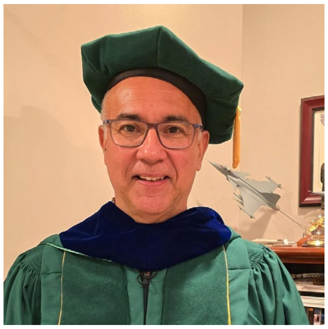
GEORGE MASON UNIVERSITY

# Senior Design Projects

*2024-2025*

## Cyber Security Engineering (CYSE) 492/493

**April 2025**



April, 2025

The CYSE 492/493 Senior Advanced Design Project or “capstone” is a year-long endeavor with challenging real-world projects for our CYSE students. We are very proud of their effort and grateful for the sponsors, subject matter experts, mentors and faculty who support this rewarding experience.

These projects are the culmination of the final experience for our Bachelor of Science in Cyber Security Engineering (BS CYSE) graduating class. Students work with a sponsoring organization using the skills they have sharpened during their curriculum.

Our industry partners have provided a multitude of inspiring and useful projects that have challenged our students to solve open-ended technical problems with their significant contribution and guided by our faculty mentors and subject matter experts. We are pleased to acknowledge how fortunate we are to have sponsorships from AVINT LLC, CGI, Criminal Investigations and Network Analysis Center and Department of Homeland Security, Department of Defense and US Army through Capstone Marketplace, Federal Communications Commission, MITRE, Noblis, Inc, and Faculties from George Mason University.

Each organization supplied not only the project but guidance throughout the year. They provided both contacts and subject matter experts for the projects. We would like to thank each of them. The success of the projects was very much driven by their expertise and commitment to our students.

We would also like to acknowledge Professor Mingkui Wei for his efforts as the instructor for the Senior Advanced Design Project. He has brought expertise and rigor to the projects and has facilitated a rich and lasting experience for our students. Also, thanks to our university faculty, Alexandre Barreto, Armin Tadayon, Catherine Jones, Christine Alonzo Yee, Henry Coffman, Jair Ferrari, and Mohamed Morsy. They have provided support and insight in very technical projects.

The Senior Design contributes to a graduating class that will make an impact on our society. Many already have employment in commercial and government jobs. Others are continuing their education through the pursuit of a Master of Science degree, including our rapidly growing MS in Cyber Security Engineering. All of our students are pioneers in a difficult but rewarding field.

We are proud of our students and want to congratulate them for their dedicated efforts and all the hard work that it has taken to reach this milestone. Thanks again to our industry sponsors, subject matter experts, mentors and faculty for their tremendous support in this endeavor.

**Paulo Costa, Ph.D.**

Chair and Professor,
Department of Cyber Security Engineering
Director,
Center of Excellence in C5I
Professor,
Systems Engineering and Operations Research Department

**Peggy Brouse, Ph.D.**

Associate Chair and Professor,
Cyber Security Engineering Department
Professor,
Systems Engineering and Operations Research Department

Thank you for being part of our industry-sponsored Senior Design course!

After two challenging semesters, we are celebrating the achievements of 117 students who worked on a diverse collection of 22 academic, government, and industry sponsored cybersecurity projects.

The goal of Senior Design is to provide students with “real-life” working experience during their senior year. Student teams work with sponsor organizations that provide customers and subject matter experts to drive projects. Each project is managed exactly as if the students were just hired by an organization and placed on an engineering team. Students are responsible for making proposals and implementing their proposed designs.

Throughout the two semesters, they are guided in technical areas by the subject matter experts and mentored by CYSE faculties in a host of professional and business skills, such as project management, communication, teamwork, ethics, professionalism, and business metrics. By working in a team, they develop leadership skills and learn to function as effective teams as they manage requirements and schedules. Student teams are responsible for managing customer relationships and addressing unforeseen challenges that arise on all projects.

This program is only possible with the devotion of our sponsor organizations who provide subject matter experts to interact with and guide the students. Thank you for engaging with our program and helping to educate students who will secure our cyber infrastructure now and in the future.

The instructor team of Alexandre Barreto, Armin Tadayon, Catherine Jones, Christine Alonzo Yee, Henry Coffman, Jair Ferrari, and Mohamed Morsy brings a wealth of experience that provides students with a wonderful source of guidance and engineering expertise.

