SETS R&D ACTIVITIES

2024-2025

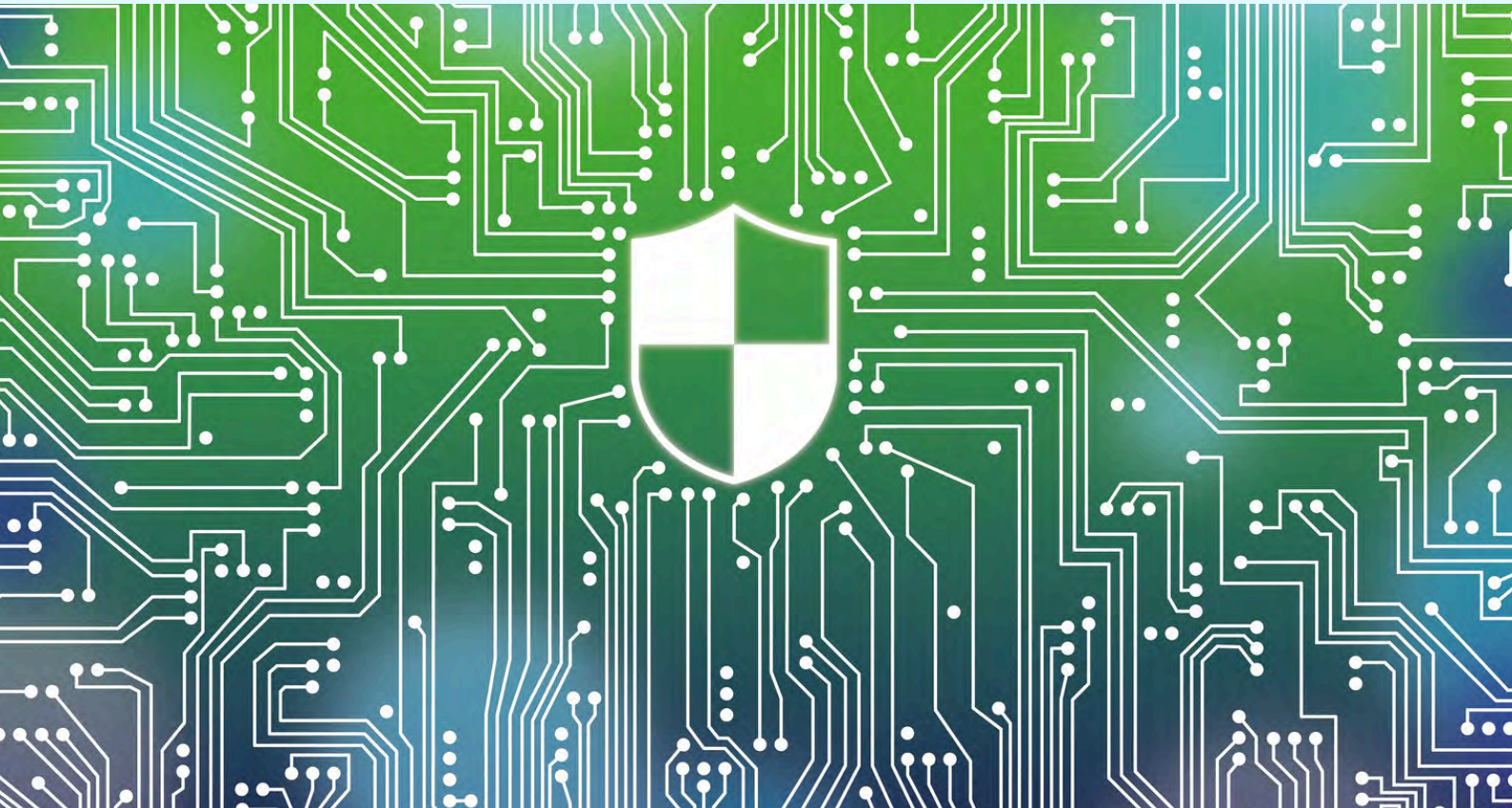
Strategy Synergy for Security

SOCIETY FOR ELECTRONIC TRANSACTIONS AND SECURITY (SETS)

Cyber Security Research and Development Organisation

(Under O/o The Principal Scientific Adviser to the Govt. of India)

www.setsindia.in



Society for Electronic Transactions and Security (SETS), an initiative under the Office of the Principal Scientific Adviser (PSA) to the Government of India has been working in the frontier of Cyber Security areas such as Cryptology, Hardware Security, Quantum Security, and Network Security. During the 2024-2025 year SETS has undertaken few extramural projects and the details of the same are given below.

