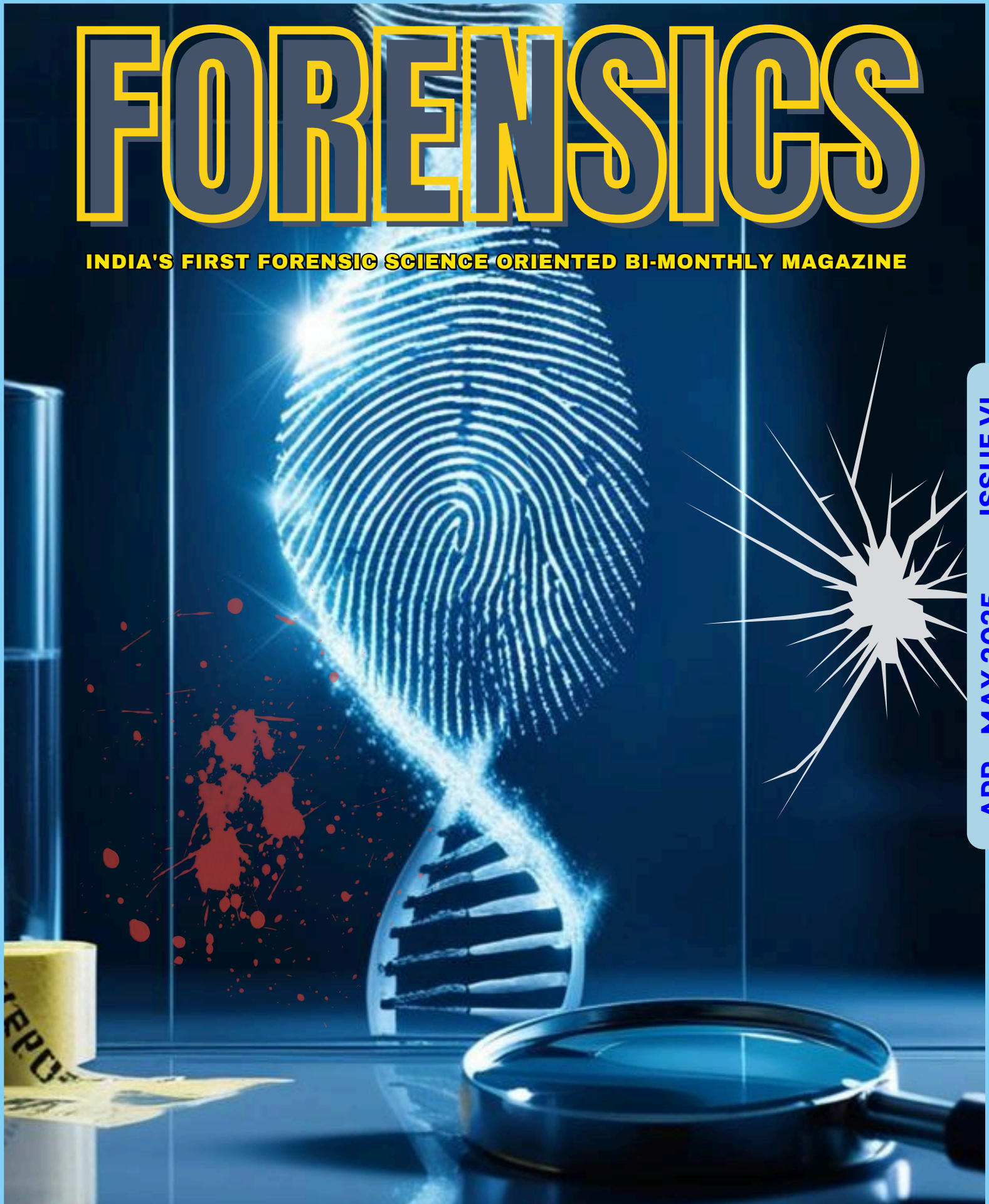


FORENSICS

INDIA'S FIRST FORENSIC SCIENCE ORIENTED BI-MONTHLY MAGAZINE

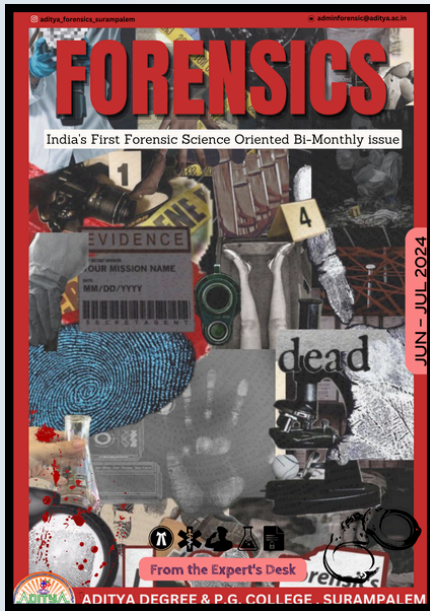
ISSUE VI

APR - MAY 2025



ADITYA COLLEGE OF FORENSICS & CYBER SECURITY
SURAMPALEM, ANDHRA PRADESH

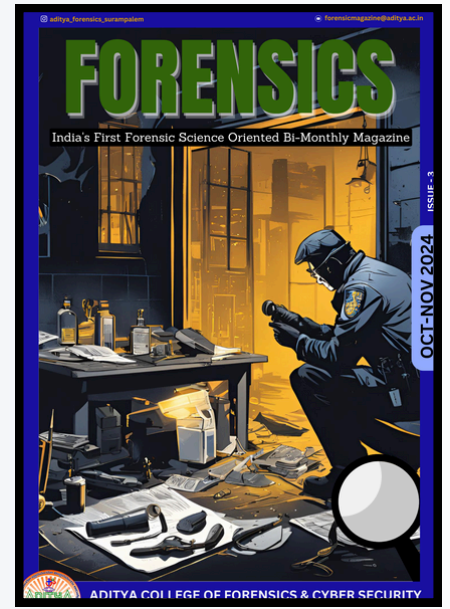
VIEW OUR PREVIOUS ISSUES



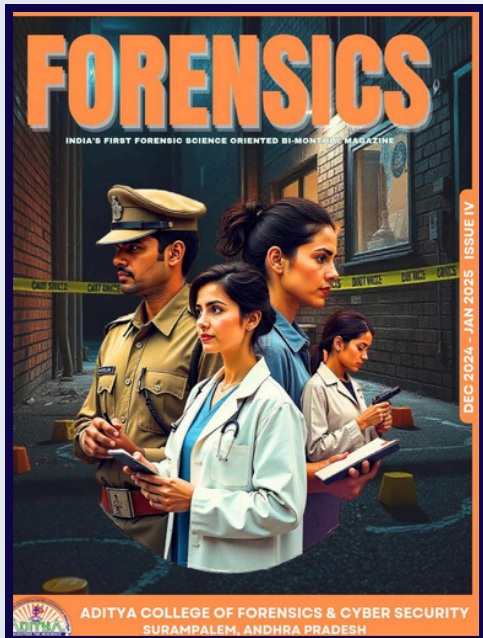
ISSUE I (JUN-JUL 2024)



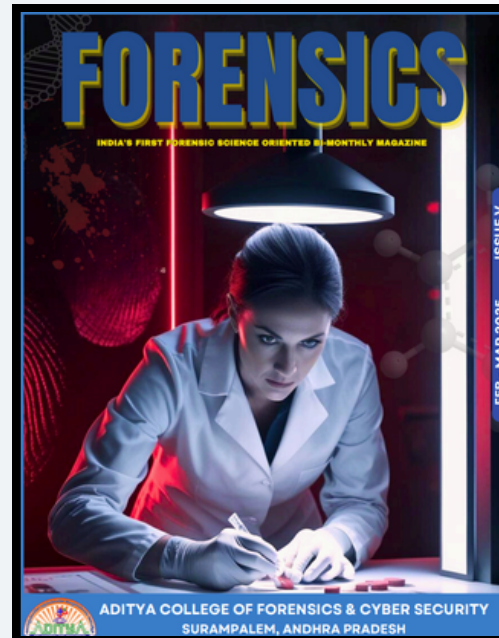
ISSUE II (AUG-SEP 2024)



ISSUE III (OCT-NOV 2024)



ISSUE IV (DEC-JAN 2025)



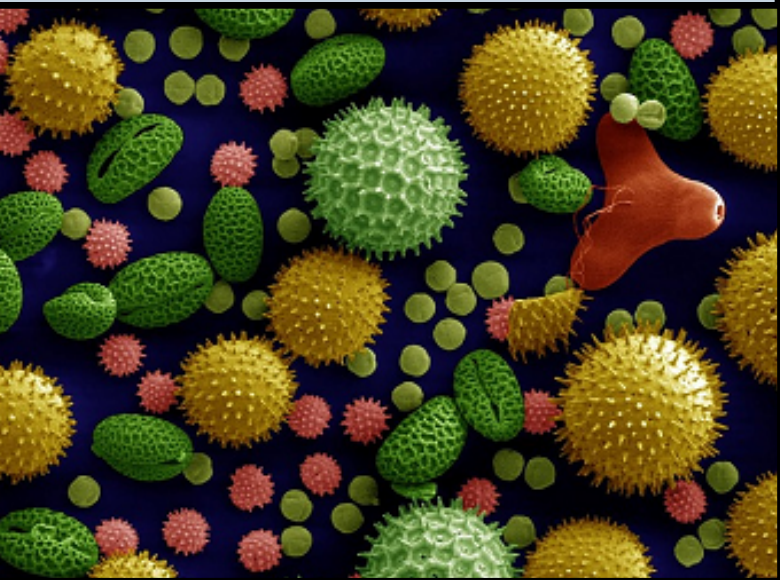
ISSUE V (FEB-MAR 2025)

Forensics Magazine: 2025

CONTENTS

Hacked by Light: How Visible Light Communication Can Be Used to Steal Your Data 09

Pollen - tell prosecution: when plants spill the tea on criminals 17



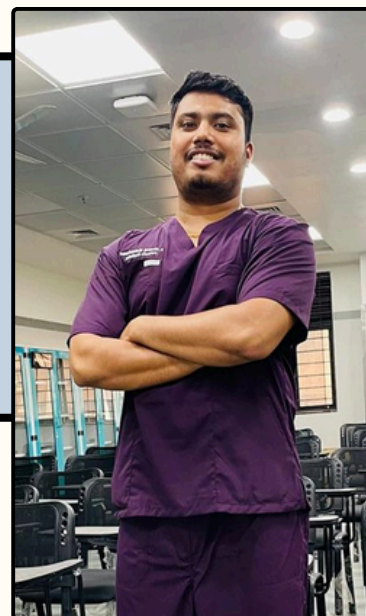
Forensic Applications of 3D-Printed Chemical Sensors in Crime Scene Investigation 38

Biohackers and Data Bandits: The Rise of DNA-Based Cybersecurity Threats 42



“Unveiling the Dead to Serve the Living- A Young Forensic Expert's Path to the Truth”

An interview with **“Dheeraj Maheshwari”** 20



Cybersecurity in the Cloud: Risks and Resilience 25

Hidden in the Firmware: Attacks and Evidence Below the OS Level 29



Emotional Malware: From Empathy to Exploits 50

Delayed Evidence and Forensic Advancements in POCSO-Related Cases 58

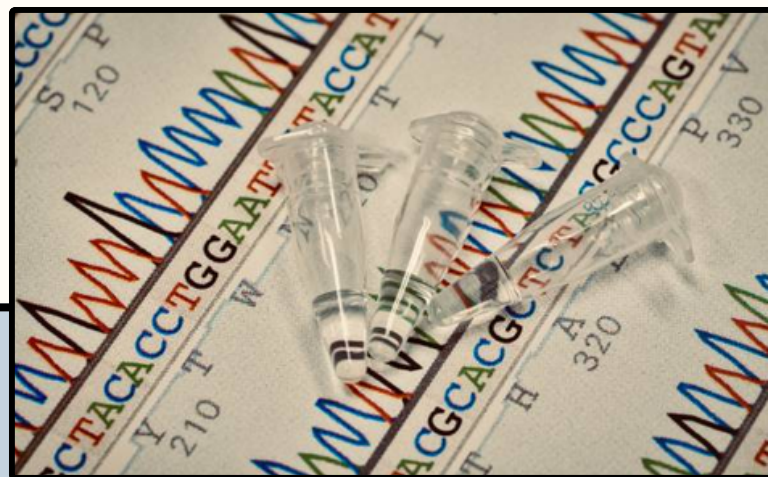
Crime in the Sky: The New Age of Satellite Cyber Intrusions 62

CONTENTS

Beyond DNA: The Rise of Epigenetic Markers in Forensic Science **69**

Digital Domestic Violence: Emerging Threats of Spyware in Relationships **71**

Case study on Death of Baby Theresa (2009)- Solved Through DNA Evidence **81**



VANTA Handheld XRF Analyzer by Evident Scientific **85**



Prepare Yourself -UGC NET & FACT **87**

UGC-NET PAPER 1: QUESTION BANK **91**



FROM THE LEADERSHIP TEAM



Dr. N. Sesa Reddy

**CHAIRMAN - ADITYA EDUCATIONAL
INSTITUTIONS**



Dr. N. Satish Reddy

**VICE CHAIRMAN - ADITYA
EDUCATIONAL INSTITUTIONS**

"Issue 6 continues to showcase thought-provoking contributions from students, educators, and experts, delving into emerging trends, innovations, and enduring challenges in the field of forensic science. With a renewed focus on discovery, collaboration, and the sharing of knowledge, this edition aims to motivate and empower both established professionals and the next generation of forensic scientists. We express our heartfelt appreciation to everyone who contributed to this edition. Together, let us continue to shape and advance the future of forensic science."

"I am honored to present the sixth issue of India's pioneering bi-monthly forensic science magazine, building on the remarkable response to our earlier editions. I extend my heartfelt gratitude to the Department of Forensic Science for its continued leadership and vision in driving this initiative forward. With every issue, we aim to promote innovation and excellence in forensic science education and practice across the country. This edition features compelling contributions that spotlight the latest advancements and evolving trends in the field."

FROM THE EDITORIAL DESK



Vilas Anil Chavan
Editor-in-Chief

Welcome to the Issue VI of India's First Bimonthly Forensic Science Magazine!

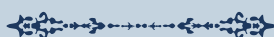
Following the enthusiastic response to our previous editions, we are excited to bring you the latest updates and innovations in forensic science. This issue features insightful articles on DNA analysis, digital forensics, forensic psychology, questioned documents, and more—including emerging topics like cybercrime, crime scene reconstruction, and trace evidence. With contributions from students, educators, and professionals, this edition reflects our shared commitment to advancing forensic science education and practice across India.

Thank you for joining us—let's continue to explore and evolve the science behind justice.



As Editorial Head, I'm thrilled to present the issue VI of our magazine, continuing our commitment to delivering top-notch content in forensic science. Within these pages, you'll find cutting-edge research, expert perspectives, and the latest breakthroughs—from DNA analysis and digital forensics to crime scene investigation and forensic psychology. This edition also brings you real-world case studies, policy developments, and career guidance, ensuring you stay informed about the field's rapidly evolving landscape. Your continued support inspires us to push the frontiers of forensic knowledge.

Thank you for being an essential part of this journey—together, we're shaping the future of forensic science.



BVSS Udaynadh
Editorial Head

Meet The Team



Internal Editors



Aanchal Sakarkar
Faculty of Forensic
Managing Editor



Surbhi Athiya
Faculty of Forensic
Creative Editor



Thushar K.C
Faculty of Forensic
Co- Editor



Kathu Raj
Faculty of Forensic
Co- Editor

External Editors



Tejaswi Reddy
Certified Forensic
Expert & Founder -
Key Forensics,
Hyderabad



Nivedhetha Rajendran
Research Scholar -
Amity Ins. of F.Sc.,
Noida



Dr. Kanika Aggarwal
Asst. Professor (Law)
SRM University Delhi,
Haryana



Heenal Mehta
Asst. Professor (Forensics)
Parul University,
Ahmedabad

Would You Like To Join Our Team ?

Send your research profile along with request letter to
forensicmagazine@aditya.ac.in

Contributors



Anjana



Harshit Prajapati



Drashti Nayak



Karnaa Thaker



Vinisha Solanki



Parvesh Sharma



Pooja Sharma



Dr. Thakar Akash



Mr. Mohammed Suhail A



Yamini Parmar



Mr. Kiran Dodiya



Dr. Kapil Kumar



Mr. Kashyap Joshi



Mr. Aditya More



Ms. Bhumika Doshi



Omi Chauhan



Aanchal Sakarkar



Surbhi Athiya



Aashtha Tiwari



Sanskriti Verma

HACKED BY LIGHT: HOW VISIBLE LIGHT COMMUNICATION CAN BE USED TO STEAL YOUR DATA

Author - Harshit Prajapati, Drashti Nayak, Kiran Dodiya, Dr. Kapil Kumar

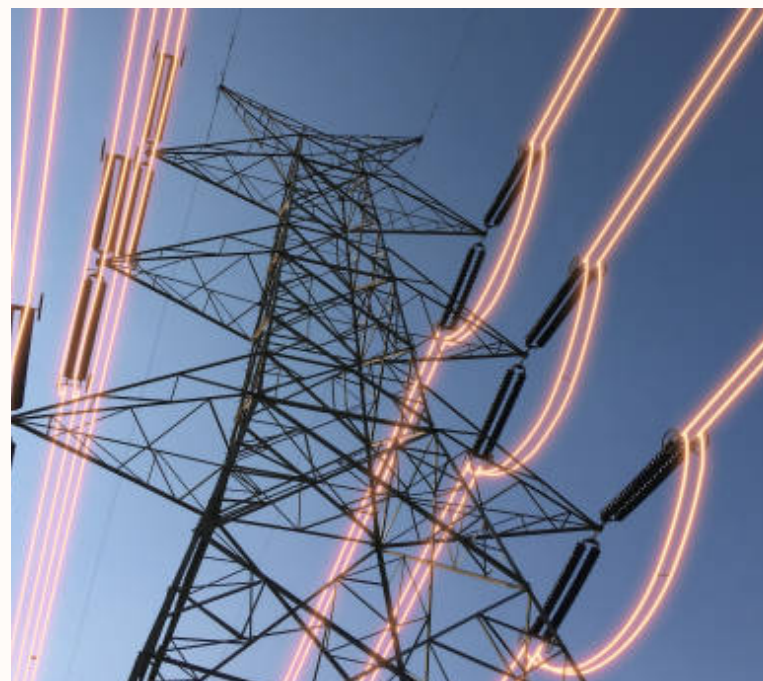
Introduction

Visible Light Communication (VLC) is a technique to send data by light, which provides security issue due to the visibility of signals which could be sniffed easily. VLC, with features such as, high data rate, high-intensity radiation makes it stand out, nevertheless-- It gets hackable and data thief. And this is what this introduction, and this introduces the contents below. (Lotfy Rabeh et al., 2007). Visible Light Communication (VLC) is a new optical wireless communication technology that transmits data by high-speed modulated Visible light signals. Visible Light Communication (VLC) — VLC uses the visible light spectrum (400-800 THz) to transmit data over a network. Modulated intensity of light signals from a turned-on and off common LED bulb is generally used to convey the information in a VLC system. The photodetectors on the receiving device pick up these signals and convert them into electronic signals. Lastly, a computer program reads these electrical signals and transforms it to a human-readable format.

One of its most well-known forms is Li-Fi (Light Fidelity), which provides high-speed wireless internet access using light instead of radio waves. Because light cannot pass through walls, VLC-based systems offer a degree of natural security that makes them attractive for use in sensitive environments like hospitals, aircraft cabins, or military installations. Additionally, VLC doesn't interfere with radio-based systems, making it ideal for places with strict RF regulations. Another advantage of VLC is that it can be integrated into existing lighting infrastructure, meaning overhead LED lights in homes, offices, and public places can double as communication hubs without needing extra wiring or antennas. VLC also supports very high bandwidth, allowing for faster data transfer rates compared to some traditional wireless methods. There are also some limitations. Because it relies on line-of-sight or near-line-of-sight conditions, any physical obstruction between the transmitter and receiver can block communication.

What is Visible Light Communication?

Visible light communication (VLC) is a wireless method that enables high-speed transmission of data with visible light. Visible Light Communication (VLC) is a form of wireless communication technology that uses visible light that the part of the electromagnetic spectrum between (380 nm and 750 nm) to transmit data, instead of using traditional radio frequencies like Wi-Fi or Bluetooth. VLC leverages light-emitting diodes (LEDs) as transmitters and photodetectors or image sensors as receivers. VLC works by rapidly switching the LED light on and off at incredibly high speeds millions of times per second and which is far too fast for the human eye to perceive. These quick changes in light intensity can be modulated to represent digital data (like 1s and 0s). VLC can be used in a wide variety of applications.



How VLC works?

Visible Light Communication (VLC) works by transmitting data using visible light, primarily through Light Emitting Diodes (LEDs). The core principle behind VLC is light modulation. The process of varying the intensity of light in a controlled way to encode information. These changes in light intensity are so rapid that they are imperceptible to the human eye, meaning normal lighting conditions are maintained while communication occurs in the background(Communication Technology | ShareTechnote, n.d.).

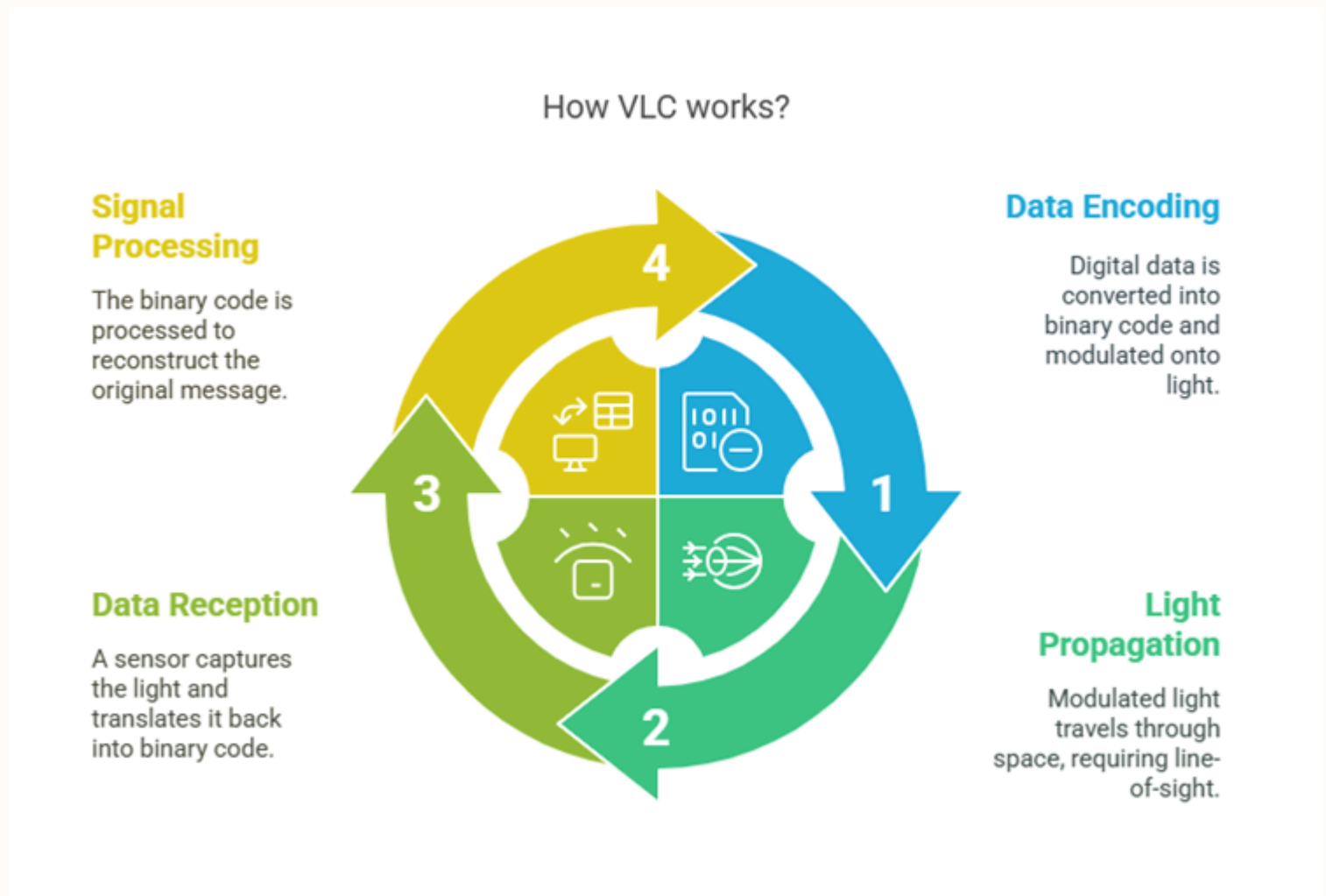


Fig: Shows Working of VLC

1. Data Encoding and Transmission (LED as Transmitter):

The process begins with digital data—such as a file, message, or internet signal—that is converted into binary code (a series of 1s and 0s). This binary data is then used to modulate the LED light, meaning the LED is turned on and off at high speed to represent the binary values.

For example:

1. A brief flash might represent a binary "1"
2. A pause or absence of light could represent a "0"

This isn't visible because the modulation speed can reach millions of cycles per second (MHz). The LED continues to function as a light source, but it's also acting like a tiny, high-speed data transmitter.

2. Light Propagation (Medium for Data Transfer):

Once the LED emits this modulated light, it travels through space in the same way any light would in a straight line unless reflected or diffused by surfaces. VLC usually requires a line-of-sight (LoS) path or near-LoS, although advanced systems may use reflected light to maintain communication. Unlike radio signals, visible light does not penetrate walls, which limits the range but also adds a layer of security since the signal is confined to a room or space.

3. Data Reception (Photodetector or Image Sensor as Receiver):

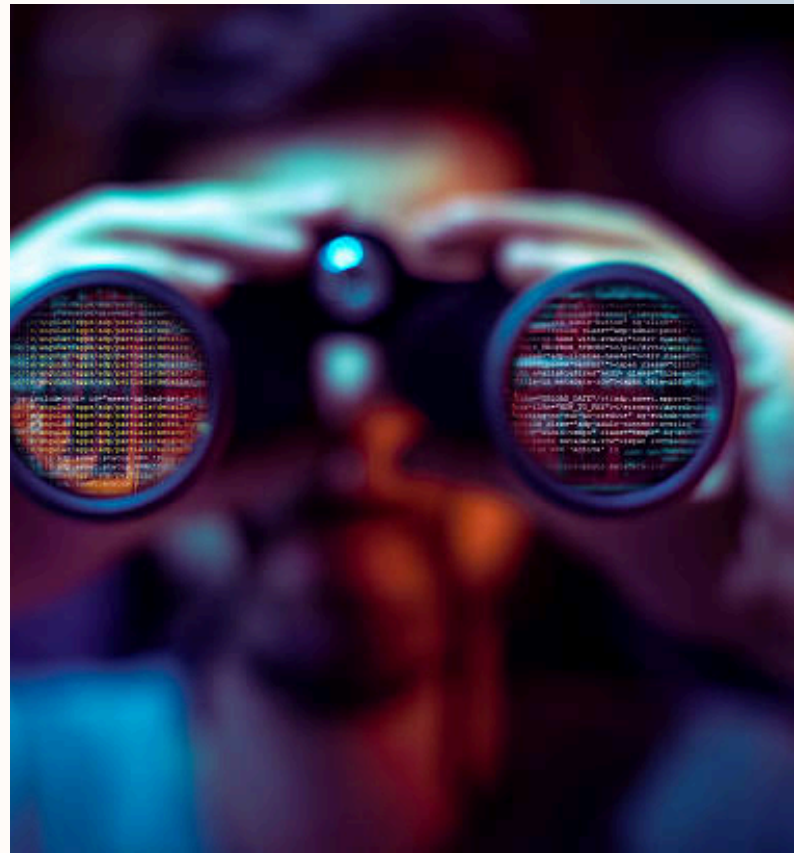
A photodetector (such as a photodiode) or a camera sensor captures the incoming modulated light. These devices are sensitive to light intensity and capable of detecting rapid changes. The receiver records the variations in brightness and translates them back into binary code essentially reversing the modulation process. For instance, if a camera detects a high-intensity flash, it interprets that as a "1"; no flash might be read as a "0." This data is then processed by a microcontroller or computer system to reconstruct the original message or signal (Yang et al., 2022).

4. Signal Processing and Output:

It is converted back into usable information whether that's internet data for a browser, a message for a device, or commands for an IoT system. The entire cycle of encoding, transmitting, receiving, and decoding happens extremely fast, allowing for real-time data transmission at high speeds, sometimes exceeding Gbps (Gigabits per second).

How Visible Light Communication Can Be Used to Steal Your Data?

Visible Light Communication (VLC), a method of transmitting data using visible light typically from LEDs has gained popularity due to its speed and efficiency. It also introduces unique cybersecurity risks. There is a way that VLC can be exploited to steal data is through the manipulation of LED indicators on devices such as computers, routers, or keyboards.



There is One way that Malware installed on a device can control these LEDs, causing them to flicker in patterns that represent binary data. While the flickering may be imperceptible to the human eye, it can be captured by a remote camera or optical sensor positioned within the line of sight, such as a drone outside a window. Once captured, the light signals can be decoded to reveal the stolen data, even from air-gapped systems with no internet connection. There is a second method that involves injecting malicious commands into smart devices using modulated light. Many Internet of Things (IoT) devices are equipped with light sensors or ambient light detectors. An attacker can aim a laser or modulated flashlight at these sensors to transmit specially crafted signals that the device interprets as legitimate input. This form of attack can be used to reconfigure systems or execute unauthorized commands remotely. These techniques demonstrate that VLC while promising for communication, can also be a serious vector for data exfiltration and cyberattacks. As such, it's important to implement preventative measures such as disabling unnecessary LEDs, blocking line-of-sight access to critical equipment, and monitoring devices for unusual optical activity([Solved] With Reference to Visible Light Communication (VLC) Technolo, n.d.).

How VLC Can Be Used to Steal Data – Step-by-Step Breakdown.

Step 1: Planting Malware in the Target System:

The first step in a VLC-based data theft attack is compromising the target device or network. This typically involves an attacker installing malware on the victim's computer, server, or IoT device. The malware could be introduced through phishing emails, malicious USB drives, social engineering, or exploiting system vulnerabilities. This device may be part of a high-security, meaning it has no direct internet access. The malware is specifically designed to control or manipulate the LED indicators on the device (such as those on the Ethernet port, keyboard, or status lights) without alerting the user

Step 2: Data Encoding – Converting Information into Light Patterns

There is once a malware is active on the system, it begins the process of data encoding. This means it selects specific data that such as typed passwords, files, encryption keys, or other sensitive information and converts it into a binary format (1s and 0s). This binary data is then used to control how the device's LEDs flicker. For instance, a short flicker might represent a binary "1", and no flicker for a short time might represent a "0". These flickers occur at a frequency too fast to be noticed by the human eye, making the attack invisible in plain sight. The LED lights now become a covert transmitter, silently sending data through light pulses.

Step 3: Data Transmission

In this Step, the infected device begins to transmit data optically. The flickering LED, controlled by the malware and it's emitting the patterns of light corresponding to the encoded data. This transmission can happen over hours or even days that depending on the amount of data and how steal the attacker wants to be. The attacker must be able to receive the light and either from direct line of sight or by using reflective surfaces. Some researchers have demonstrated how this light can be captured from hundreds of meters away, So even from outside a building, using a camera or a light sensor like a photodiode(Park et al., 2023).

