PORTFOLIO

(CURRICULUM VITAE)

// DECEMBER 2025 //

// AADITYA RENGARAJAN
BROOKLYN, NEW YORK

ABOUT ME *

(1)

AADITYA IS A CYBERSECURITY ENGINEER AND AI RESEARCHER WITH CORE SKILLS IN OFFSEC, SECURE WEB DEV, AND SCALABLE SYSTEMS.

HE'S PROFICIENT IN BUILDING AI-POWERED SECURITY TOOLS OR SECURITY-FOCUSED AI USING 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, NULLCON, AND NATIONAL FORUMS.

HE ACTIVELY BUILDS OPEN-SOURCE SOFTWARE, LEADS SECURITY COMMUNITIES AS PRESIDENT OF THE NYU CYBERSECURITY CLUB, AND CONTRIBUTES TO OFFENSIVE SECURITY RESEARCH THROUGH THE OSIRIS LAB. HIS INTERESTS CENTER ON BUILDING RESILIENT, SCALABLE, AND REAL-WORLD SECURITY AND AI SYSTEMS.

SCHOOLS I'VE BEEN TO *

NYU

NEW YORK UNIVERSITY, TANDON SCHOOL OF ENGINEERING
MASTER OF SCIENCE
CYBERSECURITY

APPLICATION SECURITY ▪ SOFTWARE SUPPLY CHAIN SECURITY ▪ POST QUANTUM CRYPTOGRAPHY ▪ NETWORK SECURITY ▪ INFORMATION SYSTEMS SECURITY ENGINEERING & MANAGEMENT ▪ PRIVACY IN THE ELECTRONICS SOCIETY ▪ PENETRATION TESTING & VULNERABILITY ANALYSIS ···

4.0/4.0 GPA (*^ ‿ *)

BUILDSPACE
* NOT A SCHOOL

buildspace

taught me entrepreneurship. iykyk

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

KNOWLEDGE AND SERVICE
1951

PSG COLLEGE OF TECHNOLOGY
BACHELOR OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING

CHEMISTRY ▪ APPLIED PHYSICS ▪ DIGITAL ELECTRONICS ▪ MICROPROCESSORS ▪ CALCULUS ▪ LINEAR ALGEBRA TRANSFORMS ▪ DISCRETE MATH ▪ PROBABILITY ▪ C PROGRAMMING ▪ PYTHON ▪ OOP ▪ DSA ▪ ADVANCED DS COMPUTER ARCHITECTURE ▪ THEORY OF COMPUTATION ▪ OPERATING SYSTEMS ▪ DBMS ▪ COMPUTER NETWORKS ▪ WIRELESS NETWORKS ▪ DISTRIBUTED SYSTEMS ▪ CLOUD COMPUTING ▪ OPEN SOURCE SYSTEMS SOFTWARE ENGINEERING ▪ DESIGN THINKING ▪ UI DESIGN ▪ WEB TECHNOLOGY ▪ ARTIFICIAL INTELLIGENCE MACHINE LEARNING ▪ CRYPTOGRAPHY ▪ BLOCKCHAIN

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, BACKENDS & SYSTEM DESIGN 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:	SECURITY ARCHITECTURE REVIEWS INCIDENT RESPONSE STRATEGY TOOLING RECOMMENDATIONS

PROJECTS

(4)

CLIENTS *

EQUATE
شركاء في النجاح
Partners in Success

ISAC

cyberange

RMN

tecko

PSG
In Nation Building since 1926

VATSIM
AVIATE EDUCATE COMMUNICATE

VATMENA
VATSIM MIDDLE EAST
& NORTH AFRICA

PSG
HOSPITALS

INSTITUTION'S
INNOVATION
COUNCIL
(Ministry of HRD Initiative)

