PORTFOLIO

(CURRICULUM VITAE)

// SEPTEMBER 2025 //

// AADITYA RENGARAJAN
BROOKLYN, NY

ABOUT ME* (1)

AADITYA IS A CYBERSECURITY ENGINEER AND AI RESEARCHER WITH CORE SKILLS IN OFFENSIVE SECURITY, SECURE WEB DEV, AND SCALABLE SEO-OPTIMIZED SYSTEMS.

HE'S PROFICIENT IN BUILDING AI-POWERED SECURITY TOOLS USING LLMs, DEEP LEARNING, DEEP RL, AND AGENTIC AI ARCHITECTURES. HIS WORK AT ISRO, INTEL & NSD BLENDS CAUSAL INFERENCE, PRIVACY-PRESERVING ML, AND CONSTRAINT-BASED AI MODELS TO TACKLE REAL-WORLD SECURITY CHALLENGES.

AS A TRAINER AND SPEAKER, HE'S EDUCATED 500+ STUDENTS AND DELIVERED TALKS AT OWASP, NULL, AND NATIONAL FORUMS.

FEATURED IN NYKAA'S SECURITY HALL OF FAME, HE FUSES ADVANCED AI REASONING WITH WEB SECURITY TO ENGINEER INSIGHTFUL, FUTURE-READY SYSTEMS.

SCHOOLS I'VE BEEN TO*

PSG COLLEGE OF TECHNOLOGY

BACHELOR OF ENGINEERING

COMPUTER SCIENCE & ENGINEERING

BUILDSPACE

*NOT A SCHOOL

taught me entrepreneurship. iykyk

https://x.com/_buildspace/status/1820332208831254892

NEW YORK UNIVERSITY

MASTER OF SCIENCE

CYBERSECURITY

(2)

DELIVERABLES *

CYBERSECURITY:	THREAT DETECTION SYSTEMS INSIDER THREAT ANALYSIS SECURITY AUTOMATION PIPELINES
AI/ML:	LLM BASED ASSISTANTS AGENTIC AI PRIVACY PRESERVING MACHINE LEARNING
WEB DEVELOPMENT:	FULL STACK WEB APPLICATIONS API DEVELOPMENT BACKEND ARCHITECTURE CUSTOM CMS & PORTALS
CYBERSECURITY TRAINING:	OFFENSIVE SECURITY BOOTCAMPS SECURE CODING WORKSHOPS GUEST LECTURES
RESEARCH & INNOVATION:	PRIVACY PRESERVING AI MITRE ATT&CK AND ATLAS INTEGRATIONS SECURITY USE CASE DESIGNING CONSTRAINT VIOLATION DETECTION SYSTEMS
CONSULTING & ADVISORY:	CYBER RISK ASSESSMENTS SECURITY ARCHITECTURE REVIEWS INCIDEDNT RESPONSE STRATEGY TOOLING RECOMMENDATIONS

(3)

PROJECTS

(4)