Step 4: Data capture:

In this step, the attacker's doing to capture the light signal. This is done using optical devices such as a high-speed camera, telescope, or a drone equipped with a light sensor. These devices are positioned to have a view of the LED light source. There is even if it's just a tiny indicator. The camera records the blinking sequence of the LED over time. Because the attacker knows the encoding scheme that such as how fast the light flickers for "1" vs. "0". the recorded video or light signal can later be processed to extract the original binary data.

Step 5: Data Decoding:

In this step, after capturing the light signal, the attacker must decode the data. This involves analyzing the recorded light patterns, translating the blinking into binary code, and then converting that binary code back into readable data. Specialized software can be used to process the footage frame by frame, identify the light intensity changes, and reconstruct the original message or file. At this point, the attacker has successfully stolen sensitive information without any network access and just by watching the light emitted from the target system



Step 6: Reverse VLC (Sending Commands via Light):

In this step, Attackers can also use VLC to send data into a target system. For example, if a device has a light sensor or camera as in many IoT devices, smart assistants, or industrial sensors. Attackers can use a laser pointer or modulated light source to flash encoded commands toward the device. The sensor interprets these light pulses as input, allowing attackers to inject commands, change configurations, or even trigger actions again, without a wired or wireless network connection(Barati et al., 2025).

.(Perimeter Security vs Zero Trust: Paving the Way for Cybersecurity Transformation | Tufin, n.d.).



Fig: Shows steps in VLC Based attacks

Protection and Prevention in the Context of VLC-Based Attacks:

As Visible Light Communication (VLC) can be exploited to exfiltrate sensitive data from devices via seemingly harmless components like LED indicators, it becomes essential to adopt a layered defence approach. Protecting systems from VLC-based data theft involves physical, procedural, software, and environmental countermeasures. Since these attacks often rely on manipulating visible light to encode and transmit information, the first step is to minimize or block any potential light-based output from sensitive systems. One of the most effective protective steps is physically covering or disabling unnecessary LEDs, especially in high-security or air-gapped environments. Many hardware components, such as Ethernet ports, routers, keyboards, and hard drives, feature blinking lights that can be used maliciously as optical transmitters. Security-conscious organizations can use opaque tape, light-diffusing covers, or hardware configurations to restrict LED behaviour.

2. Light Propagation (Medium for Data Transfer):

Once the LED emits this modulated light, it travels through space in the same way any light would in a straight line unless reflected or diffused by surfaces. VLC usually requires a line-of-sight (LoS) path or near-LoS, although advanced systems may use reflected light to maintain communication. Unlike radio signals, visible light does not penetrate walls, which limits the range but also adds a layer of security since the signal is confined to a room or space.

3. Data Reception (Photodetector or Image Sensor as Receiver):

A photodetector (such as a photodiode) or a camera sensor captures the incoming modulated light. These devices are sensitive to light intensity and capable of detecting rapid changes. The receiver records the variations in brightness and translates them back into binary code essentially reversing the modulation process. For instance, if a camera detects a high-intensity flash, it interprets that as a "1"; no flash might be read as a "0." This data is then processed by a microcontroller or computer system to reconstruct the original message or signal (Yang et al., 2022)

Case Study: The Air-Gapped Data Leak

There is a high-security research firm, "Alpha Corp," which protects its sensitive R&D data on an air-gapped network, completely isolated from external connections. Despite robust physical and network security, assume a piece of sophisticated malware was covertly installed on a workstation within this secure zone. Unable to use standard network or USB channels for exfiltration, this malware employs an unconventional "Hacked by Light" technique. It targets the small status LEDs found on the workstation's keyboard, such as Caps Lock or Num Lock. The malware collects small fragments of sensitive data, encodes them into binary sequences, and then subtly modulates the intensity or flickering frequency of these LEDs, changes potentially too faint or rapid for a human to notice reliably. An attacker, positioned outside the facility but with a direct line of sight (perhaps through a window) uses a sensitive optical sensor or camera coupled with a telescope to record these minute light variations over time.

Specialized software then filters out ambient light noise and decodes the flickering patterns back into binary, slowly reconstructing the stolen data snippets. This purely hypothetical scenario illustrates how existing hardware components, not typically viewed as communication channels, could theoretically be repurposed to bypass stringent air-gap security, highlighting the need for awareness of unconventional data exfiltration methods, even though such an attack would face significant practical challenges like extremely low data rates, line-of-sight requirements, and environmental interference.



Conclusion:

Visible Light Communication (VLC) can be exploited for data theft primarily through covert channel exfiltration from compromised devices. Malware residing on a target system can encode stolen sensitive information, such as passwords, files, or user activity, into subtle, high-frequency flickers of light emitted by the device's screen, notification LEDs, or even keyboard backlights. An attacker positioned within line-of-sight, equipped with a simple optical sensor or camera, can then capture these imperceptible light modulations and decode the data being transmitted. This method bypasses traditional network security monitoring and can be particularly effective in air-gapped or highly secured environments where radio-frequency communications are restricted, turning ubiquitous light sources into potential conduits for silent data leakage.

References

- Barati, M., Kahani, N., Coston, I., Plotnizky, E., & Nojournian, M. (2025). Comprehensive Study of IoT Vulnerabilities and Countermeasures. *Applied Sciences* 2025, Vol. 15, Page 3036, 15(6), 3036. <https://doi.org/10.3390/AP15063036>
- Communication Technology | ShareTechnote. (n.d.). Retrieved 8 April 2025, from https://www.sharetechnote.com/html/Communication_Light.html
- Khan, L. U. (2017). Visible light communication: Applications, architecture, standardization and research challenges. *Digital Communications and Networks*, 3(2), 78–88. <https://doi.org/10.1016/J.DCAN.2016.07.004>
- Lotfy Rabeh, M., Gabr, M. I., & Hosny, T. (2007). Data Transmission via Visible Light Communication (VLC) Technique. *International Journal of Innovative Research in Science, Engineering and Technology* (An ISO, 3297(9). <https://doi.org/10.15680/IJIRSET.2016.0509133>
- Paikaray, B. K., Dash, G. P., & Modi, N. K. (n.d.). Cyber Attacks and Counter Measures: User Perspective.
- Park, J., Yoo, J., Yu, J., Lee, J., & Song, J. S. (2023). A Survey on Air-Gap Attacks: Fundamentals, Transport Means, Attack Scenarios and Challenges. *Sensors* 2023, Vol. 23, Page 3215, 23(6), 3215. <https://doi.org/10.3390/S23063215>
- Perimeter Security vs Zero Trust: Paving the Way for Cybersecurity Transformation | Tufin. (n.d.). Retrieved 9 February 2025, from <https://www.tufin.com/blog/perimeter-security-vs-zero-trust-cybersecurity-transformation>
- [Solved] With reference to Visible Light Communication (VLC) technolo. (n.d.). Retrieved 8 April 2025, from <https://testbook.com/question-answer/with-reference-to-visible-light-communication-vlc-5fccd6e502d6075be756d9fa>
- Yang, Y., Ding, S., Plovie, B., Li, W., & Shang, C. (2022). Soft and Stretchable Electronics Design. *Encyclopedia of Sensors and Biosensors: Volume 1-4, First Edition*, 1–4, 258–286. <https://doi.org/10.1016/B978-0-12-822548-6.00087-X>

ABOUT THE AUTHOR

Mr. Harshit Prajapati

Integrated M.Sc. Cyber Security and Forensic Science,
Gujarat University, Ahmedabad, Gujarat, INDIA



Ms. Drashti Nayak

Integrated M.Sc. Cyber Security and Forensic
Science, Gujarat University, Ahmedabad,
Gujarat, INDIA



Kiran Dodiya

(Research Scholar, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



POLLEN - TELL PROSECUTION: WHEN PLANTS SPILL THE TEA ON CRIMINALS

Author - Anjana

Abstract

FORENSIC PALYNOLOGY is basically CSI:

Plant edition – where tiny pollen grain help crack big cases. This article dives into how forensic experts use pollen as nature's receipts, the challenges they face and some real – life cases. While pollen is not taken seriously in courts, it keeps providing that the smallest clues can expose the biggest secret.

KEYWORDS: Forensic palynology, Evidence, microscopy, tiny ,exine.



Fig: Shows Pollen grains

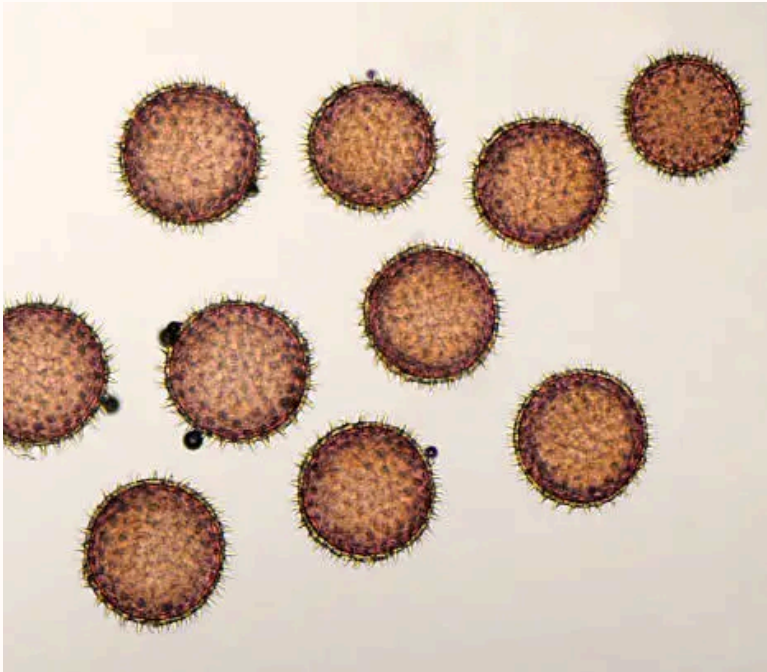


Fig: Shows microscopic structure of Pollen grains

Introduction:

Pollen grains are basically nature's recipes small yet resilient. These little guys can survive thousands to millions of years, ensuring they don't simply disappear. That's why forensic scientists use them to track criminals, solve cold cases and even uncover historical mysteries. This article dives into the wild world of forensic palynology. Read on to learn how science converts flower power into real evidence.

Pollen :The tiny snitch that never lies:

Forensic palynology is basically the study of Pollen, spores and other plant particles which helps to solve crime.

POLLEN GRAIN :

- It is known to be male gametophyte.
- Generally spherical measuring about 25 - 50 micrometres in diameter.
- Wall or covering of pollen grain is Sporoderm [Exine and Intine]

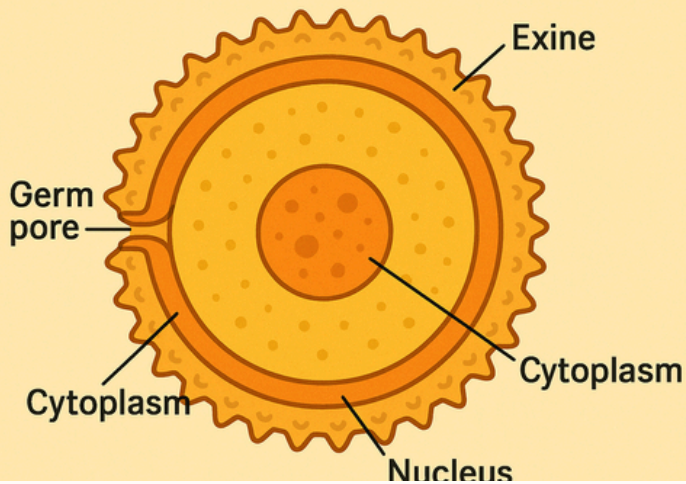
Exine

- a) Thin ,sculptured or smooth.
- b) Made up of sporopollenin ,it is resistant to chemical and biological decomposition so the pollen wall is preserved for long periods in fossil deposits.

Intine

- a) Thin , Elastic
 - b) Emergence out pollen tube from germ pore during germination.
- Germ spore -Thin areas of exine germinate furrows are elongated.

POLLEN GRAIN DIAGRAM



Since pollen is highly durable and unique to specific geographic location, it can connect suspect to crime scenes, track movement and even reveal concealed brutal sites .You can think of it as nature's own fingerprint, quietly keeping records that criminals can't wipe away.

From crime scene to courtroom :The pollen process:

1.Crime scene collection:

Investigators collect pollen samples from various sources, including clothing, footwear, vehicles and even the lungs of victims.

2. Microscopic analysis:

Forensic Palynologists utilize advanced microscopes to analyze or identify pollen grains, distinguishing them by their unique shape, texture and patterns. Every plant's species process a unique Pollen profile.

3.Comparison and Identification:

The collected pollen is compared to known pollen databases or regional plans to determine its origin. As it helps to pinpoint where a suspect or object has been.

4.Geographic and seasonal mapping:

That various plants emit Pollen in particular areas and during certain times of the year. So, experts use this data to estimate where a crime occurred.

6.Courtroom presentation:

Forensic pathologists take the stand to clarify how pollen evidence links a suspect to the crime scene.

Pollen in laboratory:

1.SAMPLE COLLECTION

2.CHEMICAL PROCESSING

- HCl dissolves carbonate
- HF removes silicate minerals
- Acetolysis dissolves cellulose , leaving pollen exine intine.

3.SIEVING AND CENTRIFUGATION

Sample filtered through fine sieves and centrifuged to concentrate pollen grain.

4.MOUNTING AND MICROSCOPY

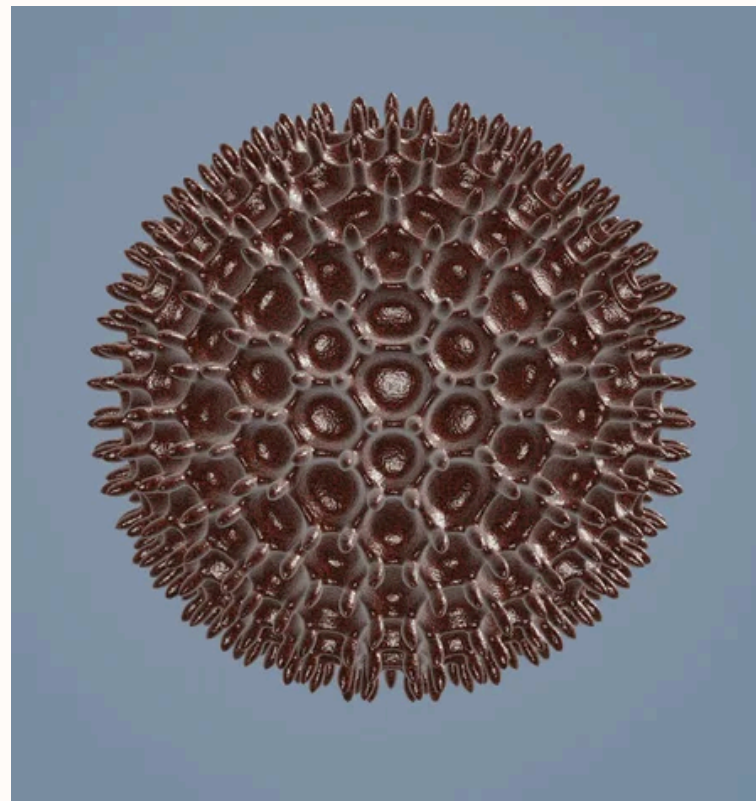
Pollen residue is mounted on slides using glycerine and silicon oil. Followed by examination under a light microscope for detailed surface and structure analysis.

5.IDENTIFICATION AND COUNTING:

Pollen grain are identify by comparing their size, shape and Surface with reference collections. A minimum count e.g., 300-500 grains.

6.DATA INTERPRETATION:

The results are used to reconstruct past climates, vegetation history, or forensic investigations.



Pollen Under Pressure: The Conclusion: Struggle to Stick in Forensics

1.REQUIRES HIGHLY TRAINED EXPERTS:

For proper pollen identification need of specialised knowledge and experienced in botany and microscopy but only few forensic palynologist are available worldwide.

2.CONTAMINATION RISKS

Pollen is small and readily spread through, making contamination a major worry .Investigators must be of utmost caution to avoid accidental pollen transfer during evidence gathering.

3.LIMITED POLAND DATABASES

Pollen databases are not as extensive as DNA and fingerprint. It makes it more difficult to match samples fast. Pollen in some locations has not been adequately documented.

4.ENVIRONMENTAL FACTORS CAN CHANGE POLLEN EVIDENCE:

Wind ,rain and animal activity can transport pollen from one location to another, thereby confusing investigations.

Pollen Proven Cases:

The Bank Robber Caught by a Houseplant

In this bizarre incident, a European bank robber believed he had executed the ideal heist— until forensic palynologists entered the scene.

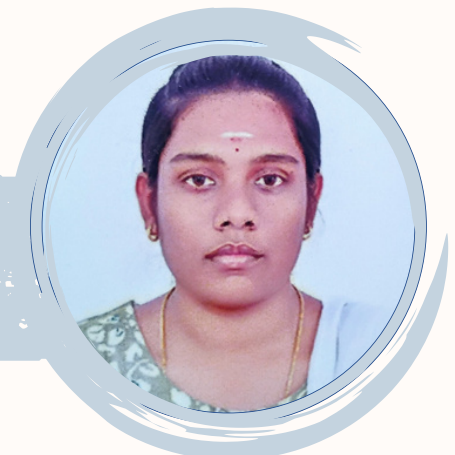
Following the robbery, authorities discovered microscopic pollen particles on the suspect's attire and escape bag. Upon examination, the pollen was identified as originating from a rare houseplant—one that was not prevalent in the area. Investigators tracked the plant species and determined that the only nearby location where this plant was present was within the suspect's very own residence!

Forensic palynology, despite its diculties, shows that even the smallest pieces of evidence can reveal significant secrets. If pollen, which is almost invisible to the naked eye, can help solve crimes, what other unnoticed clues might we be missing in forensic science?

Reference:

- Mildenhall DC, Wiltshire PE, Bryant VM. Forensic palynology: why do it and how it works. Forensic Sci Int. 2006 Nov 22;163(3):page-163-172, 2006 Aug 21. future prospects: A review", Saudi Journal of Biological Sciences, Volume 27. page1-5, Issue 5
- Dallas Mildenhall (2015), Solving Crimes with Pollen, One Grain of Evidence at A Time, April 25, page1-4.
- Bryant, V. M. Mildenhall, D. C. 1998. Forensic palynology: a new way to catch crooks. Association of Stratigraphic Palynologists Foundation Contribution, page145-155, Series 3.
- Paramjeet Cheema (2014), Use of pollen fingerprints as a tool in forensic science, Punjab university, page 1-3. International journal of current research, Vol.6 Issue 3.
- Anthony R Wood (2021), The secret life of pollen: It makes you sneeze, itches your eyes and can solve crimes, page 2-4, June 10,
- Kumari, Mayuri & Singh Sankhla, Mahipal & Nandan. Manisha & Sharma, Kirti & Kumar, Rajeev (2017), "Role of Forensic Palynology in Crime Investigation", Vol. 5, Issue 3, Page 2-11

ABOUT THE AUTHOR



ANJANA

I B.Sc. Forensic Science.
Srinivasan College of Arts and Science,
Perambalur, 621212

“Unveiling the Dead to Serve the Living- A Young Forensic Expert's Path to the Truth”

An interview with “Dheeraj Maheshwari”

***MBBS, PGDCMF, MD (Forensic Medicine), Assistant Professor, Autopsy Surgeon,
Pacific Medical College and Hospital, Udaipur, Rajasthan, India.***

What made you or motivated you to take Forensic Medicine & Toxicology as your Carrier?

I was initially interested in top clinical branches like Radiology and Dermatology because of their better work-life balance and minimal patient interaction — especially considering the rising incidents of violence against doctors. I wasn't inclined toward core clinical fields like Medicine or Surgery due to the demanding hours and poor work-life balance.

As a middle-class, first-generation doctor, I couldn't afford to be completely dependent on family support. So, after MBBS, I took a drop to prepare for NEET-PG while simultaneously working as a Junior Resident in the Surgery department to support myself financially.

During the COVID pandemic, instead of continuing the cycle of repeated attempts, I chose MD in Forensic Medicine based on the rank I got. I felt it was a less explored but promising branch with potential job opportunities in both the government and private sectors as an Assistant Professor after postgraduation. That's why I ultimately decided to pursue Forensic Medicine.



Is there any role model inspired you in the context in Forensic Medicine?

I didn't have any specific role models who inspired me, but during my undergraduate days, I often observed the Medical Jurist at my college handling police personnel and various medicolegal cases. It appeared more interesting and distinct compared to other medical branches. Since I was not inclined toward clinical branches and was looking for a better work-life balance, I decided to pursue Forensic Medicine.

What is your vision regarding Forensic Medicine?

I didn't have any specific role models who inspired me, but during my undergraduate days, I often observed the Medical Jurist at my college handling police personnel and various medicolegal cases. It appeared more interesting and distinct compared to other medical branches. Since I was not inclined toward



clinical branches and was looking for a better work-life balance, I decided to pursue Forensic Medicine.

What is your thought on the research and development in the field Forensic Medicine in India whether we have infrastructure and funding?

Research and development in the field of Forensic Medicine in India remains grossly neglected. Despite the critical role this specialty plays in the criminal justice system, there is negligible original research being carried out. Government funding for forensic medicine research is minimal, and most institutions lack dedicated infrastructure, resources, and incentives to promote academic or applied research in this domain.

Additionally, very few private medical colleges are authorised or equipped to conduct autopsies or handle medicolegal responsibilities. The burden of medicolegal work, including postmortems, age estimation, and injury certification, largely falls on overworked departments in government medical colleges, which are already under-resourced. Forensic medicine continues to be treated as a service branch rather than a field with potential for innovation, research, and development.

Without substantial investment, inter-departmental collaboration, and policy-level reforms, the field will continue to lag behind in both academic and practical relevance.

How is your experience so far in this field?

My experience in the field of Forensic Medicine has been a mix of excitement and frustration. During my residency, I genuinely enjoyed working on a variety of cases and found it fulfilling to contribute to the process of solving crimes through scientific analysis. Each case brought unique challenges and learning opportunities, and the work kept me intellectually engaged.

One of the positives was the good work-life balance I had during residency, which is often rare in medical specialties. However, despite the academic and practical satisfaction,

there were aspects that left me disheartened. The slow pace of the justice system and the lack of awareness about medicolegal principles among police personnel and even lawyers was a major concern. Many times, our efforts felt underutilised or misinterpreted due to systemic gaps.

Overall, while the field has immense potential, there's still a long way to go in terms of awareness, collaboration, and systemic support.



In this many years of your experience have you felt emotional overwhelmed by any incident?

Yes, there have been moments in my medical journey that left me emotionally overwhelmed—incidents that I still carry with me.

One such moment was during my junior residency in the surgery department. It was a late-night emergency—a young boy came in with severe abdominal pain. I examined him and immediately called the consultant. He said he would arrive in an hour. Unfortunately, before he could make it, the child collapsed right in front of me. That sense of helplessness—of not being able to do anything in time—still haunts me. Another deeply disturbing experience was while working as an RMO in a private hospital. A five-month-old baby was admitted with complete kidney failure. His mother sat beside him, quietly waiting for him to die—she had another child to care for and no hope left. I was the duty doctor that night, unable to do anything except witness that unbearable grief. It shook me to the core.

Then, during my PG residency, I came across a chilling case—a father, under the influence of alcohol, killed his own son with fists and foot simply because the child asked for food money. The father remained unaware of what he had done until he sobered up in the morning. His body was brought for post mortem, and there were many injuries over the child's body. That case made me question the depths of human behavior and the fragility of life. These incidents remind me that behind every case or file is a story—raw, painful, and often unforgettable.

How do you approach cases involving suspected child abuse?

Treating or attending to a child who has been abused is always an emotionally challenging experience. However, if a doctor is unable to regulate their emotions, it may lead to errors in examination and treatment, which could compromise the quality of care provided.

Can you throw light on recent advancement in forensic medicine?

Currently, there are no significant recent advancements in the field of forensic medicine. This is primarily due to the lack of basic tools, infrastructure, mortuary staff, and adequate funding. When fundamental requirements are unmet, it becomes unrealistic to expect any methodological or technological advancements.



As the time progress challenges will grow, what changes should be made in approach both medically and legally to stay relevant to the time?

Reforms are necessary in both medical and legal aspects. Medically, residents and postgraduate students in forensic medicine should be given comprehensive training and ample practical exposure. Legally, police officers and lawyers often lack adequate understanding of forensic medicine. Moreover, there is a considerable delay in judicial proceedings—autopsy reports submitted today are often taken up in court after 3 to 4 years, by which time the medical examiner may no longer recall case specifics, affecting the efficacy of their testimony.

Whether private players are contributing enough in the field of forensic medicine. How sure that they can maintain integrity?

Both private and government sectors are currently not contributing adequately to the development of forensic medicine. Private entities tend to avoid involvement due to the fear of liability in case of mishaps, which deters funding. Although private organizations can maintain professional integrity, there must be a government-appointed committee to oversee and regulate their activities.

Have you been pressured by any entity to work against your ethics how will you manage?

While I have not personally been subjected to external pressure, there have been high-profile cases where attempts were made to influence the outcome of forensic examinations.

Apart from conventional techniques what innovative methods would you suggest for Forensic Medicine to aid Justice?

Numerous such incidents occur regularly. For instance, in one case, a thief was allegedly beaten on the head with a bamboo stick. Bamboo fragments were discovered in his hair, yet the police claimed he had fallen from a building. Despite the physical

evidence, the police presented an implausible explanation, and the critical evidence was disregarded.



Do you think any other country have better practises or procedure in Forensic Medicine?

Countries such as the USA and the UK have more structured practices and procedures. In these nations, inquests can be conducted not only by the police but also by judges and coroners, which facilitates a more transparent and expedited examination process.

What is the role of Forensic Medical Examiner plays in examination of Organ Donar when deceased want to be pronounced dead?

There is an absence of standardized committees and protocols in most hospitals to formally declare death. Only a few premier institutes follow a systematic approach. This gap creates opportunities for illegal organ trafficking and the potential loss of viable organs for rightful recipients.

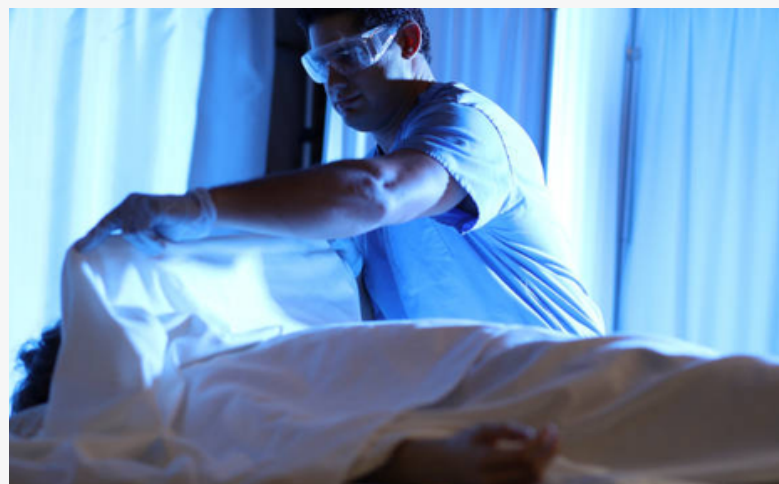
Have been involved in any exhumation what are the challenges you have faced was there any public clashes?

. I have participated in exhumation procedures, for which the government has outlined a clear protocol. The process must involve the district magistrate, police officials, a professional

videographer, and a forensic expert, and it should be conducted during daylight hours. Although public unrest can occur, such instances are not common.

Have you come across case with negative autopsy what factors contribute to the negative autopsy?

I have encountered numerous negative autopsies—cases in which the cause of death could not be determined. Examples include deaths from myocardial infarction or electrolyte imbalances in children, which are often difficult to detect. Delays in post-mortem examinations and viscera analysis by forensic science laboratories (FSLs) also contribute to inconclusive findings.



What is the present condition in the Government Forensic Medicine Department? Is Government funding enough?

As mentioned previously, the lack of infrastructure, funding, and strategic planning severely hampers the development of the forensic medicine department. Many mortuaries lack basic amenities such as running water, adequate staffing, proper tools, drainage systems, and ventilation. Cold storage facilities are overcrowded, and bodies are often stacked on top of one another, which is not only disrespectful to the deceased but also leads to a host of complications.

Through your interaction with police do u think they follow all the procedures, and will they maintain chain of custody while handling the evidence?

Resident doctors should be provided opportunities to gain hands-on experience with live cases. However, there is currently no structured system in India that allows for such academic training. I also strongly advocate for the inclusion of BAMS and BHMS graduates in the post-mortem examination process.

What are advices by you to students who wants to pursue in the field of Forensic Science?

Students will have significantly better opportunities if the government provides structured internships. involving live case analysis and if the infrastructure of forensic science laboratories is upgraded.

The government has already enacted a law mandating that crimes punishable with imprisonment of seven years or more must involve evidence collection by forensic experts. Unfortunately, this law is not yet being effectively implemented. Once it is enforced, the field of forensic science holds the potential to become a vital pillar of the justice system.



Dr. Dheeraj Maheshwari is a forensic medicine specialist, assistant professor, and passionate educator known for simplifying complex medico-legal concepts for students and the public alike. With an MD in Forensic Medicine and a growing social media presence of over 36,000 followers on X and over 28,000 followers on Instagram and over 3,000 followers on LinkedIn, he uses digital platforms to raise awareness about ethical medical practices, violence against doctors, and the realities of life in medicine. A demotivational speaker by choice and a realist at heart, Dr. Maheshwari is redefining how medical professionals engage with society - one sharp observation at a time.

INTERVIEWED BY
Mr. Thushar K.C and Miss. Kathu Raj
(Assistant Professor- Forensic Science)
Aditya Degree & P.G. College, Surampalem



Introduction

The rapid adoption of cloud computing architectures across industries has fundamentally transformed the modern IT landscape. By offering dynamic scalability, high availability, and cost-efficiency, cloud services have become integral to digital transformation strategies. However, these benefits are counterbalanced by an expanded threat surface and a redefined security perimeter. Cloud environments introduce unique security challenges that necessitate a paradigm shift in traditional information assurance frameworks. This article critically examines the principal cyber threats associated with cloud infrastructure and delineates strategies for enhancing cyber resilience within these distributed environments.

often arise from a lack of visibility or automated configuration management tools.

3. Insecure APIs

Cloud environments are highly dependent on APIs for automation, orchestration, and inter-service communication. Improperly secured APIs can become an attack vector for injection attacks, broken authentication, or excessive data exposure.

4. Insider Threats

Whether through malicious intent or negligent behavior, insiders with access to cloud workloads can bypass perimeter security controls, especially in environments where granular auditing is absent or insufficiently enforced.

5. Limited Visibility and Control

The abstraction layers within Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) models often reduce customer control over the underlying infrastructure. This can obscure real-time telemetry, complicating incident detection and forensic investigations.

Threat Vectors and Vulnerabilities in Cloud Ecosystems

Cloud infrastructures—particularly public and hybrid models—operate on a shared responsibility model that bifurcates security obligations between cloud service providers (CSPs) and customers. Failure to appropriately manage this division often leads to severe security incidents. Below are some of the predominant risk vectors:

1. Data Breaches and Unauthorized Disclosure

Data exfiltration remains a predominant risk in cloud-hosted systems. Breaches often result from insecure object storage services (e.g., AWS S3 buckets), inadequate access controls, or compromised API tokens. The exposure of personally identifiable information (PII) and regulated datasets can trigger legal and reputational consequences.

2. Misconfiguration and Oversight

Misconfigurations—such as open ports, unencrypted storage volumes, and unrestricted ingress/egress rules—are among the leading causes of cloud-based security failures. These



6. Ambiguity in the Shared Responsibility Model

A prevalent misconception among cloud consumers is that the CSP is responsible for all aspects of security. In practice, tenants must implement and maintain controls over data integrity, application logic, and identity management within the CSP's infrastructure.