Great thanks to Dr. Paulo Costa, the Department Chair, and Dr. Peggy Brouse, the Associate Chair, for their great support through the two semesters, making it a pleasant and enjoyable experience.

Finally, we want to thank our amazing students, who were brave enough to try something new. You stepped out of your comfort zones and worked hard on challenging projects. We wish you all the best as you pursue your engineering aspirations.

Sincerely,

Mingkui Wei

**Mingkui Wei, Ph.D.**

Lead Instructor, Cyber Security Senior Design

GEORGE MASON UNIVERSITY

# Sponsors

We greatly appreciate their dedicated support

Avint LLC.

CGI

noblis®

MITRE

Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

University of Mary Washington

CAPSTONE marketplace

SINE PARI

UNITED STATES FEDERAL COMMUNICATIONS COMMISSION

College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University®

U.S. DEPARTMENT OF HOMELAND SECURITY

# Project Leadership

This class is only possible because of the commitment, dedication, and spirit of the following customers, subject matter experts, and faculty mentors. Thank you!

| Project title | Sponsor | Customer Contact | Subject Matter Expert | Mentor |
|---|---|---|---|---|
| Unified Common Control Framework (UCCF) using NLP/ML based approach | AVINT LLC | Marcie Nagel | Elliot Alderson | Catherine Jones |
| Blockchain-IoT Integration for University Lab Equipment Tracking: Hardware Component | CGI | Alan Watson | Shadman Hossain | Alexandre Barreto |
| Blockchain-IoT Integration for University Lab Equipment Tracking; Software Component | CGI | Alan Watson | Shadman Hossain | Alexandre Barreto |
| Research and Implementation of Integration of the Network and Application and Workload Pillars of the Zero Trust Model to Provide Enhanced Visibility/Analytics and Automation. | CGI | Chris Lavergne | David Crawford | Christine Alonzo Yee |
| Generative AI in Cybersecurity: Offensive and Defensive Strategies for Accessibility Threats | CGI | Josh Sonnier | Josh Sonnier | Armin Tadayon |
| AI Based Role Authorization Prototype | CGI | Christopher Smith | Elliot Alderson | Christine Alonzo Yee |

# Project Leadership

This class is only possible because of the commitment, dedication, and spirit of the following customers, subject matter experts, and faculty mentors. Thank you!

| Project title | Sponsor | Customer Contact | Subject Matter Expert | Mentor |
|---|---|---|---|---|
| Fingerprinting 5G Radios for Security Application | CYSE GMU | Md Tanvir Arafin | Md Tanvir Arafin | Jair Ferrari |
| AI-Driven Threat Detection and Response System | CYSE GMU | Zhengdao Wang | Zhengdao Wang | Alexandre Barreto |
| Ghidra-LLM: Large Language Models for Static Reverse Engineering | CYSE GMU | Md Tanvir Arafin | Md Tanvir Arafin | Henry Coffman |
| LOCO: Secure Localization for Multi-Robot Systems in Dynamic Environments | CYSE GMU | Md Tanvir Arafin | Md Tanvir Arafin | Jair Ferrari |
| Industrial Automation and Control Systems Cyber Security Lab – IACS2 Lab | CYSE GMU | Ferrari, Jair | Ferrari, Jair | Alexandre Barreto |
| Enhancing Voice-AI Systems through Adversarial Defense and Voice Verification | CYSE GMU | Zhuangdi Zhu | Zhuangdi Zhu | Jair Ferrari |

# Project Leadership

This class is only possible because of the commitment, dedication, and spirit of the following customers, subject matter experts, and faculty mentors. Thank you!

| Project title | Sponsor | Customer Contact | Subject Matter Expert | Mentor |
|---|---|---|---|---|
| Drone Control Security Research | CYSE GMU | Mohamed Morsy | Mohamed Morsy | Mohamed Morsy |
| An Overview of Indoor Drone Obstacle Avoidance Research and Simplified Practical application Based on Visual Device Technology | CYSE GMU | Mohamed Morsy | Mohamed Morsy | Mohamed Morsy |
| Covert Comms to Working Dogs | Department of Defense | William Shepherd | William Shepherd | Henry Coffman |
| Detecting activity in confusing visual background | Department of Defense | William Shepherd | William Shepherd | Armin Tadayon |
| Logo Geolocation Project | Department of Homeland Security | Stephen Reuther | Jonathan Jerez | Armin Tadayon |
| Artificial Intelligence Applied to Cybersecurity Policy | Federal Communications Commission | Jeffery Goldthorp | Jeffery Goldthorp | Mohamed Morsy |