CLIENTS*

EQUATE
شركاء في النجاح
Partners in Success

ISAC

cyberange

READMENOW

tecko

PSG
In Nation Building since 1926

PSG HOSPITALS

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

VATSIM
AVIATE EDUCATE COMMUNICATE

VATMENA
VATSIM MIDDLE EAST & NORTH AFRICA

VATPRC
无线电礼仪

HACKATHONS*

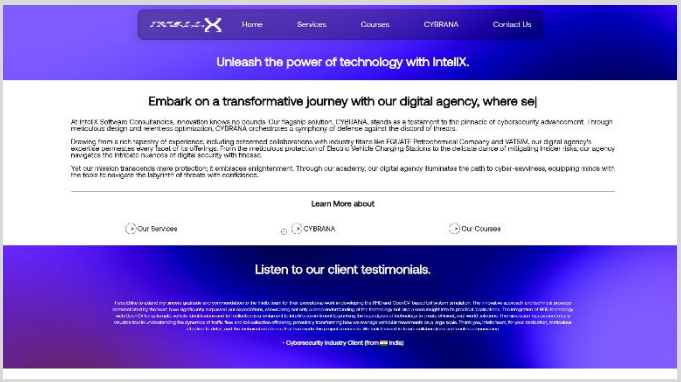
standard chartered

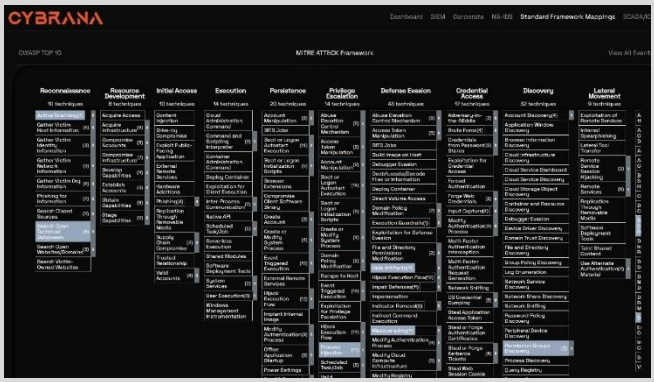
SOCIETE GENERALE

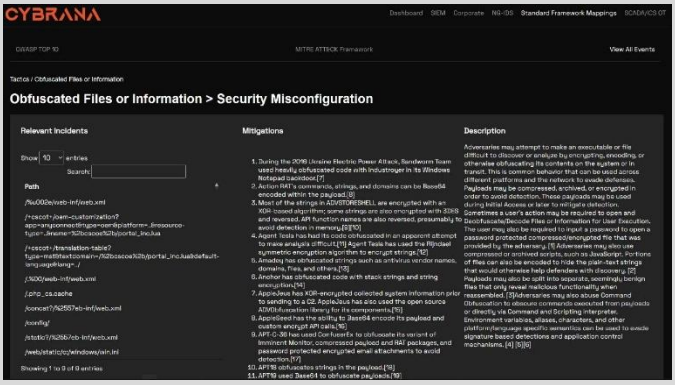
FinTech Festival India

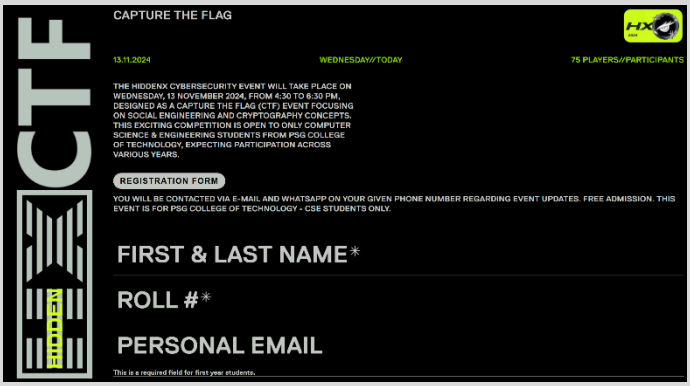
इसरो isro

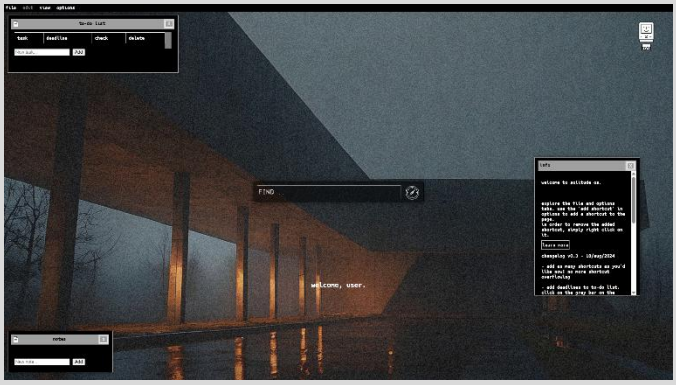
WEB DESIGN + DEV EXAMPLES





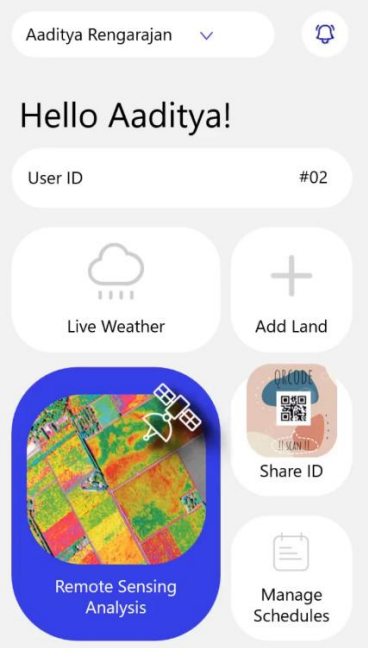


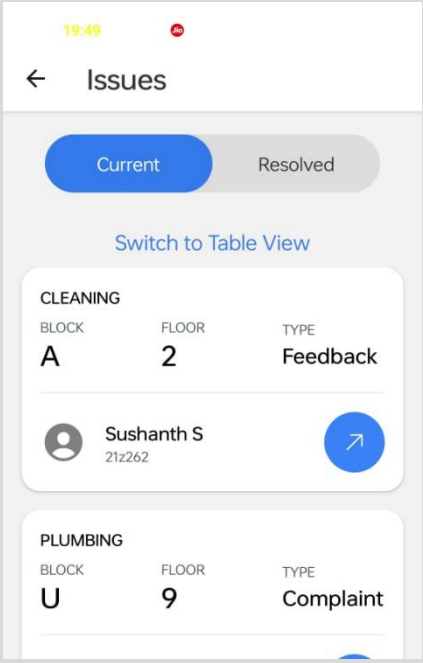




*these are functional web applications i've built over time.

MOBILE DESIGN EXAMPLES





*these are functional mobile applications i've built with people.

WORK EXPERIENCE

(5)

ORG	ROLE
intel	ai research and engg.
tecko	security software, startup research
Government of India National Remote Sensing Centre Indian Space Research Organisation ISO 9001:2015	security research and engg.
cyberange	security software engg.
EQUATE شركاء في النجاح Partners in Success	learning Infotech & s/w engg.
ISAC	dark web rsrch, cybersec.
NSD	penetration testing

RESEARCH PAPERS

(6)

Enhancing Cybersecurity Resilience with CYBRANA: A Cyber YARA/YAML-Based Resilience Firewall Solution Applied with Next-Gen AI

Abstract—The ever-increasing volume of server requests puts digital infrastructure at more risk of cyberattacks. This paper introduces CYBRANA, a cyberattack detection and mitigation system powered by AI. CYBRANA uses a Random Forest model to look into firewall and server logs for potential malicious threats. After