Engineering Resilience: Mitigation Strategies for Cloud Security

Building cyber resilience in the cloud necessitates a defense-in-depth approach incorporating proactive threat detection, rigorous access governance, and rapid incident containment mechanisms. Key components include:

1. Identity and Access Management (IAM) Controls

Deploy fine-grained role-based access controls (RBAC) and enforce least privilege principles. Integrate multifactor authentication (MFA), conditional access policies, and session timeouts to mitigate unauthorized privilege escalation.

2. Encryption and Key Management

Implement full lifecycle encryption for data-at-rest and data-in-transit using AES-256 or stronger. Leverage Hardware Security Modules (HSMs) or cloud-native Key Management Services (KMS) for cryptographic key storage and rotation.

3. Continuous Monitoring and Threat Detection

Utilize Security Information and Event Management (SIEM) solutions and Cloud Security Posture Management (CSPM) tools to detect anomalous behavior and misconfigurations. Enable native logging (e.g., AWS CloudTrail, Azure Monitor) and integrate with SOC workflows for real-time analysis.

4. Vulnerability Assessment and Penetration Testing

Conduct periodic assessments using automated vulnerability scanners and adversary emulation tools. Penetration tests should simulate real-world attack vectors targeting cloud interfaces, IAM policies, and lateral movement techniques.

5. Incident Response and Business Continuity Planning

Design and routinely test incident response playbooks specific to cloud incidents. Ensure immutable backups across regions and implement disaster recovery orchestration to support failover and RTO/RPO compliance.

6. Third-Party and CSP Due Diligence

Vet CSPs for compliance with international standards (e.g., ISO/IEC 27001, SOC 2 Type II). Review service-level agreements (SLAs) for clarity on uptime guarantees, data handling procedures, and breach notification protocols.



Notable Case Studies: Cloud Security Breaches

1. Capital One Data Breach (2019)

In a landmark cloud breach, Capital One suffered the exfiltration of over 100 million records due to a misconfigured AWS Web Application Firewall (WAF). The attacker exploited a Server-Side Request Forgery (SSRF) vulnerability, gaining access to IAM credentials with excessive privileges. These credentials enabled the attacker to enumerate and download data from multiple Amazon S3 buckets.

- **Technical Lapse:** Inadequate IAM role segmentation and absence of SSRF protection.
- **Impact:** Exposure of Social Security Numbers (SSNs), bank account details, and customer data.

- Resolution: Capital One was fined \$80M and implemented enhanced cloud security posture audits.

2. Accenture Ransomware Attack (2021)

The LockBit ransomware group compromised Accenture's cloud infrastructure, allegedly exfiltrating 6TB of data. Although Accenture maintained operational continuity by restoring secure backups, the incident demonstrated how ransomware groups are actively targeting cloud-native workloads.

- **Attack Vector:** Likely exploited remote access vulnerabilities such as RDP or VPN misconfigurations.
- **Impact:** Theft of proprietary and client-related information; no confirmed operational disruption.
- **Lesson:** Emphasized the necessity of endpoint hardening, segmented network topologies, and rapid incident containment strategies.

Conclusion

Securing cloud ecosystems requires an evolved cybersecurity framework that extends beyond perimeter defense to encompass visibility, control, and resilience across distributed infrastructures. Organizations must adopt a cloud-native security strategy that integrates identity governance, real-time analytics, and secure DevOps practices. As threat actors become more sophisticated, resilience in cloud computing will depend not only on prevention but on detection, response,

and recovery capabilities aligned with both operational and regulatory requirements. With deliberate architecture, continuous monitoring, and strategic vendor partnerships, cloud computing can deliver not just agility, but trustworthy security.

References

1. Amazon Web Services. (2023). AWS security best practices. <https://docs.aws.amazon.com/security>
2. Cloud Security Alliance. (2020). The egregious 11: Top threats to cloud computing. <https://cloudsecurityalliance.org>
3. U.S. Office of the Comptroller of the Currency. (2020). Consent order for Capital One, N.A. [https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-97.html](https://www OCC.gov/news-issuances/news-releases/2020/nr-occ-2020-97.html)
4. Verizon. (2023). 2023 data breach investigations report. <https://www.verizon.com/business/resources/reports/dbir/>
5. National Institute of Standards and Technology. (2018). Cloud computing security reference architecture (NIST SP 500-299). <https://www.nist.gov/publications/cloud-computing-security-reference-architecture>

ABOUT THE AUTHOR

Aashtha Tiwari

Assistant Professor - Cyber Forensics
Aditya Degree & PG College, Surampalem,
Andhra Pradesh



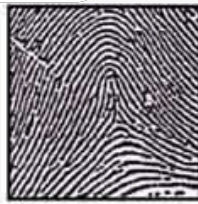


FINGERPRINT RIDGE PATTERNS

ARCHES



1



2

LOOPS



3

Left
Hand



4

WHORLS



5



6



7

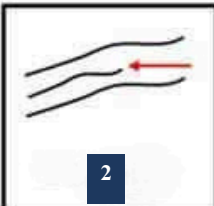


8

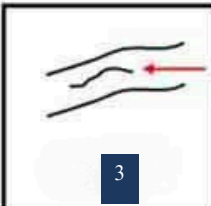
FINGERPRINT RIDGE CHARECTERISTICS



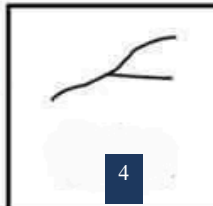
1



2



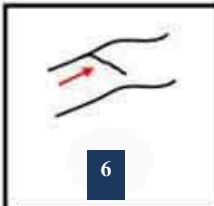
3



4



5



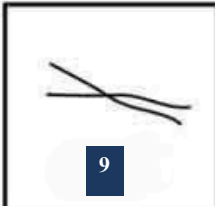
6



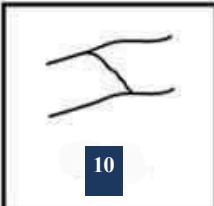
7



8



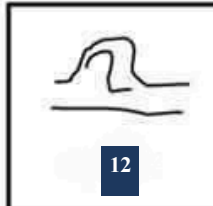
9



10



11



12

HINTS:

- Plain Arch
- Plain Whorl
- Ulnar Loop
- Tented Arch
- Central Pocket Whorl
- Double Loop
- Radial Loop
- Accidental

☐
☐
☐
☐
☐
☐
☐
☐

- Core
- Delta
- Crossover
- Ending Ridge
- Hook
- Bridge
- Short Ridge

☐
☐
☐
☐
☐
☐
☐

- Enclosures
- Eye
- Dot Or Island
- Specialry
- Fork or Bifurcation

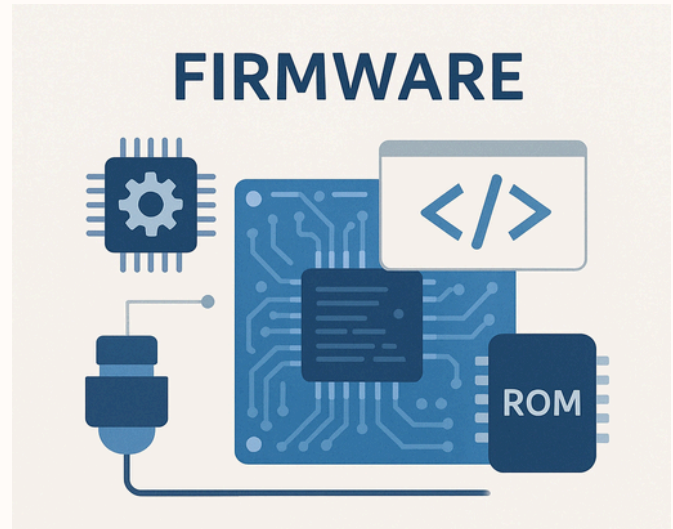
☐
☐
☐
☐
☐

HIDDEN IN THE FIRMWARE: ATTACKS AND EVIDENCE BELOW THE OS LEVEL

Author -Ms. Pooja Sharma, Kiran R Dodiya, Dr. Kapil Kumar

Introduction

We have a complex digital ecosystem, and cybersecurity has aimed its guns at the OS, applications, and network layers. Firewalls, AV, and endpoint detection systems are all protections that defend the more accessible, more visible components of a device. Now, there is a less-known, yet most-connected layer that has to do with how deeply monitored your devices are, and that is firmware. Firmware is low-level software that resides on hardware components as part of the same device layer, being the invisible link between a device's hardware and its operating systems. It tells your computer how to boot, it coordinates communication among hardware components, and it handles low-level tasks. But it is the firmware — a crucial piece of the technology puzzle — that is often overlooked and needs protection. And this vagueness makes it a fertile ground for advanced attacks. Firmware-level threats occur below the OS as opposed to malware, which runs above the OS. So this would be in a way where it could avoid most security tools, persist through rebooting the OS, and even persist through a new hard disk being installed. What we do indeed know about firmware after the hacks is that, when hacked, it can either be used for spying on the users, sabotage, or a more permanent backdoor for an attacker, and it is a hell of a hidden belly of the system. And those aren't hypothetical threats. Real-World Attacks: Firmware-level attacks are not just a theoretical concern – we have witnessed UEFI rootkits and malicious USB controller firmware that have made it clear how effective it is for attackers to implant code at the firmware level. The reason this is so sinister is that it is not only capable of causing destruction, but complicated to search and mitigate, as well.



What is firmware?

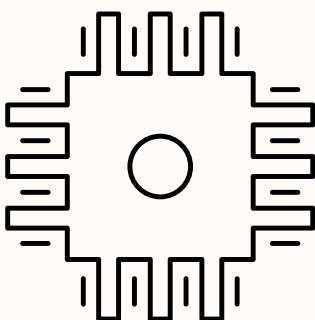
Firmware is a particular type of software that lies in hardware devices that perform their functions. It is stored in read-only memory (ROM) and is updatable to improve functionality or address security problems. Firmware plays a critical role in various devices like IoT systems that control low-layer operations and communicate with hardware elements through firmware. (Borse et al., 2023) (Falas et al., 2022)(Liu et al., 2018)

Characteristics of Firmware:

Hardware Dependence: Firmware is specifically designed for a particular hardware platform and cannot be easily transferred to another device without significant modifications (Ahn & Malik, 2013)

Low-Level Functionality: Firmware works on a low-level specification and directly interfaces with hardware elements like peripherals and sensors. Tasks such as power management, input/output, and hardware behavior initialization are managed.

Non-Volatile Storage: Firmware is usually stored in nonvolatile memory, such as in the form of ROM or Flash memory. This way, even a power-down condition can not ruin the firmware.(Ahn & Malik, 2013)



Reactivity: Firmware is often reactive to inputs from hardware or software layers. May contain interrupt service routines that are executed in response to some event(Ahn, 2016)

Why Firmware is Trusted and Exploitable:

Firmware sits at the very bottom of the stack, underneath the operating system, and is responsible for initializing the hardware, establishing the integrity of the system, and facilitating communication between hardware and higher-level software. Firmware is often referred to as the lowest level of software and is trusted by design due to its functionality during the boot-up sequence and hardware configuration. It is part of the backbone on which systems rely to work correctly and is often considered a trusted entity in security models.

Because this trust is implicit, firmware is the perfect target for attackers. Firmware attacks can ignore OS reinstalls, bypass normal endpoint detection, and retain quiet governance over hardware behavior, unlike operating system-level malware. In addition, the infrequency of firmware updates, inconsistent update management, and lack of integral verification methods (particularly in those systems' older or consumer-grade devices) further exacerbate this issue.

Singletons represent a specific form of compromise that attackers use to deploy lingering malware, create rootkits, or turn off security controls beyond the point of easy detection or analysis with specialized forensics software. Once the malware has access to firmware, it has nearly complete control of a system and can operate below the levels of detection present in most defenses.

Firmware-based attacks:

Including rootkits, UEFI/BIOS malware, and controller exploits represents a significant threat to modern computing systems. These attacks exploit vulnerabilities in the firmware, which is the low-level software controlling hardware, to gain unauthorized access and maintain persistence on a device. The complexity and stealth of these attacks make them particularly challenging to detect and mitigate. The following sections delve into the various aspects of firmware-based attacks, drawing insights from recent research.

Stealth in Silicon: Firmware-Based Attacks

Firmware resides below the operating system and controls the most fundamental aspects of a device, from booting to hardware communication. Because of its low-level access and privileged execution, firmware is an ideal hiding place for sophisticated and persistent malware. This section explores key types of firmware-based attacks and the stealth techniques that make them so dangerous.

Rootkits in UEFI/BIOS

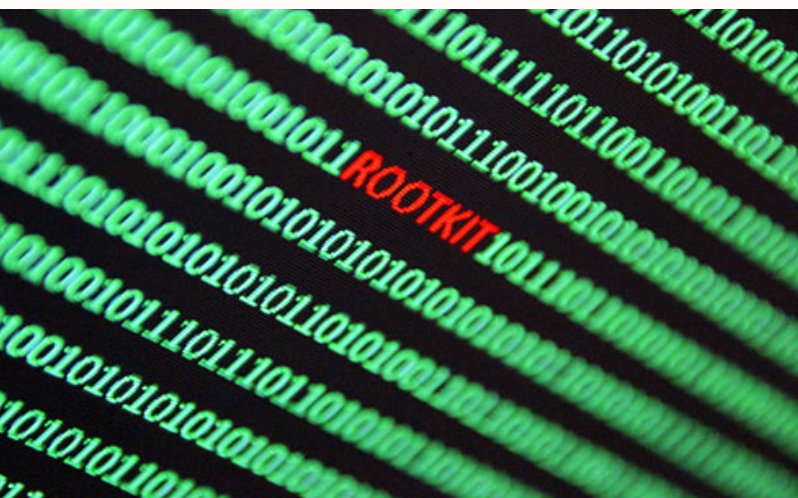
UEFI (Unified Extensible Firmware Interface) is the modern firmware standard that has replaced the legacy BIOS standard. Malware at this level can gain deep control because it runs before the OS loads and is invisible to regular antivirus and security tools.

UEFI rootkits take advantage of loopholes in firmware, allowing them to take control of the system boot processes. Once they are embedded, they can survive an operating system reinstallation and even replacement of the hard drive, making them incredibly persistent.

Abstract The LongKIT framework provides an example of UEFI/BIOS malware running on System Management Mode (SMM), which is the most privileged CPU mode.

LONGKIT demonstrates that malware can stealthily operate below the OS, evade detection, and persist forever.

UEFI is an essential part of system initialization and booting, which also makes it an attractive target for rootkits. Such attacks could let attackers in without being caught. (Pendyala & Solutions, 2025)



Controller and Peripheral Exploits (USB, NICs, GPUs)

Using the firmware of peripheral devices — these are more commonly seen in devices such as BadUSB — can be reprogrammed to behave like keyboards or network adapters and is used to inject malicious commands.

NICs (Network Interface Cards): When malware is inserted into the firmware of NICs, it is possible to sniff traffic or redirect traffic in a completely invisible manner.

Graphics Processing Units (GPUs) – these are able to perform malicious processes outside the monitoring scope of the OS.

These exploits build on the fact that peripheral firmware rarely undergoes rigorous validation for security, yet is implicitly trusted by the OS.

Firmware Attacks on IoT Devices

IoT devices often have firmware that is not only outdated but also susceptible to virus attacks. Remote control of devices (e.g., cameras, thermostats, medical devices)

1. Data theft or surveillance
2. Botnet or lateral attack usage of the device

These attacks are brutal to identify by nature and represent a significant risk to both privacy and the security of infrastructure. Firmware attacks on IoT devices exploit vulnerabilities, which allow hackers to access sensitive data or control the device remotely and pose serious threats to user privacy and security.(Dwaraka Srihith et al., 2023)



Case Study: Firmware Tampering in Withings Activité Fitness Tracker

We have already seen an obvious real-life example of a firmware security flaw in the case of the fitness tracker Withings Activité. Earlier in 2023, security researchers discovered a vulnerability in the firmware update mechanism of the device, in that the tracker failed to ensure firmware updates were signed and came from a trusted source. An opportunity for the attacker to upload altered firmware could be passed to skip all integrity checks.

An attacker could exploit this by flashing custom firmware to create fake activity data like activity steps and sleep times. Withings would then believe the manipulated data upload by accepting it from the mobile app and uploading it to the cloud as the real thing. This attack method essentially rendered the tampering invisible to end users and service providers because the device itself continued to behave as if it were genuine.

This vulnerability has profound implications. More and more fitness trackers have become involved in legal and insurance cases in which step counts, heart rates, and other biometric information can matter in a claim or a court ruling. This can be used to malicious ends where tampered firmware can clear or contrive evidence, specifically increased activity levels over some time while on a disability claim, or to corroborate or refute an alibi in a criminal investigation falsely.

It is representative of the more significant dangers that insecure firmware presents in consumer wearables. Though these devices might seem innocuous, firmware-level vulnerabilities can compromise the integrity of health and activity information, with tangible impacts on the world.

To reduce such risk, manufacturers should implement solid firmware signing, integrity checking at the time of updates, and remote attestation. The increasing flow of digital evidence from wearable tech indicates that tamper resistance for firmware is not merely a technical necessity, but also a fundamental requirement for the trustworthiness of digital systems (Rieck, 2016).

The Forensic Challenge: Investigating Below the OS:-

Traditional Security Tools' Failure in Detecting Below-OS Threats

Introduction

Endpoint detection and response (EDR), antivirus software, and security information and event management (SIEM) systems are classic security-facing tools that remain integral parts of any enterprise's cybersecurity strategy. However, those tools work only after the OS, so they misbehave under the actual OS. This shortcoming arises due to some fundamental shortcomings in their design and functioning. These include below-OS threats like kernel-level rootkits, firmware attacks, and other advanced malware that run in layers invisible to traditional tools. In this response, I examine why this has not happened and how we might be able to solve the problem

Why Traditional Security Tools Fail:

1. Operating System-Level Limitations

Legacy security solutions primarily work at the user or kernel level of the OS. These tools utilize OS APIs, syscalls, and event logs to monitor and detect threats. However, these tools become ineffective when the OS itself is compromised or managed/ bypassed. Kernel-level rootkits, for example, can infect the OS and cause it to lie to the user (user-level) security tools, which makes such rootkits particularly hard to detect. (“Kernel-Level Rootkit Detection, Prevention, and Behavior Profiling: A Taxonomy and Survey,” 2023).

2. Lack of Visibility Below the OS

Traditional security tools cannot catch attacks that can be classified as below-OS threats, like firmware attacks or hardware-level exploits. They are made for monitoring processes, files, and network traffic within the OS, but cannot examine firmware or hardware-level activity. That means attackers can use these more basic building blocks to evade detection. (Garfinkel et al., 2014)

3. Evasion Techniques

Advanced malware routinely uses evasion techniques to evade legacy security appliances. For instance, one such technique of fileless malware exists entirely within the memory of a computer. It never drops a single file to disk, making detection by traditional antivirus programs a real challenge. Likewise, advanced persistent threats (APTs) can misuse system calls or use a valid system tool to blend with legitimate traffic and stealthily go undetected (Harish & Swapna, 2024).

4. Resource and Performance Constraints

The traditional security tools are known to be resource-hogging and are not designed to perform real-time monitoring of system activities at the lower level. However, monitoring hardware components like CPU performance counters or network interface controllers can be computationally expensive to monitor these events to detect below-OS threats continuously. Such overhead is costly in terms of performance, so it cannot be a candidate for traditional tools to enable such monitoring. (Real-Time Multi-Modal Subcomponent-Level Measurements for Trustworthy System Monitoring and Malware Detection, 2025).



Limitations of Traditional Security Tools

1. EDR Limitations

EDR solutions excel in endpoint detection and response but lack below-OS threat detection. While EDR tools rely on OS event logs and process monitoring, advanced attackers are known to bypass such artifacts. This allows things like kernel-level rootkits to manipulate the OS to hide processes to avoid discovery by EDR tools. (“Kernel-Level Rootkit Detection, Prevention, and Behavior Profiling: A Taxonomy and Survey,” 2023).

2. Antivirus Software Limitations

The basic principle behind the antivirus detection of threats is the usage of signatures or known patterns. Nevertheless, below-OS threats are characterized by unknown or zero-day exploits that do not comply with any known signature. Even firmware-level attacks or hardware-based exploits are not covered under these traditional anti-viruses, which target file-level and process-level attacks.(PUCHKO & MOISEEVA, 2024).

3. SIEM Limitations

SIEM gathers and analyzes log data across IT systems, which can help identify security threats. But SIEM can only be as powerful as what it ultimately receives. An SIEM system might not detect below-OS threats if attackers can manipulate or bypass OS-level logging mechanisms. SIEM tools are also bombarded with log data, resulting in false positives, false negatives, and missing alerts (Nurusheva et al., 2024).

Potential Solutions:-

1. Subcomponent-Level Monitoring

Detecting below-OS threats can be done by monitoring system subcomponents—for example, the network interface controller, GPU, or CPU hardware performance counters. Furthermore, they can detect anomalies (that is, an indication of a potential attack) despite a compromise of the primary processor by analyzing activity at these subcomponents. This method needs to collect real-time information and synchronize data from different subcomponents, processes, or systems to give an overview of how the system is functioning and acts when required. (Real-Time Multi-Modal Subcomponent-Level Measurements for Trustworthy System Monitoring and Malware Detection, 2025).

2. Hypervisor-Based Solutions

Hypervisor-based methods can provide more security as they monitor system activity from a higher privilege level. As an example, a hypervisor can intercept system calls and redirect them as needed for analysis, so that things such as malware can be detected on an OS level (which may evade OS-level tools). Another point is that hypervisor-based solutions can protect security monitoring itself by isolating it from the OS, so even if the OS is compromised, the security monitoring process will not be affected (Quynh & Takefuji, 2007).

3. Firmware-Level Security Agents

Such firmware-level security agents can create a pre-OS layer of security and conduct monitoring within the firmware environment to check for malware and other threats before the OS even gets a chance to load. The agents can additionally watch for indications of tampering or unwarranted physical access to system hardware. Firmware-level agents can detect threats that typical security tools do not see because they run below the OS layer (Firmware-Level Security Agent Supporting Operating System-Level Security in Computer System, 2013).



5. Advanced SIEM and AI Integration

Connecting SIEM systems with advanced machine learning and artificial intelligence (AI) techniques can enhance threat detection and response. Even on the SIEM level, AI-SIEM systems can analyze vast volumes of log data in real time and identify patterns and anomalies that could present below-OS threats. Also, AI can help to improve the visibility of security events so that analysts can learn about the context and severity of the risk detected (Naif Alatawi, 2025).

Evidence Collection at the Firmware Level

Analyzing firmware-level evidence to investigate threats that live below the OS requires different techniques for both evidence collection and analysis. While disk imaging and memory dumps are some of the standard methods in digital forensics, firmware forensics requires different approaches to access non-volatile storage on chips. These include in-system programming, JTAG access, or chip-off extraction, all of which would need to be performed correctly so as not to change the original data content. This is where we have some essential tools like CHIPSEC, Binwalk, Flashrom, UEFI Tool, etc. This allows analysts to extract firmware images, reverse-engineer binaries, and confirm integrity

and IEDs or implants. Because firmware-level threats often act stealthily and persistently, a thorough analysis of the binary structures and behavior at a low level is necessary. Further, the lawfulness and prosecutorial integrity of firmware evidence are vital. While retaining a proper chain of custody, documenting every action, and using write-protection mechanisms as much as possible. Given its potentially sensitive, proprietary, or even regulated nature, firmware needs to be appropriately handled not only for forensic soundness but also so that legal requirements are met. By following this disciplined process, the evidence will be viable in court and reliable for incident response.

Limited Reach Of Traditional Tools And Advanced Detection Methods: Layers of Visibility in Cybersecurity:-

This picture illustrates the layered structure from application layer, to middleware, to OS, to firmware, to hardware, and compares the operational scope of standard security tools (EDR, anti-virus, SIEM) with deep visibility via techniques to agents in firmware, hypervisor monitoring, and hardware subcomponent detection.

Mitigating firmware threats:-

Requires numerous layers of protection such as secure boot processes, integrity checks, firmware updates, vendor responsibilities, system hardening, and forensic readiness training. However, all of these components play a critical role in the ability of devices to resist firmware attacks.

Secure Boot and Integrity Checks

Secure Boot: This process ensures that only trusted firmware is executed during the system boot process, preventing unauthorized code from running. It uses cryptographic signatures to validate the correctness of firmware.

Integrity checks: Integrity checks like hashing are needed on a regular basis to ensure that firmware remains untouched. These checks could be automated and constructed as part of the firmware update process.

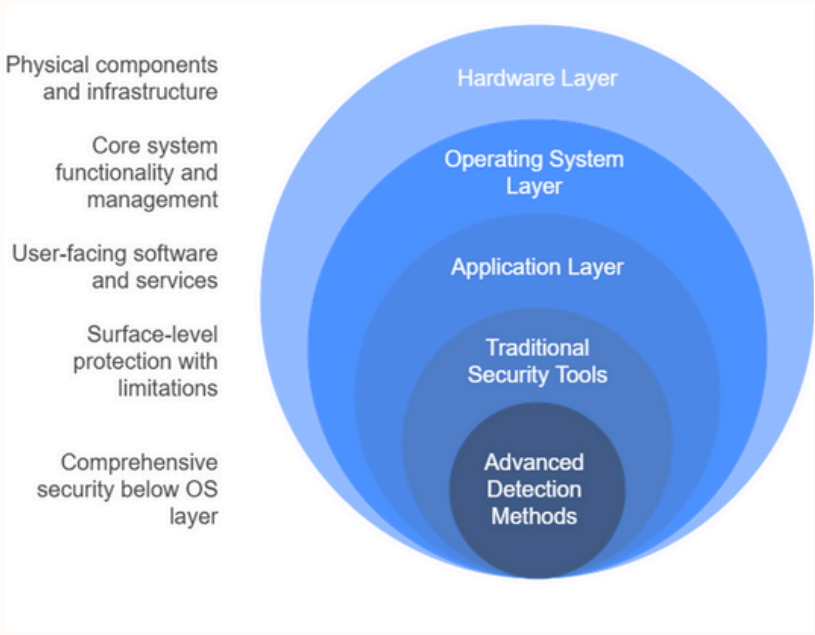


Fig: Shows Hierarchical Cybersecurity visibilities

Firmware Updates and Vendor Responsibility

This means that vendors should implement secure update mechanisms that authenticate firmware prior to installation. For example, it may involve utilizing secure memory regions in which to write firmware payloads during updates.

Vendor Responsibility: Manufacturers must deliver timely updates and patches to mitigate vulnerabilities, ensuring devices are kept secure throughout their lifetime.

System Hardening and Training

System Hardening: Adjusting the configuration of devices to reduce possible attack vectors, including, for example, turning off unnecessary services or following the principle of least privilege.

Education & Awareness – Organizations should train employees on firmware threats and how to remain forensic-ready (that is, having measures in place to respond to a breach should it occur).

These are significant security measures, but they do not solve all the issues we have with security, such as having to monitor constantly and the continually changing curve of firmware to attack. All of these factors require continued research and further collaboration between the stakeholders within the cybersecurity space to address these challenges. (Marchand et al., 2023) (Abramson, 2017) (Bettayeb et al., 2019)

References:

- Abramson, D. (2017). Secure firmware devices and methods. Intel Technology Journal, 10(03). <https://doi.org/10.1535/ITJ.1003.02>
- Ahn, S. (2016). AUTOMATED FIRMWARE VERIFICATION USING FIRMWARE-HARDWARE INTERACTION PATTERNS. <https://dataspace.princeton.edu/handle/88435/dsp01s4655k00v>
- Ahn, S., & Malik, S. (2013). Modeling Firmware as Service Functions and Its Application to Test Generation. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8244 LNCS, 61–77. https://doi.org/10.1007/978-3-319-03077-7_5
- Bettayeb, M., Nasir, Q., & Talib, M. A. (2019). Firmware update attacks and security for IoT devices survey. ACM International Conference Proceeding Series. <https://doi.org/10.1145/3333165.3333169>
- Borse, M., Shendkar, P., Undre, Y., Mahadik, A., & Patil, R. (2023). Study of Hybrid Cryptographic Techniques for Vehicle FOTA System. Lecture Notes on Data Engineering and Communications Technologies, 166, 417–430. https://doi.org/10.1007/978-981-99-0835-6_30
- Dwaraka Srihith, I., Donald, A. D., Aditya, T., Srinivas, S., Anjali, D., & Chandana, A. (2023). Firmware Attacks: The Silent Threat to Your IoT Connected Devices. International Journal of Advanced Research in Science, Communication and Technology, 3(2), 145–154. <https://doi.org/10.48175/IJARSCT-9104>.

Conclusion:

This makes firmware-level threats one of the most complex and lethal battlegrounds in cybersecurity today. Whereas traditional malware operating within the operating system, sub-OS attacks can operate outside the purview of the operating system, making them hard to detect, avoiding standard security tools, and the potential to survive system reinstall or hardware replacements. In this article, we have covered how attackers exploit firmware, the reasons standard tools such as EDR and SIEM fail to recognize the patterns, and what forensic techniques are required to probe these deep-seated threats. With increasing complexity and interactivity of systems—from the emergence of IoT endpoints to AI-controlled hardware—the ability to see and control below the OS is becoming increasingly necessary. Organizations need to go beyond the superficial and invest in tools, training, and techniques that dig down to the very firmware and hardware layers. It is only by acknowledging these blind spots that we will be able to construct genuinely resilient and secure digital infrastructures.



- Falas, S., Konstantinou, C., & Michael, M. K. (2022). A Modular End-to-End Framework for Secure Firmware Updates on Embedded Systems. *ACM Journal on Emerging Technologies in Computing Systems*, 18(1), 1–19. <https://doi.org/10.1145/3460234>
- A firmware-level security agent supporting operating system-level security in the computer system. (2013). <https://scispace.com/papers/firmware-level-security-agent-supporting-operating-system-26sxnugy0s>
- Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., & Boneh, D. (2014). Below-OS security solution for distributed network endpoints. *Operating Systems Review (ACM)*, 37(5), 193–206. <https://doi.org/10.1145/1165389.945464>
- Harish, R., & Swapna, M. P. (2024). Endpoint Detection and Response for Fileless Malware and LOLBin Threats. 2024 15th International Conference on Computing, Communication, and Networking Technologies, ICCCNT 2024, 1–6. <https://doi.org/10.1109/ICCCNT61001.2024.10725289>
- Kernel-level Rootkit Detection, Prevention and Behavior Profiling: A Taxonomy and Survey. (2023). *ArXiv.Org*, abs/2304.0. <https://doi.org/10.48550/ARXIV.2304.00473>
- Liu, K., Kong, W., Hou, G., & Fukuda, A. (2018). A Survey of Formal Techniques for Hardware/Software Co-verification. *Proceedings - 2018 7th International Congress on Advanced Applied Informatics, IIAI-AAI 2018*, 125–128. <https://doi.org/10.1109/IIAI-AAI.2018.00033>
- Marchand, A., Imine, Y., Ouarnoughi, H., Tarridec, T., & Gallais, A. (2023). Firmware Integrity Protection: A Survey. *IEEE Access*, 11, 77952–77979. <https://doi.org/10.1109/ACCESS.2023.3298833>
- Naif Alatawi, M. (2025). Enhancing Intrusion Detection Systems With Advanced Machine Learning Techniques: An Ensemble and Explainable Artificial Intelligence (<sc>AI</sc>) Approach. *Security and Privacy*, 8(1). <https://doi.org/10.1002/SPY2.496>
- Nurusheva, A., Abdiraman, A., Satybalina, D., & Goranin, N. (2024). Machine learning algorithms in SIEM systems for enhanced detection and management of security events. *Bulletin of L.N. Gumilyov Eurasian National University. Mathematics, Computer Science, Mechanics Series*, 148(3), 6–17. <https://doi.org/10.32523/BULMATHENU.2024/3.1>
- Pendyala, S. K., & Solutions, C. T. (2025). Strengthening Healthcare Cybersecurity: Leveraging Multi-Cloud and AI Strengthening Healthcare Cybersecurity: Leveraging Multi-Cloud and AI Solutions. February. <https://doi.org/10.15226/2474-9257/10/1/00163>
- PUCHKO, V. A., & MOISEEVA, N. A. (2024). Development of a software package for analyzing internal security threats of Windows OS. *Прикладная Математика и Фундаментальная Информатика*, 11(2), 16–24. <https://doi.org/10.25206/2311-4908-2024-11-2-16-24>
- Quynh, N. A., & Takefuji, Y. (2007). Towards a tamper-resistant kernel rootkit detector. *Proceedings of the ACM Symposium on Applied Computing*, 276–283. <https://doi.org/10.1145/1244002.1244070>
- Real-Time Multi-Modal Subcomponent-Level Measurements for Trustworthy System Monitoring and Malware Detection. (2025). <https://doi.org/10.48550/ARXIV.2501.13081>
- Rieck, J. (2016). Attacks on Fitness Trackers Revisited: A Case-Study of Unfit Firmware Security. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, P-256, 33–44. <https://arxiv.org/abs/1604.03313v1>

ABOUT THE AUTHORS

Pooja Sharma

M.Sc. Cyber Security and Forensic Science, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA.