VATPRC

HACKATHONS *

standard
chartered

Qualcomm

Google

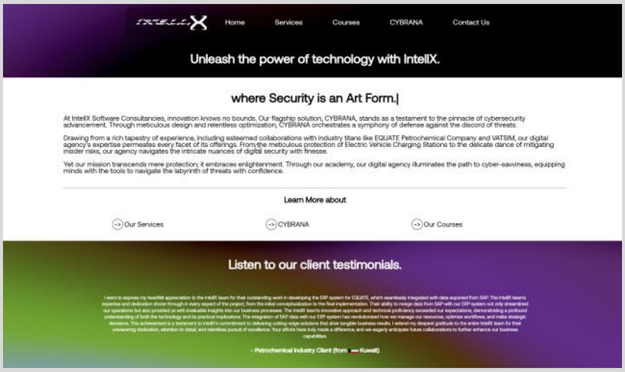
SOCIETE
GENERALE

FinTech
Festival India

इसरो isro

WEB DESIGN + DEV EXAMPLES

SECURITY × ENGINEERING × DESIGN



Unleash the power of technology with IntellX.

where Security is an Art Form.|

At IntellX Software Consultancies, innovation knows no bounds. Our flagship solution, CYBRANA, stands as a testament to the pinnacle of cybersecurity advancement. Through meticulous design and relentless optimization, CYBRANA orchestrates a symphony of defense against the discord of threats.

Drawing from a rich tapestry of experience, including esteemed collaborations with industry titans like EQUATE Petrochemical Company and VATSIM, our digital agency's expertise permeates every facet of its offerings. From the meticulous protection of Electric Vehicle Charging Stations to the delicate dance of mitigating insider risks, our agency navigates the intricate nuances of digital security with finesse.

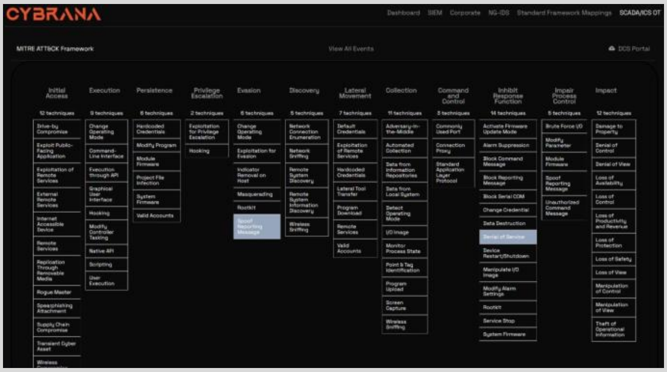
Yet our mission transcends mere protection; it embraces enlightenment. Through our academy, our digital agency illuminates the path to cyber-savviness, equipping minds with the tools to navigate the labyrinth of threats with confidence.

Learn More about

Listen to our client testimonials.

I want to express my heartfelt appreciation to the IntellX team for their outstanding work in developing the ERP system for EQUATE, which seamlessly integrated with data exported from SAP. The IntellX team's expertise and dedication shone through in every aspect of the project, from the initial conceptualization to the final implementation. Their ability to merge data from SAP with our ERP system not only streamlined our operations but also provided us with invaluable insights into our business processes. The IntellX team's innovative approach and technical proficiency exceeded our expectations, demonstrating a profound understanding of both the technology and its practical implications. The integration of SAP data with our ERP system has revolutionized how we manage our resources, optimize workflows, and make strategic decisions. This achievement is a testament to IntellX's commitment to delivering cutting-edge solutions that drive tangible business results. I extend my deepest gratitude to the entire IntellX team for their unwavering dedication, attention to detail, and relentless pursuit of excellence. Your efforts have truly made a difference, and we eagerly anticipate future collaborations to further enhance our business capabilities.

