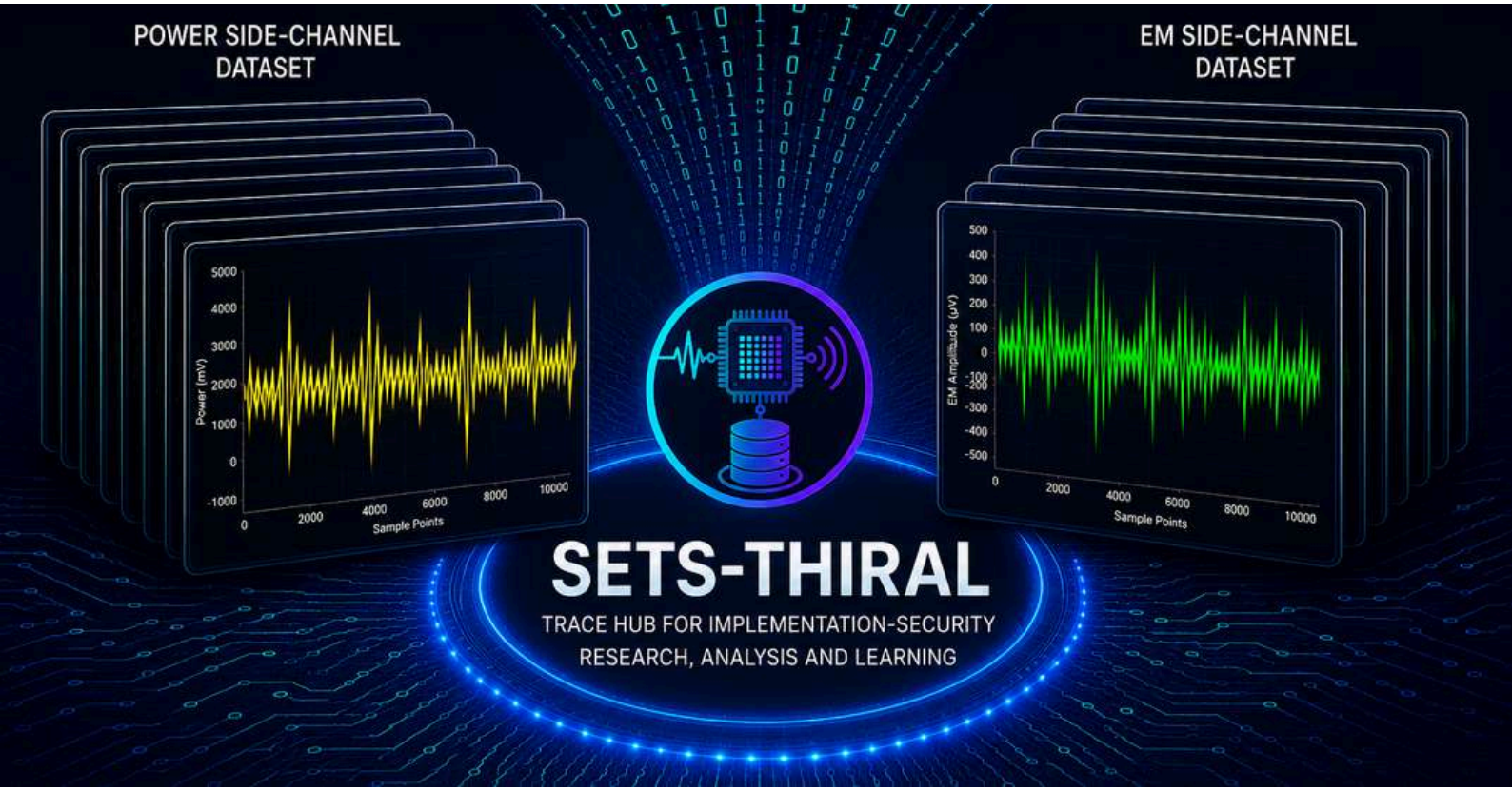
Office of the Principal Scientific Adviser to the Government of India

Strategy and Synergy for Security



SETS-THIRAL Dataset Repository

Trace Hub for Implementation-security Research, Analysis and Learning

SETS-THIRAL (Trace Hub for Implementation-security Research, Analysis and Learning) is an open repository of side-channel datasets developed by SETS to advance implementation security research. It provides datasets from cryptographic hardware implementations, including protected and unprotected designs, to support physical leakage analysis, security evaluation and reproducible benchmarking for side-channel analysis. The repository enables statistical and AI-based analysis and serves as an open resource for the hardware security research community.