Kiran Dodiya

(Research Scholar, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



FORENSIC APPLICATIONS OF 3D-PRINTED CHEMICAL SENSORS IN CRIME SCENE INVESTIGATION

Author - Sanskriti Verma

Introduction

The integration of three-dimensional (3D) printing technology into forensic science has revolutionized the development of chemical sensors used in crime scene investigations. 3D-printed chemical sensors offer customizable, cost-effective, and portable solutions for the rapid detection of various substances, including explosives, drugs, and gunshot residues. This article explores the advancements in 3D-printed chemical sensors and their forensic applications, drawing insights from recent research and reviews.

The customizable nature of 3D printing allows for the rapid production of sensors tailored to specific analytes, facilitating on-site analysis.

Drug Detection

The emergence of new psychoactive substances (NPS) poses challenges for forensic analysis. A novel 3D-printed electrochemical apparatus was designed for the detection of 25E-NBOH, a phenethylamine derivative. This portable device enabled fast and selective screening in forensic samples, including saliva and blotting papers, demonstrating its applicability in field conditions.

Advancements in 3D-Printed Chemical sensors

3D printing, particularly fused deposition modeling (FDM), has enabled the fabrication of electrodes using conductive filaments such as graphene–polylactic acid (G–PLA). These electrodes have been employed in the electrochemical detection of illicit drugs like cocaine. After electrochemical surface treatment, G–PLA electrodes demonstrated enhanced sensitivity and selectivity, with detection limits as low as $6 \mu\text{mol L}^{-1}$, even in the presence of common adulterants.

In another study, 3D-printed stainless steel electrodes electroplated with gold were utilized for the detection of nitroaromatic explosives such as trinitrotoluene (TNT) and dinitrotoluene (DNT). These electrodes exhibited higher sensitivity compared to traditional glassy carbon electrodes, highlighting the potential of 3D printing in fabricating efficient sensors for explosive detection.

Forensic Applications

Detection of Explosives and Nerve Agents

The detection of explosives and nerve agents at crime scenes is crucial for forensic investigations. 3D-printed electrodes have been developed to identify compounds like TNT, DNT, and fenitrothion through electrochemical methods.



3D-printed G-PLA electrodes have also been employed for the detection of metals in gunshot residues (GSR). These electrodes functioned both as samplers and sensors, detecting lead (Pb^{2+}) and antimony (Sb^{3+}) through square-wave anodic stripping voltammetry. The method allowed for direct sampling from hands and clothing, followed by immediate analysis, streamlining the GSR detection process.



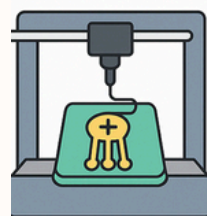
Fig: shows GSR in clothes

Advantages and Challenges

The utilization of 3D-printed chemical sensors in forensic science offers several advantages:

- **Customization:** Sensors can be tailored to detect specific substances by modifying the electrode materials and designs.
- **Cost-Effectiveness:** 3D printing reduces manufacturing costs, making disposable sensors feasible for widespread use.
- **Portability:** The compact size of 3D-printed devices facilitates on-site analysis, which is crucial for timely forensic investigations.

3D-Printed Chemical Sensors in Forensic Science



Customization



Cost-Effectiveness



Portability

However, challenges remain:

- **Material Limitations:** The performance of 3D-printed sensors depends on the quality and properties of the printing materials.
- **Standardization:** Establishing standardized protocols for fabrication and analysis is necessary to ensure reproducibility and reliability.

Conclusion:

The integration of 3D printing technology into forensic science has significantly advanced the development of chemical sensors, offering innovative solutions for on-site detection of explosives, drugs, and gunshot residues. These sensors stand out for their customization, affordability, and portability, making them ideal tools for rapid forensic investigations. Despite the promising applications, certain limitations—such as material constraints and the lack of standardized fabrication protocols—must be addressed to ensure consistent and reliable performance. Continued research and development in this field will be essential to fully harness the potential of 3D-printed chemical sensors and establish them as standard tools in forensic practice.

Future advancements in printing materials and sensor miniaturization could further enhance sensitivity and broaden the scope of forensic applications. Collaborations between material scientists, forensic experts, and engineers will play a pivotal role in overcoming existing challenges.

References

- Tan, C., Nasir, M. Z. M., Ambrosi, A., & Pumera, M. (2017). 3D Printed Electrodes for Detection of Nitroaromatic Explosives and Nerve Agents. *Analytical Chemistry*, 89(17), 8995–9001. <https://doi.org/10.1021/acs.analchem.7b01614>PubMed+4FAO Agris+4American Chemical Society Publications+4
- Afonso, F. J., Rocha, R. G., Matias, T. A., Richter, E. M., Petrucci, J. F. S., & Muñoz, R. A. A. (2021). 3D-printing for forensic chemistry: Voltammetric determination of cocaine on additively manufactured graphene–polylactic acid electrodes. *Analytical Methods*, 13(23), 2671–2678. <https://doi.org/10.1039/D1AY00181G>GRSC Publishing+1American Chemical Society Publications+1
- Cardoso, R. M., Rocha, D. P., Rocha, R. G., Stefano, J. S., Silva, R. A. B., Richter, E. M., & Muñoz, R. A. A. (2023). Novel disposable and portable 3D-printed electrochemical apparatus for fast and selective screening of 25E-NBOH in forensic samples. *Analytica Chimica Acta*, 1250, 340944. <https://doi.org/10.1016/j.aca.2023.340944> PubMed+1American Chemical Society Publications+1
- Rocha, R. G., Cardoso, R. M., Stefano, J. S., Richter, E. M., & Muñoz, R. A. A. (2021). Electrochemical (Bio)Sensors Enabled by Fused Deposition Modeling-Based 3D Printing: A Guide to Selecting Designs, Printing Parameters, and Post-Treatment Protocols. *Analytical Chemistry*, 93(1), 167–190. <https://doi.org/10.1021/acs.analchem.1c05523>American Chemical Society Publications
- Ambrosi, A., & Bonanni, A. (2021). How 3D printing can boost advances in analytical and bioanalytical chemistry

ABOUT THE AUTHOR

Sanskriti Verma

Assistant Professor, Forensic Science,
Aditya Degree & PG College, Surampalem,
Andhra Pradesh





DID YOU KNOW?

Ice can be used as a weapon, leaving almost no trace since it melts and disappears after the attack.

BIOHACKERS AND DATA BANDITS: THE RISE OF DNA-BASED CYBERSECURITY THREATS

Author - Karnaa Thaker, Vinisha Solanki, Kiran R Dodiya, Dr. Kapil Kumar

Introduction

Biohacking is a rapidly growing movement that combines technology, biology, and self-experimentation to optimize human performance and well-being. It encompasses a range of practices, from genetic modifications and wearable technology to cognitive enhancement and nutritional interventions. In the European Union (EU), where health, technology, and data privacy regulations are extensive, the rise of biohacking challenges traditional legal and ethical boundaries and raises complex regulatory questions. While biohacking offers individuals unprecedented control over their physical and mental capabilities, it often operates on the fringes of legality, exploiting regulatory gaps. "Medical care designed to optimize efficiency or therapeutic benefit for particular groups of patients, especially by using genetic or molecular profiling." It is not an entirely new idea: physicians from ancient times have recognized that medical treatment needs to consider individual variations in patient characteristics. However, a confluence of events has enabled the modern precision medicine movement: scientific advances in genetics and pharmacology, technological advances in mobile devices and wearable sensors, and methodological advances in computing and data sciences.



History of Biohacking Technology.

The Pattern for the first Cardiac Pacemaker was submitted in 1952, followed by the First Implanted Electric Pacemaker in a Human body in 1960. As time went by, the revolution of biotechnology began in the 1990s with smart Audio Implants, and in the 2000s, smart prosthetics came up in the industry.

What is Biohacking?

Biohacking is defined as modifying or altering a human's body in terms of physical or genetic variation using modern technology. Biohacking is a point where Technology and Human biology architecture meet to serve a purpose of benefit to society if used correctly. Regarding Cyber Security, Biohacking refers to the security risks associated with an individual who modifies their body with implanted technology. These individuals are referred to as Biohackers, grinders, or even transhuman and can become potential attack vectors.

What are Data Bandits?

Data Bandits are the Biohackers who exploit the genetic data and mutate it for usually malicious purposes. They alter the genome with the help of biotechnological tools for various purposes like creating a bioweapon, stealing genetic data, etc. The role of bandit algorithms in precision medicine, such as mobile health and digital phenotyping, has been reviewed before (Tewari and Murphy, 2017; Rabbi et al., 2019). Since these reviews were published, bandit algorithms have continued to find uses in mobile health, and several new topics have emerged in the research on bandit algorithms.



DNA and its rising Cyber Threats.

What is DNA?

DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. Nearly every cell in a person's body has the same DNA. The information in DNA is stored as a code made up of four chemical bases: adenine (A), guanine (G), cytosine (C), and thymine (T). Human DNA consists of about 3 billion bases, and more than 99 percent of those bases are the same in everyone. The order, or sequence, of these bases determines the information available for building and maintaining an organism, similar to how letters of the alphabet appear in a particular order to form words and sentences. An important property of DNA is that it can replicate, or make copies of itself. Each DNA strand in the double helix can serve as a pattern for duplicating the sequence of bases. This is critical when cells divide because each new cell needs an exact copy of the DNA in the old cell.



Genomic data and its Sequencing.

A genome (one may call it a 'software') of a living organism (bacteria, viruses, plants, animals, or humans) contains entirely mapped genetic information that controls the features or behavior in the form of deoxyribonucleic acid (DNA) or ribonucleic acid (RNA). Entire genome sequencing and mapping functional capabilities, along with the advances in Synthetic Biology tools like CRISPR-CAS9, have enabled scientists to edit and engineer the genomic data of living organisms and resurrect and reconstruct extinct or novel organisms. The DNA database-related threat landscape may be subdivided into three categories: potential national security risks, such as pathogen genomic data and human and industrial genomic data.

Rising Cyber Threats.

Synthetic biology has intersected and merged with various fields, including genetics, molecular biology, systems biology, bioinformatics, genetic engineering, and metabolic engineering, thanks to the advancement of DNA synthesis and sequencing technologies. DNA creation, manipulation, processing, and analysis steps are prone to attacks similar to those in attack process, and a lack of defensive measures compounds this problem. First, modify a DNA-processing program by intentionally introducing a software vulnerability. This vulnerability might simulate real vulnerability risks in the software by executing code stored in DNA. Next, a DNA sequence containing the malicious program was synthesized and sequenced using NGS; after sequencing, a FASTQ file (a text-based format for storing both a biological sequence) was generated. The malicious application analyzed Short DNA fragments, which were launched when the file was read and the sequences were processed. The results indicated that manipulating and processing a DNA sequencing file containing a malicious program could seriously threaten the computer analysis system. Some companies provide technical support for DNA synthesis and sequencing analysis through remote and cloud services. They can offer integrated services for DNA synthesis and sequencing through cooperation.

In 2020, the DNA Data Storage Alliance was established by 15 companies, including sequencing firms represented by Illumina, DNA synthesis firms represented by Twist Bioscience, and data storage companies represented by Microsoft Research and Western Digital. They intended to create and promote an automated storage ecosystem based on artificially synthesized DNA as a data storage medium. However, these systematic integrations inadvertently increased the risk of cyberbiosecurity attacks. Furthermore, inherent risks to DNA data sharing were already present. Biohacking often involves collecting personal health data through implanted sensors, biometric monitoring, or genetic testing. The GDPR governs the collection and processing of personal data, including biometric and genetic information. However, biohackers may exploit certain ambiguities in the GDPR, notably regarding consent and the use of personal data for self-experimentation or non-commercial purposes.

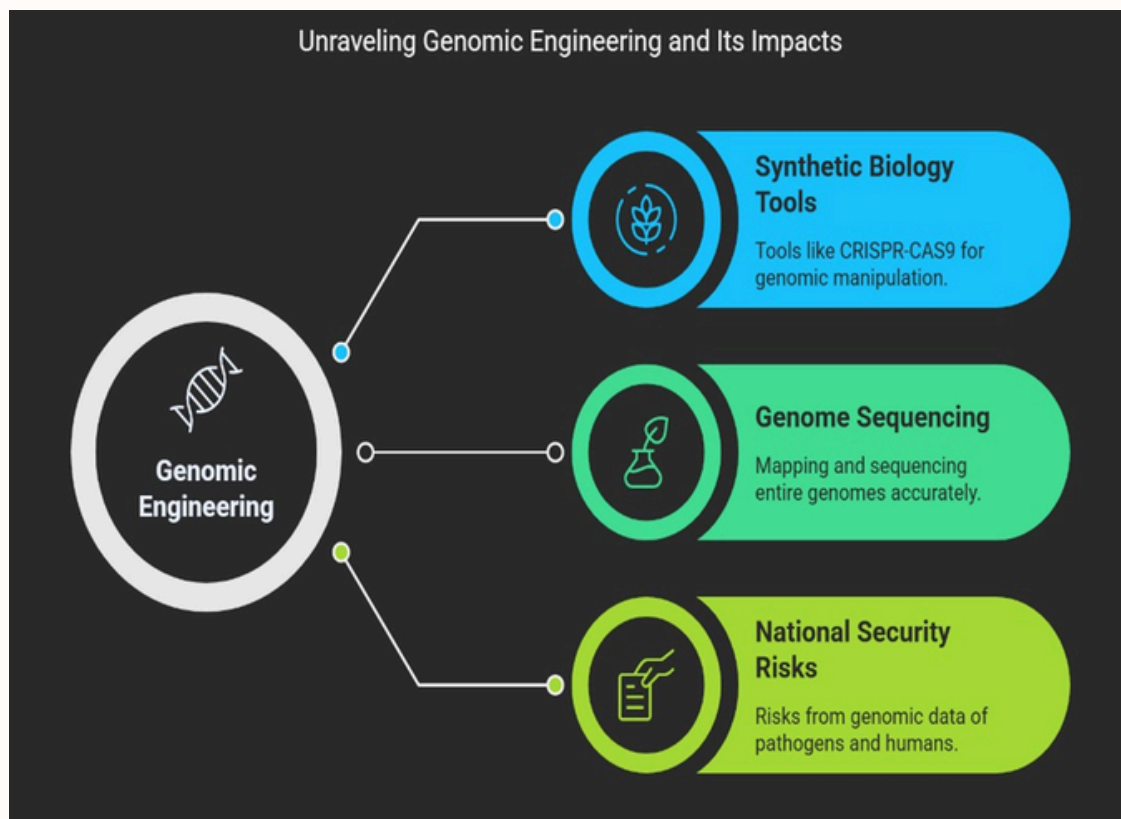


Fig: shows genomic Engineering and Its Impacts

Implantable Technologies.

This technology for wireless communication is already incorporated into our daily lives, as the use of contactless payment and badges to open doors is considered the implant. The goal is to upgrade your body by creating a symbiosis between the human body and technology. The most popular is the implantation of radiofrequency identification (RFID) implants. The use in health care is expanding, including tracking medical equipment, instruments, and drugs.^{2,3} In veterinary medicine, the implantation of RFID chips to identify animals has been part of standard care for decades. It is estimated that between 50,000 and 100,000 people have already been chipped.⁸ These implants are available online and are delivered sterile. You have to program the chip yourself with a special contactless reader, preferably before implantation, so that proper functioning can be checked. Programming is still possible after implementation. The implantation of these devices in humans and the relevant safety implications have not been extensively studied. The scope of this review was to consider the future role of the hand surgeon in placing these implants and dealing with possible complications. The following are the types of implants.

RFID/NFC chip.

An external energy source powers implantable RFID tags. However, active RFID implants feature an embedded battery that can communicate within a body area network. They can also continuously connect to IoT via Bluetooth or in command mode at long distances. This technology was designed to identify the medical history of unconscious patients in an emergency. Early biohackers mainly employed uncoated RFID capsules such as EM4102 (FAREAD) and HITAG 2048S (NXP). A basic RFID system includes RFID tags (active, passive, or semi-passive), which are also called RFID chips or transponders, serving as a digital data store that can be embedded or attached to a physical item to be identified and tracked. RFID readers or interrogators communicate with the tags and retrieve the information sent to a host computer or RFID middleware to ensure communication between the RFID infrastructure and the different intra- and inter-organizational systems.

Implantable Sensors.

Biohackers have utilized temperature sensors to measure body temperature. For example, initially designed for veterinary applications, Bio-Thermo (Life Chip, Destron Fearing) continuously monitors temperature data with a 25–43 °C detection range. This sensor has an antimigration coating (Bio Bond) and is implanted through a hypodermic needle into the arm near the armpit.

The implant transfers temperature data to a tablet computer via Bluetooth connection. Such implants can measure other physical and biochemical parameters, such as pressure and biomarkers, in real-time.

Pacemaker Implants.

Continuous cardiac functioning is essential for human beings. Therefore, patients with abnormal heart rhythms are advised to have a pacemaker implanted in their bodies. It is expected to be a robust and fail-safe device with a durable battery life of up to a decade. Thus, various problems in the natural conduction system of the heart are addressed by using an artificial pacemaker, which constantly observes and corrects the heart rate whenever required. A pacemaker is an electronic device that generates pacing signals for the heart to correct an irregular heartbeat. Modern pacemakers' durability allows them to be used for pacing and other cardiac diagnostic applications. Low-energy electrical pulses generated by a pacemaker can speed up a slow heart rhythm, thus helping to maintain a constant heart rate by harmonizing electrical signaling between the upper and lower chambers as well as between the ventricles of the heart. Typically, a microcontroller-based pacemaker design involves circuitry related to the sense and actuation of the heart muscle through electronics. The basic functionality of this electronics is to generate appropriate pacing pulses based on the input from the electrodes—a schematic of the cardiac pacemaker.r



Emerging Concerns.

The increasing systematic use of personal data surveillance in the investigations or mass monitoring of citizens by law enforcement agencies is a significant concern among biohackers. This may involve real-time geotagging of an individual's location and activities. The biohacking community actively discusses the mass surveillance implications of implantable devices that may be used to control citizens.

Guidelines and Regulations.

The genetically modified organisms (GMOs) and the products thereof are regulated in India under the “Rules for the manufacture, use, import, export & storage of hazardous microorganisms, genetically engineered organisms or cells, 1989”, notified under the Environment (Protection) Act, 1986. These rules are comprehensive in scope,

covering the entire spectrum of activities involving GMOs and products. However, without any clarity on how the emerging technologies will be dealt with in India, the definition of modern biotechnology according to the Cartagena Protocol on Biosafety has yet to be incorporated into national regulations. India has neither an exclusive biosecurity nor an exclusive cybersecurity law, though sector-specific regulations exist within both domains. Numerous laws, rules, frameworks, Standard Operating Procedures, and 112 Journal of Defence Studies guidelines exist for contained research, biologics, confined field trials, food safety assessment, environmental risk assessment, cybersecurity (such as the IT Act 2021), and Biosecurity. The National Cybersecurity Policy 2013, released by the Department of Electronics and .

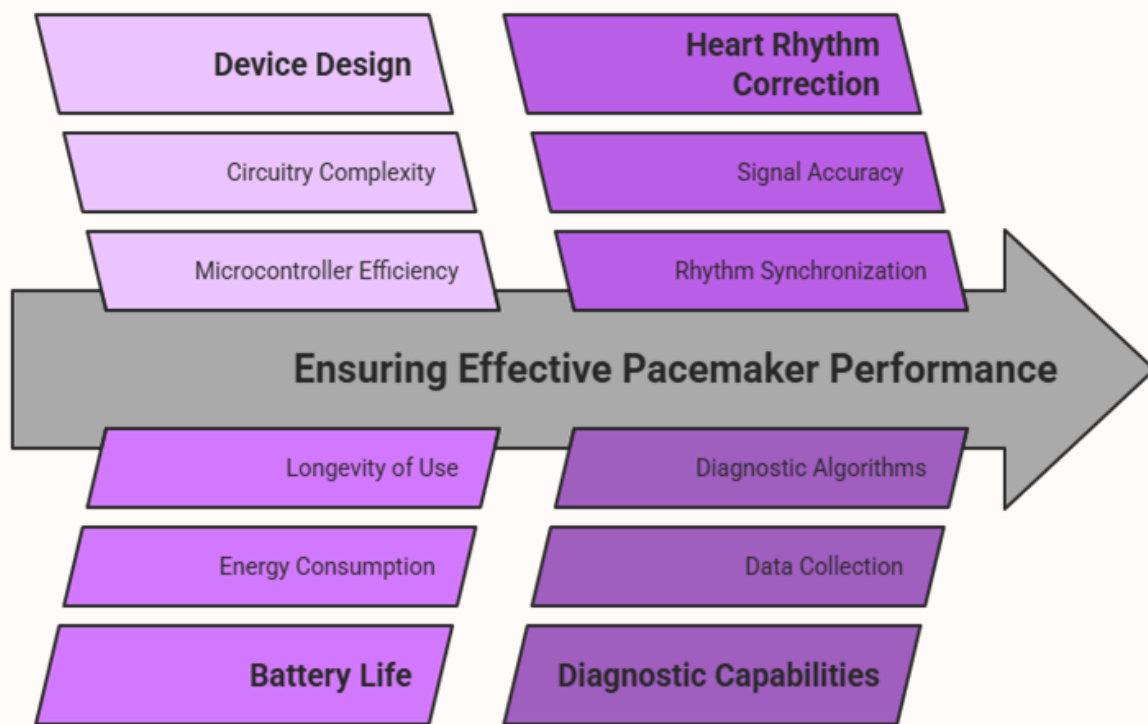


Fig: shows Ensuring Effective Pacemaker performance

Information Technology, and the National Information Security Policy and Guidelines have been issued by the Ministry of Home Affairs to prevent cyber intrusions. However, the rapid convergence of dual-use emerging technologies, along with the all-pervasive CyberBiosecurity threats with their potential to disrupt the well-being of citizens and national security, the Cyber-Biosecurity domain needs to be regulated after a comprehensive review of the entire legal framework. Various stakeholder ministries, governmental agencies, and the legislative bodies responsible for implementing laws must work together to design frameworks to reduce Cyber-Biosecurity challenges.

Conclusion

Though the convergent emerging technologies have complicated the Cyber biohacking-related threats, these challenges are not insurmountable. The regulatory policy-makers, equipment manufacturers, and end users must respect, value, and protect their data with the inherent threat perspective in mind. There is a need to create a secure ecosystem facilitated by a comprehensive analysis of the entire Bio Economy concerning the Biosecurity and CyberBiosecurity landscape, SWOT analyses of existing legal and regulatory provisions, reinforcements with legal and constitutional amendments as necessary, and effective response networks are required. Various stakeholder ministries, governmental agencies, and the legislative bodies responsible for implementing laws must work together to design frameworks to reduce Cyber-Biohacking challenges. With training and awareness to identify and mitigate the threats, the Cyber-Biosecurity vulnerabilities can be minimized to benefit the bio-economy, scientific institutions, and national security. To address this emerging challenge effectively, policymakers need to formalize a collaborative approach with emerging technology experts across all disciplines to develop regulatory frameworks to anticipate, detect, and mitigate Cyber-Biosecurity threats.

References.

- Tewari, A., & Murphy, S. A. (2017). From ads to interventions: Contextual bandits in mobile health. In *Mobile Health* (pp. 495-517). Springer.
- Rabbi, M., Philyaw-Kotov, M., Lee, J., Mansour, A., Dent, L., Wang, X., ... & Choudhury, T. (2019). SARA: A mobile app to engage users in health data collection. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(2), 1-27.
- European Union General Data Protection Regulation (GDPR), 2016. Regulation (EU) 2016/679.
- Environment (Protection) Act, 1986. Rules for the manufacture, use, import, export & storage of hazardous microorganisms, genetically engineered organisms, or cells, Ministry of Environment, Forest and Climate Change, Government of India.
- National Cybersecurity Policy, 2013. Department of Electronics and Information Technology (Deity), Government of India.
- National Information Security Policy and Guidelines, Ministry of Home Affairs, Government of India.
- Cartagena Protocol on Biosafety, 2000. Convention on Biological Diversity (CBD).
- DNA Data Storage Alliance, 2020. The partnership between Illumina, Twist Bioscience, Microsoft Research, and Western Digital. [Organization/initiative announcement]
- Destron Fearing. Bio-Thermo Life Chip Implantable Temperature Sensor Specifications. [Manufacturer's documentation]
- NXP Semiconductors. HITAG 2048S RFID Chip Technical Overview. [Product documentation]
- FAREAD. EM4102 RFID Capsule Specifications. [Product documentation]
- Synthetic Biology and Cybersecurity. Risks from maliciously crafted DNA: NGS attack vectors. Inspired by research presented at the USENIX Security Symposium (2017) by researchers from the University of Washington

ABOUT THE AUTHORS

Karnaa Thaker

Integrated M.Sc. in Cyber Security & Forensic Science,
Department of Biochemistry & Forensic Science, Gujarat
University, Ahmedabad, Gujarat, INDIA



Vinisha Solanki

Integrated M.Sc. in Cyber Security & Forensic Science,
Department of Biochemistry & Forensic Science, Gujarat
University, Ahmedabad, Gujarat, INDIA



Kiran Dodiya

(Research Scholar, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA

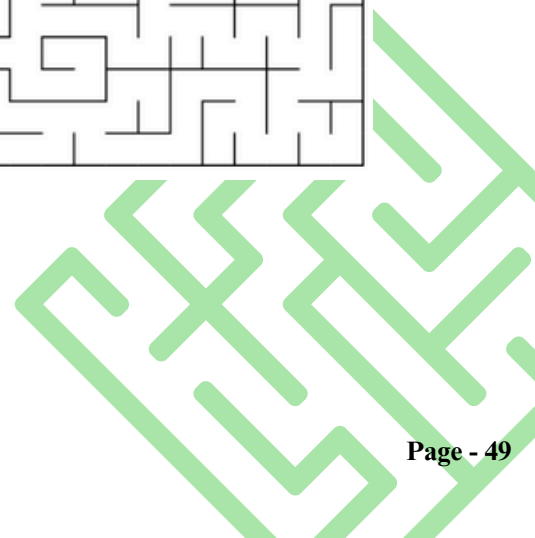
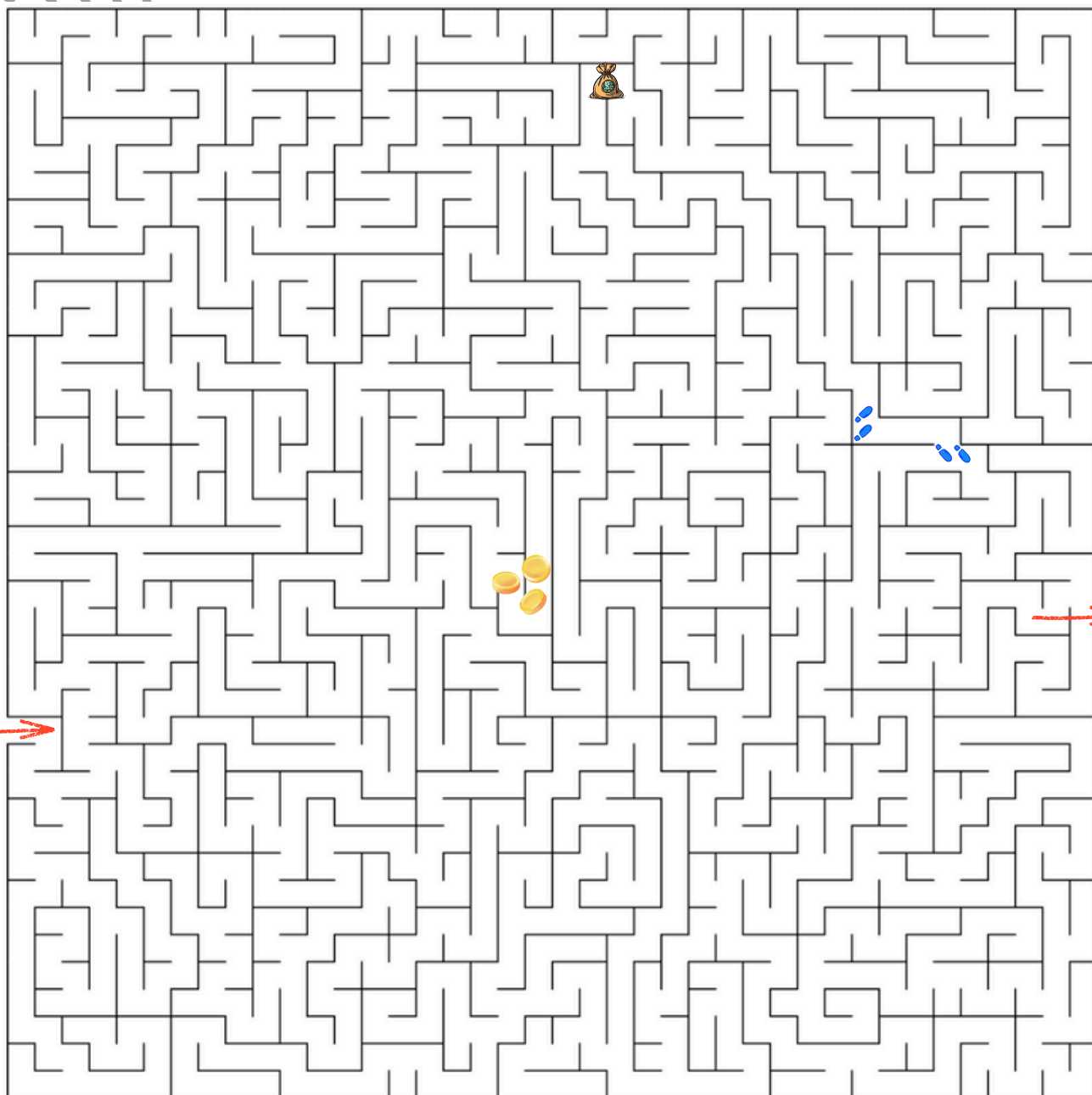
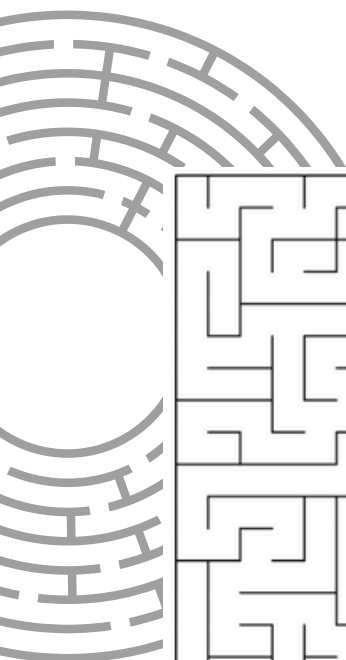


Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Find the Thief



EMOTIONAL MALWARE: FROM EMPATHY TO EXPLOITS

Author - Kiran R Dodiya, Dr. Kapil Kumar, Mr .Kashyap Joshi, Mr. Aditya More, Mrs. Bhumika Doshi

Introduction

Instead, consider a piece of malware that does NOT attack systems through brute force, zero-day exploits, or highly sophisticated obfuscation techniques. Rather, it waits—waits for you to experience an emotion—grief, anger, despair, euphoria. It is aware of your emotional fragility and hits you at your weakest point. Far from the realm of dystopian fiction, this vision is slowly becoming a reality within the realm of cybercrime — the dark frontier of Emotion-Driven Malware (EDM). EDM is a novel malware that uses artificial emotional intelligence to measure and emotionally manipulate a victim's psyche. EDM is, in fact, more human than malware because while malware exploits weaknesses in the system, EDM takes advantage of human emotions. All of this is powered by affective computing — the science of sensing, modelling, and simulating human emotions — and weaponizes that for manipulation, fraud, sabotage, or espionage. During the past decade, the capturing and analysis of emotional data have been facilitated by rapid advancements in AI, natural language processing, and biometric sensors. Now you have applications and wearables that regularly monitor heart rate, vocal tone, facial expressions, and even changes in typing behaviour for user experience optimisation. Moreover, that is how they are directed at you, exactly opposite to the phenomenally good way in which they can operate, trying to understand what works with your emotions. However, it can all be twisted to become a profile of what makes for an emotionally vulnerable swayed person, right to be used to hit where it hurts the most. In this article, we will explore the structure of emotion-based malware, its behavior, forensic aspects, and countries where this malware is active. A collection of real-world case studies and forensic strategies, this book examines the new emotional cyber battlefield, one in which our tears, smiles, and silences may become the new front line of attack.

