IARE
INSTITUTE OF
AERONAUTICAL ENGINEERING

HIGH IMPACT PRACTICES (HIPS)

CYBER SECURITY PROJECTS (CSP)

INFORMATION PACKET

2024 - 2025

Appreciate IARE students who are showing interest in the High Impact Projects (HIP) - Cybersecurity Project Program at the Institute of Aeronautical Engineering!

Cybersecurity team members work as part of a research group of students, research scholars, and faculty members to tackle novel research and design problems around a theme. Students who join SRI teams earn academic credits (RBL / PBL) for participating in design/discovery efforts that assist faculty and students with research and development issues in their areas of expertise.

Cybersecurity teams are:

- Collaborative Research – This is an excellent opportunity for students who are committed to research towards social developments and emerging needs for the industry.
- Internship Activity – The project coordinator listed current research areas for offering internships to either a single student or a team size of most two students. The coordinator allotted two mentors based on the research area and facilitated exclusive research laboratories for selected SRI students. This SRI project bridges the gap between academic learning and real-world social applications. It helps for enhancing the professional development
- Long-term - Each student may participate in a project for up to three months (January to March / May to July / September to November).

The primary goal of HIP is to provide a level of consistency, expertise, and diversity of thought in emerging research areas that will allow them to gain hands-on experience in academic or industrial research environments through this internship project.

- Provide students with immersive exposure to empirical research, experimental design, hypothesis formulation, data acquisition, statistical analysis, and technical reporting under expert mentorship.
- Integrate student researchers into ongoing faculty-led research programs, thereby enhancing research throughput.
- Contribute to the development of a vibrant research ecosystem that aligns with the institution’s strategic goals in innovation, interdisciplinary collaboration, and knowledge production.
- Equip students with domain-specific research competencies, fostering critical thinking, problem-solving, and technical communication skills that are essential for advanced academic or industrial careers.
- Promote high-impact research outcomes for social applications, climate change, water management, effective energy usage, agriculture, etc.
- Encourage translational research and innovation with potential for intellectual property generation, prototype development.
- **The research theme of this HIP - Cybersecurity project also focuses on the challenges presented by the Sustainable Development Goals (SDGs).**

IARE Sustainability Development Goals (SDGs) highlighted with Blue Colour Font	
SDG #1	End poverty in all its forms everywhere
SDG #2	End hunger, achieve food security and improved nutrition and promote sustainable agriculture
SDG #3	Ensure healthy lives and promote well-being for all at all ages
SDG #4	Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all
SDG #5	Achieve gender equality and empower all women and girls

SDG #6	Ensure availability and sustainable management of water and sanitation for all
SDG #7	Ensure access to affordable, reliable, sustainable and modern energy for all
SDG #8	Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all
SDG #9	Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation
SDG #10	Reduce inequality within and among countries
SDG #11	Make cities and human settlements inclusive, safe, resilient and sustainable
SDG #12	Ensure sustainable consumption and production patterns
SDG #13	Take urgent action to combat climate change and its impacts
SDG #14	Conserve and sustainably use the oceans, seas and marine resources for sustainable development
SDG #15	Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss
SDG #16	Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels
SDG #17	Strengthen the means of implementation and revitalize the Global Partnership for Sustainable Development

The following research domains are recommended for HIPs - Cybersecurity Projects, and selected students should find the research gap and frame the problem statements from any one of the themes below.

1. Cyber Threat Intelligence for Secured Systems Integration (**SDG #17)**
2. Ethical Hacking & Penetration Testing to Identify and Classify Vulnerabilities **(SDG #15)**
3. AI-Driven Phishing Detection and Email Security Solutions **(SDG #9)**
4. Blockchain-based Secure Identity Management Systems **(SDG #16)**
5. IoT Device Security and Privacy in Smart Environments **(SDG #11)**
6. Cloud Security Solutions for Privacy-Preserving Data Storage and Access **(SDG #9)**
7. Digital Forensics for Cybercrime Investigation and Evidence Recovery **(SDG #16)**
8. Ransomware Detection and Mitigation using Behavior-Based Analysis **(SDG #8)**
9. Cybersecurity Awareness and Education using Gamification Techniques **(SDG #4)**
10. Security and Risk Assessment Frameworks for Critical Infrastructure Protection **(SDG #13)**

In order to participate in HIP, you must formally apply and be accepted by the project coordinator. To proceed, please mail to the project coordinator, Dr. M Purushotham Reddy (dr.purushothamreddy@iare.ac.in), Head of IT. This will bring up all available open positions tagged as SRI projects. When submitting a project document and an updated résumé, include a statement regarding why you are interested in working with the team to which you are applying.

Please note that participation by the HIP team requires registration for the accompanying research statement from any of the specified domains. More information will be provided to all selected HIP applicants who have been offered a position.

If you have any questions about a particular team, please contact the team's faculty mentor(s).
We encourage you to contemplate this fascinating new opportunity. We look forward to receiving your application submission!