analysis of flagged logs to extract request paths, CYBRANA then maps YAML rules to look for known attack pattern detection. Upon successful detection, CYBRANA classifies the attack type and severity (using CVSS scoring) by mapping it to the MITRE CAPEC framework®. This approach bridges the gap between existing cybersecurity frameworks and server log analysis, enabling a novel security pipeline. By automating threat detection and mitigation, CYBRANA enhances the security posture of digital infrastructure.

Index Terms—Firewall, NIDS, Log Analysis, Random Forest, MITRE, CVSS Scoring, SIEM, SOC

// with Dr. G. R. Karpagam

*IEEE International Conference on Computer Vision and Machine Intelligence (IEEE CVMI), 2024 at IIIT Allahabad, India

Enhancing the Resilience of Privacy-Preserving Machine Learning using Adversarial Techniques

Abstract—This paper introduces a novel approach to enhance privacy-preserving machine learning (PPML) by integrating adversarial techniques with Homomorphic Encryption (HE) and Differential Privacy (DP). Privacy-preserving machine learning (PPML) plays a key role in privacy protection. Current methods like homomorphic encryption (HE) and differential privacy (DP) aim to strike a balance between keeping data private and making sure models work well. This method embeds adversarial attacks within model optimization, strengthening resistance to privacy breaches while maintaining high model performance. Experimental results across various datasets achieving an accuracy of 89% in HE and DP demonstrate that this approach effectively balances privacy and utility, outperforming traditional PPML methods in safeguarding sensitive data without compromising model accuracy.