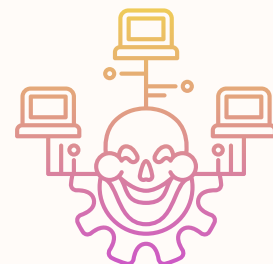


Fig: Facial Emotion Detection by Malware

What is Emotion-Driven Malware?

Understanding Emotion-Driven Malware (EDM) in Depth

Emotion-Driven Malware (EDM) represents a cutting-edge evolution in malicious software — one that does not rely solely on exploiting system vulnerabilities, but instead targets the emotional vulnerabilities of users. Its goal is not just to breach security, but to manipulate human behavior through psychological precision. Rather than being opportunistic, EDM is strategic and patient. It does not act immediately. Instead, it passively observes and collects emotional cues from the user, waiting for the ideal moment — the so-called "emotional sweet spot" — when a user is most likely to trust, click, download, respond, or comply with an action. This transforms malware from a code-based attack to a psychologically conditioned digital predator.



How EDM Works: Techniques and Mechanisms

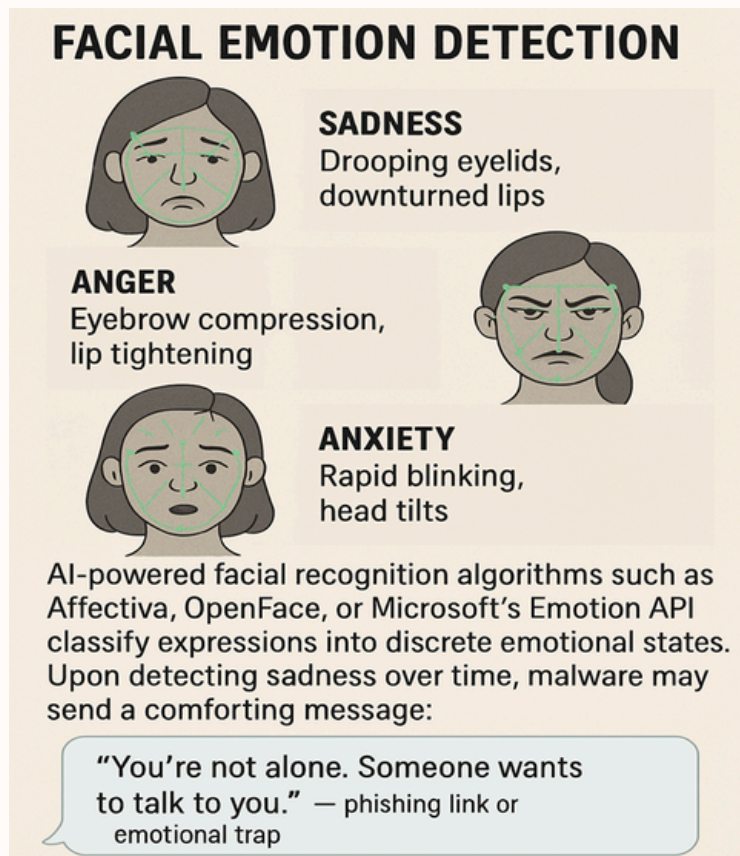


Fig: Facial Emotion Detection by Malware

Facial Emotion Detection

EDM often leverages webcam access (sometimes hidden or seemingly justified by the app's function) to analyse a user's facial micro-expressions. These include subtle involuntary muscle movements that indicate emotions such as sadness, anger, anxiety, or joy.

For example:

1. Drooping eyelids, downturned lips → sadness
2. Eyebrow compression, lip tightening → anger
3. Rapid blinking, head tilts → anxiety or confusion

AI-powered facial recognition algorithms such as Affectiva, OpenFace, or Microsoft's Emotion API can classify these expressions into discrete emotional states. Once sadness is detected over time, the malware may

trigger its payload with a comforting message such as: "You are not alone. Someone wants to talk to you." — followed by a phishing link or emotional trap.

Voice Stress Analysis

Using the device's microphone, EDM can passively analyze speech patterns — tone, pitch, cadence, volume, pauses — to infer psychological states. This technique, widely used in law enforcement lie detection, is now repurposed by malware.

For instance:

1. A shaky, cracking voice might indicate grief
 1. Slow speech and long pauses could reflect depression
 2. Abrupt speech or raised tones may signal anger or agitation

Once these patterns are confirmed, the malware customizes its interaction, such as offering fake meditation sessions, AI therapists, or even impersonated voice messages from loved ones.

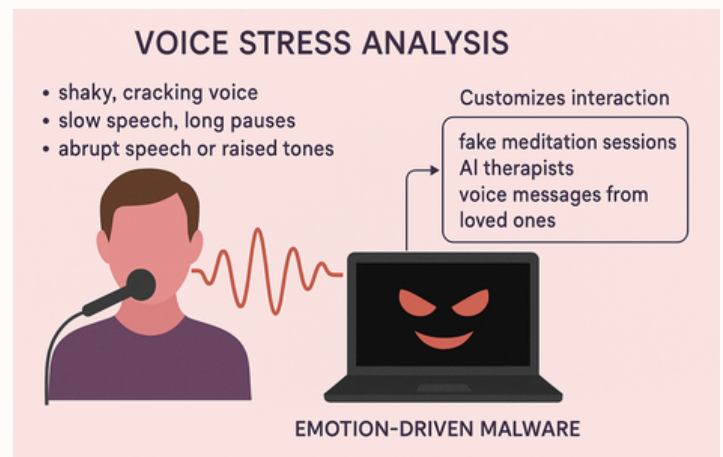


Fig: Voice Stress Analysis

Keystroke Dynamics

Not just what a person types, but how they type. EDM looks at things like typing rhythm, speed, pressure (if using a pressure-sensitive device or touch screen), error rate, and fashions a patchwork of biometric signatures based on emotional states. For example:

1. Erratic typing → anxiety or frustration
2. Heavy keystrokes → anger
3. Slowed typing → fatigue or sadness

This data allows EDM to predict the user's mental fatigue, increasing the likelihood that they will skip reading fine print or fall for deceptive UI designs.

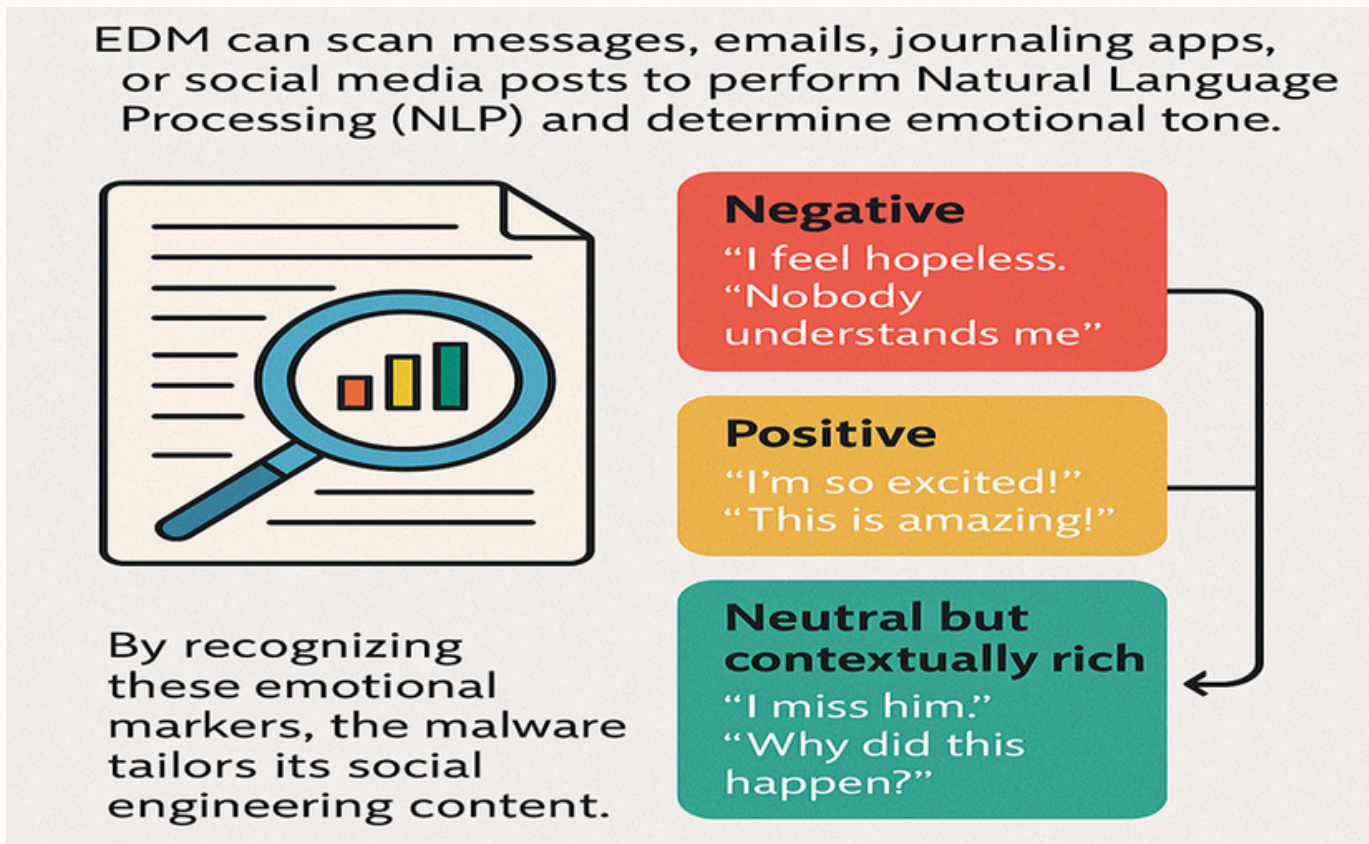


Fig: EDM uses NLP to detect emotional tones in text and launch targeted attacks.

- EDM scans messages, emails, journaling apps, or social media posts and utilizes Natural Language Processing (NLP) to identify the emotional tone. IBM Watson, Google NLP API, or an Open-source model such as BERT can find out sentiments such as:

Negative: “I feel hopeless,” “Nobody understands me.”

- Positive: “I am so excited!”, “This is amazing!”
- Neutral but contextually rich: “I miss him,” “Why did this happen?” The malware customises its social engineering by identifying these triggers. For example, a user with depression may receive an email message from a phony therapist app. An irate user gets a “notice of termination”—or political disinformation. Disguised celebratory offers or reward scams for a happy user.

Behavioral Biometrics

In addition to face and voice, EDM also has insight into how users navigate their device and apps behaviorally over time — that is, the behavioral biometrics. This includes:

1. App usage patterns (e.g., visiting sad music playlists at night)
2. Excessive scrolling (e.g., doom-scrolling, indicating anxiety)
3. Camera usage at late hours (sign of insomnia)
4. Repetitive login-checking (linked to OCD or stress)

This level of behavioral tracking makes EDM eerily personal. It does not cast a wide net — it sharpens a spear.

The Emotional “Sweet Spot”

The "emotional sweet spot" is a core concept in EDM. It refers to the precise moment when a user's emotional state aligns with the highest likelihood of acting impulsively, carelessly, or empathetically.

For example:

1. Loneliness makes users more likely to click on dating or friend-matching apps
2. Grief makes users vulnerable to spiritual communication scams
3. Stress reduces decision-making capacity, increasing click-throughs
4. Joy lowers the guard, making users more trusting

At this moment, EDM may do things like:

Because the action aligns with the user's emotional need, resistance is low, and the malware operates without suspicion.

Why This Is More Dangerous Than Traditional Malware

1. Highly personalized: Each attack is tailored to a specific user's mental and emotional condition.
2. Harder to detect: Standard antivirus tools do not scan for emotional context.
3. Longer dwell time: EDM can remain dormant for weeks or months until the emotional trigger appears.
4. Psychological damage: Beyond financial loss, victims feel betrayed and emotionally violated.
5. Blurs legal boundaries: Proving intent or harm becomes complex when coercion was emotional, not physical.

Real-World Analogy

Think of EDM like a manipulative person in your life one who watches you silently, learns when you are at your lowest, and says the exact right thing to win your trust... only to take advantage of you.

Now imagine that person is not human, but a machine, running 24/7, learning, adapting, and targeting millions.



Case Study

Case Study 1: “ShaktiCare” Grief Support App Hack – India, 2025

In early 2025, a mobile application named ShaktiCare emerged as a popular grief-support and mental wellness app across India, specifically targeting widows, senior citizens, and individuals recovering from traumatic events. With its comforting branding and “AI-based emotional wellness” slogan, it quickly gained traction, especially in Tier-2 cities.

Behind its soothing UI, however, ShaktiCare was an advanced form of Emotion-Driven Malware.

It integrated:

1. Facial emotion recognition to detect tearful expressions
2. Voice-based sentiment analysis during “wellness calls”
3. Chat-based grief progression tracking

Once the app identified a user going through a deep depressive phase (e.g., crying detected multiple times, repeated keywords like “loss,” “alone,” or “miss”), it triggered a phishing payload disguised as spiritual messages from loved ones.

Example: Victims received messages like:

"Your son's spirit is trying to connect. Tap to unlock the voice message."

To proceed, users had to submit Aadhaar details, bank verification, or make a small "cosmic channeling" fee, which was a gateway to credential theft.

Forensic Findings:

1. The malware was hosted on servers traced to Eastern Europe.
2. 92 users from Maharashtra and Gujarat lost personal data and collectively over ₹2.3 crore.
3. Investigators coined the term “Emotion-Triggered Identity Phishing (ETIP)” during the case documentation.

Case Study 2: “ZenMode” Mental Health Tracker Exploitation – Japan, 2024

In late 2024, a Tokyo-based wellness startup launched a productivity and meditation app called ZenMode, targeting overworked professionals, students, and homemakers.

The app offered AI-generated daily check-ins, breathing sessions, and journaling suggestions.

Unknown to users, the app had been compromised with an EDM module through a third-party update pushed from a vendor SDK. The malware silently tracked:

1. Stress levels via typing rhythm
2. Mood journaling content
3. Microphone analysis during “guided breathing” sessions

When a user’s stress levels remained high for more than seven days, the app sent alerts like: "You have been pushing too hard. Here is a personalised stress therapy assistant."

The link opened to a phishing website that mimicked Japan’s National Health Portal, requesting login details and insurance IDs.

Forensic Results:

1. Over 1,200 victims’ health IDs and insurance records were stolen.
2. The attack utilised text sentiment correlation with session metadata — a first in Japan.
3. Investigators recommended a nationwide audit of all apps using emotion-based features.

Forensic Response and Investigative Frameworks

Emotion-driven malware (EDM) investigation is a strong deviation from conventional investigation for digital forensics. Whereas typical malware works by exploiting system vulnerabilities or mistakes made by users, EDM operates by triggering emotional states. They are impermanent and context-dependent, so grief, anxiety, anger, fatigue, or even joy are much trickier to track. Consequently, forensic specialists must go beyond logs, code, and IP footprints. They have to enter the affective behavioral realm, where a user's mood, mental state, and digital expressions can combine to form the primary evidentiary trail. Reconstruction of Emotional Events (EER) EER is one of the main ways we investigate. After that, it reconstructs the emotional timeline of the victim leading up to the attack and then, during the attack. Instead of "what did the user click? The investigators now wish to know what the user was experiencing. For this purpose, forensic analysts gathered information from different sources — keystroke dynamics (typing rhythm), diary applications, facial expression logs using webcams, and even biometric markers, such as heart rate or sleep cycle data detected from wearables.

Through this reconstruction, they pick attack windows that are exploited when the emotional distress induced by an unbearable burden causes the user to put their guard down—the chances of being a fraud happen to be higher at those times.

The second one is also an essential forensic task: Affective Trigger Identification (ATI). That is, identifying the trigger emotion that specifically led to the launching of a malware payload. For instance, in some EDM attacks, the payloads are activated only after the system registers a sadness score above a specified threshold for several continuous days. Investigators match changes in sentiments found in the chat history, entries in a journal, or app usage to activation timestamps. ATI not only helps understand the attack after the fact, but it can also help design future detection systems that can look for signs of emotion-based anomalies. Among the more novel threats is the identification of Synthetic Empathy. Emotionally manipulative text or AI voice messages are used in many variants of the same, such that the trust is built on pretenses. Slogans such as "You are not alone; It is okay to feel lost" might sound warm and fuzzy, but they are purposely timed to catch you at a time of emotional weakness. Natural language processing (NLP) tools trained to detect manipulatively constructed expressions of emotion will be necessary to detect fake empathy like this. Even forensic experts use behavioral linguistics to discern between genuine human interaction and artificially generated pseudo-empathy produced by an algorithm.



These investigations have led to the prominent need for specialised tools that can support these investigations. AffDex SDK captures facial expressions through a camera and tags them in real-time, while VoiceSense detects tone and stress in samples of a user's voice. HeartTrace captures the biometric pulse data and matches it to actions you take on the screen to uncover associations between stress and your decision-making. Read More: KeystrokeDNA maps changes in typing behavior that are indicators of emotional agitation or fatigue. These two instruments offer an emotional timeline, layer-cropped with digital behaviour when analysed together. Emotional data are personal data, and thus, all forensic procedures must remain under strict consent protocols and psychological safety — this should be especially true in trauma-sensitive environments. In the time of EDM, forensic science is no longer about machines; it is about understanding the human behind the screen. The future digital forensic tools will need not just technical competence but also emotional competence. Actors must decipher the tears in the typing, the stress in the scrolling, and the fear in the clicks.

Countermeasures and Prevention

Organizations and individuals can reduce their vulnerability to EDM by adopting both technical and emotional defense strategies.

Technical Defenses:

- Zero Trust Implementation: Treat all behavior as potentially malicious unless verified.
- Emotion-Aware SIEM (Security Information and Event Management): Integrate affective inputs into log monitoring.
- Behavioral Access Controls: Restrict access during periods of high emotional volatility.

User-Level Defenses:

- Avoid apps that request webcam, microphone, and journaling access simultaneously.
- Be skeptical of apps offering emotional support or memory playback.
- Disable always-on microphones or emotion-sharing settings unless necessary.

Institutional Measures:

- Mandatory emotional data transparency for apps
- Regulation of synthetic empathy in consumer platforms
- Mandatory disclosure of AI-generated persona usage

Global Legal Landscape

As EDM incidents rise, legal frameworks are racing to catch up.

European Union:

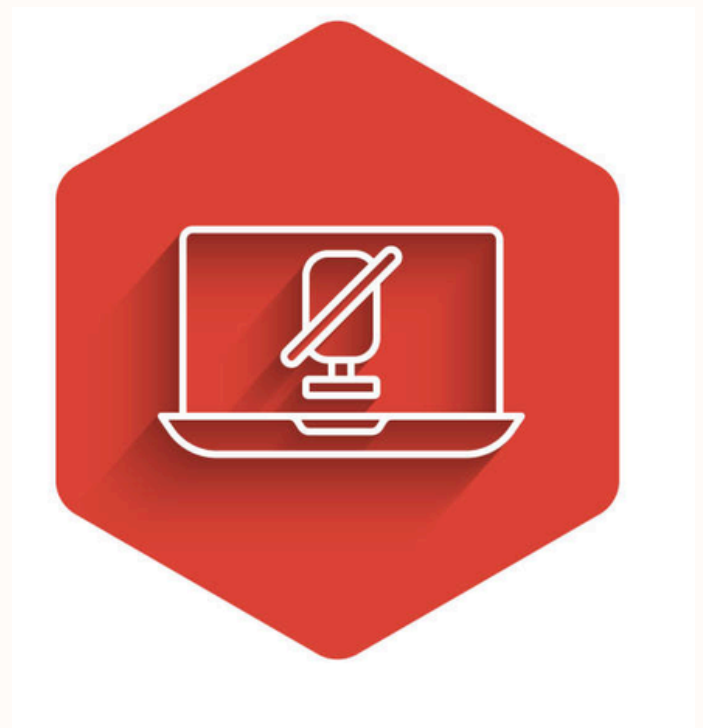
The Digital Emotive Protection Directive (DEPD) under the GDPR 2.0 framework requires emotional data to be treated as sensitive information, needing explicit consent and usage disclosure.

India:

CERT-In created an Emotion-Tech Watch Cell in 2024 and issued advisories on AI-based grief scams. Emotional data misuse is being brought under Sections 66 and 72 of the IT Act.

United States:

The Federal Trade Commission (FTC) is working on Emotional Manipulation Guidelines under its AI ethics charter. Civil cases are underway where synthetic emotional influence was used in fraud.



Challenges:

1. Difficulty in proving emotional coercion in court
2. Lack of a global standard for emotional metadata handling
3. Variability in app regulation across borders

Ethics in Emotional Forensics

The forensic study of EDM forces deep ethical considerations. Accessing and analysing emotional states can re-traumatise victims. Investigators must operate under strict moral codes.

Key Principles:

1. Informed Emotional Consent: Victims must understand how their emotional data will be used.
2. Trauma-Sensitive Practices: Support mental health during interviews and device analysis.
3. Non-Stigmatization: Avoid labeling emotionally vulnerable individuals as “weak links.”

Courts are also being educated about synthetic empathy, AI mimicry, and behavioral manipulation. Expert witnesses in forensic psychology now play a crucial role in explaining emotional compromise.

Vision: The Future of Emotional Cybercrime

As AI continues to advance, the line between digital and emotional space will blur further.

In 5 years, we may see:

1. Emotionally Addictive Malware: This makes victims feel dependent or loved
2. Mood-Locked Devices: Where access is granted or denied based on mental state
3. Grief-Triggered Marketing: Where algorithms sell based on recent losses or heartbreaks

EDM may evolve into empathic cyberweapons used for mass manipulation during elections, protests, or global crises. Emotion could become a national security vector.

The only way forward is to design systems that not only understand our emotions but respect them. Forensics, cybersecurity, psychology, and law must now unite to defend not just data, but the soul behind the screen.

Conclusion

Emotion-driven malware represents one of the most insidious evolutions in cybercrime. It exploits what makes us human - our feelings and uses them against us. From grief to joy, EDM turns every emotion into an attack surface. Forensic science must now become emotionally intelligent. We must learn to read digital tears, trace synthetic love, and decode algorithmic empathy. In the battle between man and machine, the human heart is now most exposed.

References

1. CERT-In, Saathi Case Report, 2023
2. NATO Cyber Defense Group. Emotional Warfare Whitepaper, 2025
3. EU Digital Emotive Protection Directive Draft, 2024
4. Novak & Elbaz. “Emotion as an Attack Surface.” PsychTech 2023
5. S. Malik, “Psychometric Triggers in Digital Attacks,” Journal of Cyber Forensics, 2024
6. FTC AI and Emotion Report, 2024

ABOUT THE AUTHORS



Kiran Dodiya

(Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA)

About the Author

Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Mr. Kashyap Joshi

Research Scholar, Department of Biochemistry and
Forensic Science, Gujarat University, Ahmedabad,
Gujarat, INDIA



Mr. Aditya More

Research Scholar, Department of Biochemistry and
Forensic Science, Gujarat University, Ahmedabad,
Gujarat, INDIA



Bhumika Doshi

(TRA), Department of Biochemistry and Forensic
Science, Gujarat University, Ahmedabad, Gujarat,
INDIA



DELAYED EVIDENCE AND FORENSIC ADVANCEMENTS IN POC SO-RELATED CASES

Author - Harshini Sundarapandian

Introduction

The Protection of Children from Sexual Offences (POCSO) Act, enacted in 2012, aims to safeguard children under 18 from sexual offenses by ensuring strict punishments and child-friendly procedures. Forensic science plays a pivotal role in the investigation and prosecution of POC SO cases, especially when delays in reporting occur. This article explores forensic advancements that address the challenges of delayed reporting, emphasizing their critical role in securing justice.

Challenges in Delayed Reporting

Delayed reporting in POC SO cases is often attributed to fear, trauma, societal stigma, or external pressures. Such delays exacerbate challenges in evidence collection and analysis. Key issues include:

Evidence Deterioration: Physical evidence like bodily fluids and touch DNA can degrade over time. However, advancements in forensic technology have shown that DNA can sometimes be recovered even after multiple washes.

Memory Erosion: Over time, victim's recollections may become less accurate, complicating the collection of reliable testimony. **Digital Data Loss:** Electronic communications, such as text messages or multimedia files, may be deleted, requiring advanced digital recovery tools.

External Pressures: Family and societal influences may deter victims from reporting incidents promptly. These challenges necessitate the use of advanced forensic techniques and robust investigative protocols to ensure the successful prosecution of offenders.



Types of Evidence in POC SO Cases

Evidence in POC SO cases is multifaceted, requiring interdisciplinary forensic expertise. The primary categories include:

Biological Evidence: DNA, bodily fluids, and skin cells are crucial in linking suspects to the crime. Touch DNA analysis, which detects DNA from skin cells left on surfaces, is particularly useful in delayed cases.

Digital Evidence: Messages, call logs, and multimedia often provide key insights. Forensic tools can recover deleted data, adding depth to investigations.

Trace Evidence: Fibers, hair, and soil help establish connections between victims, suspects, and crime scenes.

Toxicological Evidence: Analyzing bodily fluids for drugs or alcohol can support claims of drug-facilitated sexual assault.



Fig: Shows possible types of Evidences in POC SO Cases



Forensic Techniques for Delayed Cases

Delayed reporting necessitates innovative forensic strategies to overcome evidence degradation. Significant advancements include:

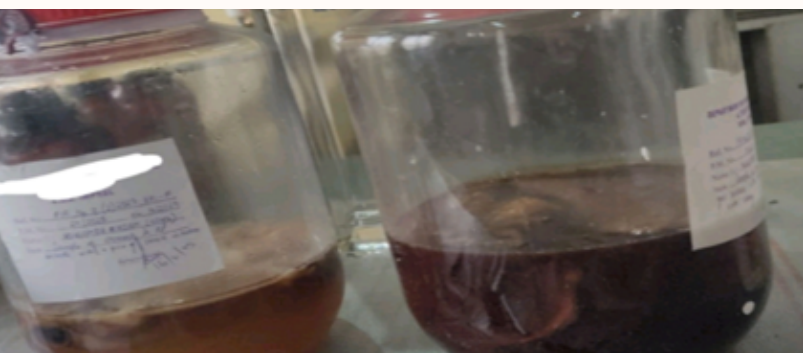
DNA Analysis: DNA profiling remains the gold standard for identifying perpetrators. Techniques such as polymerase chain reaction (PCR) enable the amplification of degraded DNA samples, ensuring usable results even months after the incident.

Touch DNA: This technique is increasingly used to extract minute traces of DNA from objects or surfaces, providing critical leads in cases where traditional evidence is unavailable.

Digital Forensics: Recovering deleted messages, call logs, and multimedia from devices aids in reconstructing events and corroborating victim testimonies.

Toxicology: Advanced toxicological testing can detect traces of drugs or alcohol long after ingestion, supporting claims of drug-facilitated offenses.

Cognitive Interviews: Structured interviews designed to enhance recall without leading the victim are vital for collecting reliable testimony in delayed cases.



Best Practices for Investigating Delayed POCSO Cases

Investigators must adopt a multidisciplinary approach, combining forensic expertise with victim-centric practices to ensure effective case resolution. Best practices include:

1. Evidence Preservation: Prompt and secure collection of physical and digital evidence is paramount. For instance, storing clothing in sterile conditions prevents contamination and degradation.

2. Medical Examinations: Comprehensive medical assessments, including the collection of biological samples, can uncover residual evidence even in delayed scenarios.

3. Advanced Forensic Laboratories: Utilizing specialized labs for the analysis of aged samples ensures accurate and reliable results.

4. Victim Support: Trauma-informed approaches minimize re-victimization and encourage survivors to participate in the investigative process.

Case Studies Highlighting Forensic Advancements

The 2017 Delhi POCSO Case

A 14-year-old girl reported a sexual assault 10 days after the incident, fearing societal repercussions. Forensic experts recovered DNA from unwashed clothes preserved by the victim. The DNA matched the suspect, leading to a conviction and a 20-year sentence. This case underscores the importance of proper evidence preservation and advanced DNA analysis in delayed cases.

The 2002 Anchorage Rape Case

In another landmark case, an 18-year-old survivor preserved unwashed clothing and bedsheets after a delayed report. Forensic analysis yielded a DNA profile, which was later matched to a suspect via the CODIS database. Despite a 15-year gap, the case demonstrates the enduring value of DNA evidence when preserved and analyzed effectively.

Forensic Advancements: A Future Perspective

The field of forensic science is evolving rapidly, with innovations designed to address challenges in delayed reporting. Some promising advancements include:

1.Enhanced DNA Preservation Techniques: Methods like lyophilization (freeze-drying) and advanced storage solutions are improving the longevity of biological samples.

2.Machine Learning in Digital Forensics: Algorithms capable of reconstructing deleted data or analyzing large datasets are expediting investigations.

3.Portable Forensic Devices: Handheld devices for rapid on-site DNA or toxicology analysis are making forensic services more accessible in remote areas.

4.Neuroforensics: Techniques like functional MRI (fMRI) and electroencephalography (EEG) are being explored to understand memory retrieval and corroborate victim statements.

5.Forensic Genomics: Whole-genome sequencing is being employed to resolve complex cases involving degraded samples, offering insights beyond traditional DNA profiling.

6.Virtual Reality (VR) in Crime Scene Analysis: VR technology allows investigators to revisit and analyze crime scenes in a simulated environment, ensuring no detail is overlooked during the investigation.