I . Cyber Security R&D Initiatives

SETS is executing the following government supported projects by various funding agencies including Office of Principal Scientific Adviser (PSA), Ministry of Electronics and Information Technology (MeitY), National Security Council Secretariat (NSCS), Department of Science & Technology (DST), Defence Research and Development Organisation (DRDO), POWERGRID Centre of Excellence in Cybersecurity (PGCoE), National Supercomputing Mission (NSM) and National Quantum Mission (NQM).

1. Enabling Secure Boot in RISC-V Processors using Post Quantum Secure Schemes

The primary objective of the project is to demonstrate secure boot functionality in a RISC-V environment using both classical and post-quantum secure cryptographic signature schemes, along with a mechanism for on-chip generation of keys.

In the first approach, the entire secure booting process will be implemented and demonstrated on a Field-Programmable Gate Array (FPGA) using a RISC-V softcore processor integrated with the required cryptographic primitives.

In the second approach, the FPGA device containing the developed cryptographic implementations will be interfaced with a physical RISC-V processor kit to demonstrate secure boot functionality.

In the third approach, the requisite cryptographic schemes will be implemented in software and executed directly on the RISC-V processor to demonstrate secure boot. As part of the project deliverables, SETS will implement classical and a suitable NIST post-quantum secure signature candidate and demonstrate secure boot in a RISC-V secure environment, along with a mechanism for on-chip key generation. SETS is collaborating with C-DAC to enable Secure-boot of VEGA Processor.

2. Development of PKI-based Digital Certificates for IoT Device Security

The primary objective of the project is to develop a compact Public Key Infrastructure (PKI) framework for IoT devices, enabling generation and management of digital certificates.

SETS will develop a firmware to generate Certificate Signing Requests (CSR), store and parse digital certificates on the device, and communicate with a Certificate Authority (CA) server through APIs and also provide a Proof of Concept (PoC) for embedding digital certificates in IoT surveillance devices using a compact PKI framework and document the implementation.

Development of a PKI application for IoT device lifecycle management, including a PoC using Smart CCTV device has been completed.The digital certificate as per IETF standard has been implemented and integrated with TLS 1.3 handshake for secure device authentication and communication. This work is being carried out by SETS along with Controller of Certifying Authorities (CIA) and Industry.

3. Internet of Things (IoT) Sandbox development and nationwide establishment

The primary objective of the project is to establish a comprehensive IoT security ecosystem and sandbox environment.This is a Collaborative effort with other R&D and academic institutions.

As part of the project deliverables, SETS will develop framework for formal verification of cryptographic algorithms and software tools for privacy analysis and IPv6 security assessment that can be integrated into the IoT security sandbox environment. Formal verification tools have been explored and executed IPv6 security compliance testing. In the coming year, the focus will be on developing a framework for formal analysis using open-source tools, integrating and testing these tools within the sandbox environment, exploring privacy frameworks for IoT devices, and developing tools for IPv6 security profiling and secure IPv6 stack evaluation.

4. Automation and Setting up of a reference plan for validating cryptographic algorithms and modules

This project is being carried out by SETS, Chennai, C-DAC Bangalore (lead agency), IIT Madras, IIT Kharagpur and STQC. The project aims to establish a reference laboratory for evaluating and mitigating non-invasive side-channel attacks on cryptographic modules in accordance with ISO/IEC 17825. Under this project, SETS is responsible for developing the Side Channel Analysis (SCA) evaluation setup and automation tools, along with defining testing methodologies and procedures for SCA evaluations.

Activities include implementing non-invasive attack techniques and developing automated frameworks for evaluating cryptographic implementations. The project also supports capacity building and technology transfer to identified testing laboratories for conducting standardized SCA evaluations.