- ✔ 21 Datasets with ~350 GB of Traces & Metadata
- ✔ Power & EM Side-Channel Datasets
- ✔ Various Cryptographic Algorithms & Hardware Platforms
- ✔ For Startups, Innovators & Researchers

Available on IndiaAI AI Kosh

Scan to access the Repository

NSM — An Initiative of Government of India

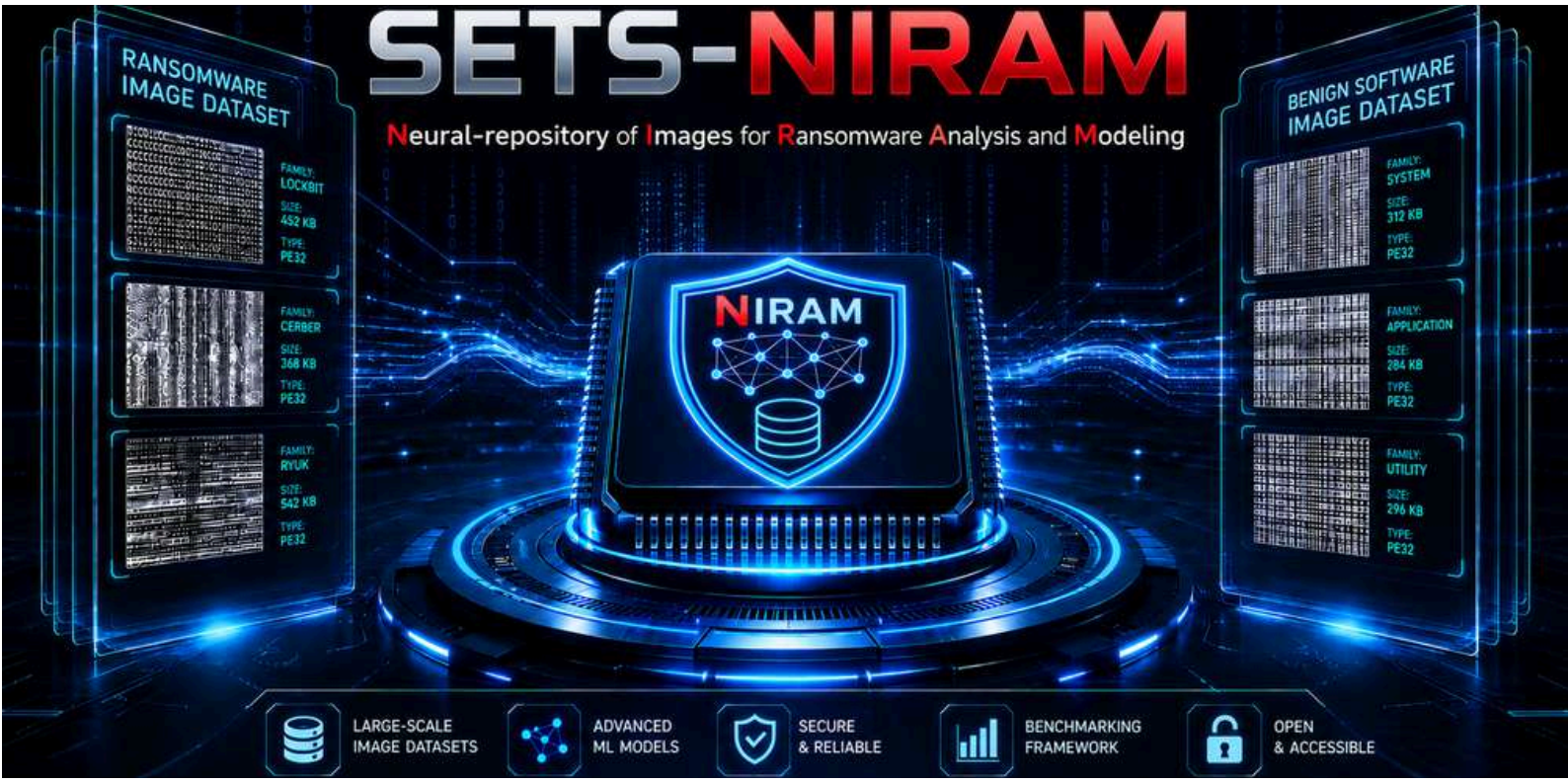
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

विज्ञान एवं प्रौद्योगिकी मंत्रालय
MINISTRY OF SCIENCE AND TECHNOLOGY

aiकोष

Office of the Principal Scientific Adviser to the Government of India

Strategy and Synergy for Security



SETS- NIRAM

Neural-repository of Images for Ransomware Analysis and Modeling

SETS-NIRAM (Neural-repository of Images for Ransomware Analysis and Modeling) is an open repository of ransomware image datasets developed by SETS to advance ransomware research and detection studies. It comprises visual analysis artifacts derived from executable files of ransomware and benign software implementations, enabling comparative ransomware research through advanced image processing and machine learning technologies. The repository holds non-executable image representations of binaries, supporting visual pattern exploration, image-based classification and reproducible benchmarking for the cybersecurity research community.