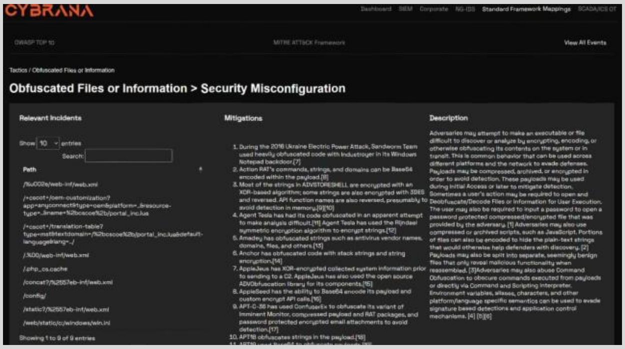
- Petrochemical Industry Client (from Kuwait)



MITRE ATT&CK Framework

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message	
Replication Through Removable Media	Native API				
Rogue Master	Scripting				
Spearphishing Attachment	User Execution				
Supply Chain Compromise					
Transient Cyber Asset					
Wireless Compromise					

Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
	Point & Tag Identification		Denial of Service		Loss of Safety
	Program Upload		Device Restart/Shutdown		Loss of View
	Screen Capture		Manipulate I/O Image		Manipulation of Control
	Wireless Sniffing		Modify Alarm Settings		Manipulation of View
			Rootkit		Theft of Operational Information
			Service Stop		
			System Firmware		



Tactics / Obfuscated Files or Information

Obfuscated Files or Information > Security Misconfiguration

Relevant Incidents

Show 10 entries

Search:

Path
/%u002e/web-inf/web.xml
/+cscot+/oem-customization?app=anyconnect&type=oem&platform=..&resource-type=..&name=%2bcscoe%2b/portal_inc.lua
/+cscot+/translation-table?type=mst&textdomain=/%2bcscoe%2b/portal_inc.lua&default-language&lang=../
/.%00/web-inf/web.xml
/.php_cs.cache
/concat?/%2557eb-inf/web.xml
/config/
/static?/%2557eb-inf/web.xml
/web/static/c:/windows/win.ini

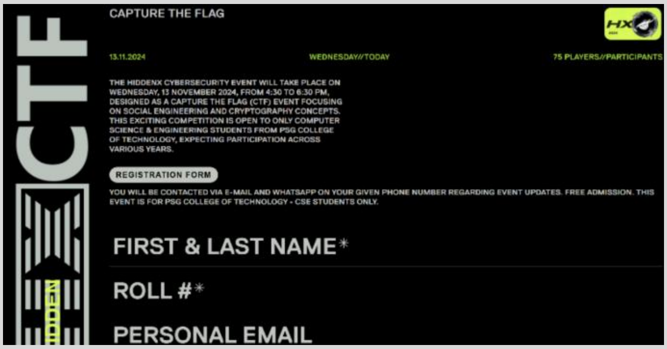
Showing 1 to 9 of 9 entries

Mitigations

1. During the 2016 Ukraine Electric Power Attack, Sandworm Team used heavily obfuscated code with Industroyer in its Windows Notepad backdoor.[7]
2. Action RAT's commands, strings, and domains can be Base64 encoded within the payload.[8]
3. Most of the strings in ADVSTORESHELL are encrypted with an XOR-based algorithm; some strings are also encrypted with 3DES and reversed. API function names are also reversed, presumably to avoid detection in memory.[9][10]
4. Agent Tesla has had its code obfuscated in an apparent attempt to make analysis difficult.[11] Agent Tesla has used the Rijndael symmetric encryption algorithm to encrypt strings.[12]
5. Amadey has obfuscated strings such as antivirus vendor names, domains, files, and others.[13]
6. Anchor has obfuscated code with stack strings and string encryption.[14]
7. AppleJeus has XOR-encrypted collected system information prior to sending to a C2. AppleJeus has also used the open source ADVObfuscation library for its components.[15]
8. AppleSeed has the ability to Base64 encode its payload and custom encrypt API calls.[16]
9. APT-C-36 has used ConfuserEx to obfuscate its variant of Imminent Monitor, compressed payload and RAT packages, and password protected encrypted email attachments to avoid detection.[17]
10. APT18 obfuscates strings in the payload.[18]

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and Deobfuscate/Decode Files or Information for User Execution. The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. [1] Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. [2] Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. [3]Adversaries may also abuse Command Obfuscation to obscure commands executed from payloads or directly via Command and Scripting Interpreter. Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. [4] [5][6]