Cyber Threat Intelligence for Secured Systems Integration

Dr. M Purushotham Reddy, Professor & Head, Dept. of IT - Faculty Mentor

GOALS

The primary goal of this project is to explore the seamless integration of Cyber Threat Intelligence (CTI) into the architecture, deployment, and ongoing operation of secure information systems. As cyber threats become more adaptive and persistent, this initiative aims to shift from reactive defenses to a proactive, intelligence-led security posture. By embedding CTI at all levels of system integration, the project will develop methods to predict, detect, and neutralize threats before they exploit system vulnerabilities.

Key objectives include the design of a modular integration framework that enables real-time ingestion, analysis, and application of threat intelligence across all system layers. This encompasses the use of structured threat data (e.g., IOCs, TTPs, threat actor profiles) and the alignment of CTI with critical integration points within IT and OT systems. The approach promotes contextual threat awareness, system hardening, and dynamic incident response capabilities.

The project will also emphasize intelligent automation and adaptive response mechanisms, leveraging artificial intelligence and machine learning to enhance system integration processes. These systems will be capable of continuous monitoring, anomaly detection, and self-adjustment in response to emerging threats. Compliance with industry standards and integration with GRC (governance, risk, and compliance) models will ensure sustainable security posture and regulatory alignment. Importantly, the initiative seeks to balance automation with human oversight, making threat intelligence machine-actionable yet human-interpretable, supporting cybersecurity analysts in high-stakes environments.

METHODS & TECHNOLOGIES

The project will utilize modern threat intelligence sharing protocols such as STIX/TAXII to enable standardized, automated CTI exchange. Machine learning algorithms will be developed for detecting anomalies in system integration pipelines. SIEM platforms (e.g., Splunk, QRadar) will support centralized monitoring and correlation of logs and security events. Additionally, Threat Intelligence Platforms (TIPs), EDR solutions, and integration-focused behavioral analytics tools will be deployed to simulate attacks, detect vulnerabilities, and enhance incident response readiness. The integration process will follow DevSecOps methodologies to ensure that security is embedded across the development and deployment lifecycle.

MAJORS & AREAS OF INTEREST

The Cyber Threat SRI team needs a diversity of skills:

- Design CTI ingestion and dissemination mechanisms for secure systems integration.
- Architect and implement systems that integrate security and intelligence from the ground up.
- Train and deploy models for pattern recognition and predictive threat analysis in integration workflows.
- Implement security automation and continuous compliance checks during system build and deployment.
- Correlate security data with integration logs for real-time threat detection.
- Enable automated and structured threat information exchange between integrated systems.
- Identify systemic risks at the integration layer and propose mitigation strategies.
- Design response playbooks tailored to integrated environments and CTI-driven alerts.

- Automate threat intelligence application across integrated systems using scripting languages (e.g., Python, Bash).

MENTOR CONTACT INFORMATION

Dr.M Purushotham Reddy
Email: dr.purushothamreddy@iare.ac.in

PARTNERS & SPONSORS

None

Ethical Hacking and Penetration Testing for Assessment of Cyber Attacks to Classify Vulnerability

Dr. M Purushotham Reddy, Professor & Head, Dept. of IT - Faculty Mentor

GOALS

This project is focused on leveraging ethical hacking and penetration testing methodologies to proactively identify, exploit, and classify vulnerabilities within modern IT systems and applications. In today's complex cyber landscape, organizations face an expanding attack surface, making traditional vulnerability management insufficient. This initiative aims to establish a comprehensive vulnerability assessment framework through controlled, authorized attacks that mimic real-world adversary behavior.

The primary objective is to uncover security weaknesses in systems before they can be exploited by malicious actors. This includes everything from misconfigurations and unpatched software to insecure coding practices and logic flaws. By performing systematic penetration tests, the project seeks to classify vulnerabilities based on impact, exploitability, and severity using standards such as CVSS (Common Vulnerability Scoring System).

A key goal is to integrate penetration testing into DevSecOps pipelines, promoting secure development practices and continuous security validation. The project also emphasizes the role of automated and manual testing tools in enhancing assessment coverage and reliability. Through detailed reporting and risk analysis, the findings will support strategic remediation planning, helping organizations prioritize security efforts effectively.

METHODS & TECHNOLOGIES

The project will employ both automated scanning tools and manual testing techniques across networks, web applications, APIs, cloud environments, and endpoints. Tools may include: Kali Linux toolset (e.g., Nmap, Metasploit, Burp Suite, Nikto, SQLmap), Vulnerability Scanners like Nessus, OpenVAS, and Qualys, Web Application Testing tools like OWASP ZAP and Burp Suite Pro, Social Engineering Simulations (phishing, pretexting) where applicable and ethical, Custom Scripting using Python, Bash, or PowerShell for automation or exploitation, CVSS scoring for risk classification and prioritization.
Testing will follow established standards and frameworks, such as OWASP Top 10, MITRE ATT&CK, and NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment).