# Project Leadership

This class is only possible because of the commitment, dedication, and spirit of the following customers, subject matter experts, and faculty mentors. Thank you!

| Project title | Sponsor | Customer Contact | Subject Matter Expert | Mentor |
|---|---|---|---|---|
| Artificial Intelligence Safety – Team Alpha | MITRE | Rock Sabetto | Devesh Agarwal<br>Sruthi Chavali<br>Maxwell Dueltgen | Catherine Jones |
| Software Security During the Rise of AI – Team Zulu | MITRE | Rock Sabetto | Sujay Kandwal<br>Joseph Walter | Christine Alonzo Yee |
| The Design of a Framework for Synthetic PCAP Data Generation and Network Simulation | Noblis | Dayton Jung | Eric Epstein | Henry Coffman |
| The Design of a Comparative Analysis System for RAG Pipelines vs. Large Context Window LLMs | Noblis | Tamrin Swann | Tracey Raynourn | Catherine Jones |

# Project Teams

GEORGE MASON UNIVERSITY

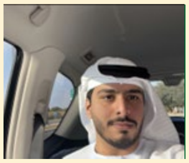
# Unified Common Control Framework (UCCF) Using NLP/ML Based Approach

Sadi Jafrey

Nikita Cheban

Dinh Tran

Anisha Suri



Khalaf Almheiri

SMEs: Suresh Subbaratinam

## CHALLENGE

This project involves Python tools like scikit and NumPy, usage of annotation tools including prodigy, and spaCy techniques to consolidate all the information from frameworks including ISO27001, NIST 800-53r5, HIPAA, NIST CSF, and PCI-DSS. The project also called for development of some custom tools based on predefined spaCy functionalities, like employment of soft-cosine similarity and Levinstein distance. It's a rigorous process of teaching a language model to visually detect cybersecurity terminologies and produce a unified common control framework or UCCF.

## Sadi Jafrey

Herndon, VA.

**Aspiration:** I'd like to learn more about ai in cybersecurity including lattice-based cryptography and key management.

**Class Comment:** This project gave me the opportunity to learn new tools, make professional connections, and experience just how fast-paced and straightforward industry work can be. Looking forward to working on similar projects or even projects in other areas.

## Dinh Tran

Falls Church, VA.

**Aspiration:** I aspire to be a Technical Support Specialist, leveraging my Security+ knowledge and troubleshooting skills to advance into cybersecurity roles.

**Class Comment:** This project taught me to develop NLP models that automate security control classification. I gained skills in training models and visualizing compliance relationships - valuable for addressing complex regulatory requirements.

## Khalaf Almheiri

Fairfax, VA.

**Aspiration:** I aim to strengthen my cybersecurity skills by applying machine learning and NLP to automate and enhance compliance processes.

**Class Comment:** This project provided valuable hands-on experience in annotating regulatory controls using tools like Prodigy and spaCy. It strengthened my understanding of how NLP and ML can be effectively applied to streamline cybersecurity compliance and contributed to my growth as a future cybersecurity professional.

## Nikita Cheban

Fairfax, VA.

**Aspiration:** I aspire to deepen my knowledge and enhance my skills in cybersecurity as I work toward becoming a Cybersecurity Engineer.

**Class Comment:** This project not only provided me with real-world cybersecurity experience using various tools, but it also broadened my perspective on AI in cybersecurity and how it is transforming the industry for the better.

## Anisha Suri

Chantilly, VA.