CAPTURE THE FLAG

13.11.2024 WEDNESDAY//TODAY 75 PLAYERS//PARTICIPANTS

THE HIDDENX CYBERSECURITY EVENT WILL TAKE PLACE ON WEDNESDAY, 13 NOVEMBER 2024, FROM 4:30 TO 6:30 PM, DESIGNED AS A CAPTURE THE FLAG (CTF) EVENT FOCUSING ON SOCIAL ENGINEERING AND CRYPTOGRAPHY CONCEPTS. THIS EXCITING COMPETITION IS OPEN TO ONLY COMPUTER SCIENCE & ENGINEERING STUDENTS FROM PSG COLLEGE OF TECHNOLOGY, EXPECTING PARTICIPATION ACROSS VARIOUS YEARS.

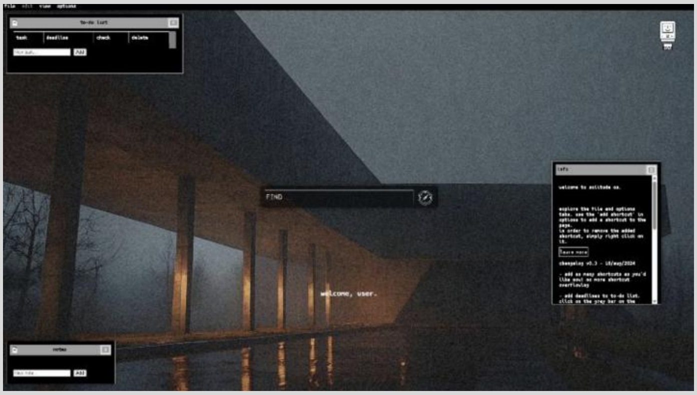
REGISTRATION FORM

YOU WILL BE CONTACTED VIA E-MAIL AND WHATSAPP ON YOUR GIVEN PHONE NUMBER REGARDING EVENT UPDATES. FREE ADMISSION. THIS EVENT IS FOR PSG COLLEGE OF TECHNOLOGY - CSE STUDENTS ONLY.

FIRST & LAST NAME*

ROLL #*

PERSONAL EMAIL



info

welcome to solitude os.

explore the file and options tabs. use the 'add shortcut' in options to add a shortcut to the page.
in order to remove the added shortcut, simply right click on it.

learn more

changelog v0.3 - 18/aug/2024

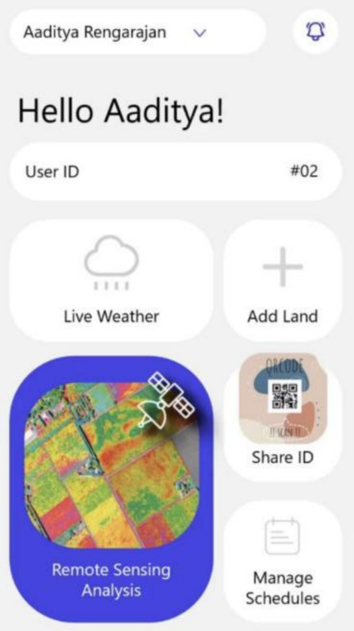
- add as many shortcuts as you'd like now! no more shortcut overflowing

- add deadlines to to-do list. click on the grey bar on the

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

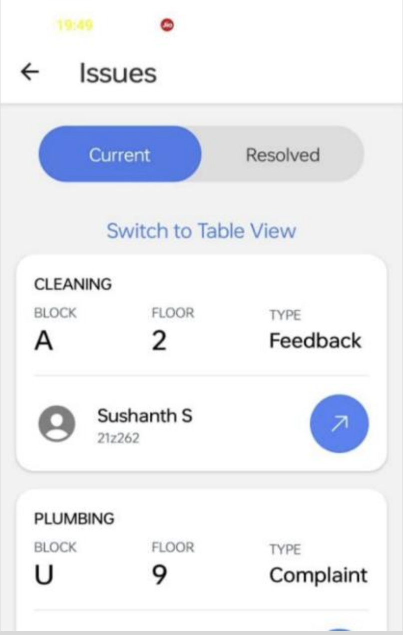
MOBILE DESIGN EXAMPLES

SECURITY × ENGINEERING × DESIGN



Hello Aaditya!