RESEARCH, DESIGN, & TECHNICAL ISSUES

- Inconsistent Testing Environments – Difficulty in replicating real-world infrastructure and attack surfaces for accurate and repeatable vulnerability assessments.
- Tool Limitations & False Positives – Automated tools like Nessus, Nmap, or Metasploit may produce unreliable results, leading to false positives or missed vulnerabilities.
- Vulnerability Classification Complexity – Mapping discovered exploits to severity scores (e.g., CVSS) and attack frameworks (e.g., MITRE ATT&CK) requires deep contextual analysis and precision.
- Legal and Ethical Constraints – Testing boundaries must comply with cybersecurity laws and ethical hacking standards to avoid unauthorized access or data exposure.
- Limited Dataset Access – Lack of access to real-world exploit data and enterprise environments restricts effective research validation and threat simulation accuracy.
- Integration with SDLC – Difficulty in feeding vulnerability assessment outputs into secure development practices for continuous improvement of software security.

MAJORS & AREAS OF INTEREST

This Ethical Hacking and Penetration Testing SRI team needs a diversity of skills:

- Ethical Hacking & Red Team Operations – Simulate attacks to uncover real-world vulnerabilities and test system defenses.

- Vulnerability Assessment – Identify and categorize weaknesses using both automated scanners and manual validation techniques.
- Web and Application Security Testing – Test common attack vectors such as XSS, SQLi, CSRF, and authentication flaws.
- Operating Systems and Network Security – Evaluate internal and external threats across different platforms and network configurations.
- Security Tool Proficiency – Use and customize professional-grade tools such as Metasploit, Burp Suite, and Nmap.
- Penetration Testing Methodologies – Apply structured approaches like OSSTMM, PTES, and OWASP.
- Scripting and Exploitation – Develop and execute custom scripts to automate tests or demonstrate proof-of-concept exploits.
- Security Reporting & Risk Communication – Deliver technical findings in a format understandable to both technical and non-technical stakeholders.

MENTOR CONTACT INFORMATION

Dr.M Purushotham Reddy
Email: dr.purushothamreddy@iare.ac.in

PARTNERS & SPONSORS

None

AI-Driven Phishing Detection and Email Security Solutions

Dr. M Purushotham Reddy, Professor & Head, Dept. of IT - Faculty Mentor

GOALS

This project aims to develop and implement AI-driven solutions to detect, prevent, and mitigate phishing attacks—one of the most prevalent and damaging cyber threats targeting users through email. As phishing techniques become increasingly sophisticated, traditional signature-based detection methods often fall short. This initiative focuses on leveraging machine learning (ML) and natural language processing (NLP) to analyze and classify email threats in real time, providing a scalable and adaptive defense mechanism.

The core objective is to design a framework that automatically identifies suspicious patterns, linguistic anomalies, and malicious behaviors in email content and metadata. This includes detecting spear-phishing, business email compromise (BEC), and credential harvesting campaigns by analyzing sender reputation, payloads, URL redirection, attachment behavior, and message context.

The project also aims to integrate AI-based detection models into secure email gateways (SEGs) and cloud-based email platforms (e.g., Microsoft 365, Google Workspace). Emphasis will be placed on user awareness and response automation, such as intelligent email flagging, real-time warnings, and automatic quarantine of threats. By combining AI capabilities with threat intelligence feeds and human-in-the-loop verification, the system will enhance the overall email security lifecycle, reducing false positives while improving detection precision.

METHODS & TECHNOLOGIES

The project will leverage a combination of AI techniques and security technologies, including:

- Natural Language Processing (NLP) for semantic and contextual analysis of email content
- Supervised and unsupervised machine learning models for phishing classification
- Deep learning techniques (e.g., LSTM, CNNs) for detecting subtle patterns in email structure and metadata
- Phishing Detection Datasets (e.g., Enron dataset, PhishTank, open-source threat corpora)
- Threat Intelligence Integration for URL, IP, and attachment reputation scoring
- Email Security Gateways (e.g., Proofpoint, Mimecast) and APIs for interception and analysis
- Cloud Email Security APIs (e.g., Google Cloud Security, Microsoft Graph Security)
- User Feedback Loops to improve model accuracy through real-time validation

MAJORS & AREAS OF INTEREST

The following majors or areas of interest are identified in this theme of research work:

- Artificial Intelligence & Machine Learning – Develop and train models for real-time phishing detection and adaptive learning.
- Natural Language Processing – Analyze linguistic patterns, social engineering techniques, and deceptive communication tactics.
- Cyber Threat Intelligence – Enrich AI models with contextual threat data from phishing campaigns.
- Email Security & Protocols – Understand and secure SMTP, SPF, DKIM, and DMARC configurations.
- Security Automation & Orchestration (SOAR) – Automate incident response workflows and user alerting.

- Cloud Security – Implement and test security layers in cloud-native email platforms.
- Data Labeling & Annotation – Curate and label phishing datasets for supervised learning.
- Human Factors in Security – Design systems that enhance user awareness without overwhelming them.

MENTOR CONTACT INFORMATION

Dr.M Purushotham Reddy
Email: dr.purushothamreddy@iare.ac.in

PARTNERS & SPONSORS

None

Blockchain-based Secure Identity Management Systems

Dr. U Sivaji, Associate Professor, Dept. of IT - Faculty Mentor

GOALS

The primary goal of this project is to design and implement a decentralized, tamper-resistant identity management system using blockchain technology. Traditional identity systems are often siloed, vulnerable to breaches, and offer limited user control over personal data. This initiative aims to address these limitations by leveraging blockchain's immutability, transparency, and distributed architecture to create secure and privacy-preserving digital identity frameworks.