5. Design and development of Post Quantum FIDO2 (Fast Identity online) Authentication Framework

The project focuses on the design and development of a Post-Quantum Cryptography (PQC) enabled FIDO2 authentication framework to support secure password-less authentication systems resilient to future quantum computing threats.

The work involves integrating post-quantum cryptographic algorithms with the FIDO2 framework, along with the development of PQC-supported device authenticators and Web Authentication APIs. The project also includes implementation of classical and post-quantum cryptography based FIDO2 solutions on hardware authenticators and integration with enterprise services to demonstrate secure authentication mechanisms for web-based applications.

6. Development of Secure Post Quantum Public Key Infrastructure

The project is being carried out by SETS in collaboration with IIT (Madras), IIIT (Kurnool), C-DAC (Noida), with C-DAC Bangalore as the lead agency. The primary objective of the proposed project is to develop a robust and scalable Post-Quantum Public Key Infrastructure (PQ-PKI) framework to enable secure and future-ready communication systems.

The project focuses on the design and implementation of quantum-resistant cryptographic algorithms and their integration into both hardware and software platforms. It aims to support secure identity management, authentication, and data protection using advanced cryptographic techniques. Also includes evaluation and validation of implementations against potential security threats, including side-channel attacks. Additionally, it targets the development of secure protocols, certificate management systems, and deployment-ready solutions for practical applications. SETS has developed the algorithm validation framework and side-channel analysis (SCA) framework for cryptographic algorithms, including post-quantum cryptography (PQC) algorithms such as ML-KEM and ML-DSA. SETS performs algorithm validation and SCA for the hardware implementations developed by C-DAC Bengaluru.

SETS is also working on testing at cryptographic module and carrying out side - chanel Analysis of crypto implementation.

7. Development of IP for post-processing stack

The primary objective of this work is to design and develop a post-processing stack for Quantum Key Distribution (QKD) systems, enabling the transformation of raw keys into secure cryptographic keys.

The stack focuses on implementing essential modules such as sifting, parameter estimation, error correction, error verification, privacy amplification, and authentication to ensure key integrity and confidentiality. The solution targets efficient hardware implementation on FPGA platforms to support high-throughput and real-time processing requirements. It also includes comprehensive validation, performance analysis, and security assessment of all modules. Additionally, the project aims to deliver a scalable and deployment-ready post-processing framework supporting multi-protocol QKD systems.

8. Privacy Preserving Techniques using Homomorphic Encryption of Genomics Data

This project is being jointly implemented by SETS Chennai and C-DAC Pune. The overall objective is to develop a framework for privacy preservation based on homomorphic encryption for genomics data encryption and analysis.

The role of SETS is to contribute towards comparison of various homomorphic encryption schemes, development of architecture for genomics data and prototype implementation. The Bio-Informatics team from C-DAC Pune will conduct the literature survey on genomics data, data collection, pre-processing, and testing and validation.

9. Establishment of hardware testing facility

This project is to establish infrastructure to evaluate hardware vulnerabilities and to evolve a comprehensive testing procedure to evaluate hardware devices. The project is being implemented in two phases for the strategic sector.

II. Product & Solutions

SETS as part of internal R&D and product development initiatives has initiated the development of the following solutions:

1. SETS Virtual Private Network (VPN)

SETS VPN is a Virtual Private Network (VPN) solution in the form of VPN Client developed for Android, Windows and Linux devices. SETS VPN App is built on the top of Wire Guard Client to facilitate remote access VPN services between the device such as cell phones, tablets, Desktops, Laptops etc. and the SETS VPN Server which resides as a gateway device in a private network. SETS VPN provides secure communication with its corresponding Server over an untrusted public channel like Internet. SETS VPN ensures user authentication, content protection and integrity protection of user's data traversing over the Internet. SETS VPN is currently being used by various government agencies.

VPN can be deployed for providing secure access to any enterprise networks, university/school campus networks, e-Governance, banking and finance, corporations.