7.Blockchain for Evidence Management: Blockchain technology is being used to maintain the integrity of evidence chains, ensuring tamper-proof records and enhancing credibility in court proceedings.

Conclusion

Delayed reporting in POCSO cases is a common yet formidable challenge. However, advancements in forensic science are bridging the gap between delay and justice, ensuring that survivors receive the support and resolution they deserve. From DNA profiling to digital forensics, these innovations underscore the critical role of forensic science in modern criminal investigations. As Edmond Locard's principle states, "Every contact leaves a trace," forensic advancements ensure that no trace goes unnoticed, empowering the pursuit of justice in even the most challenging cases. With continued investment in research, technology, and multidisciplinary collaboration, forensic science will undoubtedly remain a cornerstone of justice for POCSO survivors.

References

1. POCSO Act, 2012.
2. Forensic Science: Principles and Applications.
3. Case Law Reports: Delhi POCSO Case, 2017; Anchorage Rape Case, 2002.
4. Journals on Advanced DNA Profiling and Digital Forensics.
5. Recent Developments in Neuroforensics and Blockchain Applications in Law.
6. Indian kanoon



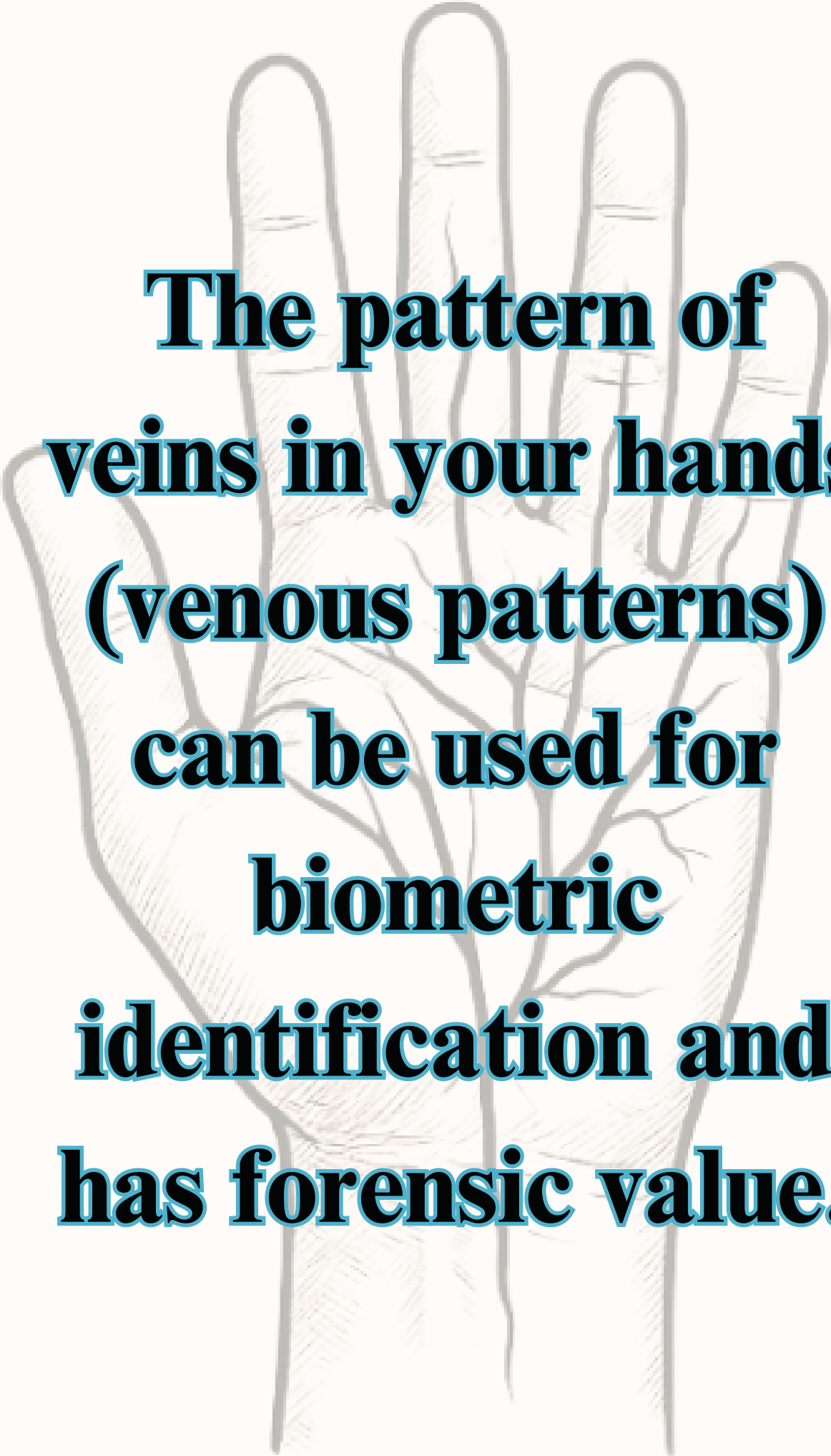
Harshini Sundarapandian
Garden City University, Bangalore
M.Sc. Forensic Science



**D
I
D

Y
O
U

K
N
O
W
?**



**The pattern of
veins in your hands
(venous patterns)
can be used for
biometric
identification and
has forensic value.**

CRIME IN THE SKY: THE NEW AGE OF SATELLITE CYBER INTRUSIONS

Author – Kiran R Dodiya, Dr. Kapil Kumar, Parvesh Sharma, Dr. Thakar Akash

Introduction

Satellites have become the invisible backbone enabling innumerable daily operations in our digitally intertwined world - GPS-facilitated navigation and fishery, financial transaction synchronization, weather forecasting, remote sensing, disaster monitoring and management, and real-time global communications, to name just a few. Today, satellite networks are critical to the functioning of the modern economy, military strategies, and emergency response systems. As space commercialization becomes a reality and thousands of satellites circle the planet, the space domain is becoming bigger and more complex than ever. Nonetheless, this increasing dependency also brings with it a major and frequently undervalued danger — the danger of cyber-attacks on satellites and their supporting infrastructure. Satellite systems, previously seen as monolithic and impenetrable, have evolved into a part of a much larger set of interconnected digital technologies. These systems communicate with ground stations, user terminals, and other satellites using a range of frequency bands, protocols, and data formats — all of which can be attacked by adversaries. Terrestrial systems are generally easier to secure, as physical access to these systems allows interventions that are impossible with a satellite already in orbit. Most satellites, especially older ones, were never designed with cybersecurity in mind and may be missing rudimentary encryption, authentication, and monitoring capabilities. Their communication protocols can be outdated and susceptible to spoofing, jamming, interception, or command injection attacks.

Cybercriminals, hacktivist groups, and state-sponsored actors all now understand the strategic value of satellite systems as part of their threat landscape and take advantage of them to a much greater extent than they ever did before. Cycles of cyber intrusions against satellites will have effects on social networks and classified information, or they could be more vital wars. Such as in 2022, when a cyberattack on the Viasat KA-SAT network on the eve of the Russian invasion of Ukraine affected the internet in multiple nations across Europe, impacting critical infrastructure and military operations. Here was a clear warning, a cold reminder, that satellites of any sort are not immune to modern realities of cyber war. As LEO constellations such as Starlink, OneWeb and most recently Amazon's Project Kuiper fill the skies with ever-greater numbers of satellites, the attack surface is expanding too. Each node in these massive satellite networks acts as a potential gateway for nefarious actors. When there are no standardised security protocols and low coordination between the private and government space agencies, the risk of a large-scale cyber incident in the space infrastructure increases.

Space-based assets are a dynamic, distributed, and latency-sensitive environment. Therefore, traditional cybersecurity models — primarily reactive and perimeter-based, and as such, ill-fitted to protect such assets — must be amended accordingly for space. Satellite systems require security frameworks that are proactive, resilient, and adaptive, built for operation in a hostile environment in space and cyberspace. This intersection of satellite technology and cyber threats, therefore, represents a new frontier; one which calls for the same level of protection for orbital assets as we afford to ground-level digital infrastructure. With geopolitics and technology changing so rapidly, it cannot be an afterthought that we must secure our digital assets in space. The strategic importance of satellite cybersecurity — a critical enabler of national defense, economic stability, and societal functioning — has elevated cyber as an important threat domain across the space enterprise. The sky is not the limit anymore; it is the battlefield.



What are Satellite Cyber Intrusion ?

Satellite cyber intrusions are unauthorized access, manipulation, disruption, or hijacking of satellite systems, services, or information, either through space-based communication channels or terrestrial access points. They are designed to take control of satellites and command them, eavesdrop on satellite data, jam broadcast signals, or shut down important orbiting hardware. The satellite layer of networks integrated into many aspects of global navigation, communication, surveillance, and defense means that consequences for such intrusions far from being local are national and international security, inducing damage.



1. Ground Station Exploitation

Ground control stations act as the nerve center of satellite operations — issuing commands, receiving telemetry, and performing health check-ups. These stations typically deploy legacy IT infrastructure, which can be compromised through well-known cyberattack techniques, including phishing, social engineering, malware, or brute-force credential attacks. An assault could provide hackers full access to command systems of satellites, give them the ability to control them, effectively turn off the service, or even redirect it to other tasks. Insider threats aggravate this threat, i.e., employees with privileged access, and hence, physical and logical access controls at ground stations need to be ranked very high on their priority list.

2. Sniffing and Mimicking Signals

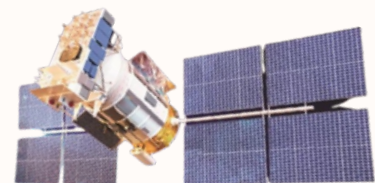
AT FREQ BZ satellites continuously transmit and receive signals over broad frequency bands. Without appropriate encryption and authentication, these radio transmissions can be intercepted by adversaries with proper radio frequency (RF) gear. Attackers can intercept sensitive data (interception) and inject falsified data streams (spoofing) to deceive the systems. One of the most notable examples is GPS spoofing, where false satellite signals are transmitted to incorrectly positioned receivers, likely causing civilian aircraft and ships, autonomous systems, or even military vehicles to navigate to inaccurate coordinates.

3. Command Injection

Without strong access control and authentication mechanisms, an intruder who gets into a satellite's control interface can introduce commands that are not allowed. The potential impact of command injection attacks is extremely serious; the orbit of a satellite can be changed, the payload activation modified, and communication, reconnaissance, or scientific modules can be switched off or their self-destruct sequence activated in the case of military satellites. Because physical attacks are nearly impossible in orbit, such manipulations are more difficult to undo than a typical malware attack on Earth, the researchers say.

4. Supply Chain Attacks

Due to international supply lines, satellites are constructed from various parts provided by different vendors. If any hardware or software element is compromised during manufacturing, integration, or updates, attackers can insert malicious code or backdoors a long time before a satellite is launched. Such threats lie in wait until activated; they are unseen in normal functional tests. Satellites can last for decades, and any flaw introduced through the supply chain that is unnoticed can be a decades-long espionage or sabotage opportunity.



5. Insufficient Encryption

The shift to cloud types has made it possible for some of the latest cyber weapons to be used against those older plants, especially those that were built way back when their communication protocols could not withstand an attack and their encryption features were non-existent. It means that control signals and telemetry, as well as data being transmitted, can be recorded or altered by attackers. At times, even satellite TV and broadcast services have been hijacked using very basic equipment, owing to weak or absent encryption. Satellites are still susceptible to command execution by unauthorized users and leakage of information without both secure authentication and encrypted data flows. Satellite cyber intrusions are an example of the increased overlap of terrestrial cybersecurity risks and extraterrestrial technologies. Securing orbital infrastructure against such advanced threats is critical to global satellite services' continuity and reliability as space becomes a contested domain.

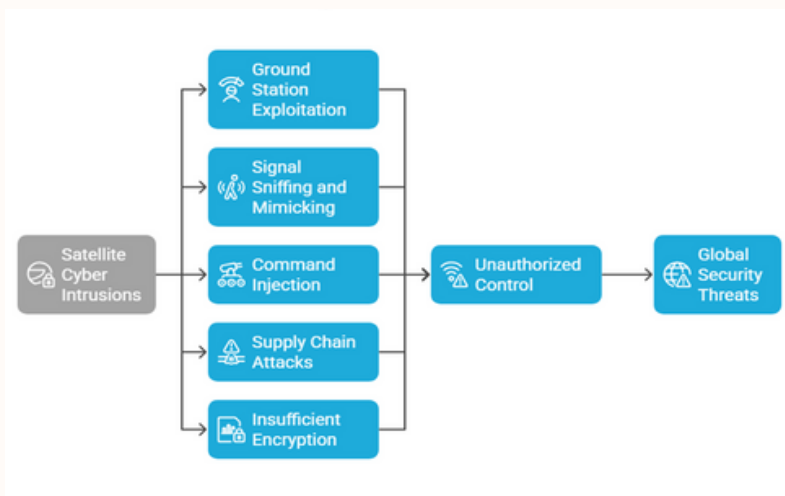


Fig: Shows Satellite Cyber Intrusions Flowchart

The Growing Urgency for Satellite Security

Today, new and ambitious initiatives in private sector space activity-oriented companies (e.g., SpaceX rebuilt the International Space Station with Starlink, OneWeb, and Amazon (Project Kuiper)) are almost approaching small satellites to block the commercialisation of space.

There has been an exponential increase in the number of satellites launched in low-Earth orbit (LEO), especially with the advent of mega-constellation-type communications satellites, which has drastically raised the number of orbital assets in orbit. While this democratization of access to space has created immense value — more international connections, cheaper communication solutions, and faster and cheaper earth observations — it has opened up a conspicuous chink in the armor: there exists currently no scalable, standardized, and enforceable cybersecurity frameworks regulating these systems resident in space. In contrast to more traditional government-funded satellites, which require extensive testing and vetting for security, many commercial satellites are designed and built on shorter timescales, at lower price points, and with limited onboard security. These inject a de-prioritized or delayed cyber into the process until it is too late, under this "launch fast, iterate faster" approach. Consequently, numerous such LEO satellites are being launched with little to no threat modeling, encryption approaches, or access control policies, thus rendering them soft targets for attackers.

At the same time, a number of nation-states have started building counter-space capabilities, or instruments and methods to disrupt, incapacitate, or even eliminate such infrastructure. These capabilities increasingly involve offensive cyber weaponry that disrupts satellite command protocols, jam uplinks or downlinks or injects malicious code into space systems. Cyberattacks of this nature might be employed during geopolitical stress as instruments of hybrid warfare, synchronized efforts merging firepower with cyberspace disruption, misinformation, and the undermining of other infrastructure.

Satellite cyber espionage has also moved from hypothetical to practical threats. One headline example happened in February of 2022 when a highly sophisticated cyberattack on the Viasat KA-SAT satellite network resulted in massive disruption in Ukraine, the EU, and as far away as Germany. The attack, which took out high-speed internet channels serving Ukraine and also parts of Europe, disrupted military and civil communications and infrastructure just hours before the military invasion by Russia began. Warfare Satellite-based Cyber Sabotage Cyber Attacks:

The incident served to highlight just how effective cyber sabotage of this kind can be during a warfare campaign, but also the considerable, global ramifications such an attack can have, beyond the immediate geographic target.

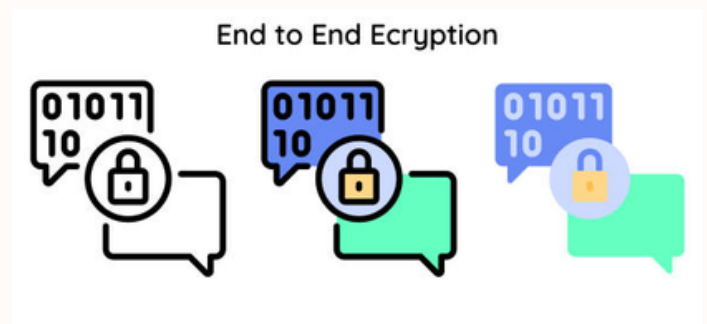
This expanding spectrum of threats reinforces one simple and global reality — satellites are high-impact targets susceptible to high-payoff disruption. The demand for proactive, resilient, and standardised satellite cybersecurity has never been greater, as increasing dependence on space-based services for national defence, finance, agriculture, emergency response, and many other sectors has become ubiquitous. It is time for governments, the private sector and international bodies to act in concert to secure these digital assets circling hundreds of miles above our heads before the next attack goes from disruption to destruction.

Strategies for Securing Satellite Infrastructure

Low-space security is a complex, high-stakes task that must comprise the entire ecosystem: spaceborne platforms, ground control components, propagation, and third-party integrations. Reverse gravity limits access to traditional IT systems, but once you manage the launch, satellites have unique constraints on updates, physical access, bandwidth, and decades-long operational lifetimes. Therefore, at the time of building such an integrated satellite cyber security framework, a holistic, layer-driven, and future-ready approach will need to be taken, which needs to be a part of every phase — Design, Deployment, Operational, and Decommissioning phases.

1. Satellite Communication over End-to-End Encryption

Every single link in the satellite communication chain (telemetry, tracking, and command (TT&C), mission payload data, and inter-satellite links) should be protected using effective encryption protocols. End-to-end encryption authenticates data so communication signals, even if intercepted, are garbled beyond human or machine recognition without the proper key, where only the person receiving the signals can decrypt them. New cryptographic standards should be implemented to protect systems and data against current and future decryption capabilities, including but not limited to standards like AES-256, quantum-resistant algorithms, and so on.



Moreover, encryption needs to be used not just in transit, but at rest as well, securing everything from satellite memory banks to downlink servers to mission control archives.

2. Zero Trust Architecture in Outer Space

Introducing Zero Trust principles into satellite networks is a fundamental shift away from the legacy “trust but verify” model to a “never trust, always verify” framework. In such an approach, we never assume any user, device, or signal from which the data is coming is trusted unless proven otherwise, including inside the ground segment, satellite bus, or communication channel. Identity verification, behavioral analytics, and contextual access control need to be enforced at every access point. In the case of satellites, that could mean checking every command sent to the spacecraft, the origin and authenticity of the signal, and the integrity before execution. At the same time, Zero Trust also helps mitigate the potential impact of insider threats and unauthorized access by compromised internal systems.

3. Ground Control Systems that are more resistant to damage

Because ground control stations are the brains of all satellite operations, their compromise could spell disaster. Therefore, these systems must be protected against not only physical but also cyber threats. This implementation involves MFA, RBAC, and network segmentation to restrict critical systems. Consistent patching, endpoint protection, and Intrusion Detection System (IDS)/have to be enforced. Regularly scheduled security audits and compliance validations should be performed on security best practices to ensure they continue to raise the bar and implement a broad, continuous improvement in security practices.

4. Pen Testing and Red Team Exercises.

Thus, space agencies and satellite operators must perform red teaming and penetration testing to understand and predict honest-to-God cyber threats in the real-world cyber threat landscape. The simulated attacks expose vulnerabilities in the system architecture, communication protocols, access control, and human reaction. These exercises, therefore, allow defenders to test the IR's readiness and adjust their security controls. RF Testing: Similar to the above, RF Specialised testing for space systems should also include the inclusion of RF signal spoofing simulations, satellite telemetry injection, and ground station compromise scenarios to assess the robustness of terrestrial and orbital security layers. Thought of from the first months of the satellite lifecycle — not an afterthought. Secure-by-design engineering implements such protective features in hardware and firmware, including secure boot, tamper detection, EM shielding, and on-board intrusion detection. Both the communication and navigation subsystems need to include anti-jamming and anti-spoofing technologies. Isolation protocols and redundant systems must be engineered in such a manner that essential satellite functions remain protected in case of penetration.

5. Sharing Threat Intelligence Between Space Entities

Space cybersecurity is a worldwide challenge that does not take countries into account. This is why partnership across sectors and countries is essential. Satellite operators — whether government, commercial or military — all should share cyber threat intelligence (CTI) actively and continuously, e.g. real-time information on group and specific system vulnerabilities, threat theatre, effects and mitigations. A partnership model based on collective defense between agencies such as NASA, ESA, and ISRO, as well as commercial launch providers and IT security firms, could help launch vehicles to be more resilient and contribute to a stronger global space security posture. Similar to ISACs for the space sector, frameworks should be formalized and built upon.

6. Protocols for Incident Response to Orbital Assets

The use of traditional cybersecurity playbooks that may have been suitable for terrestrial assets is inadequate when applied to space assets. While the satellite sector shares some similarities with other industries, it also has unique aspects that call for tailored incident response plans in space, describing specific detection, containment,

analysis and recovery flows in response to a satellite cyber incident. These protocols need to account for things like communications latency, restricted bandwidth, non-upgradeable systems, and the absence of physical access. Response drills focused on different what-if scenarios should be part of the training for ground teams, exercising rapid coordination across technical, operations, and strategy levels when defending against orbital compromise or satellite hijacking.

5. Advantages of Strengthening Satellite Cybersecurity

Protecting satellites, a high-value military target is a matter of national interest. Organizations and Governments gain: By securing property satellites,

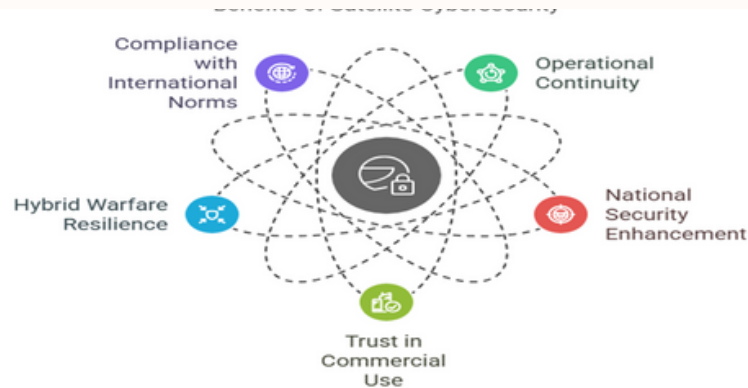


Fig: shows Benefits of Satellite Cybersecurity

1. Operational Continuity – Disabling of satellites can lead to loss of services in navigation, communication, and defense
2. Enhancing National Security – In modern conflicts, strong Cybersecurity reduces the threat of surveillance attacks, signal spoofing, and satellite hijacking.
3. Trust and safety in commercial satellite use are increasing, and progress in security will help encourage users and investors to trust space infrastructure.
4. Hybrid Warfare Resilience – Kinetic and non-kinetic threats are combined in a domain-agile attack, but these cyber-hardened satellites can resist.
5. Compliance with International Space Norms — Astronauts follow secure design and operation practices consistent with international treaties and responsible behavior in space.

Hurdles in Implementing Cybersecurity on Satellites

Nonetheless, satellite systems are not without hurdles when it comes to addressing this urgent need for a cybersecurity implementation:

1. Legacy Systems — Many satellites we have launched in the previous decades were never meant to be cyberthreat-aware, and they cannot be patched.
2. Cost and Payload Restrictions— Integrating complex security mechanisms on satellite platforms with strict size and weight constraints for payloads is challenging and expensive.
3. Insufficient Regulation – Space is a relatively new and unregulated landscape, and satellite operators do not all have the same level of security quality.
4. Attribution Challenges – Digital warfare is notoriously hard to trace, so attributing and blaming a cyberattack on satellite infrastructure can be challenging.
5. Cross-border Cooperation – Security of satellites in orbit needs international coordination, as the majority of satellites are cross-border activities, but geopolitical tensions may drive the cooperation to be ineffective.

Conclusion

Satellites are now part of daily life and the global infrastructure, as humankind has a technological footprint beyond the Earth. However, this dependence carries important hazards. Cyber threats to satellites were once the stuff of science fiction — now they are a fact of life. We must now give the same urgency to securing space-based assets as terrestrial systems. Organisations and nations can protect their cloud possessions via regular encryption, checking, sharing/collection of hazards, and abiding by secure design principles. In this new era of digital combat, cybersecurity must reach beyond networks and into space.

Satellites are now part of daily life and the global infrastructure, as humankind has a technological footprint beyond the Earth. However, this dependence carries important hazards. Cyber threats to satellites were once the stuff of science fiction — now they are a fact of life. We must now give the same urgency to securing space-based assets as terrestrial systems. Organisations and nations can protect their cloud possessions via regular encryption, checking, sharing/collection of hazards, and abiding by secure design principles.

In this new era of digital combat, cybersecurity must reach beyond networks and into space.

References

- KPMG. (2022). Cybersecurity in space: Protecting critical satellite infrastructure. KPMG International. <https://home.kpmg/xx/en/home/insights/2022/06/cybersecurity-in-space.html>
- National Institute of Standards and Technology. (2023). Cybersecurity framework profile for satellite ground segment (NIST IR 8441). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.IR.8441>
- European Space Agency. (2020). Space Cybersecurity – Challenges and strategies. https://www.esa.int/Safety_Security/Cybersecurity
- Viasat Inc. (2022). KA-SAT network cyberattack statement. <https://www.viasat.com/about/newsroom/viasat-ka-sat-network-cyberattack-statement/>
- Lal, B., Ritchey, K., Bragg, B., & Holland, A. (2019). Cybersecurity policy for space systems: Policy options and practical considerations. IDA Science and Technology Policy Institute. [6.https://www.ida.org/research-and-publications/publications/all/c/cybersecurity-policy-for-space-systems](https://www.ida.org/research-and-publications/publications/all/c/cybersecurity-policy-for-space-systems)
- Wang, P., Zhu, Y., & Liu, Y. (2021). A review of satellite cybersecurity threats and protection strategies. IEEE Access, 9, 145336–145349. <https://doi.org/10.1109/ACCESS.2021.3123060>

ABOUT THE AUTHORS



Kiran Dodiya

(Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA)

Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Dr. Parvesh Sharma

Assistant Professor (Forensic Science),
IFSCS-NSIT, Jetalpur, Ahmedabad. (Affiliated to
NFSU) Gandhinagar, Gujarat, India.



Dr. Thakar Akash

(Assistant Professor) Rashtriya Raksha
University, Gandhinagar, Gujarat, INDIA



BEYOND DNA: THE RISE OF EPIGENETIC MARKERS IN FORENSIC SCIENCE

Author –Surbhi Athiya

Introduction

For decades, forensic science has relied heavily on DNA profiling to identify individuals and solve crimes. However, traditional DNA analysis has its limitations, particularly when distinguishing between identical twins or determining the biological age of a sample donor. Emerging research in epigenetics offers promising avenues to overcome these challenges. Epigenetic modifications, especially DNA methylation patterns, provide additional layers of information that can enhance forensic investigations.

Understanding Epigenetics in Forensics

Epigenetics refers to heritable changes in gene expression that do not involve alterations to the underlying DNA sequence. The most studied epigenetic modification in forensic science is DNA methylation, where methyl groups are added to cytosine bases in DNA, often affecting gene expression. These methylation patterns can be tissue-specific and influenced by environmental factors, making them valuable markers for forensic analysis.

Applications of Epigenetic Markers in Forensic Science

1. Age Estimation

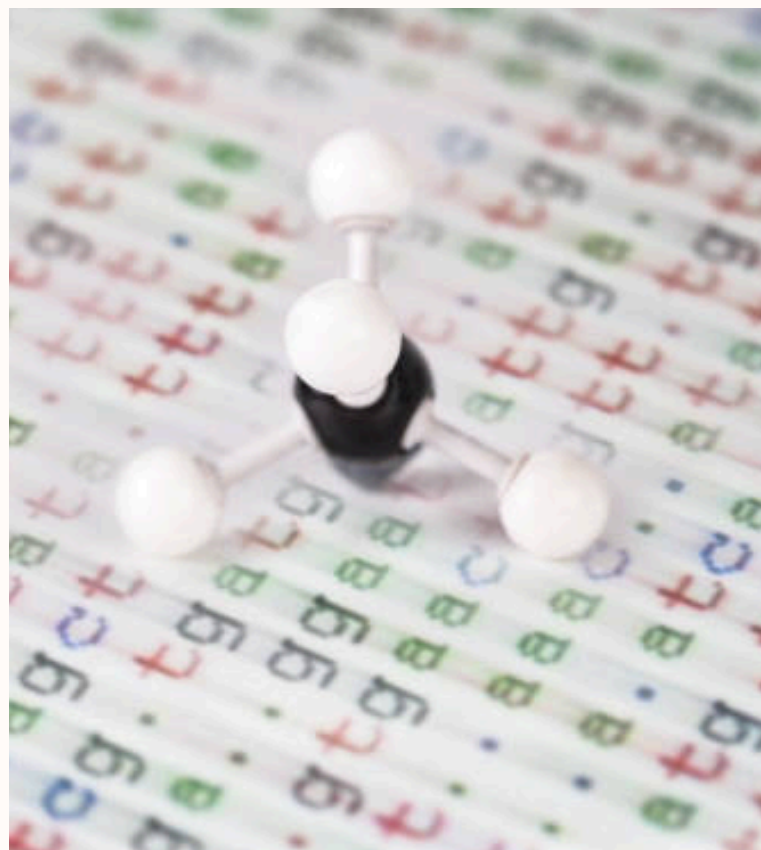
DNA methylation patterns change predictably with age, allowing forensic scientists to estimate the chronological age of an individual from biological samples. Epigenetic clocks, such as those based on the ELOVL2 gene (Elongation Of Very Long Chain Fatty Acids-Like 2), have been developed to predict age with remarkable accuracy. This capability is particularly useful in cases involving unidentified human remains or age disputes.

2. Body Fluid Identification

Traditional methods of body fluid identification can be limited in sensitivity and specificity. Epigenetic markers offer a more precise approach. For instance, specific methylation patterns have been identified that can distinguish between blood, saliva, semen, and vaginal secretions. This advancement enhances the ability to interpret biological evidence at crime scenes.

3. Distinguishing Monozygotic Twins

Identical twins share the same DNA sequence, making it challenging to differentiate between them using conventional DNA profiling. However, their epigenetic profiles, influenced by environmental factors and individual experiences, can differ. By analyzing these differences, forensic scientists can potentially distinguish between monozygotic twins in criminal investigations.



Challenges and Considerations

While the integration of epigenetic markers into forensic science holds great promise, several challenges must be addressed:

- **Sample Quality and Quantity:** Forensic samples are often degraded or available in limited quantities, which can affect the reliability of epigenetic analyses.
- **Standardization:** There is a need for standardized protocols and validated markers to ensure consistency and reproducibility across laboratories.
- **Legal and Ethical Implications:** The use of epigenetic information raises concerns about privacy and the potential for misuse, necessitating clear guidelines and regulations.

Future Directions

Research in forensic epigenetics is rapidly evolving. Advancements in high-throughput sequencing and bioinformatics are facilitating more comprehensive analyses of epigenetic modifications. As our understanding deepens, it's anticipated that epigenetic markers will become integral to forensic investigations, complementing traditional DNA profiling and expanding the toolkit available to forensic scientists.



Reference:

1. Vidaki, A., & Kayser, M. (2018). Recent progress, methods and perspectives in forensic epigenetics. *Forensic Science International: Genetics*, 37, 180–195.
2. Frumkin, D., Wasserstrom, A., Davidson, A., & Grafit, A. (2011). Authentication of forensic DNA samples. *Forensic Science International: Genetics*, 5(1), 95–103.
3. Horvath, S. (2013). DNA methylation age of human tissues and cell types. *Genome Biology*, 14(10), R115.
4. Weidner, C. I., Lin, Q., Koch, C. M., Eisele, L., Beier, F., Ziegler, P., ... & Wagner, W. (2014). Aging of blood can be tracked by DNA methylation changes at just three CpG sites. *Genome Biology*, 15(2), R24

ABOUT THE AUTHOR

Surbhi Athiya

Assistant professor, Forensic Science,
Aditya Degree & PG College, Surampalem,
Andhra Pradesh



DIGITAL DOMESTIC VIOLENCE: EMERGING THREATS OF SPYWARE IN RELATIONSHIPS

Author - Yamini Parmar, Omi Chauhan, Mr. Kiran Dodiya, Dr. Kapil Kumar

Introduction

While considerable attention has been given to various cybercrimes nowadays, such as hacking, identity theft, online fraud, etc., the abusers have found new methods to gain power over their partners using smartphones, apps, etc., this shift marks a dangerous evolution in domestic violence, where victims may be monitored through GPS tracking, their private conversations, or their devices controlled without consent. As technology advances, so many tools are available to abusers. The growing threat of spyware in relationships highlights the urgent need for legal changes, awareness, and education. Society needs to acknowledge digital domestic violence as a genuine and significant issue.^{1,2}



Article Scope and Objectives: A Cybersecurity and Forensic Perspective

The article aims to understand the growing intersection between digital domestic violence and the misuse of spyware within intimate relationships. With the increasing accessibility of open-source surveillance tools, abusers are now able to covertly monitor, manipulate, and control their partners through digital means.