Key objectives include developing a self-sovereign identity (SSI) model, where individuals maintain control over their personal credentials and share them selectively with third parties. The project will explore the use of smart contracts to manage authentication, verification, and access control without relying on centralized authorities. It will also investigate zero-knowledge proofs and cryptographic hashing techniques to ensure that identities are verifiable without exposing sensitive information.

The system will be designed to support interoperability across institutions, enabling secure and unified identity management in sectors such as finance, healthcare, education, and government services. Emphasis will also be placed on compliance with data privacy regulations like GDPR and emerging digital identity standards (e.g., W3C Verifiable Credentials). Ultimately, the goal is to develop a secure, scalable, and user-centric identity management solution that empowers users and reduces identity fraud.

METHODS & TECHNOLOGIES

- Blockchain Platforms – Implementation using platforms like Ethereum, Hyperledger Fabric, or Polygon for distributed identity ledgers.
- Smart Contracts – Use of Solidity or Chaincode to encode verification logic, revocation rules, and access policies.
- Decentralized Identifiers (DIDs) – Adoption of W3C DID standards to uniquely identify users without a central authority.
- Verifiable Credentials – Management of claims that can be cryptographically validated and selectively disclosed.
- Zero-Knowledge Proofs (ZKPs) – Techniques to validate identity attributes without revealing the underlying data.
- Encryption & Hashing – Use of cryptographic techniques like SHA-256 and elliptic curve cryptography (ECC) for data protection.
- Interoperability Standards – Integration with OpenID Connect, OAuth 2.0, and emerging digital identity protocols.
- User Interfaces – Development of mobile and web-based wallets to manage digital identities and consent.

RESEARCH, DESIGN, & TECHNICAL ISSUES

In general, SRI team members will be involved in Blackchain based security face Challenges include ensuring scalability of blockchain networks, maintaining low latency for real-time verification, and addressing key management and data revocation complexities. Usability and user adoption are also critical, as is balancing privacy, transparency, and compliance. Additionally, designing robust governance models for decentralized identity ecosystems is an ongoing research focus.face challenges in handling large-scale heterogeneous data from various sources, ensuring compliance with data privacy laws, and integrating legacy systems with modern computing technologies. Designing systems that balance accuracy, security, and usability is technically and ethically demanding.

MAJORS & AREAS OF INTEREST

These areas are listed below in this theme of work:

The SRI team welcomes participants with backgrounds in the following areas:

- Blockchain Development & Cryptography – Building smart contracts and understanding secure transaction mechanisms.
- Identity & Access Management (IAM) – Designing systems that manage user identity, roles, and authentication securely.
- Distributed Systems & Networking – Understanding the infrastructure and performance aspects of decentralized platforms.
- Cybersecurity & Privacy Engineering – Applying secure design principles to protect user identities and consent.
- Regulatory Compliance & Ethics – Ensuring the identity system meets legal and ethical standards for data usage and storage.
- Full Stack Development – Creating frontend and backend interfaces for user-friendly identity management applications.
- Cloud Infrastructure & DevOps – Deploying decentralized applications (dApps) on scalable, secure cloud environments.
- User-Centered Design – Designing intuitive interfaces and workflows to improve adoption and usability of digital ID systems.

MENTOR CONTACT INFORMATION

Dr.U Sivaji
Email: u.sivaji@iare.ac.in

PARTNERS & SPONSORS

None

IoT Device Security and Privacy in Smart Environments

Dr. U Sivaji, Associate Professor, Dept. of IT - Faculty Mentor

GOALS

This project focuses on addressing the growing security and privacy challenges associated with Internet of Things (IoT) devices in smart environments, including homes, cities, healthcare systems, and industrial applications. As IoT devices become increasingly pervasive, they also expand the potential attack surface, often lacking adequate security mechanisms and transmitting sensitive data over unsecured networks.

The primary goal is to design and implement robust, scalable security frameworks that safeguard data integrity, ensure device authentication, and preserve user privacy in interconnected environments. A key objective is to assess vulnerabilities in common IoT protocols (e.g., MQTT, CoAP), firmware, and wireless communications. The project will develop and test countermeasures such as lightweight cryptographic algorithms, secure boot mechanisms, zero-trust access control models, and intrusion detection systems tailored for resource-constrained IoT devices.

Another aim is to explore privacy-preserving techniques such as data anonymization, edge computing, and differential privacy to reduce reliance on centralized cloud services. The project will simulate and evaluate threat scenarios like device spoofing, man-in-the-middle attacks, and data exfiltration in smart environments, providing real-world validation of security models.

METHODS & TECHNOLOGIES

- IoT Communication Protocol Analysis – Security assessment of MQTT, CoAP, Zigbee, Bluetooth LE, and LoRaWAN.