2. SETS Public Key Infrastructure Suite for Enterprise Security

Post-quantum digital certificates can be used for managing the identity and security of users and devices in a quantum internet era. Quantum Safe Digital Certificate solution, implemented by SETS, allows enterprises and security professionals to generate a quantum-safe PQ key, X.509v3 digital certificate for CA and Client and utilize these certificates for digital authentications and signatures.

CA Software is useful for Certifying Authorities and for Enterprises that uses Digital Signature for their internal workflows. SETS CA Solution is being used by government agencies.

3.SETS Ransomware Early Detection Solution (REDS)

Design and development of an AI-based security tool for early detection of ransomware activity in Windows systems through system behaviour monitoring and alert generation. Detailed testing and pilot deployment of REDS has been initiated.

4. SETS Public Key Infrastructure (PKI) for Blockchain

Design and development of a PKI framework for permissioned blockchain networks to support identity management, certificate-based authentication, secure transaction signing, and cryptographic key management, with integration initiated with government applications.

5. SETS Quantum Random Number Generator (QRNG)

A Quantum Random Number Generator (QRNG) device offers high-quality random sequences using unique properties of quantum physics. QRNG exploits nature's inherent randomness. SETS developed a portable QRNG for consumer applications. This can be consumed as hosted service and available as component for integration into any device that may require random number. Applications such as CAPTCHA/SMS generation may also be able to leverage QRNG. SETS is working towards QRNG as service.

III. Contributions to National Missions

1. National Supercomputing Mission (NSM)

NSM is steered jointly by the Department of Science and Technology (DST) and Ministry of Electronics and Information Technology (MeitY). Under the NSM, Artificial Intelligence (AI) for Cyber Security (CS) is a consortia project along with SETS, Chennai, C-DAC Bengaluru, IIT Madras, IIT Jodhpur and IIT Delhi.

AI & Cybersecurity Initiative

The core objective of the AICS Artificial Intelligence for Cybersecurity project is to develop a national R&D capability that uses Artificial Intelligence (AI) to strengthen Cyber Security, and also make AI systems more secure and trustworthy. SETS is contributing towards application of AI for Side-chanel Analysis of Ransomware analysis

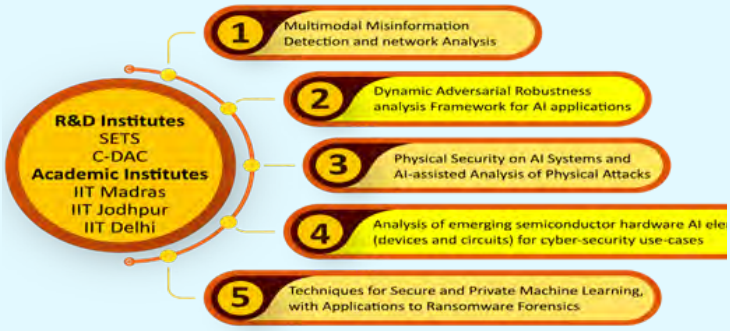


Figure 1 : AI & Cybersecurity R&D under NSM

2. National Quantum Mission (NQM) Quantum Communication Thematic Hub

Quantum Internet with Local Access (QuILA): This project aims to build a long-distance quantum key distribution (QKD) network with intermediate secure nodes and metro-area quantum access networks at the endpoints.

Lead by IIT Madras, SETS Chennai along with other collaborating agencies are contributing to this project. SETS contribution includes development and deployment of advanced quantum key distillation and authentication protocols, the design of secure node architectures, and frameworks for interoperability in hybrid quantum-classical environments. Additionally, SETS is actively involved in standardization and policy-level contributions for QKD network deployment and integration within national infrastructure.

Quantum Computing Thematic Hub

Programmable photonic quantum computing using qubits encoded in different degrees of freedom of a photon: The main objective of this initiative is to design and develop an optimized architecture of a scalable gate-based programmable photonic quantum computing system with inbuilt fault tolerance.

Lead by IISc Bangalore, SETS will focus on the design and implementation of quantum error correction (QEC) solutions tailored for photonic systems, and will explore cryptographic applications of the photonic quantum computer.

The emphasis will be on leveraging quantum computational advantages to strengthen secure communication, authentication, and related security protocols.