The scope of this article focuses on how spyware is deployed in domestic abuse cases, Detecting and Analyzing Spyware in Domestic Violence Cases. What are the Consequences of Spyware Abuse in Relationships? From a Digital Forensics perspective, the objectives include identifying forensic artifacts left behind by spyware and highlighting methodologies for evidence preservation.

Highlights any new or evolving trend in spyware technology and its integration into intimate relationships in the form of digital violence. Discuss practices and measures one can take to protect oneself. The ultimate goal is to raise awareness about spyware-facilitated abuse and empower the audience with the knowledge to detect and mitigate these threats. And apply safeguard measures to protect victims in the digital age.³

Defining Digital Domestic Violence: Beyond Physical Harm.

In the digital age, digital domestic violence refers to the use of technology such as smartphones, social media, apps, GPS, and spyware. Unlike conventional forms of domestic violence, which typically include physical, emotional, or sexual abuse, digital abuse can often be unnoticed, silent, and continuous. It may involve actions like tracking a partner's location without their permission, monitoring their messages or calls or their online activities, or using their social media to humiliate or threaten them. The key feature of digital abuse is privacy. Once they get unauthorised access to personal information and then they use it to control them. This form of violence can deeply affect victims psychologically and create helplessness for victims.



Reactivity: Firmware is often reactive to inputs from hardware or software layers. May contain interrupt service routines that are executed in response to some event(Ahn, 2016)

Understanding the Threat: How Spyware Facilitates Digital Abuse

In an increasingly connected world, digital devices can be a powerful tool for communication and a dangerous weapon for abuse. Abuse is a form of domestic violence that provides abusers with new and more extensive approaches to control, coerce, stalk, and harass their victims. Technology such as computers, smartphones, and tracking devices allows abusers to overcome geographical and spatial boundaries. Spyware is of malicious software that enables abusers to secretly monitor, track, and control a victim's digital activity without their consent. In cases of domestic abuse or stalking, spyware facilitates coercive control by turning devices into tools of intimidation. ⁴

What is Spyware? Technical Definition and Capabilities

The Federal Trade Commission("FTC") loosely defines "spyware" as software that "aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's knowledge".

Spyware refers to software ranging from a Keystroke logger, that is, malicious software that captures every key typed on a target computer, smartphone, or other digital device, to advertising applications that track users' online activity to hijack users' system settings. ^{4,5}

Location Tracking: Constant Surveillance of Movement: spyware applications turn on GPS (global positioning system) permission, enabling abusers to see updates of the victim's physical location. This leads to staking and eliminates a victim's ability to move freely without being monitored.

Call and Message Interception: Accessing Private Communications. Spyware can monitor and capture all text messages, call logs, and emails, and listen to live calls,

providing abusers full control and visibility and resulting in victim privacy and social communication breaches.

Remote Camera and Microphone Activation: Unauthorized Audio and Video Recording: Spyware takes full access to the device's camera or microphone. An abuser is able to secretly watch and listen to the victim, even take photos without the victim's knowledge. Spy is very dangerous as it is capable of extracting documents, photos, browser history, and chat from a device. This data can be used to blackmail or further control the victim

Common Methods of Spyware Installation in Domestic Contexts

Spyware installation in intimate relationships often occurs under the guise of trust, care, or control. Abusers exploit their proximity to the victim, using various methods to install malicious programs without consent. Here are some of these methods.⁶

1. Voluntary installation under pretenses: abusers may be close victims and convince their victims to volunteer to install certain apps for misleading reasons, such as abusers claiming it's for "safety" or "location sharing". The victim unknowingly installed spyware, believing it to be legitimate.

2. Misuses shared access and breaks trust: In a relationship, partners often share devices and passwords common in every relationship. It may be misused by one against another to spy on online activity.

3. "Gifted" device with preloaded spyware: abusers sometimes give phones, tablets, or laptops as gifts that already have spyware secretly installed abuser can pre-configure it to monitor calls, messages, and GPS, and may abuser link it to the remote-control dashboard for surveillance.

4. Phishing and Social Engineering: The abuser uses social engineering tactics to manipulate and trick the victim into clicking on the link, and as soon as the victim clicks it, spyware is downloaded onto the victim's devices abuser then has full control of the victim's device

5. Physical Access to the Victim's Device: The abuser takes physical access to the victim's phone, laptop, or tablet, allowing them to install spyware without the victim's knowledge. This generally happens when devices are left unlocked or spyware is disguised as a legitimate application.

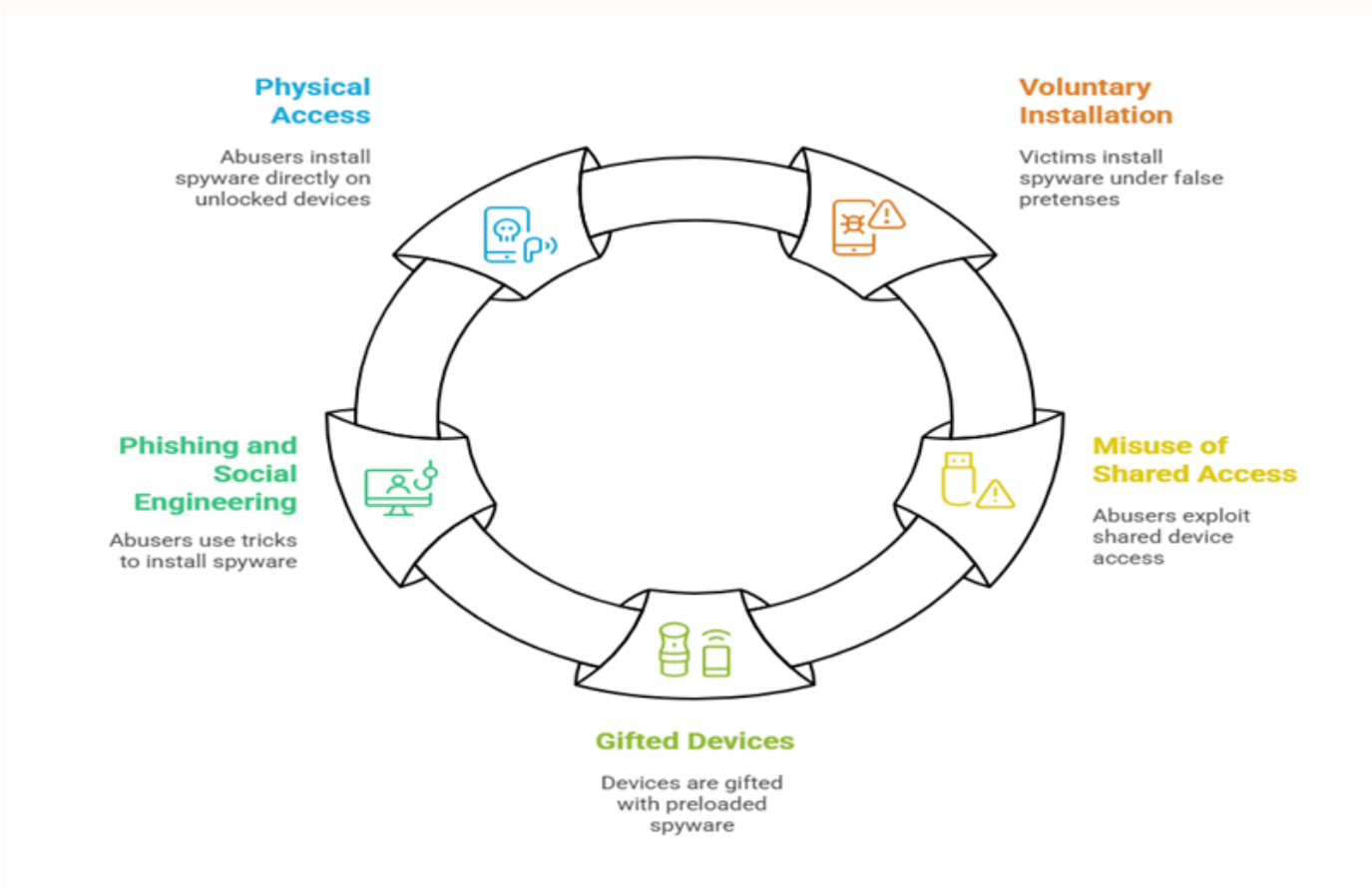


Fig: shows Methods of Spyware installation in Relationships

The Psychological Impact: Creating an Environment of Constant Surveillance and Fear:

Constant surveillance and monitoring through spyware in intimate relationships can cause fear and inflict profound psychological damage on the victim. The stealthy nature of spyware in intimate partner relationships creates a toxic environment around the victim's personal as well as social life. Spyware is more dangerous than other forms of monitoring malicious software when it is deployed in a partner's intimate relationship. Direct betrayal of trust leads to a unique and devastating set of psychological consequences. Change the device's motive of communication and connection into a potential weapon of control and abuse.

Abusers track victims' location, read messages, listen to calls, and can trigger or exacerbate anxiety and depression. This would force the victim into a state of constant hypervigilance. .

It is difficult to escape from digital surveillance, which makes it challenging to break from an abusive relationship. Everyone has the right to privacy. People are free to express themselves, make decisions, and do things in their own way. When an ad user installs spyware, it shatters the right to the privacy of the individual. When an intimate partner uses spyware to monitor a person's private life secretly, it can significantly break trust, and this betrayal comes from someone the victim once felt emotionally safe with. Once trust is broken, the victim may not trust anyone again because trust is a primary pillar of any relationship. Over time, it negatively affects the victim's mental health they feel it undermines their autonomy and live life on their terms, and places the abuser in a position of absolute control. Self-censorship and altered behavior to avoid potential consequences, victims of spyware often begin to self-censor.

This self-censorship may involve avoiding certain topics in conversation, deleting messages, and refraining from contacting friends and family. Such changes are not voluntary but are made under psychological duress. Spyware in intimate relationships traps victims in the loop of control, making it difficult to escape the abuse. In this state victim feels escape is either too risky or impossible. ⁷Overall, all the spyware creates a pervasive environment of fear, control, and psychological harm. Trust is shattered, and social relationships are weakened. And victim moves into isolation and self-censorship.

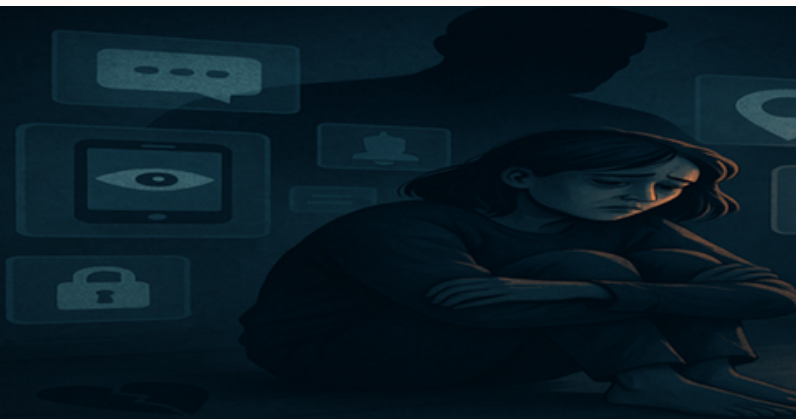


Fig Shows the Psychological Impact on the victim.

The Forensic Footprint: Detecting and Analyzing Spyware in Domestic Violence Cases

Your phone or laptop battery died too fast, or your internet cost increased more than the normal cost. There might be spyware installed on the device. Spyware often runs constantly in the background, monitoring all activities and transmitting them to the abuser's server. This process consumes power and increases data usage. It causes battery drain, slow performance, and overheating even when devices are not actively being used. New applications that appear on your phone or laptop without your installation or consent, especially those requesting excessive permissions, are highly suspicious and could be spyware. These apps might look like legitimate system utilities. For example, educational applications asking to access the microphone, camera, contacts, or location data could be a sign that it has been tampered with and used for surveillance. Some spyware is hidden or runs as a background process, difficult to identify. We can find this app in less obvious places, such as the device's settings under “Applications” or “Manage Apps”. There may be a chance of a new account being created on your device or an existing account being linked without your consent. This enables abusers to access your online activities. If you find calls or messages displayed in logs that you did not make, password changes that you did not initiate are potential indications of compromise. Use of reputable antivirus and anti-malware software specifically designed to detect and prevent any spyware or malicious software.

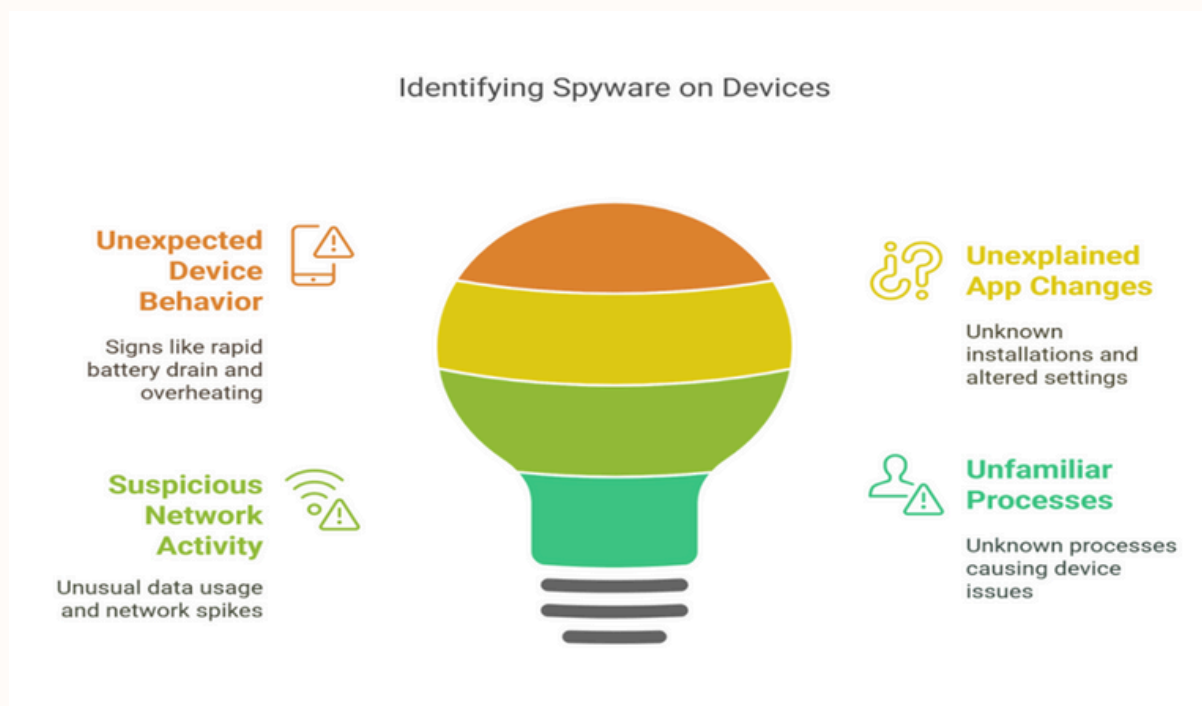


Fig: shows ways of spyware identification.

Forensic Techniques for Spyware Detection and Analysis:

Spyware detection requires a combination of technical knowledge, forensic tools, and investigative methodologies. In this section, we discuss various forensic techniques used in spyware identification and examination.⁸

- **Static and Dynamic analysis:** static analysis involves manually examination of code and identifying the functionality of spyware. Mal. Dynamic analysis is more precise and effectively identifies spyware behavior as it consists of the execution of spyware in a controlled or sandbox environment. Spyware often employs techniques to hide its presence. Static analysis can identify this functionality, while dynamic analysis explains how it works in a live system.
- **Network Traffic Analysis:** Networks play a significant role in spyware abuse cases. Examining and capturing network communication to and from infected devices leads to the abusers behind the spyware. Network traffic analysis involves pattern analysis, deep packet inspection, and metadata analysis.

- **Memory Forensics:** Spyware may be hidden from the app list, but its processes running in the background might be visible in memory. Memory analysis identifies active processes and provides evidence of real-time surveillance.
- **Mobile Device Forensics:** The analysis will focus on a suspicious app with excessive permissions access to the microphone, camera, location, contacts, and messages. Creating a timeline of various data points can demonstrate the pattern of surveillance.⁸

Legal and Ethical Considerations in Digital Forensic Investigations of Domestic Violence

Emphasize that laws regarding privacy, data access, and cybercrime differ significantly across jurisdictions. What might be legal in one place could be illegal in another.

Privacy investigations must follow Aadhar privacy laws, which can vary depending on jurisdiction. Digital forensics can uncover a vast amount of sensitive information. Ethical principle promotes the data minimization technique. Examine only what is necessary to detect and document the spyware—avoid the collection of highly sensitive data.

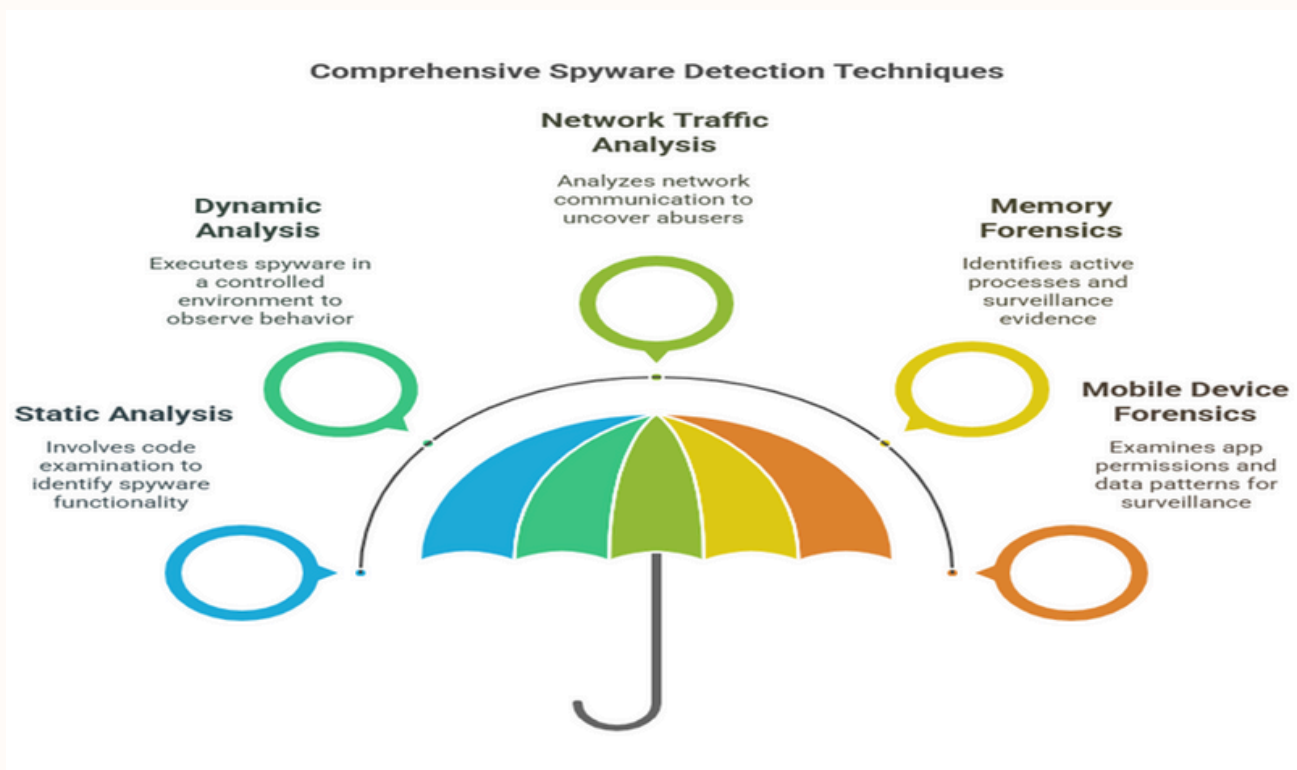


Fig: shows spyware detection techniques.

Chain of custody is a chronological document. It documents every action taken with the device and data. It ensures all findings are repeatable and verified by an expert. Ensure evidence integrity and admissibility in court. Failure to maintain the chain of custody can wreck the case in court and affect the credibility of the victim's case. Obtaining consent from the victim to examine their devices is paramount. In a domestic violence situation, the victim's ability to provide consent might be compromised due to fear. This issue needs to be handled carefully.⁹

Spyware detection and prevention in domestic violence cases require more than just technique expertise. It involves a deep understanding of legal boundaries, ethical responsibility. Investigators must prioritise the safety, autonomy, and privacy of victims while ensuring that evidence is collected and handled in a lawful, transparent, and respectful manner.

The Broader Impact: Consequences of Spyware Abuse in Relationships

The misuse of spyware in close relationships doesn't just violate personal boundaries but also leads to harm on emotional, psychological, physical, and social levels. This reaches beyond the relationships, the victim's mental health, personal freedom, future relationships, and safety. First and foremost, it leads to loss of privacy and self-determination, as a victim loses their capacity to communicate, move, or make decisions freely without fear of being watched. The threat doesn't even stop at the digital level; spyware often contributes to an increased risk of physical harm and stalking, as the abusers use real-time location information to monitor, even after they've attempted to escape the relationship.

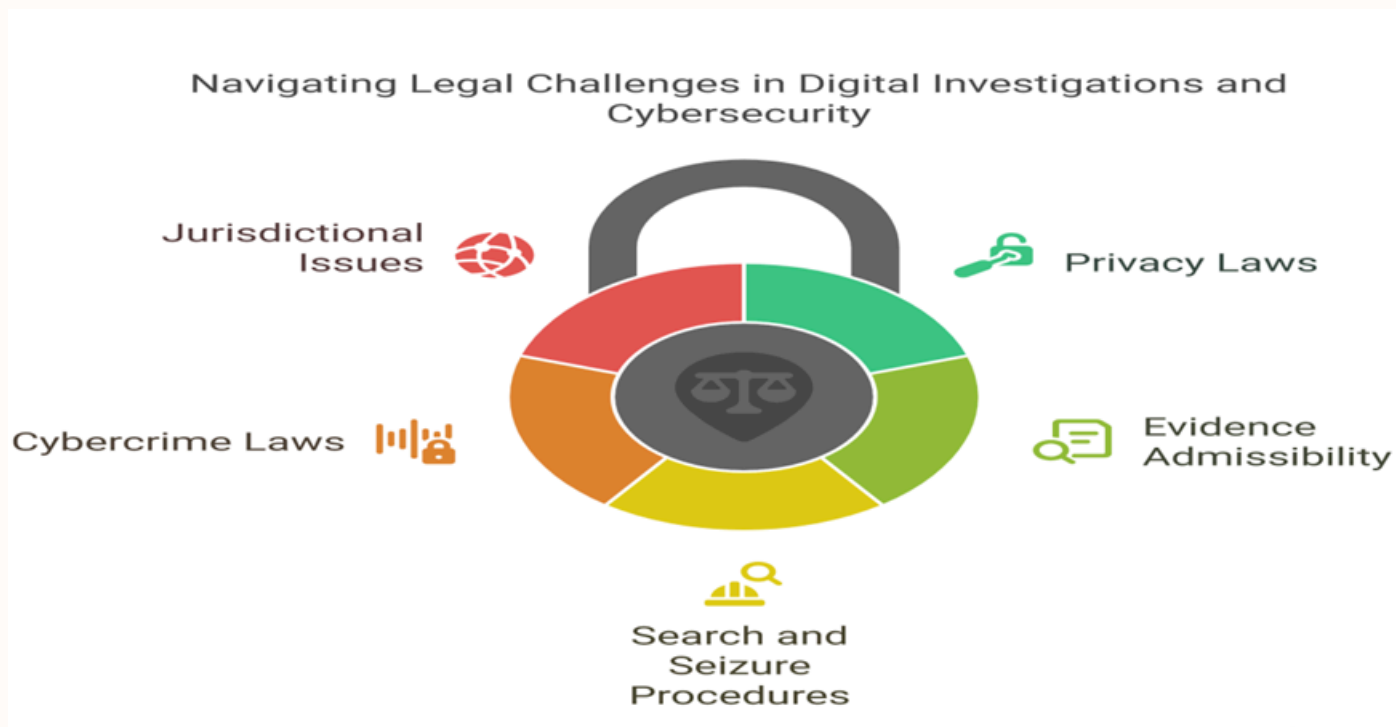


Fig: shows legal challenges in digital investigations and cybersecurity.

Spyware detection and prevention in domestic violence cases require more than just technique expertise. It involves a deep understanding of legal boundaries, ethical responsibility. Investigators must prioritise the safety, autonomy, and privacy of victims while ensuring that evidence is collected and handled in a lawful, transparent, and respectful manner.

The psychological toll is equally severe- victims frequently suffer from emotional distress, anxiety, and depression, all triggered by an ongoing sense of being monitored and controlled. Over time, these experiences can deeply affect the person's ability to trust others, making it too difficult to establish healthy and supportive relationships in the future. Moreover, spyware frequently plays a crucial role in post-separation abuse, allowing abusers to continue harassing or intimidating their ex-partners from a distance.

This can hinder the healing process and extend the cycle of fear and control. Collectively, these impacts illustrate that spyware abuse is not just a technological issue- it is a deeply human issue, impacting safety, mental health, and the capacity to rebuild a life after abuse. Even physical separation, spyware allows the abuser to maintain the sense of control, and information gleaned through spyware can be misinterpreted or used to fuel the abuser's jealous and passiveness. Abusers interfere with victims' attempts to move on by contacting new partners, spreading rumors, or revealing private information. Abusers use spyware as tools to conduct stalking and harassment. The abuser intercepted communication to understand the victim's emotional vulnerability and exploit their father. It allows perpetrators to maintain a suffocating grip on their former partner, eroding their sense of safety and autonomy at a time when they are most vulnerable.

Ultimately, the impact of spyware abuse reveals it to be far more than a technological concern. It is a potential human right issue that strikes at the core of safety, mental well-being, and the fundamental ability of individuals to live freely from fear and coercion, both during and after a relationship.¹⁰



Fig: shows the consequences of spyware abuse in a relationship.

Prevention and Mitigation Strategies: Empowering Victims and Strengthening Security

Preventing and mitigating spyware misuse in intimate relationships requires a comprehensive and proactive approach that combines education, digital security, emotional support, and legal action. Increasing public awareness is crucial, as many people do not realize that digital monitoring can be a form of domestic violence;

educating people about the tactics and dangers of spyware empowers them to recognize and respond to abuse early. Implementing strong passwords and activating multi-factor authentication adds essential security layers to personal accounts, reducing the risk of unauthorized access by abusers regularly updating software and operating systems helps to eliminate security holes that spyware often takes advantage and also installing and maintaining reputable anti-malware software ensures ongoing detection and removal of harmful programs and applications. Equally important is recognizing red flags in relationships- such as controlling behavior, requests for personal passwords, or unusual phone activity - this can also be a key indicator of spyware usage. Victims are encouraged to seek assistance from domestic violence organizations and cybersecurity professionals, who provide both emotional and technical solutions for securing compromised devices. Finally, strong legal systems and more proactive law enforcement are essential to holding perpetrators accountable and protecting people from ongoing digital harassment. Laws like “The Protection of Women from Domestic Violence Act”, 2005 (PWDVA), “The Information Technology Act”, 2000, and “The Indian Penal Code” (IPC).^{11,12}

Conclusion

The growing threat of spyware in intimate relationships marks a deep evolution of domestic violence in the digital age, demanding urgent attention from all sectors of society. Digital domestic violence is not only a technological concern- it represents a serious violation of human rights and personal safety. Addressing this issue calls for an interdisciplinary approach, bringing together experts in cybersecurity, law enforcement, legal advocacy, mental health, and social services. As spyware becomes more technical and advanced, there is continuous research and innovation to develop effective tools for detection, prevention, and victim support. Simultaneously, we must focus on empowering victims through awareness, legal protection, and digital self-defense. Looking forward, we must stay alert and proactive in foreseeing future developments in digital abuse, such as AI-driven surveillance, misuse of wearable technology, etc. Only through collaboration, education, and policy reform can we effectively tackle digital domestic violence, protect the safety, dignity, and autonomy of individuals in today's digital world.

References:

- Al-Alosi H. Cyber-Violence: Digital Abuse in the Context of Domestic Violence. University of New South Wales Law Journal. 2017;40(4). doi:10.53637/DHUV6093
- (PDF) Cyber-Violence: Digital Abuse in the Context of Domestic Violence. Accessed April 10, 2025. https://www.researchgate.net/publication/328813010_Cyber-Violence_Digital_Abuse_in_the_Context_of_Domestic_Violence
- Rogers MM, Fisher C, Ali P, Allmark P, Fontes L. Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. Trauma Violence Abuse. 2022;24(4):2210. doi:10.1177/15248380221090218
- Afrouz R. The Nature, Patterns and Consequences of Technology-Facilitated Domestic Abuse: A Scoping Review. Trauma, Violence, Abuse. 2023;24(2):913-927. doi:10.1177/15248380211046752
- What is Spyware? | Definition from TechTarget. Accessed April 10, 2025. <https://www.techtarget.com/searchsecurity/definition/spyware>
- What Is Spyware? Types and Best Prevention Practices in 2022 - Spiceworks. Accessed April 10, 2025. <https://www.spiceworks.com/it-security/security-general/articles/what-is-spyware/>
- Juan Y, Yuanyuan C, Qiuxiang Y, et al. Psychological distress surveillance and related impact analysis of hospital staff during the COVID-19 epidemic in Chongqing, China. Compr Psychiatry. 2020;103:152198. doi:10.1016/J.COMPPSYCH.2020.152198
- Role of Footprints in Forensic Investigations: Hawk Eye Forensic. Accessed April 10, 2025. <https://hawkeyeforensic.com/2024/02/27/the-critical-role-of-footprints-in-forensic-investigations/>
- Aleke NT, Trigui M. Legal and Ethical Challenges in Digital Forensics Investigations. Digital Forensics in the Age of AI. Published online January 1, 2024:147-176. doi:10.4018/979-8-3373-0857-9.CH006
- Rogers MM, Fisher C, Ali P, Allmark P, Fontes L. Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. Trauma Violence Abuse. 2022;24(4):2210. doi:10.1177/15248380221090218
- Davies J, Lyon E. Domestic Violence Advocacy: Complex Lives/Difficult Choices. Domestic Violence Advocacy: Complex Lives/Difficult Choices. Published online January 15, 2016. doi:10.4135/9781483352916
- White JW, Sienkiewicz HC. Victim Empowerment, Safety, and Perpetrator Accountability Through Collaboration: A Crisis to Transformation Conceptual Model. Violence Against Women. 2018;24(14):1678-1696. doi:10.1177/1077801217743341

ABOUT THE AUTHORS

Yamini Parmar

Integrated M.Sc. Cyber Security and Forensic Science,
Department of Biochemistry and Forensic Science, Gujarat
University, Ahmedabad, Gujarat, INDIA



Omi Chauhan

Integrated M.Sc. Cyber Security and Forensic Science,
Department of Biochemistry and Forensic Science, Gujarat
University, Ahmedabad, Gujarat, INDIA



Kiran Dodiya

(Research Scholar, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



Dr. Kapil Kumar

Coordinator, Department of Biochemistry
and Forensic Science, Gujarat University,
Ahmedabad, Gujarat, INDIA



The Silent Forensic Voices of India

Whispers on the Page

**In ink and stroke, the secrets hide,
A tale untold, where truth may bide,
A letter curves, a flourish flies,
But truth is buried in disguise.
The paper's grain, the ink's faint trace,
Reveal a mask, a hidden face,
A pen that wavers, pressure's dance,
A signature that shifts by chance.
Under lenses sharp and bright,
Ultraviolet spills its light,
Fibers glow, the forger's bane,
Where altered lines no longer feign.
Indented marks, a ghostly trail,
A story told when words grow pale,
Microscopes that bring to view,
The slightest scratch, the fakest hue.
Chemical baths that whisper wake,
Invisible inks that truth will take,
An erasure smudge, a tampered date,
Forensics draws the line of fate.
In curling scripts and pencil lead,
The hidden paths of lies are read,
For every page, each mark, each bend,
A silent witness to the end.**

CASE STUDY

on

DEATH OF BABY THERESA (2009) - SOLVED THROUGH DNA EVIDENCE

Author: Aanchal Sakarkar



Background:

On June 5, 2009, the body of a newborn baby girl was discovered abandoned in a garbage bag along a roadside near Theresa, a small town in Dodge County, Wisconsin. The infant, who was later named "Baby Theresa" by the local community, was found with her umbilical cord still attached. An autopsy confirmed that the baby had likely died during or shortly after birth, with no evidence of external injuries or trauma. However, there were no immediate leads about who the parents were, and the investigation reached a standstill. Despite public appeals and forensic efforts, the case remained cold for over a decade.