- Device Authentication & Encryption – Use of TLS, DTLS, ECC, and symmetric key cryptography for secure device pairing and communication.

- Secure Firmware Development – Implementation of secure boot, firmware validation, and over-the-air (OTA) update security.

- Intrusion Detection for IoT – Deployment of lightweight, ML-based IDS tailored to constrained devices and anomaly detection.

- Edge & Fog Computing – Processing sensitive data closer to the source to reduce latency and privacy risks.

- Threat Modeling & Penetration Testing – Simulation of attacks on IoT networks and evaluation of mitigation strategies.

- Privacy Engineering – Integration of privacy-by-design principles using anonymization and consent-aware data handling.

- IoT Security Frameworks – Adoption of NIST IoT security guidelines and OWASP IoT Top 10 for standards-based design.

RESEARCH, DESIGN, & TECHNICAL ISSUES

IoT security introduces challenges like heterogeneity of devices, resource constraints, lack of unified standards, and patch management difficulties. Balancing performance with security in low-power devices, securing device-to-device communication, and ensuring user trust while minimizing data exposure are ongoing design concerns. Real-world testing and continuous monitoring are essential due to the dynamic threat landscape.

MAJORS & AREAS OF INTEREST

The faculty mentors and research coordinator for the team are looking for SRI team members interested in:

- Embedded Systems & IoT Engineering – Securing firmware, communication stacks, and hardware-software interfaces.
- Cybersecurity & Network Security – Designing defenses against network-level attacks in IoT ecosystems.
- Machine Learning for Security – Developing lightweight ML models for anomaly and intrusion detection in edge devices.
- Privacy-Preserving Computing – Applying cryptographic and statistical methods to protect user data.
- Wireless Communication Protocols – Studying vulnerabilities and countermeasures in IoT-specific communication protocols.
- Cloud & Edge Architecture – Securing distributed data processing models for real-time IoT analytics.
- Threat Intelligence & Risk Assessment – Identifying and mitigating IoT-specific risks through proactive analysis.
- Compliance & IoT Policy – Aligning systems with international IoT privacy and security standards.

MENTOR CONTACT INFORMATION

Dr.U Sivaji
Email: u.sivaji@iare.ac.in

PARTNERS & SPONSORS

None

Cloud Security Solutions for Privacy-Preserving Data Storage and Access

Dr. S Satheesh Kumar, Professor, Dept. of IT - Faculty Mentor

GOALS

This project aims to design secure, privacy-aware cloud architectures that enable individuals and organizations to store and access sensitive data without compromising confidentiality, integrity, or availability. As cloud adoption continues to grow across sectors like healthcare, finance, and government, so do concerns about unauthorized access, data leakage, and lack of control over outsourced data.

A core goal is to develop end-to-end encryption, access control, and privacy-enhancing technologies to ensure secure cloud storage and fine-grained data sharing. The project focuses on integrating confidential computing, zero-knowledge proofs, secure multiparty computation, and homomorphic encryption to enable computations on encrypted data without revealing its content. Another key objective is to implement role-based and attribute-based access control models (RBAC/ABAC) that enforce dynamic, context-aware permissions.

Furthermore, the project explores the integration of auditing, logging, and key management systems to track data access in real time and mitigate insider threats. Emphasis will be placed on compliance with global data privacy regulations such as GDPR, HIPAA, and CCPA, as well as alignment with best practices for data sovereignty and lifecycle security in multi-cloud and hybrid cloud environments.

METHODS & TECHNOLOGIES

- Blockchain Platforms – Implementation using platforms like Ethereum, Hyperledger Fabric, or Polygon for distributed identity ledgers.
- Smart Contracts – Use of Solidity or Chaincode to encode verification logic, revocation rules, and access policies.
- Decentralized Identifiers (DIDs) – Adoption of W3C DID standards to uniquely identify users without a central authority.
- Verifiable Credentials – Management of claims that can be cryptographically validated and selectively disclosed.
- Zero-Knowledge Proofs (ZKPs) – Techniques to validate identity attributes without revealing the underlying data.
- Encryption & Hashing – Use of cryptographic techniques like SHA-256 and elliptic curve cryptography (ECC) for data protection.
- Interoperability Standards – Integration with OpenID Connect, OAuth 2.0, and emerging digital identity protocols.
- User Interfaces – Development of mobile and web-based wallets to manage digital identities and consent.

RESEARCH, DESIGN, & TECHNICAL ISSUES

Challenges include ensuring scalability of blockchain networks, maintaining low latency for real-time verification, and addressing key management and data revocation complexities. Usability and user adoption are also critical, as is balancing privacy, transparency, and compliance. Additionally, designing robust governance models for decentralized identity ecosystems is an ongoing research focus.