User ID #02



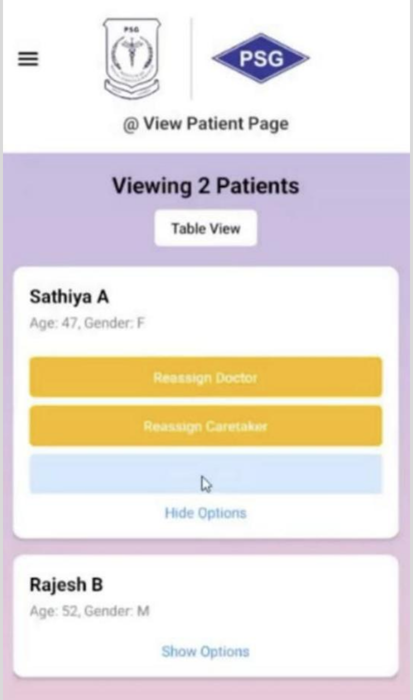
CLEANING

BLOCK	FLOOR	TYPE
A	2	Feedback

Sushanth S
21z262

PLUMBING

BLOCK	FLOOR	TYPE
U	9	Complaint



Viewing 2 Patients

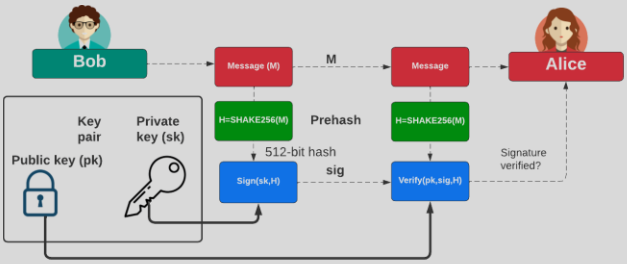
Sathiya A
Age: 47, Gender: F

Rajesh B
Age: 52, Gender: M

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

SECURITY DESIGN EXAMPLES

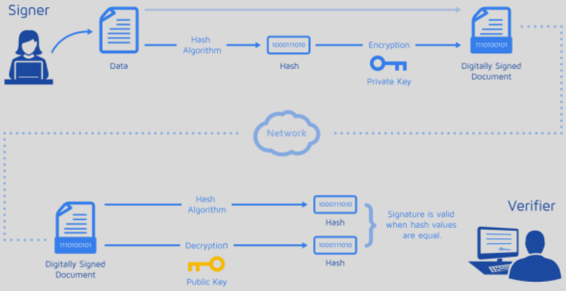
SECURITY × ENGINEERING × DESIGN

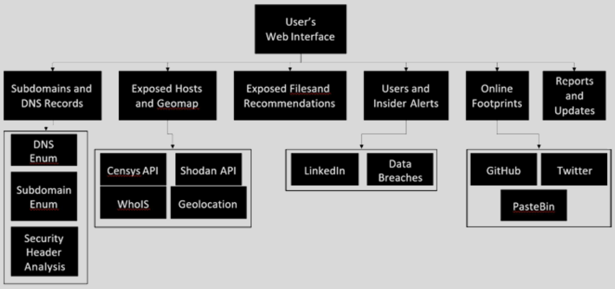


HAWK

a python re-implementation of a post quantum crypto framework (pedagogy)

arbitrary-order secure multi-sign algorithm for document signing





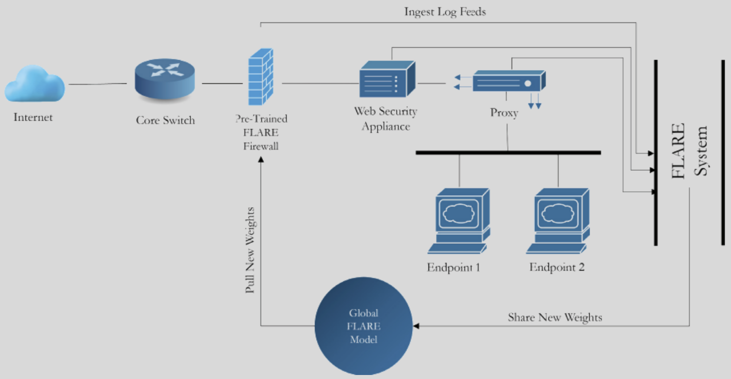
SentinelEye

public visibility security framework for organizations

* these are functional security software i've built + research work i've published over time