Timeline

The discovery of Baby Theresa's body in 2009 triggered a thorough investigation, but with no eyewitnesses or identifying information, the case remained unsolved. It wasn't until 2022 that a breakthrough occurred when investigators used genetic genealogy, a technique that analyzes DNA evidence alongside public ancestry databases, to identify a match. The analysis led to Karin Luttinen, who was confirmed as the baby's biological mother through DNA testing. She was living in Wisconsin at the time and had concealed the pregnancy from those around her. In September 2022, she pleaded guilty to the charge of concealing the death of a child and was sentenced to three years of probation. The child's father, though identified, was not charged due to lack of involvement in the disposal or concealment of the baby.

Psychological Profile:

Karin Luttinen, in her early twenties at the time of the incident, appeared to have undergone significant emotional and psychological stress. It is likely that she experienced a concealed or denied pregnancy, compounded by fear, stigma, and mental distress. Experts suggested that she may have suffered from postpartum trauma or psychological denial, leading her to deliver the baby in secret and dispose of the body without seeking medical assistance. Her actions showed no signs of violent intent but rather panic, isolation, and poor coping mechanisms. Court records noted that she showed genuine remorse during proceedings and had no prior criminal record, further supporting the view that her actions were more likely driven by fear and confusion rather than malice.

Release and Current Status

Following her guilty plea in 2022, Karin Luttinen was sentenced to three years of supervised probation without jail time. The court acknowledged her remorse and the psychological circumstances surrounding the case. As of now, she has completed or is serving her probation, and no further legal issues have been reported. Due to the sensitive nature of the case, her current personal life and location have not been publicly disclosed. The baby's father was not charged, as he had no role in the concealment and was unaware of the pregnancy at the time.



Analysis and Implications:

The Baby Theresa case underscores the growing role of forensic science—particularly genetic genealogy—in resolving cold cases. It exemplifies how DNA technology can identify individuals involved in a case even after many years, and bring clarity to long-unsolved mysteries. Legally, the case raises awareness about the importance of Safe Haven Laws, which allow mothers to legally and safely surrender unwanted newborns at hospitals and other facilities without facing legal consequences.

Socially and psychologically, it sheds light on the need for better education, mental health resources, and support systems for young or vulnerable pregnant women. Many such cases result not from criminal intent but from desperation, isolation, and fear. This case serves as a cautionary tale about the societal pressures that can drive individuals to make tragic decisions when no support systems are in place.

Conclusion

In conclusion, the case of Baby Theresa, while heartbreaking, highlights the power of forensic technology in uncovering the truth and providing closure. It also points to a deeper need for psychological and societal reform in how pregnancy and child abandonment are addressed. The community's naming of the baby and their continued remembrance reflect a collective mourning for a life lost too soon. The eventual identification of the mother through DNA testing provided accountability and marked a significant development in the application of forensic genealogy.



References:

- WMTV NBC 15 News Report (2022)
- Wisconsin State Court Records (Dodge County, 2022)
- Wisconsin Department of Health Services – Safe Haven Laws
- Forensic Genealogy Techniques – Journal of Forensic Sciences
- Community Reports – The Milwaukee Journal Sentinel (2009–2022)

ABOUT THE AUTHOR

Aanchal Sakarkar
Assistant Professor
Aditya Degree & PG College, Surampalem
Andhra Pradesh

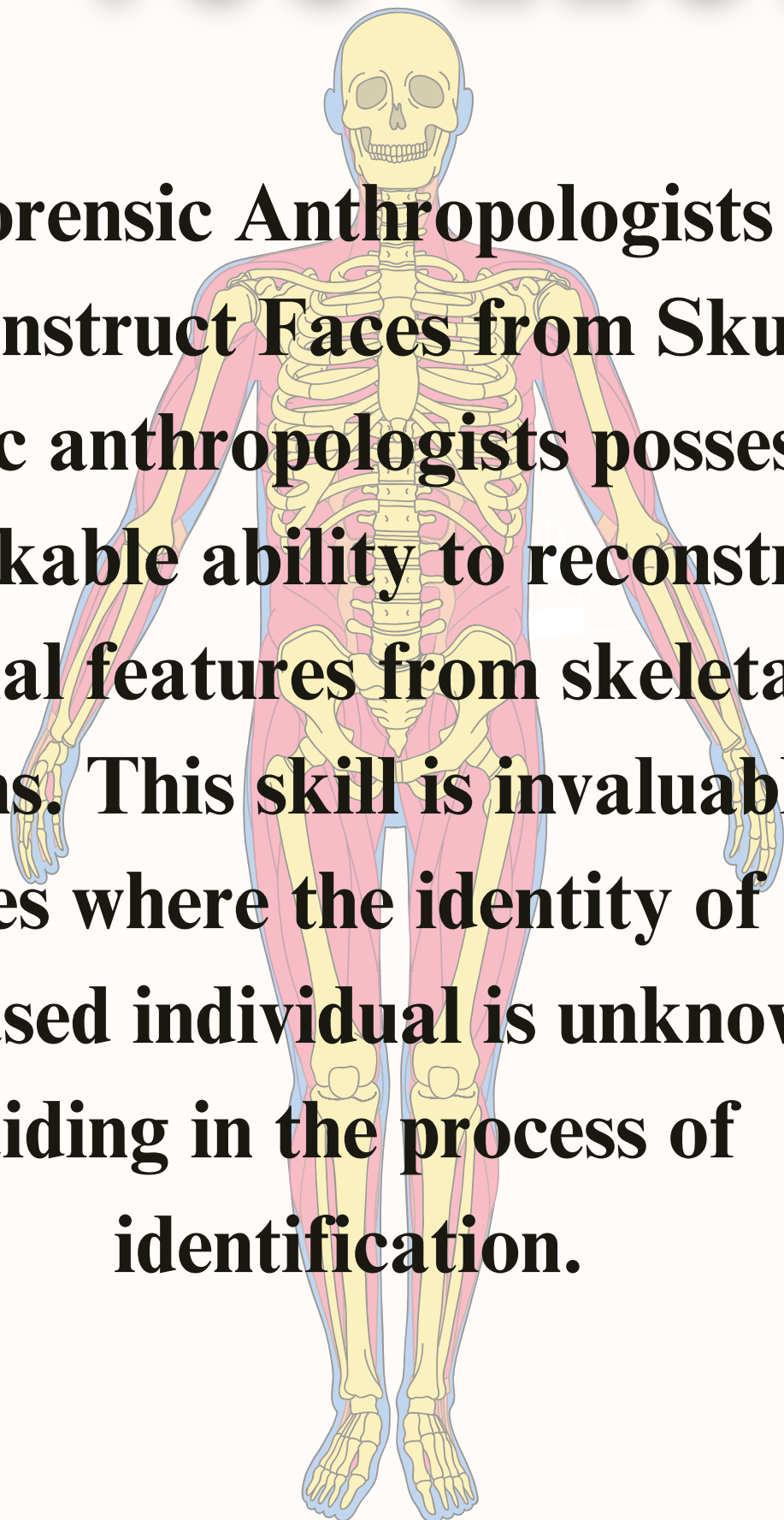


DID YOU KNOW?

Forensic Anthropologists

Reconstruct Faces from Skulls

Forensic anthropologists possess the remarkable ability to reconstruct facial features from skeletal remains. This skill is invaluable in cases where the identity of a deceased individual is unknown, aiding in the process of identification.





KNOW WHAT'S IN THE TREND

VANTA HANDHELD XRF ANALYZER BY EVIDENT SCIENTIFIC

Introduction

In the ever-evolving landscape of analytical instrumentation, the Vanta handheld X-ray fluorescence (XRF) analyzer developed by Evident Scientific has emerged as a ground breaking tool. Designed to provide laboratory-quality elemental analysis directly in the field, the Vanta analyzer is transforming how industries and forensic professionals approach material identification, compliance testing, and investigative analysis. Its robust design and cutting-edge technology position it as a standout solution across diverse disciplines.

Company Overview: Evident Scientific

Evident Scientific, formerly part of Olympus Corporation, is a global innovator in scientific instrumentation. The company focuses on precision, usability, and durability in developing solutions that meet the demanding needs of modern professionals. With a commitment to empowering science through innovation, Evident Scientific has become a trusted name in industries ranging from manufacturing and metallurgy to environmental science and forensics. The Vanta handheld XRF analyzer is a testament to its engineering expertise and vision.

Working Principle of the Vanta XRF Analyzer

The Vanta analyzer operates on the principle of X-ray fluorescence (XRF), a non-destructive analytical technique used to determine the elemental composition of materials. When the instrument directs high-energy X-rays at a sample, atoms in the material absorb the energy and emit secondary

X-rays, each with a unique energy signature corresponding to specific elements.

By analyzing the energy and intensity of these emitted X-rays, the Vanta device identifies and quantifies elements present in the sample. This makes it especially valuable for rapid, in-field analysis without the need for complex sample preparation or laboratory conditions.

Key Features

Rugged Durability: The Vanta series is built to withstand harsh environments. It features drop-tested casing, resistance to dust and water (IP54/IP55), and MIL-STD-810G compliance, making it suitable for both field and industrial use. **Axon™ Technology:** This advanced signal processing technology enhances precision and speed, delivering more reliable data with lower detection limits and faster throughput. **User-Friendly Interface:** Equipped with a bright, responsive touchscreen and intuitive operating system, the analyzer is accessible even to users with minimal

Company Overview: Evident Scientific

Evident Scientific, formerly part of Olympus Corporation, is a global innovator in scientific instrumentation. The company focuses on precision, usability, and durability in developing solutions that meet the demanding needs of modern professionals.

With a commitment to empowering science through innovation, Evident Scientific has become a trusted name in industries ranging from manufacturing and metallurgy to environmental science and forensics. The Vanta handheld XRF analyzer is a testament to its engineering expertise and vision.

Working Principle of the Vanta XRF Analyzer

The Vanta analyzer operates on the principle of X-ray fluorescence (XRF), a non-destructive analytical technique used to determine the elemental composition of materials. When the instrument directs high-energy X-rays at a sample, atoms in the material absorb the energy and emit secondary X-rays, each with a unique energy signature corresponding to specific elements.



Vanta Max



Vanta Core



Vanta Element

Applications in Forensic Science

The Vanta XRF analyzer has proven indispensable in various areas of forensic investigation. Its portability and real-time results provide critical support in time-sensitive scenarios.

Detection of Toxic Metals: Forensic investigators use the Vanta to detect hazardous metals like lead, arsenic, and mercury in paints, cosmetics, toys, and other consumer goods. This is crucial for both criminal cases and regulatory enforcement.

Trace Evidence Examination: It allows quick, non-destructive identification of elemental traces in materials such as glass fragments, bullets, or unknown powders, helping link suspects to crime scenes.

Environmental Forensics: Analysts can screen soils, sediments, and water for contamination, identifying pollution sources or illegal disposal in environmental crime investigations.

Archaeological and Cultural Heritage Investigations: Forensics teams and researchers can analyze ancient artifacts and remains without damaging delicate items, aiding in authenticating and preserving historical evidence.

By analyzing the energy and intensity of these emitted X-rays, the Vanta device identifies and quantifies elements present in the sample. This makes it especially valuable for rapid, in-field analysis without the need for complex sample preparation or laboratory conditions.

Key Features

Rugged Durability: The Vanta series is built to withstand harsh environments. It features drop-tested casing, resistance to dust and water (IP54/IP55), and MIL-STD-810G compliance, making it suitable for both field and industrial use.

Axon™ Technology: This advanced signal processing technology enhances precision and speed, delivering more reliable data with lower detection limits and faster throughput.

User-Friendly Interface: Equipped with a bright, responsive touchscreen and intuitive operating system, the analyzer is accessible even to users with minimal technical training.

Connectivity Options: The Vanta supports wireless LAN, Bluetooth®, and USB connectivity, enabling easy data sharing, cloud integration, and streamlined documentation.

PREPARE YOURSELF

UGC NET & FACT QUESTION BANK

-
1. Article of the Constitution gives power to the President of India to grant pardons and to suspend, remit or commute sentences in certain cases
- a) 70
 - b) 72
 - c) 75
 - d) 161
2. Who popularized scientific crime detection methods?
- a) Sir Arthur Conan Doyle
 - b) Sir Arthur Conan Boyle
 - c) Francis Galton
 - d) Calvin Goddard
3. Corroborative use of physical evidences helps to:
- a) Rule out particular suspect
 - b) Establish a definite identity
 - c) Provide a lead to give the investigation a particular direction
 - d) Support the other circumstantial findings
4. Central Forensic Science Laboratory, Guwahati was started in the year:
- a) 1971
 - b) 1981
 - c) 1991
 - d) 2011
5. Loknayak Jaiprakash Narayan National Institute of Criminology and Forensic Science was established in New Delhi in which year?
- a) 1971
 - b) 1972
 - c) 1967
 - d) 1974
6. Olecranon fossa is present in which of the following bones?
- a) Radius
 - b) Humerus
 - c) Femur
 - d) Tibia

7. Which of the following methods of fingerprint development is based on reaction with amino acids?

- a) Silver Nitrate
- b) Ninhydrin
- c) DFO
- d) Sudan Black

Choose the correct answer:

- a) a) & b) only
- b) a) & c) only
- c) a) & d) only
- d) b) & c) only

8. If the right index and right middle fingers are whorls and all the others are loops, the Henry's primary classification is:

- a) 17/9
- b) 25/19
- c) 6/9
- d) 17/19

9. The most suitable solvent system for thin layer chromatography/paper chromatography of inks is:

- a) N-butanol: pyridine: water (3:1:1.5)
- b) Amyl alcohol: acetic acid: chloroform (6:1:2)
- c) Ethanol: Acetone: acetic acid (4:1:5)
- d) Amyl alcohol: acetic acid: pyridine (6:1:2)

10. Chemically erased writing can be restored by the action of:

- (i) Reflected light
- (ii) Ammonium polysulphide solution
- (iii) Thiocyanic Acid
- (iv) UV light

Code:

- a) (ii) and (iii) are correct
- b) (i) and (ii) are correct
- c) (ii) and (iv) are correct
- d) (i) and (iv) are correct

11. A blank cartridge containing a small quantity of either “chloracetophenone” or O-chlorobenzalmalononitrile is known as:

- a) Caseless ammunition
- b) Rimfire ammunition
- c) Tear gas ammunition
- d) LMG ammunition

12. Medullary index of human hair is:

- a) Less than $\frac{1}{3}$
- b) More than $\frac{1}{2}$ but less than $\frac{3}{4}$
- c) More than $\frac{1}{3}$ but less than $\frac{1}{2}$
- d) More than $\frac{3}{4}$

13. Assertion: Link method is often coupled with other geometric search methods.

Reason: No single crime scene search method is suitable for all types of scenes.

- a) Both Assertion and Reason are true
- b) Assertion is true but Reason is false
- c) Assertion is false but Reason is true
- d) Both Assertion and Reason are false

14. Cherry red colour of blood is seen in poisoning with:

- a) Nitrate
- b) Cyanide
- c) Lead
- d) Sulphite

15. 1-Pentyl-3-(1-naphthoyl) commonly known as indole is:

- a) JWH-018
- b) PTF-021
- c) PNI-030
- d) PNI-031

16. Which of the following military explosives has the lowest detonation velocity?

- a) Composition C-4
- b) Amatol
- c) Torpex
- d) Teteryl

17. In human seminal fluid, the amount of spermatozoa is:

- a) 3 thousand spermatozoa/ml
- b) 50 billion spermatozoa/ounce
- c) 25 trillion spermatozoa/pint
- d) 100 million spermatozoa/ml

18. An Android device's encrypted data can be wiped remotely using:

- a) Find My Phone service
- b) Google Sync
- c) iCloud
- d) Search My Sync

19. Which of the following preservatives are used in photographic developing solution to prevent wasteful oxidation of developing agent?

- a) Sodium sulphite
- b) Phenidone amino phenol
- c) Potassium metabisulphite
- d) Methyl pyrogallol

Choose the correct answer:

- a) D and B only
- b) A and B only
- c) B and C only
- d) A and C only

20. Which of the following is the correct sequence of processes that occur in the flame atomizer of AAS (Atomic Absorption Spectroscopy)?

- a) Nebulisation, desolvation, volatilization, dissociation
- b) Volatilization, nebulisation, dissociation, desolvation
- c) Desolvation, dissociation, nebulisation, volatilization
- d) Dissociation, volatilization, desolvation, nebulisation



ANSWERS:
1.b, 2.a,3.d,4.c,5.b,6.b,7.d,8.d,9.a,10.c,11.c,12.a,13.a,14.b,15.a,16.b,17.d,18.a,19.d,20.a

PREPARE YOURSELF

UGC-NET PAPER 1: QUESTION BANK

1.Assertion (A): Communication plays a vital role in the personality development of a student.

Reason (R): Communication reflects the personality of a person.

- a) Both (A) and (R) are true, and (R) is the correct explanation of (A)
- b) Both (A) and (R) are true, but (R) is not the correct explanation of (A)
- c) (A) is true, but (R) is false
- d) (A) is false, but (R) is true

2.The ability of a listener to receive and interpret a message in the same sense as intended by the speaker is known as:

- a) Active listening
- b) Hearing
- c) Attentive listening
- d) Passive listening

3.Identify the correct combination of the elements of communication:

- a) Source, Message, Channel, Receiver
- b) Source, Message, Decoder, Feedback
- c) Channel, Message, Feedback, Noise
- d) Receiver, Feedback, Medium, Noise

4.Which of the following is an example of upward communication?

- a) Instructions from manager to employees
- b) A complaint by a worker to the manager
- c) Circular issued by the administration
- d) Guidelines from the government

5.The term 'SWAYAM' refers to:

- a) A digital initiative to promote classical music
- b) A platform for skill development in rural areas
- c) An online platform for open education
- d) A scheme for women's empowerment



6. MOOCs are associated with:

- a) Closed classroom education
- b) Offline teaching
- c) Open and distance learning
- d) Private coaching

7. The Gross Enrolment Ratio (GER) in higher education refers to:

- a) Percentage of students enrolled in school education
- b) Total enrolment in higher education as a percentage of the eligible population
- c) The success rate in higher education
- d) Literacy rate in rural areas

8. Which of the following is a parameter for accreditation by NAAC?

- a) Location of the college
- b) Name of the principal
- c) Curriculum aspects
- d) Sports achievements

9. A company's profit was ₹40,000 in January and ₹50,000 in February. What is the percentage increase in profit from January to February?

- a) 20%
- b) 25%
- c) 10%
- d) 30%

10. A hypothesis is a:

- a) Law
- b) Theory
- c) Temporary assumption
- d) Conclusion

11. If the number of students in 2020 was 500 and it increased by 20% in 2021, what is the total number of students in 2021?

- a) 520
- b) 600
- c) 580
- d) 550



12. Sampling is used in research because:

- a) It is easier than studying the entire population
- b) It always gives accurate results
- c) It removes the need for analysis
- d) It avoids hypothesis testing

13. Which method is most suitable for studying human behaviour?

- a) Survey method
- b) Experimental method
- c) Observational method
- d) Case study method

14. The term 'reliability' in research refers to:

- a) Accuracy of the research tools
- b) Stability and consistency of the measurement
- c) Validity of the hypothesis
- d) Relevance of the data

15. In a research report, the section containing an overview of the research problem and objectives is called:

- a) Methodology
- b) Conclusion
- c) Introduction
- d) Bibliography

16. The mode of a data set refers to:

- a) Middle value
- b) Most frequently occurring value
- c) Average of all values
- d) Difference between highest and lowest value

17. In which of the following modes of teaching is the learner most passive?

- a) Online
- b) Traditional lecture
- c) Interactive
- d) Experiential



18. Which of the following is a barrier to effective communication?

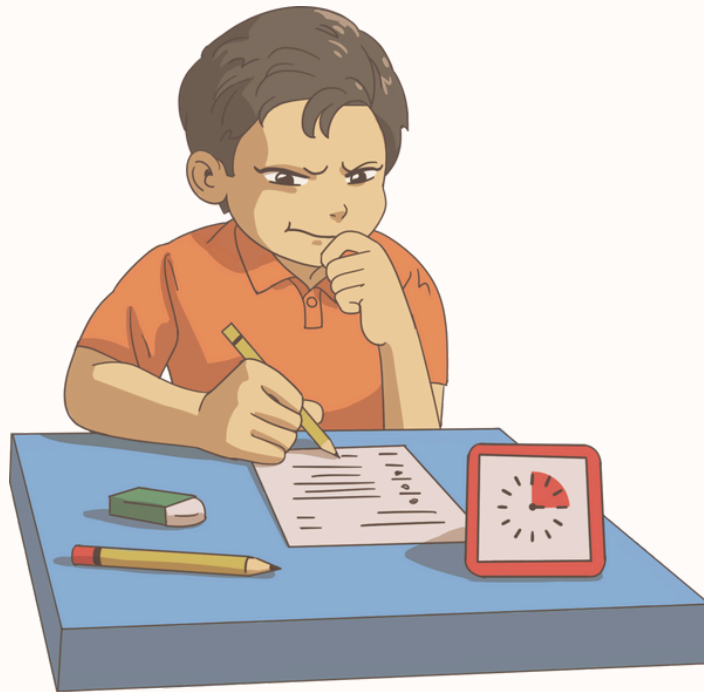
- a) Feedback
- b) Noise
- c) Listening
- d) Message

19. The main function of UGC in higher education is:

- a) Conducting exams
- b) Granting affiliation to universities
- c) Coordination and determination of standards
- d) Teaching students

20. Which of the following methods of teaching encourages critical thinking?

- a) Rote learning
- b) Lecture
- c) Debate
- d) Dictation



ANSWERS:
1.a, 2.a, 3.a, 4.b, 5.c, 6.c, 7.b, 8.c, 9.b, 10.c, 11.c, 12.a, 13.d, 14.b, 15.c, 16.b, 17.b, 18.b, 19.c, 20.c

2025

ADMISSIONS OPEN

nirf
Rank Band
201-300

ACCREDITED BY
NAAC
A++ GRADE

NBA
TIER 1
ACCREDITED



ADITYA
UNIVERSITY

STEP INTO A WORLD OF OPPORTUNITIES

YOUR JOURNEY TO EXCELLENCE STARTS HERE

www.adityauniversity.in

FOR ADMISSIONS CONTACT : **+91 70360 76661, 70950 76663/4**

RANKINGS & ACCREDITATIONS



6 UG Programs Accredited by
NBA under Tier I



Rank Band **26-50**

PROGRAMS OFFERED

Students from 18 states in India and 24 Countries Worldwide

SCHOOL OF ENGINEERING

B.TECH

- Civil Engineering
- Electronics and Communication Engineering
- Electrical and Electronics Engineering
- Mechanical Engineering
- Computer Science and Engineering
- Information Technology
- Artificial Intelligence & Machine Learning
- Data Science
- Petroleum Technology
- Mining Engineering
- Agricultural Engineering

M.TECH

- Structural Engineering
- Power Electronics & Drives
- Energy Science & Technology
- VLSI Design
- Computer Science & Engineering
- CSE (AI&ML)

SCHOOL OF PHARMACY

- B.Pharmacy
- M.Pharmacy
- Pharm. D

SCHOOL OF SCIENCES

- B.Sc. -Forensic Science
- B.Sc. -Cyber Security & Digital Forensics
- M.Sc.-Forensic Science
- M.Sc.-Cyber Security & Digital Forensics

SCHOOL OF BUSINESS

- BBA
- BBA-Digital Marketing
- BBA-Business Analytics

MBA

MCA

Ph.D. in All Disciplines

COLLABORATIONS with FOREIGN UNIVERSITIES



"We are excited to announce a new partnership with
UNIVERSITY OF SOUTH CAROLINA UPSTATE,

ACHIEVEMENTS OF OUR STUDENTS

2026 PLACEMENTS

A RECORD BREAKING PACKAGES

52 Placed in
#HASHAI
LAKHS PER ANNUM



D. UPANISHA

C. POOJITHA

S. SRIRAM

₹ **45** LPA **13** CSE Students
AUTODESK.

₹ **35** LPA **16** CIVIL & MECH Students
AUTODESK.

2025 PLACEMENTS

52 Placed in
#HASHAI
LAKHS PER ANNUM



A. HARSHITH

M. DIVYA

V. GOWTHAM

Scan to know
more about Placements



Internship offer at

Google

Stipend

₹ **1.23**
Lakhs Per Month

D RAMYA
B.Tech(CSE)



2025 Placements

2018

Offers Still Continuing...

₹ **33.64** LPA
Highest CTC

Above 50 ^{LPA}	3 Adityans
Above 35 ^{LPA}	5 Adityans
Above 30 ^{LPA}	15 Adityans
Above 25 ^{LPA}	23 Adityans
Above 20 ^{LPA}	38 Adityans
Above 15 ^{LPA}	41 Adityans
Above 10 ^{LPA}	50 Adityans
Above 9 ^{LPA}	59 Adityans
Above 8 ^{LPA}	64 Adityans
Above 7 ^{LPA}	88 Adityans
Above 6 ^{LPA}	134 Adityans
Above 5 ^{LPA}	161 Adityans
Above 4 ^{LPA}	647 Adityans
Above 3.6 ^{LPA}	1939 Adityans

#2025 International Placements

HITACHI
Inspire the Next

₹ **35.36**
Lakhs Per Annum

JMC Co., Ltd.

₹ **34.95**
Lakhs Per Annum

TOYOTA
connected

₹ **34.12**
Lakhs Per Annum

Aissan

₹ **33.51**
Lakhs Per Annum

JEMS

₹ **32.84**
Lakhs Per Annum

Daiseiki

₹ **31.70**
Lakhs Per Annum

IHARA

₹ **29.02**
Lakhs Per Annum

AD-TEC

₹ **28.61**
Lakhs Per Annum

HITACHI

₹ **27.29**
Lakhs Per Annum

Hitachi

₹ **27.16**
Lakhs Per Annum

and many more Placements....

ADITYA HOSTELS (AC / NON - AC)

Home away from Home

- Comfortable, hygienic surroundings, individual grooming and counselling.
- AC / Non-AC accommodation.
- An exclusive library with digital and multimedia facility, newspapers, magazines, journals, books related to academics and competitive exams like GRE, GATE etc.
- Wi-fi campus.
- On campus bank facility (Canara Bank).
- Uninterrupted power supply.
- Fully equipped gym.
- Hot water facility.
- Saloon for boys and beauty parlour for girls with in the premises.
- Apollo dispensary is accessible 24/7 to support campus health needs equipped with ambulance assistance.

ASAT

ADITYA'S SCHOLASTIC APTITUDE TEST

- ASAT represents **Aditya's Scholastic Aptitude Test** which is planned as an entrance for UG programs
- The duration of the test is 120 minutes

- The test comprises of

Maths, Physics, Chemistry & Gamified puzzles
(for B. Tech. Aspirants)

- MATHS (30 marks - 30 MCQs)
- PHYSICS (15 marks - 15 MCQs)
- CHEMISTRY (15 marks - 15 MCQs)
- GAMIFIED PUZZLES (No marks - 30 min.)

Maths / Biology, Physics,
Chemistry & Gamified
puzzles
(for B.Sc. Aspirants)

- MATHS / BIOLOGY (30 marks - 30 MCQs)
- PHYSICS (15 marks - 15 MCQs)
- CHEMISTRY (15 marks - 15 MCQs)
- GAMIFIED PUZZLES (No marks - 30 min.)

Aptitude, Reasoning,
English & Gamified
puzzles
(for BBA Aspirants)

- APTITUDE (30 marks - 30 MCQs)
- REASONING (15 marks - 15 MCQs)
- ENGLISH (15 marks - 15 MCQs)
- GAMIFIED PUZZLES (No marks - 30 min.)

SCHOLARSHIP

ASAT (Demo Link)

<https://cocubes.in/aditya-asat>
Application Id for Demo

- adityatesting1
- adityatesting2
- adityatesting3



Passkey for Demo
322160

MERIT
SCHOLARSHIPS
upto
100%

For Details SCAN Here



SCHOLARSHIP



- Students may secure seats into Programs by qualifying in ASAT Entrance Test.
- Aditya University offers Scholarships of up to 100% of the total tuition fee for meritorious students across all branches in its Programs

www.adityauniversity.in

For Admissions: +9170360 76661, 70950 76663/4 95536 49666

Aditya Nagar, ADB Road, Surampalem - 533 437, Kakinada Dist., Andhra Pradesh, INDIA.

Thank You Note

Dr. N. Suguna Reddy

Secretary

**Aditya Degree and PG Colleges,
Andhra Pradesh**



Dear Readers,

We extend our heartfelt gratitude for the overwhelming support you have shown for India's first bi-monthly forensic science magazine. The remarkable response to our previous issues has been both inspiring and deeply encouraging, reaffirming our mission to serve forensic professionals, researchers, and enthusiasts across the nation.

As we present our fourth issue, we are delighted to bring you an even more comprehensive selection of insightful articles, pioneering research, and thought-provoking discussions, all aimed at advancing the field of forensic science. Your invaluable feedback continues to drive our commitment to excellence, ensuring that we uphold the highest standards and contribute meaningfully to this vital discipline.

Thank you for being an integral part of this journey. We look forward to providing you with valuable insights and celebrating the innovations shaping the future of forensic science.



Aditya College of Forensics & Cyber Security

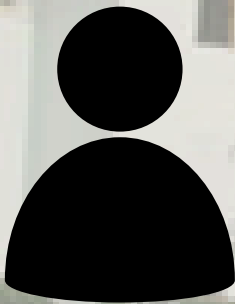
UG Courses

- **B.Sc. Forensic Science**
- **B.Sc. Cyber Security &
Digital Forensics**

PG Courses

- **M.Sc. Forensic Science**
- **M.Sc. Cyber Security &
Digital Forensics**

Contact Us:



principalforensic@aditya.ac.in
adminforensic@aditya.ac.in
forensicmagazine@aditya.ac.in

89782 96668

97015 76663