MAJORS & AREAS OF INTEREST

The SRI team welcomes participants with backgrounds in the following areas:

- Blockchain Development & Cryptography – Building smart contracts and understanding secure transaction mechanisms.
- Identity & Access Management (IAM) – Designing systems that manage user identity, roles, and authentication securely.
- Distributed Systems & Networking – Understanding the infrastructure and performance aspects of decentralized platforms.
- Cybersecurity & Privacy Engineering – Applying secure design principles to protect user

identities and consent.
- Regulatory Compliance & Ethics – Ensuring the identity system meets legal and ethical standards for data usage and storage.
- Full Stack Development – Creating frontend and backend interfaces for user-friendly identity management applications.
- Cloud Infrastructure & DevOps – Deploying decentralized applications (dApps) on scalable, secure cloud environments.
- User-Centered Design – Designing intuitive interfaces and workflows to improve adoption and usability of digital ID systems.

MENTOR CONTACT INFORMATION

Dr.S Satheesh Kumar
Email: s.satheeshkumar@iare.ac.in

PARTNERS & SPONSORS

None

Digital Forensics for Cybercrime Investigation and Evidence Recovery

Dr. S Satheesh Kumar, Professor, Dept. of IT - Faculty Mentor

GOALS

This project is dedicated to advancing the field of digital forensics through the development of tools, methodologies, and frameworks for investigating cybercrimes and recovering critical digital evidence. In an era marked by rising cyberattacks, data breaches, and online fraud, digital forensics plays a pivotal role in identifying perpetrators, understanding attack vectors, and supporting legal proceedings with admissible digital evidence.

A key objective is to build capabilities in data acquisition, preservation, analysis, and presentation across various platforms, including computers, mobile devices, cloud environments, and IoT ecosystems. The project will emphasize the forensic recovery of deleted, encrypted, or obfuscated data using both manual techniques and automated forensic tools. It will also explore timeline analysis, malware reverse engineering, network traffic analysis, and live memory forensics to reconstruct the sequence of events and attacker behaviors.

Legal and ethical considerations, such as chain of custody, data integrity, and privacy compliance, are integral to this work, ensuring that evidence remains valid in judicial contexts. The goal is to produce comprehensive digital forensic reports and design workflows that integrate with law enforcement and incident response protocols, ultimately aiding in faster and more reliable cybercrime resolution.

METHODS & TECHNOLOGIES

- Disk & Memory Forensics – Use of tools like Autopsy, FTK, Volatility, and Belkasoft for analyzing hard drives and RAM dumps.

- Network Forensics – Capturing and inspecting network traffic using Wireshark, Zeek, and tcpdump to identify intrusion patterns.

- Mobile Device Forensics – Extraction and analysis of data from Android and iOS devices using tools like Cellebrite and MOBILedit.

- Cloud & IoT Forensics – Investigating virtual machines, cloud storage artifacts, and IoT logs from distributed environments.

- Malware Analysis & Reverse Engineering – Deconstructing malware binaries using Ghidra, IDA Pro, and sandbox environments.

- File System Analysis & Data Carving – Recovery of hidden, fragmented, or deleted files across FAT, NTFS, ext4, and other systems.

- Live & Post-Mortem Forensics – Acquiring evidence from active systems without tampering with volatile data.

- Digital Evidence Chain Management – Implementation of tamper-proof logging, evidence tagging, and integrity checks.

RESEARCH, DESIGN, & TECHNICAL ISSUES

Digital forensics investigations face challenges like data volume explosion, anti-forensics techniques, encrypted storage, and cross-platform evidence correlation. Ensuring real-time evidence acquisition from remote and cloud environments, maintaining legality, and preserving privacy are key technical and ethical considerations. The increasing use of AI in cybercrime also requires analysts to stay ahead with evolving analysis techniques.

MAJORS & AREAS OF INTEREST

This theme is interested in a variety of majors, including but not limited to:

- Cybercrime Investigation – Techniques for identifying, tracking, and prosecuting cybercriminals.
- Digital Forensics & Incident Response (DFIR) – Systematic response and analysis of digital security incidents.
- Malware Analysis & Threat Intelligence – Understanding advanced persistent threats and analyzing attack vectors.
- Forensic Tool Development – Designing automated tools and scripts for digital investigation workflows.
- Data Recovery & Integrity Verification – Retrieving and authenticating digital artifacts from compromised systems.
- Ethical Hacking & Cyber Law – Bridging the technical and legal aspects of cyber investigations.
- Computer & Network Forensics – Deep diving into logs, packets, and system traces to uncover unauthorized activity.
- Legal Compliance & Chain of Custody – Maintaining legal standards in evidence acquisition and reporting.

MENTOR CONTACT INFORMATION

Dr. S Satheesh Kumar
Email: s.satheeshkumar@iare.ac.in

PARTNERS & SPONSORS

None

Ransomware Detection and Mitigation using Behavior-Based Analysis

Dr. A Karthik, Assistant Professor, Dept. of IT - Faculty Mentor

GOALS

The objective of this project is to develop intelligent, behavior-based detection and mitigation strategies to combat the growing threat of ransomware attacks. Traditional signature-based methods are often ineffective against rapidly evolving ransomware variants and zero-day threats. Therefore, this project focuses on analyzing behavioral patterns associated with ransomware activities, such as abnormal file access, encryption routines, privilege escalation, and lateral movement.