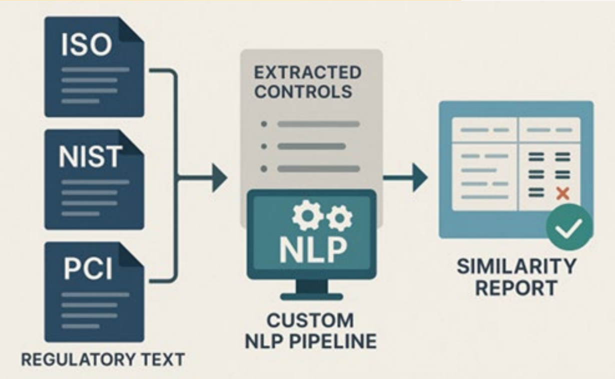
**Aspiration:** I aspire to keep growing and expanding my knowledge in protecting digital infrastructure and start working as an Information Systems Security Engineer.

**Class Comment:** This project opened many doors for me to grow and learn, whether it be familiarizing myself with different tools, learning the importance of NLP/ML, and even getting a glimpse of the professional setting that I will be soon entering.

Project Sponsor: Avint LLC

Avint LLC.

# Unified Common Control Framework (UCCF) Using NLP/ML Based Approach



In today's cybersecurity landscape, organizations are burdened with overlapping and ever-evolving regulatory frameworks such as NIST 800-53r5, NIST CSF, ISO/IEC 27001, HIPAA, and PCI-DSS. Each framework requires a tailored compliance effort, which becomes inefficient, error-prone, and expensive when approached separately. The purpose of this project is to design a Unified Common Control Framework (UCCF) that consolidates these varied requirements into a single structure. By leveraging Natural Language Processing (NLP) and Machine Learning (ML), the project aims to automate the mapping of similar controls across frameworks, enabling organizations to test once and comply with many—significantly reducing the burden of compliance while enhancing accuracy and adaptability.

Our project analyzes regulatory texts from major compliance standards to identify overlapping control requirements. By feeding manually extracted control descriptions into a custom NLP pipeline, the system can semantically compare controls and map them to unified representations. The output is a structured similarity report that suggests which controls from different standards are functionally equivalent. This approach helps organizations reduce redundancy, streamline audits, and improve regulatory alignment.

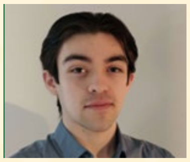
Our project follows a step-by-step process that combines NLP/ML to simplify compliance work. It starts by manually pulling control requirements from different frameworks and formatting them in a consistent way using JSONL files. Our team trained a custom language model with spaCy, tailored specifically for this domain. Using that model, the system then compares the control descriptions using soft cosine similarity—which helps capture the meaning behind the words, not just their appearance. These comparisons reveal which controls are similar across frameworks, and the results are sorted and saved in an Excel file.

Project Sponsor: Avint LLC

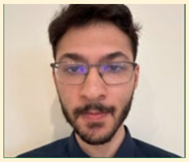
Avint LLC.

# CGI Federal – Blockchain: Hardware

Daniel Huynh



Noah Ramsden



Gazi Essawi

Rida Hasan

Farzam Noori

SMEs: Shadman Hossain, Alan Watson

## CHALLENGE

This project aims to create an efficient and reliable asset management system using IoT, blockchain, and large language model technologies. The system's purpose is to provide intelligent tracking and transparent supply chain logistics management, which would streamline location tracking, maintenance operations, and equipment checkouts. The focus of the hardware side was to use smart device technologies to generate an alert system that synthesizes input data from a set of environmental sensors and AI video analysis.

## Daniel Huynh

Fairfax, VA.

**Aspiration:** I aspire to continuously learn and adapt to the latest advancements in technology in order to develop solutions that improve digital infrastructure while integrating cyber security.

**Class Comment:** This class has given me the opportunity to explore new technologies while collaborating with a team to integrate project components.

## Gazi Essawi

Fairfax, VA.

**Aspiration:** I aspire to continue learning and strengthening my cyber security foundation and apply learned skills both offensive and defensively to protect critical assets.

**Class Comment:** This class has given me an opportunity to develop a product with a team and produce deliverables simulating a working environment.

## Farzam Noori

Fairfax, VA.

**Aspiration:** I aspire to innovate through technology and entrepreneurship, creating solutions that enhance efficiency, security, and everyday life while making a positive impact on others.

**Class Comment:** This class taught me how to turn complex technologies into real-world solutions, blending innovation with purpose to create systems that make a difference.