SECURITY DESIGN EXAMPLES

SECURITY × ENGINEERING × DESIGN

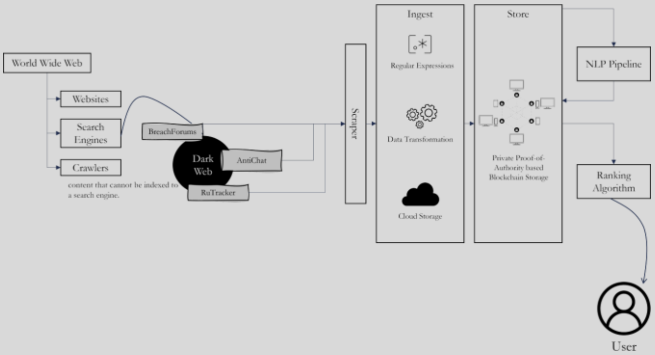


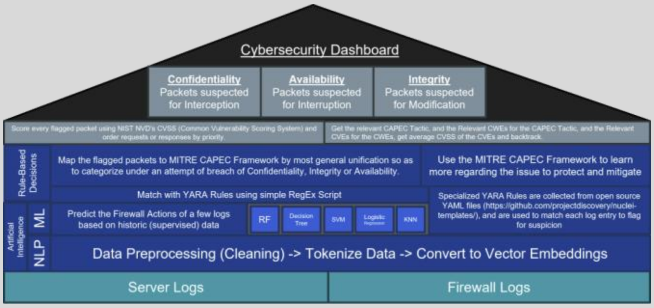
FLARE

a federated learning firewall architecture

SHADOW

an ML-based dark web PII-leak detection system





Score every flagged packet using NIST NVD's CVSS (Common Vulnerability Scoring System) and order requests or responses by priority.

Get the relevant CAPEC Tactic, and the Relevant CWEs for the CAPEC Tactic, and the Relevant CVEs for the CWEs, get average CVSS of the CVEs and backtrack.

Map the flagged packets to MITRE CAPEC Framework by most general unification so as to categorize under an attempt of breach of Confidentiality, Integrity or Availability.

Use the MITRE CAPEC Framework to learn more regarding the issue to protect and mitigate

Match with YARA Rules using simple RegEx Script

Specialized YARA Rules are collected from open source YAML files (https://github.com/projectdiscovery/nuclei-templates/), and are used to match each log entry to flag for suspicion

Predict the Firewall Actions of a few logs based on historic (supervised) data

Data Preprocessing (Cleaning) -> Tokenize Data -> Convert to Vector Embeddings

CYBRANA

a machine-learning based firewall

* these are functional security software i've built + research work i've published over time

WORK EXPERIENCE

(5)

ORG	ROLE
intel®	ai research and engineering
tecko	security software, startup research
इसरो isro nrsc Government of India National Remote Sensing Centre Indian Space Research Organisation ISO 9001:2015	security research and engineering
cyberange	security software engineering
EQUATE شـركاء في النجاح Partners in Success	learning infotech and software engineering
ISAC	dark web research, cybersecurity
NATIONAL SECURITY DATABASE NSD	penetration testing

RESEARCH PAPERS

(6)

Prompt-Aware MCP Security: Using ShardGuard To Compartmentalize LLMs for Safer MCP Actions

Abstract—Large Language Models (LLMs) are powerful in part due to the wide array of prompts they can successfully handle. While many efforts have been made to improve MCP security, a prompt's context is an essential (and missing) aspect of MCP security. This work demonstrates that it is not only necessary to consider prompt- context, but it is also possible to do so in a secure and automated manner. Our architecture shows that an LLM can be an effective tool at devising a compartmentalized, prompt-specific, least-privilege decomposition for various complex prompts. We demonstrate that this technique provides best-effort, least-privilege security which reduces the unnecessary MCP server tools available to an LLM. It does this while handling prompts an unprotected LLM could handle. This happens without substantially increasing the LLM costs. Furthermore, our design is backwards compatible with existing MCP servers / tools, LLMs, and frameworks. Our prototype, ShardGuard, is freely available with an Apache 2.0 license.