A key goal is to design a real-time monitoring and response framework that identifies early indicators of ransomware execution before critical damage occurs. This involves collecting and profiling system behaviors, I/O patterns, process interactions, and network communication in both normal and compromised environments. The project will apply machine learning and statistical analysis to distinguish malicious behavior from benign anomalies.

Another crucial component is the development of automated mitigation responses, such as process isolation, file access blocking, and backup restoration, to reduce the impact of detected attacks. In addition, the project emphasizes continuous learning models that evolve with attacker tactics and adapt to changes in user behavior or system configuration. Integration with Endpoint Detection and Response (EDR) and SIEM systems will ensure comprehensive visibility and rapid containment.

METHODS & TECHNOLOGIES

- Behavior-Based Detection Models – Use of decision trees, anomaly detection, clustering, and supervised learning (e.g., SVM, Random Forests).
- System Activity Monitoring – Tracking file system, registry, process, and memory behavior using tools like Sysmon, Auditd, and OSQuery.
- Dynamic Malware Sandboxing – Execution of suspicious files in isolated environments to observe ransomware behavior (e.g., Cuckoo Sandbox).
- Threat Intelligence Integration – Correlation with known IOCs and TTPs from CTI feeds for hybrid detection.
- Real-Time Mitigation Engines – Automation of protective actions using scripts or APIs that interact with operating systems and security tools.
- Incident Simulation & Testing – Emulating ransomware scenarios in virtual labs to validate detection efficacy and response times.
- Data Backup Strategies – Integration with immutable and versioned backups to support rapid recovery post-attack.
- Security Orchestration – Use of SOAR platforms to automate response workflows and alert handling.

RESEARCH, DESIGN, & TECHNICAL ISSUES

Behavioral detection must overcome challenges like false positives, evasion techniques, polymorphic ransomware, and user-specific baselines. Ensuring lightweight monitoring with minimal system impact and tuning models to avoid alert fatigue are essential design concerns. The project also addresses secure storage and logging of behavioral data, as well as ensuring trustworthiness in automated response actions.

MAJORS & AREAS OF INTEREST

The following are identified the works in the following majors and/or with a background and interest in the areas listed below:

- Malware Behavior Analysis – Investigating how ransomware operates and propagates within target systems.

- Machine Learning in Security – Training models to classify and detect malicious activity based on behavior.

- Operating System Internals – Understanding low-level OS functions for better visibility and control over ransomware activities.

- Incident Response & Containment – Designing workflows to halt infections and recover data securely.

- Security Automation & SOAR – Implementing automated decision-making in threat response pipelines.

- Cyber Threat Intelligence (CTI) – Integrating external threat data with internal detection strategies.

- EDR & SIEM Integration – Leveraging Splunk, QRadar, or Elastic Security for monitoring and analytics.

- Resilience Engineering – Developing recovery and continuity strategies to withstand ransomware disruptions.

MENTOR CONTACT INFORMATION

Dr. A Karthik
Email:a.karthik@iare.ac.in

PARTNERS & SPONSORS

None

Cybersecurity Awareness and Education using Gamification Techniques

Dr. A Karthik, Assistant Professor, Dept. of IT - Faculty Mentor

GOALS

The primary goal of this project is to enhance cybersecurity awareness and education among users by leveraging gamification techniques to make learning more engaging, interactive, and effective. Traditional cybersecurity training often suffers from low engagement and retention rates; this project aims to transform cybersecurity education into a dynamic, user-centric experience that fosters proactive security behavior.

Key objectives include designing and developing gamified learning modules, simulations, and challenge-based activities that cover essential topics like phishing recognition, password hygiene, secure browsing, social engineering risks, and incident reporting. The project will also research motivational design strategies such as badges, leaderboards, progress bars, storytelling, and rewards systems to encourage continuous learning and user participation.

Additionally, the project aims to measure knowledge acquisition, behavior change, and risk reduction resulting from gamified interventions. User feedback and data analytics will be used to continuously refine content and game mechanics. The ultimate goal is to create scalable cybersecurity education platforms that can be deployed in schools, corporations, and public initiatives to build a strong, security-aware culture.

METHODS & TECHNOLOGIES

- Gamification Platforms – Development using Unity, Unreal Engine, or web-based platforms (e.g., HTML5, JavaScript, React) for interactive learning environments.

- Game Design Mechanics – Application of points, badges, missions, narratives, and leaderboards to enhance user motivation.

- Scenario-Based Learning – Simulating real-world cybersecurity challenges like phishing emails, password cracking, and insider threats.

- Behavioral Analytics – Tracking user progress, engagement levels, and learning outcomes using analytics dashboards.

- Adaptive Learning Systems – Personalizing the difficulty and content based on individual performance and knowledge gaps.

- Mobile Learning (mLearning) – Developing responsive, mobile-first designs to make cybersecurity training accessible anywhere.

- User Experience (UX) Design – Focusing on intuitive interfaces and rewarding experiences to maintain learner engagement.

- Assessment & Feedback Systems – Building quizzes, mini-games, and surveys to assess knowledge retention and practical application.