## Noah Ramsden

Fairfax, VA.

**Aspiration:** I hope to utilize the skills that I've gained through my education to guide communities and develop tools to protect people and to help them adapt in a world of rapidly evolving technology.

**Class Comment:** This class has provided me with an opportunity to tackle problems with real-world implications while allowing me to develop my collaborative abilities and adaptability to fast-paced changes.

## Rida Hasan

Fairfax, VA.

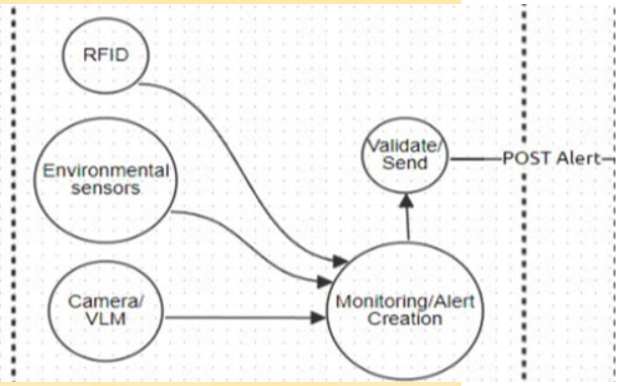
**Aspiration:** I intend to continue studying cyber security engineering and work on more cyber-physical systems, critical infrastructure and national security related projects.

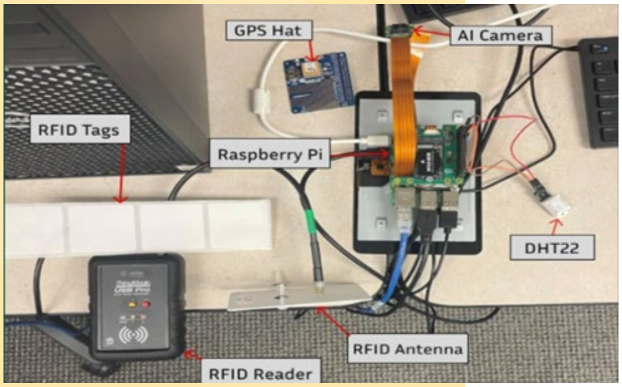
**Class Comment:** I appreciate that this class allowed us the opportunity to work on a research/development project with a sponsor and present our work at a conference.

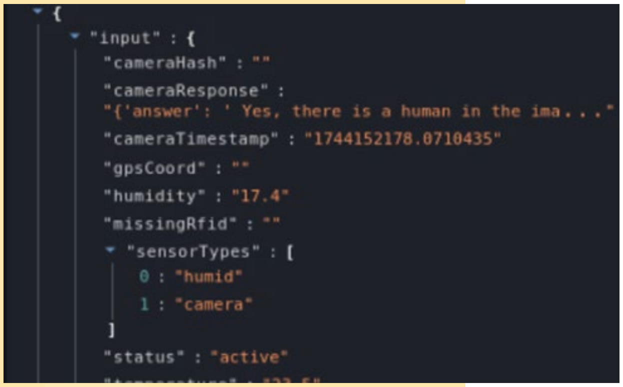
Project Sponsor: CGI Federal

CGI

# CGI Federal – Blockchain: Hardware







```
{
  "input" : {
    "cameraHash" : ""
    "cameraResponse" :
    "{'answer': ' Yes, there is a human in the ima..."
    "cameraTimestamp" : "1744152178.0710435"
    "gpsCoord" : ""
    "humidity" : "17.4"
    "missingRfid" : ""
    "sensorTypes" : [
      0 : "humid"
      1 : "camera"
    ]
    "status" : "active"
```

Our project aims to create a modernized and efficient asset tracking and management system using an integrated hardware and software system.

The proposed system will utilize hardware components such as sensors and RFID readers which will send collected data to software components including a blockchain which will be queried by an AI chatbot.

The focus of the hardware side was to use smart device technologies to generate an alert system that synthesizes input data from a set of environmental sensors and AI video analysis. The hardware components utilized include the following:

DHT22 sensor to monitor temperature and humidity.

AI Video camera for monitoring and pairing with a VLM for analysis of feed.

RFID reader and tags to identify objects and ensure they stay within environmental bounds.