- ✔ ~1,000 Grayscale & RGB Images of Ransomware & Benign Samples
- ✔ Non-Executable Representations
- ✔ Reconstruction Computationally Infeasible
- ✔ Visual Pattern Exploration Classification

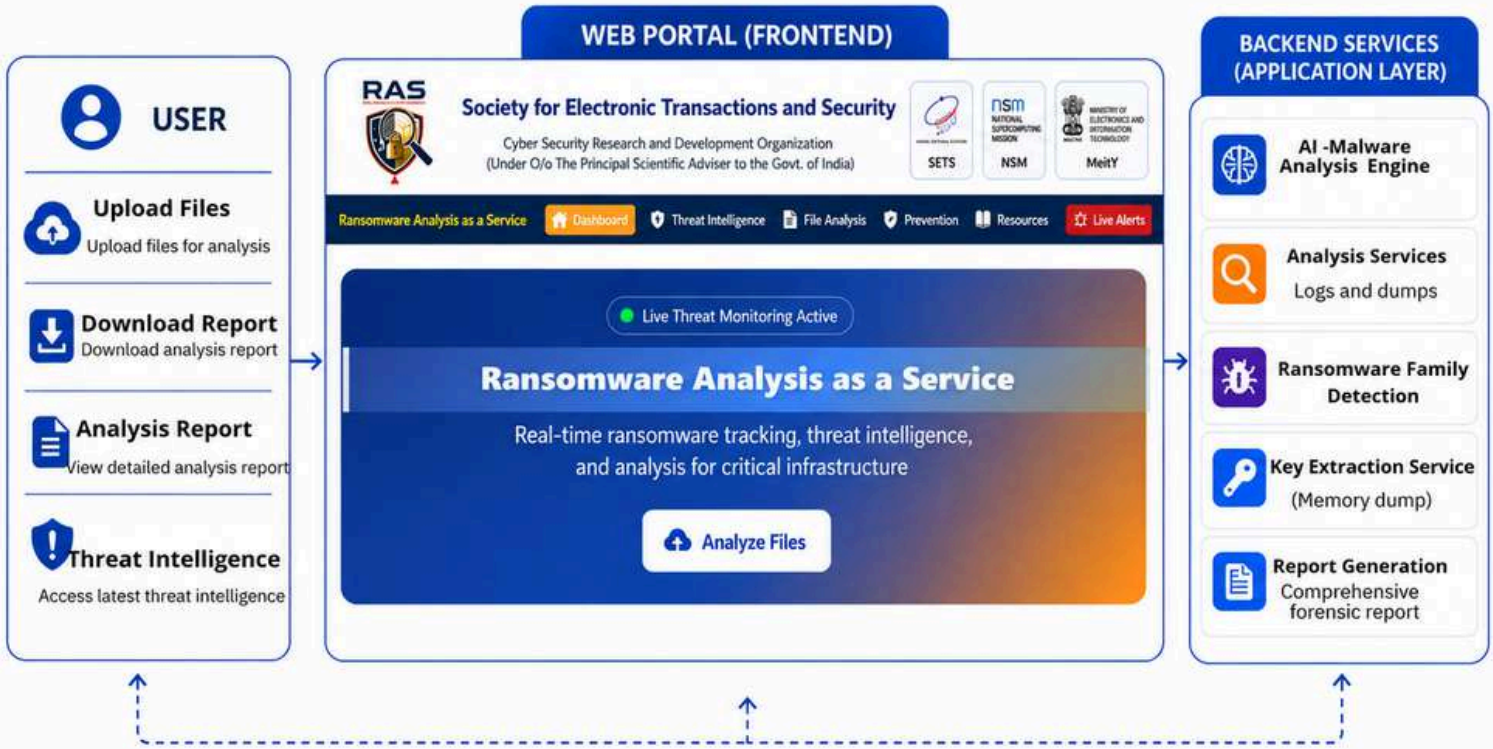
Available on IndiaAI AI Kosh

Scan to access the Repository

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

विज्ञान एवं प्रौद्योगिकी मंत्रालय
MINISTRY OF SCIENCE AND TECHNOLOGY

aiकोष



SETS-RAS - Ransomware Analysis as a Service

SETS-RAS is a privacy-preserving analysis platform developed by SETS to support victims of ransomware attacks. It enables secure investigation of suspect files, process/network logs without exposing sensitive or confidential data to external parties, addressing the fear that reporting an attack could compromise private information. The platform also analyzes memory dumps to identify the encryption algorithm in use and, where possible, retrieve cryptographic keys directly from memory. The platform identifies ransomware families from ransom notes or encrypted files and provides available decryptors to support recovery for organizations, responders, and the cybersecurity community.

- ✔ Confidential Analysis of Suspect Files and Process/Network Logs
- ✔ Privacy-Preserving Mechanisms Applied Before Analysis
- ✔ For Victims, Incident Responders & Researchers

Scan to access the Website