Also, Applications such as Quantum Credentials are being investigated to provide highly secure, quantum-resistant identity verification mechanisms and quantum tokenized signature schemes. Additional areas of work include the design and implementation of quantum error correction schemes to enhance reliability, as well as the integration of photonic quantum computing capabilities into next-generation cryptographic infrastructures, enabling robust, scalable, and future-proof security solutions.

IV. Contributions towards National Level Roadmap

1. Transition to PQC

SETS under the guidance of the O/o the Principal Scientific Adviser, Controller of Certifying Authorities (CCA) and MeitY have jointly prepared a roadmap transition to Post-Quantum Cryptography (PQC). This was done based on consultation and brain-storming discussions held involving 40+ Industries including startups involved in the development of

Hardware Security Module (HSM), Cryptography and PKI, Semiconductor and Embedded system and R&D org., Academia & Strategic agencies. The report includes details on PQC enabled applications, Protocol systems and libraries, Crypto-Agility, R&D PoC implementation, Hybrid/Pure PQC approaches, Awareness & capacity development. The report is submitted to National Quantum Mission (NQM), DST and is available at SETS website.

2. **National Roadmap on Hardware Security**

Hardware Security becomes as essential focus in design and deployment of any digital infrastructure from consumer electronics to advanced industrial control systems due to the increasing cyber threats. Hardware security encompasses the protection of IP cores, integrated chips, and supply chain of each hardware component from manufacturing to deployment. Ensuring the security of hardware components is crucial in safeguarding against compromising of confidentiality, integrity, and system availability.

Under the guidance of the Office of the PrincipalScientific Adviser (PSA) to the Government of India, SETS prepared the roadmap for hardware security involving 35 Indian Industries involving Fabless design, IDMs (Integrated Design and Manufacturing), Startups, R&D org., Academia & Strategic agencies at NIAS Auditorium, IISc Bangalore, on October 4, 2024.

The roadmap outlines the current strategic areas of focus, global initiatives, current national scenario, emerging threats, and important goals to strengthen the security of hardware components in our country. Discussion on the implementation of the roadmap is being done with the leading ministries.

From the design phase to deployment and lifecycle management, the document provides insights into strategic priorities and actionable solutions for hardware security challenges against any threats. The roadmap also highlights the immediate security concerns, mid-term goals and long-term goals that can be implemented in a phased manner.

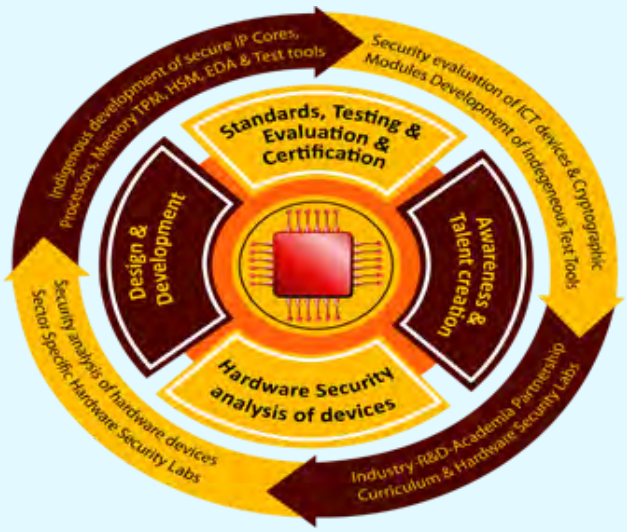


Figure 2 : Hardware Security Roadmap

Events

SETS has been contributing to knowledge dissemination by way of conducting training programs, workshops, seminars, conferences and expert talks. The list of such activities is detailed below:

1. Open workshop conducted by SETS for the preparation of the **National Roadmap on Hardware Security** with Indian industries, R&D organisations and Academia; at NIAS Auditorium, IISc Bangalore, on October 4, 2024. Around 35 industries participated in the event and gave feedback as inputs for the preparation of the roadmap.

Snapshot of the brainstorming discussions held at NIAS Auditorium, IISc Bangalore on 4th October 2024 on National Roadmap on Hardware Security.