Index Terms—Adversarial Techniques, Differential Privacy, Homomorphic Encryption, Data Augmentation, Resilience, Privacy-Preserving Machine Learning

// with Lohith Senthilkumar, Amitha Lakshmi Raj, Arun US

*2024 IEEE International Conference on Distributed Systems, Computer Networks and Cybersecurity, Bangalore, India

Enhancing ADS-B using SAABE: Secure Authentication and Avionic Broadcast Encryption

Abstract—Automatic Dependent Surveillance-Broadcast (ADSB) systems are integral to modern aviation but face significant security challenges due to the inherent broadcast nature of the system. Unlike earlier and less targeted attacks, modern cyberattacks are more organized and sophisticated, often targeting specific groups, which leaves many users unaware of the vulnerable resources within the aero-cyberspace. The freedom on information access in the skies has led many malicious actors to expose, leak, spoof and anonymously attack this space. Therefore, creating methods to ensure confidentiality, integrity and availability for communication systems in the aerospace is a critical concern. ADS-B transmissions can be accessed through the simple web exploration by submitting query forms to retrieve the needed information, but it is not as simple in all cases. ADSB Transmissions can also be spoofed to jam the radar view of Air Traffic Controllers. This paper proposes a framework for an update on ADS-B communication techniques to ensure confidentiality and integrity.

Index Terms—ADS-B, Secure Communication, Cryptography, Aviation Cybersecurity, Cybersecurity, Blockchain, Information Security, AFTN, RSA, HMAC

// with Akshay Perison Davis, Navaneetha Krishnan KS, R Vishal, Subhasri Shreya S L

*2025 IEEE International Conference on Machine Learning & Cybernetics (ICMLC), Bali, Indonesia

FLARE: Federated Learning and Resilient Encryption for Firewalls

Abstract—Traditional firewalls rely on static rule-based mechanisms, where rules are manually defined and often written in specialized languages. While effective to a degree, these rules are inherently limited and can be easily bypassed by new and evolving types of malwares, leading to significant security vulnerabilities. To address these challenges, we propose FLARE: Federated Learning and Resilient Encryption, a novel machine learning-based firewall solution. FLARE dynamically analyzes past network connections to predict and determine the appropriate actions for incoming traffic, thereby adapting to emerging threats in real-time. Given the sensitive nature of firewall data, which often contains confidential information, the training of machine learning models poses significant privacy risks. FLARE mitigates these risks by incorporating federated learning, allowing the model to learn from decentralized data sources without requiring raw data to be shared. To further enhance privacy, we introduce an encryption layer that ensures the central model learns from encrypted weights, preventing exposure of sensitive information known to the local model. This combined approach not only improves the resilience of firewalls but also safeguards the confidentiality of the data used in training, offering a robust solution for modern cybersecurity challenges.

Keywords—Federated Learning, Next Generation Firewall, Random Forest, Firewall, MITRE

// with Lohith Senthilkumar

*7th International IEEE PUNECON 2024,
Defence Institute of Advanced Technology,
Pune, India

SHADOW: A framework for Systematic Heuristic Analysis and Detection of Observations on the Web

Abstract—The cyberspace contains vast amounts of information that are crucial for cybersecurity professionals to gather threat intelligence, prevent cyberattacks, and secure organizational networks. Unlike earlier and less targeted attacks, modern cyber-attacks are more organized and sophisticated, often targeting specific groups, which leaves many users unaware of the vulnerable resources within the cyberspace. The increasing freedom on information access in the deep and dark web has led many organizations to identify their data loose on these spaces. Therefore, creating methods to crawl and extract valuable information from the deep web is a critical concern. Some deep web content can be accessed through the surface web by submitting query forms to retrieve the needed information, but it is not as simple in all cases. This paper proposes a system of framework to identify these leaks and notify relevant parties on the same in-time.

