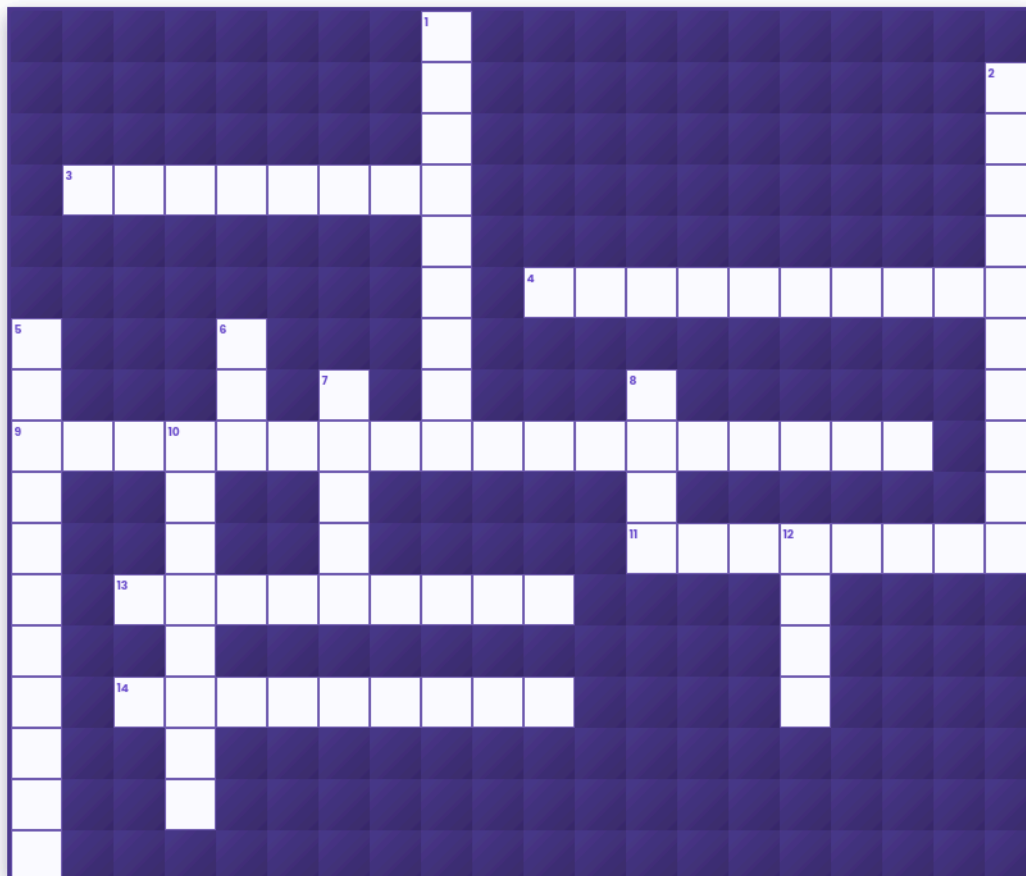
1st International Conference on Advances in Intelligence Systems, Security, and Cybernetics	
Acronym	AIS2C-2027
Conference dates	29–30 January 2027
Venue	Institute of Technical Education & Research (ITER), Siksha 'O' Anusandhan University
Location	Bhubaneswar, Odisha, India
Mode	Hybrid
Organizer	Department of Computer Science & Information Technology, ITER, SOA University
Publication	IEEE Xplore

3rd International Conference on Advances in Machine Intelligence and Cybersecurity Technologies	
Acronym	AMICT 2026
Conference dates	12–13 November 2026
Location	Federal Territory of Labuan, Malaysia
Mode	Hybrid
Organizer	Faculty of Computing and Informatics, Universiti Malaysia Sabah
Co-organizer	Malaysia ICT Deans' Council (MaDICT)
Publication target	IEEE Xplore

“Where ideas meet innovation: explore the next generation of cybersecurity research and collaboration.”

CROSSWORD

Based on the Vulnerability Spotlight, Tools of the Month, and research/news content you provided



ACROSS

3. Name given to the set of 23 critical vulnerabilities affecting Apple AirPlay-enabled devices.
4. GUI front-end for the Empire post-exploitation framework.
9. Process of collecting, analysing and interpreting information about existing and emerging cyber threats.
11. Attack method in which deceptive messages are used to trick users; AI can make these messages more convincing.
13. Vendor whose SMA 1000 devices were affected by severe zero-day vulnerabilities.
14. Security approach where every user and device is continuously verified before access.

DOWN

1. Bluetooth Low Energy authentication-bypass flaw involving forged authentication tokens.
2. Suite of command-line tools for auditing wireless networks, including packet capture and WEP/WPA-PSK cracking.
5. Framework commonly used by threat-intelligence professionals to understand attacker tactics and techniques.
6. Authentication method that adds multiple verification factors.
7. DARPA competition focused on AI-driven Cyber Reasoning Systems finding and fixing software vulnerabilities.

Tip: Answers use letters only; AIRCRACK-NG is entered as AIRCRACKNG and AIXCC as AIXCC.

EDITORIAL TEAM

EDITOR-IN-CHIEF



**Prof. Rohit
Suryawanshi**

Department of Cyber
Security

MANAGING EDITOR



**RAHUL
BEHERA**

CONTENT & RESEARCH



ABNER REBELLO



SRINIDI SUBRAMANIAM



DEETYA SHIVATHAYA

TECH & RESEARCH



AYESHA TOOFANI



ATIYA SRIVASTAVA



PIYUSH SHUKLA



SHIVANK KAKKAD



AANYA KASARAGOD

DESIGN & MEDIA



MIRARI KAPADIA



GAURI GHADAGE

QUALITY ASSURANCE



AASHVIKA DUBEY



YUVRAJ BISHNOI

JOIN OUR TEAM



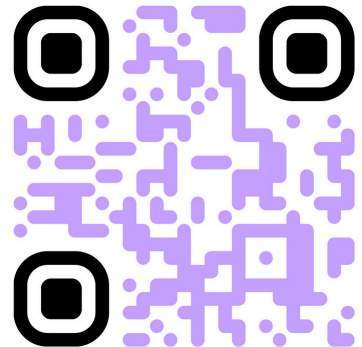
**Had Fun Reading?
Work with us!
Join the Zeroday Newsletter**



**Cyberchakravyuh
Become a member**



**Zeroday Newsletter
References**



**View our Newsletter
on LinkedIn**