This alert system is generated through functions on our Raspberry Pi which are then processed in a format acceptable to the smart contract hosted on a blockchain endpoint. The Pi itself will host an on-device visual language model (VLM) known as Moondream to allow for real time analysis of video input. The current VLM configuration detects if a person is within frame of the video, generating an alert if these conditions are met. The modularity of the hardware components utilized allows our system to fulfill a large quantity of use cases.

Project Sponsor: CGI Federal

# CGI Federal – Blockchain: Software

William Watson

Minh Nguyen

Eric Kim

Alex Trinh

Ronitt Murjany

Sophia Riehl

SMEs: Shadman Hossain, Alan Watson

## CHALLENGE

This project aims to create an efficient and reliable asset management system using IoT, blockchain, and large language model technologies. The system aims to provide intelligent tracking and transparent supply chain logistics management, streamlining location tracking, maintenance operations, and equipment checkouts. The software side focused on creating an efficient and reliable asset management system using IoT, blockchain, and Large Language Model technologies to provide secure, intelligent tracking and transparent supply chain logistics management.

## William Watson

Fairfax, VA.

**Aspiration:** I aspire to be a leader within the cybersecurity field and to use the knowledge that I gained from pursuing my certifications and education to make it happen.

**Class Comment:** This class has given me insight on how to lead a team proactively and efficiently. I've also learned how to research new technology and apply it to an experimental project.

## Eric Kim

Fairfax, VA.

**Aspiration:** I aspire to use my skills and knowledge in the cybersecurity field, leveraging my education, certifications, and military experience to strengthen digital security.

**Class Comment:** This class has given me insight on the importance of communication, taking responsibility, and working together as a team.

## Ronitt Murjany

Fairfax, VA.

**Aspiration:** I aspire to work in cybersecurity consulting within the government space, applying my technical skills to help protect national interests and deliver effective cyber solutions.

**Class Comment:** This class helped me apply cybersecurity concepts to real scenarios and strengthened my skills in research, technical writing, and teamwork during group projects.

## Minh Nguyen

Fairfax, VA.

**Aspiration:** I aspire to apply the knowledge I gained from my time at Mason to help protect people and their digital assets.

**Class Comment:** This class has given me insight on real-world work experience. I've learned about the importance of teamwork, communication, and time management.

## Alex Trinh

Fairfax, VA.

**Aspiration:** I aspire to work in cyber security within the government contracting space, I want to teach and help in national security interests through innovative cyber solutions.

**Class Comment:** This class has helped me understand how to apply cybersecurity principles in real-world scenarios. I've improved my skills in teamwork, problem-solving, and managing technical challenges as part of a collaborative project.

## Sophia Riehl

Fairfax, VA.

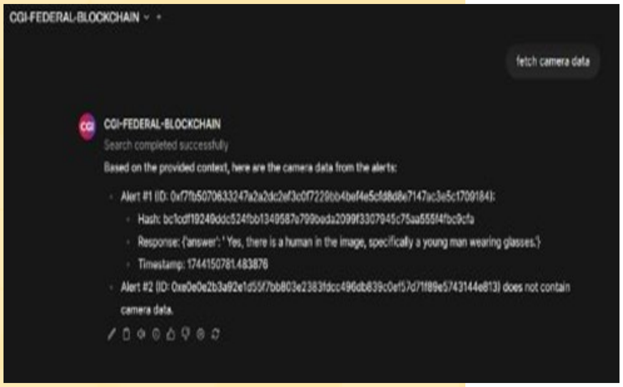
**Aspiration:** I aspire to apply the knowledge I gained from my time at Mason to the United States Army as a 2nd Lieutenant, to help protect and serve my country.

**Class Comment:** This class has taught me how to utilize and understand new software as well as to harness my communication skills when working with a team.