Index Terms—Data Breach, Named Entity Recognition, Ranking, Cybersecurity, Snowball Sampling, Blockchain, Attack Tree, Web Scraping, Wayback Machine

// with Lohith Senthilkumar, Neelesh P, Akhil R

* IEEE International Conference on Artificial Intelligence, Metaverse, and Cybersecurity 2024, Rochester Institute of Technology, Dubai (UAE)

ASTRA: A Cyber-Threat Intelligence Framework for Advanced Security Threat Response and Analysis

Abstract—This paper introduces ASTRA (Advanced Security Threat Response and Analysis), a novel system designed to enhance cybersecurity operations. ASTRA connects to multiple STIX (Structured Threat Information Expression) threat feeds, offering a comprehensive dashboard that includes a lookup interface, a visualizer tool, and a log analysis tool to detect Indicators of Compromise (IOCs) from any log file. The challenge addressed by this paper lies in the limitations of current cybersecurity methods, which predominantly rely on manual signature development and static rules for threat detection and mitigation. Presently, cybersecurity strategies often struggle to keep pace with the dynamic nature of modern threats, leading to gaps in protection. ASTRA's novelty lies in its ability to dynamically analyze and respond to threats in real-time, significantly reducing the time and effort required to identify and mitigate cyber risks. The system's microservice architecture and private blockchain further enhances its adaptability, scalability, and security, making it an ideal solution for modern cybersecurity challenges.

*Submitted for Publication

Leveraging detection of Data Breaches by applying Snowball Sampling

Abstract—With the data being circulated and stored on the internet increasing, the number of data breaches occurring globally has seen a drastic rise and it is happening in an organized manner. This causes a serious threat to both individual and organizations. Though the organizations have a security team to monitor the breaches, the individuals are unaware that their data being breached is a serious issue. This paper addresses the above issue through detection using snowball sampling and preserving privacy using Blockchain technology. Efforts have been taken to validate this system through threat modeling by employing misuse case diagrams and attack trees.

Keywords— Data Breach, Snowball Sampling, Blockchain, Attack Tree, Web Scraping

// with Dr. G R Karpagam, Subhasri Shreya S L, Mithilesh, Santhoshi

*International Conference on High Performance and Intelligent Computing 2022, PSG College of Technology, Coimbatore, India

LOCKNET - Logs on Crypto Key Network

Abstract— LOCKNET - Logs on Crypto Key Network - Ensuring Transparency focuses on the topic of Network-Based Intrusion Detection Systems (NIDS). NIDS inspects traffic and detects any malicious network activity. It analyses user accounts, firewall logs, file integrity, database server logs, etc. The concept of blockchain can be used to improve a NIDS. To put it into simple words, blockchain revolves around linked lists. Each node or block of a linked list will store certain information. Blockchain also utilizes the concept of hashing for improved security. A specific encryption algorithm must be used to ensure that the blockchain system works well. The choice of which encryption algorithm will be used extensively depends on several factors. Three algorithms were analyzed. These include symmetric searchable encryption, asymmetric searchable encryption, and Triple DES algorithms. Three experiments were conducted to determine the best encryption algorithm to use.

Keywords— Intrusion Detection System, Encryption Technique, key, NIDS

// with Aswath Harish, Vaikunt Ramakrishnan,
Navaneetha Krishnan KS

*Submitted for Publication

SNAT: Secure Network Auditing in Transactions Logs

Abstract—Blockchain systems are essentially based on dis- tributed digital ledgers and are vulnerable to security and privacy risks. Thus, there is a need to employ encryption methods on these systems. Numerous factors have to be considered before determining which encryption algorithm can be employed. An analysis was conducted on three existing algorithms namely Homomorphic encryption, Identity-based encryption and Attribute-based encryption. The optimal encryption algorithm was found using a sequence of three experiments.

Keywords—Network-Based Intrusion Detection Systems (NIDS), inspect network traffic and detect any potentially harmful behavior. Combining Secure Network Auditing in Transactions Logs (SNAT) with NIDS will produce novel results.

// with Swetha M, Soorya Subramani

*Submitted for Publication

CONTACT ME!

EMAIL(S):	AADITYA.R@IEEE.ORG AADITYA.R@NYU.EDU
PHONE(S): (MESSAGE ME FOR IT)	(+91) ****** **430 (+965) **** ***55 (+1)********28
WEBSITE(S):	AADITYA.INTELLX.IN INTELLX.IN