INFUSE 2025: International Conference on Frontiers of Unified Science and Exploration

Contribution ID: **140** Type: **Oral**

Uncovering Digital Trails in IoT networks: AI-enhanced signal field-based Network Forensics

Network forensics represents an essential area within digital forensics that emphasizes the gathering, documentation, and examination of network traffic to identify the sources and techniques behind security incidents or breaches of policy. In contrast to evidence stored on disks, network information is transient and constantly changing—often retrievable only if it has been proactively captured using tools like packet sniffers or flow capture systems. The research focuses on tackling present difficulties, including the examination of encrypted traffic, handling large data streams, and addressing anti-forensic tactics, while showcasing cutting-edge solutions such as radio signal strength-based packet sniffing, AI-enhanced anomaly detection, machine learning-driven pattern identification, and sophisticated decryption methods—particularly in cloud and IoT settings. This study intends to function as a straightforward, summarised guide for incident responders and forensic professionals aiming to comprehend the evolving landscape of network-oriented digital investigations.

Author: MOHANDAS, Priya (Assistant Professor)

Co-authors: Ms DAS, PRIYANKSHA (JAIN (Deemed-to-be University)); Mr NATARAJAN, VISHNU VENKATESH (JAIN (Deemed-to-be University))

Presenter: MOHANDAS, Priya (Assistant Professor)

Track Classification: Forensic Sciences