Project Sponsor: CGI Federal

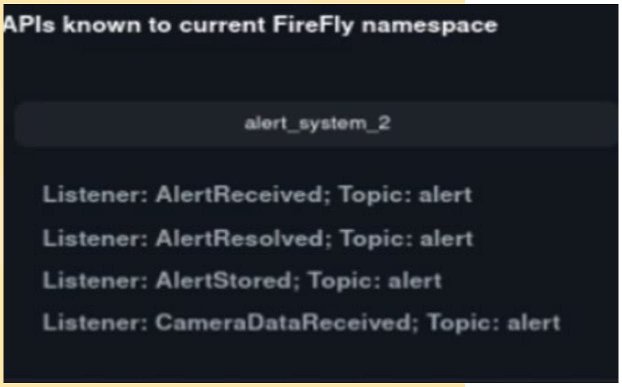
CGI

# CGI Federal – Blockchain: Software



Based on the provided context, here are the camera data from the alerts:

- Alert #1 (ID: 0xf7fb5070633247a2a2dc2ef3c0f7229bb4bef4e5cfd8d8e7147ac3e5c1709184):
  - Hash: bc1cdf19249ddc524fbb1349587e799beda2099f3307945c75aa555f4fbc9cfa
  - Response: {'answer': ' Yes, there is a human in the image, specifically a young man wearing glasses.'}
  - Timestamp: 1744150781.483876
- Alert #2 (ID: 0xe0e0e2b3a92e1d55f7bb803e2383fdcc496db839c0ef57d71f89e5743144e813) does not contain camera data.