// with a team under Professor Justin Cappos at the Secure Systems Laboratory (SSL) at New York University's Tandon School of Engineering

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 Allahabad, 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 Padmanabh and Akhil Ramalingam

* International Conference on Artificial Intelligence, Metaverse and Cybersecurity (ICAMAC), 2024 at Dubai, UAE

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 malware, 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.

Index Terms—Training , Adaptation models , Data privacy , Analytical models , Firewalls (computing) , Federated learning , Predictive models , Data models , Encryption , Random forests

// with Lohith Senthilkumar

* IEEE Pune Section International Conference (PuneCon), 2024 at Pune, 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—Training , Resistance , Differential privacy , Accuracy , Computational modeling , Machine learning , Data augmentation , Data models , Homomorphic encryption , Resilience

// with Lohith Senthilkumar, Amitha Lakshmi Raj and Arun U S

* International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC), 2024 at Bengaluru, India

Estimation of Warfarin Dosage using a Specialized XGBoost-based Pharmacogenomic Machine Learning Model and Evaluation using XAI

Abstract—Warfarin is a commonly used anticoagulant for which dosing needs to be individually optimized highly tightly to match against the potential for bleeding and thrombotic side effects. We introduce herein in this article a machine learning system that makes use of clinical, genetic, and demographic information to predict warfarin patient-specific dosing. Our method is becoming more sophisticated with various iterations starting from a baseline model, then an optimal XGBoost model incorporating polynomial feature expansions, and finally ending with an optimized gradient boosting implementation coded from scratch. Model performance is evaluated on R2 metrics complemented with explainability tests using SHAP and LIME, hence achieving accuracy and interpretability to clinical decision-making.

Index Terms—Measurement , Machine learning algorithms , Explainable AI , Computational modeling , Predictive models , Boosting , Genetics , Polynomials , Iterative methods , Hemorrhaging

// with Akshay Perison Davis, Navaneetha Krishnan K S, R Vishal, Subhasri Shreya S L and Jayashree L S

* International Conference on Machine Learning and Cybernetics (ICMLC), 2025 at Bali, Indonesia

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.

***System deployed at National Remote Sensing Centre (NRSC, ISRO), 2024 at Hyderabad, India**

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 possess 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 modelling by employing misuse case diagrams and attack trees.

Index Terms—Data Breach, Snowball Sampling, Blockchain, Attack Tree, Web Scraping

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

* International Conference on High Performance and Intelligent Computing (ICHPIC), 2022 at Coimbatore, India

COMMUNITY INVOLVEMENT *

Founder, The Eye - Student-Run Society for Cybersecurity at PSG College of Technology

President, Cybersecurity Club at New York University, Tandon School of Engineering

CSC

Board Member, the Offensive Security, Incident Response, Internet Security Lab (the OSIRIS Lab), NYU

Speaker and Member, Open Web Application Security Project (OWASP)

OWASP
Open Web Application
Security Project

IEEE
Advancing Technology
for Humanity

Student Member, IEEE

(7)

CONTACT ME!

EMAIL(S):	AADITYA.R@IEEE.ORG AADITYA.R@NYU.EDU ***********A@GMAIL.COM
PHONE(S):	(+91) ******* 430 (+1) ******** 28
WEBSITE(S):	AADITYA.INTELLX.IN

* SEMI-REDACTED PERSONAL INFORMATION IS FOR VERIFICATION THROUGH # OF CHARACTERS.

(8)