2. SETS in association with IMSc and CMI under the aegis of CRSI organized the Silver Jubilee edition of the Indocrypt between 18 and 21 December, 2024

Snapshot of 25th Edition of INDOCRYPT 2024 International Conference organized by SETS along with IMSc chennai, CMI and Anna University during December 18th to 21, 2024 at Chennai.

3. Brainstorming with industry on "Transition Towards Post Quantum Cryptography (PQC) for Public Key Infrastructure (PKI)"

Snapshot of Brainstorming Session on Transition towards PQC held on 27 thSept. 2024 at SETS Chennai .

4. Memorandum of understanding between SETS and MCTE this MoU is to strengthen cyber security, quantum security and information security capabilities. The MoU was signed in the agust presence of Prof. Ajay Kumar Sood, Principal Scientific Advisor (PSA) to the Government of India & President SETS, and Dr. Parvinder Maini, Scientific Secretary, O/o PSA to Government of India on 20 September 2024 at O/o PSA New Delhi.

Snapshot of MoU between SETS and MCTE in the presence of Prof. Ajay Kumar Sood, Hon'ble Principal Scientific Advisor (PSA) to the Government of India & President SETS on 20 September 2024.

5. On 4th September 2024, S. Krishnan, Secretary, Ministry of Electronics and Information Technology (MeitY) launched the 'Vishvasya' - Blockchain Technology Stack. It is designed to provide Blockchain-as-a-Service (BaaS) with a geographically distributed infrastructure to support various permissioned Blockchain based applications.

Snapshot of the launch of Vishvasya -Blockchain Technology Stack by Shri. S. Krishnan , IAS, Hon'ble Secretary, Ministry of Electronics & Information Technology (MeitY) On 4th September 2024 at MeitY, Delhi.

23rd Foundation Day of SETS

SETS celebrated its 23rd Foundation Day at its headquarters in Chennai on 25th June 2024. The event was graced by Prof. Ajay Kumar Sood, Hon'ble Principal Scientific Adviser and President SETS, who delivered the presidential address. Dr Sanjay Bahl, Director General, Indian Computer Emergency Response Team (CERT-IN), MeitY, Government of India delivered the Foundation Day Talk, where he emphasized the growing cybersecurity needs of the nation and the important role played by SETS in strengthening India's cybersecurity ecosystem.

A Special Address was delivered by Dr Parvinder Maini, Scientific Secretary, O/o the Principal Scientific Adviser to the Government of India, who highlighted the importance of continued research and collaboration in emerging areas of cybersecurity and digital technologies.

During the occasion, the Quantum Security Lab at SETS was inaugurated by the Hon'ble PSA, marking an important milestone in strengthening research and development in quantum-safe cybersecurity technologies. The event also served as an opportunity for SETS to receive guidance and directions from the Hon'ble PSA, Scientific Secretary, experts, and well-wishers who have been supporting and mentoring the organization in advancing its research initiatives and aligning its activities with national priorities.

A Technology Session was organized by SETS scientists, followed by an Open House product demonstration, providing a platform to present ongoing work, discuss emerging research areas, and interact with experts and stakeholders.

On the occasion, the VPN team at SETS was also felicitated for the successful large-scale deployment of a VPN solution for the strategic sector, recognizing their significant contribution towards developing and implementing indigenous cybersecurity solutions.

Snapshot of 23rd Foundation Day Celebrations of SETS on 25th June 2024

Snapshot of the Inauguration of Quantum Security Lab at SETS by Prof. Ajay Kumar Sood, Hon'ble Principal Scientific Advisor (PSA) to the Government of India held on 25th June 2024

SETS Hands on Training

SETS team conducted specific hands-on training during the year as given below:

1. SETS has conducted a five-day hands-on training session on "FPGA implementation of post-processing for QKD" from 11th to 15th November 2024.

2. SETS has conducted a two-day training program on the "SETS VPN solution" to the officials from 21 Signal Corps, Indian Army at New Delhi from 25th February 2025 to 26th February 2025

Strategy Synergy for Security

SOCIETY FOR ELECTRONIC TRANSACTIONS AND SECURITY (SETS)

Cyber Security Research and Development Organisation

(Under O/o The Principal Scientific Adviser to the Govt. of India)

www.setsindia.in