RESEARCH, DESIGN, & TECHNICAL ISSUES

This SRI will address the following challenges:

Challenges include designing meaningful game mechanics that balance education and entertainment without trivializing cybersecurity risks. Ensuring accessibility across different demographics, measuring the effectiveness of behavioral change, and preventing gaming of the system (e.g., superficial participation) are critical concerns. Technical issues involve realistic scenario modeling, low-bandwidth optimization, and data privacy considerations for user data collected during gameplay.

MAJORS & AREAS OF INTEREST

This theme is identified in the following majors and/or with a background and interest in the areas listed below:

- Cybersecurity Awareness & Training – Educating diverse audiences on key cybersecurity practices and risk mitigation.
- Game Design & Development – Creating engaging interactive experiences that align with educational objectives.
- Human-Computer Interaction (HCI) – Studying how users interact with cybersecurity content and optimizing their learning journey.
- Educational Technology (EdTech) – Applying digital innovation to improve teaching and training outcomes.
- Behavioral Psychology in Cybersecurity – Understanding and influencing user behavior to promote secure practices.
- Web & Mobile App Development – Building scalable, accessible learning platforms for various devices.
- User Experience (UX) Research – Designing intuitive, motivational interfaces based on user feedback and testing.
- Data Analytics & Assessment – Measuring learning effectiveness through user performance and engagement analytics.

MENTOR CONTACT INFORMATION

Dr. A Karthik
Email: a.karthik@iare.ac.in

PARTNERS & SPONSORS

None

Remote Sensing in Agriculture, Crop Yield Prediction & Analytics

Dr. B Mallikarjuna, Professor, Dept. of IT - Faculty Mentor

GOALS

The main goal of this project is to develop comprehensive security and risk assessment frameworks tailored to the protection of critical infrastructure (CI) such as energy grids, water systems, healthcare facilities, transportation networks, and financial services. Given the vital role that critical infrastructure plays in societal stability, targeted cyberattacks or operational disruptions can have catastrophic consequences.

This project aims to create a dynamic framework that identifies, categorizes, and prioritizes risks based on threat likelihood, system vulnerabilities, and potential impact. The framework will incorporate threat modeling, vulnerability assessment, impact analysis, and resilience planning. Special emphasis will be placed on addressing emerging threats such as ransomware, nation-state cyberattacks, insider threats, and cascading failures across interconnected systems.

A further objective is to align the framework with established standards and guidelines such as the NIST Cybersecurity Framework (CSF), NIST SP 800-30 Risk Assessment Guidelines, ISO 27001/27005, and sector-specific regulations. The project also aims to support the development of automated risk scoring and visualization tools to enable proactive decision-making for infrastructure owners and cybersecurity teams.

METHODS & TECHNOLOGIES

- Risk Assessment Methodologies – Application of NIST SP 800-30, ISO 27005, FAIR model (Factor Analysis of Information Risk).
- Threat Modeling – Using STRIDE, PASTA, or attack tree modeling to identify and analyze potential threats.
- Vulnerability Assessment Tools – Deployment of Nessus, OpenVAS, or QualysGuard for system and network vulnerability scanning.
- Critical Infrastructure Simulation – Modeling interdependencies between CI sectors using simulation tools like MATSim or specialized CI simulators.
- Cyber Threat Intelligence (CTI) Integration – Incorporating threat feeds and advisories to update risk profiles dynamically.
- Security Control Frameworks – Mapping and recommending controls using NIST CSF, CIS Controls, or sector-specific standards (e.g., NERC CIP for energy).
- Visualization Platforms – Use of dashboards (e.g., Power BI, Kibana) to present risk scores, threat landscapes, and mitigation plans.
- Incident Impact Analysis – Performing tabletop exercises and scenario simulations to evaluate response readiness and resilience.

RESEARCH, DESIGN, & TECHNICAL ISSUES

Key challenges include accurately modeling complex interdependencies across CI systems, quantifying risk for low-frequency but high-impact events, and balancing security with operational efficiency. Data scarcity, incomplete asset inventories, and evolving threat vectors also complicate assessment efforts. The project must ensure that risk frameworks are adaptable to emerging technologies (like IoT and 5G) and future threat scenarios.

MAJORS & AREAS OF INTEREST

- Risk Management & Assessment – Identifying and quantifying cybersecurity and operational risks.
- Critical Infrastructure Protection (CIP) – Understanding and securing essential systems and services.
- Threat Modeling & Attack Simulation – Predicting potential attack paths and system vulnerabilities.
- Cybersecurity Governance & Compliance – Aligning with standards like NIST, ISO, and sector-specific regulations.
- Incident Response Planning – Designing resilient frameworks to manage and recover from attacks on critical infrastructure.
- Data Analytics for Risk Visualization – Building dynamic dashboards that communicate risk posture and security metrics.
- Cyber-Physical Systems Security – Addressing the convergence of operational technology (OT) and information technology (IT) in CI environments.
- Disaster Recovery & Business Continuity – Ensuring systems can rapidly recover from disruptions or attacks.

MENTOR CONTACT INFORMATION

Dr. B Mallikarjuna
Email: b.mallikarjuna@iare.ac.in

PARTNERS & SPONSORS

None