APIs known to current FireFly namespace

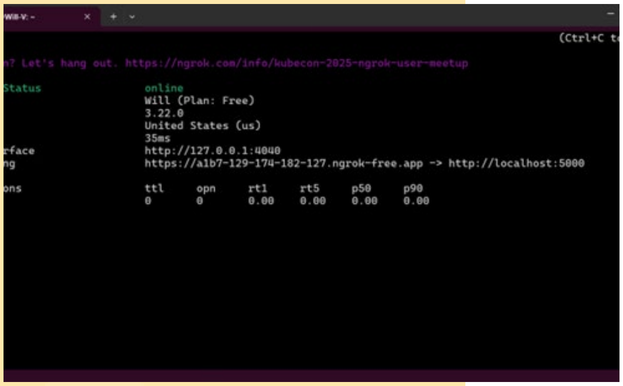
alert_system_2

Listener: AlertReceived; Topic: alert

Listener: AlertResolved; Topic: alert

Listener: AlertStored; Topic: alert

Listener: CameraDataReceived; Topic: alert



```
                                                                            (Ctrl+C t
n? Let's hang out. https://ngrok.com/info/kubecon-2025-ngrok-user-meetup

Status                        online
                              Will (Plan: Free)
                              3.22.0
                              United States (us)
                              35ms
rface                         http://127.0.0.1:4040
ng                            https://a1b7-129-174-182-127.ngrok-free.app -> http://localhost:5000

ons                           ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Our project focuses on the software components of the asset management system, consisting of blockchain storage, smart contracts, and an AI chatbot.

The Raspberry Pi sends alert data to the blockchain API, which contains a smart contract that automates storage on-chain and off-chain.

Mistral: instruct is the base AI model used to power the logical processing due to its lightweight requirements and cost-efficiency. Open WebUI, a prebuilt interface, is used to streamline user interaction with the chatbot.

The AI chatbot can take user input and use that information while contacting the blockchain smart contract that returns alert data. Currently, the system can only take one search filter parameter per user query.

A Python script imported into Open WebUI's Tool feature allows the chatbot to connect to the blockchain API when enabled.

Ngrok, a secure tunneling service for local host servers, was used to connect the Hyperledger firefly blockchain and the AI chatbot.

# Research and Implementation of Integration of the Network and Application and Workload Pillars of the Zero Trust Model to Provide Enhanced Visibility/Analytics and Automation

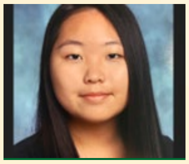
Saira Akram

Maimoonah Chaudhry

Harshal Modi

Kevin Palatty

Johnny Tran


Rachel Wang

SMEs: David Crawford

## CHALLENGE

As technology advances and cyber threats continuously evolve, traditional security models relying solely on perimeter defenses have become inadequate. Our project provides the foundation for a fully functional Zero Trust Architecture (ZTA) model to enhance security by enforcing strict access controls and network segmentation through comprehensive data analysis of network traffic in CGI's Defend-C lab environment and Python scripts generating effective firewall rulesets for network segmentation in the lab environment through the Palo Alto REST API.

## Saira Akram

Sterling, VA.

**Aspiration:** My goal is to become a successful cybersecurity analyst specializing in Zero Trust Architecture. I aspire to apply my hands-on skills to establish my own company, providing cybersecurity solutions to organizations.

**Class Comment:** This course provided me with valuable hands-on experience, enhancing my technical skills and teamwork. Working on this project improved my problem-solving and communication skills while also giving me the opportunity to explore new tools and expand my knowledge in cybersecurity.

## Harshal Modi

Gainesville, VA.

**Aspiration:** My aspirations are to gain technical knowledge on a wide variety of cybersecurity concepts to make me more useful for practical cybersecurity skills.

**Class Comment:** This course taught me many practical skills, mainly on networking, Zero Trust, and scripting, I also learned how to be a part of a team and how companies set deadlines and goals that we had to follow rigidly. These skills will help tremendously in my future career aspirations.

## Johnny Tran

Gainesville, VA.

**Aspiration:** My aspiration is to gain knowledge and experience in the cybersecurity industry. I aspire to become a cybersecurity analyst with my skills and land a remote job in this field while also keeping up with emerging cyber threats.

**Class Comment:** This class provided an interactive experience with a taste of what working on projects in this industry would be like. I had a great experience working on this project with my peers and it helped to refine my skills with cybersecurity challenges that I will face in the real world.

## Maimoonah Chaudhry

Chantilly, VA.

**Aspiration:** My goal is to keep growing my skills and work on projects with real impacts and help protect companies from cyber threats. I'm interested in learning more about Zero Trust Security and build strong and reliable systems.

**Class Comment:** This course taught me how to work on real-world problems with a team. I got hands-on experience, and learned how to solve challenges using different tools. It gave me a better understanding of what it's like to work in the cybersecurity field.

## Kevin Palatty

Gainesville, VA.

**Aspiration:** My goal is to graduate with a degree in Cyber Security Engineering and begin my professional work career post-graduation. I aspire to deepen my knowledge in ZTA as it's the future of modern security and resilience.

**Class Comment:** This course gave me unique hands-on experience working with industry professionals in an actual work environment outside the classroom. I learned a lot of new concepts and got to practice actual implementation which you do not get in a lot of other courses.

## Rachel Wang

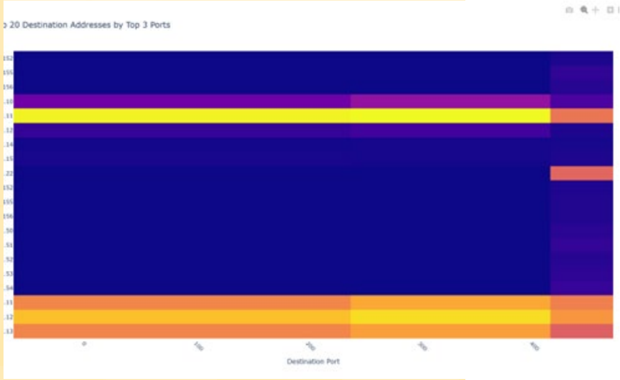
Burke, VA.

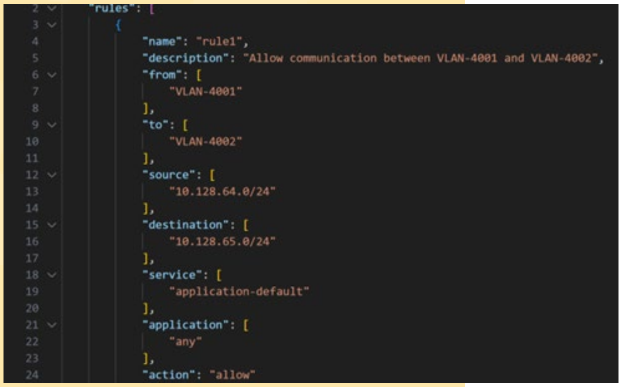
**Aspiration:** I plan to become a cybersecurity analyst and help organizations implement effective cyber solutions to strengthen their systems. I want to leverage my knowledge & skills to solve today and tomorrow's cybersecurity challenges.

**Class Comment:** This course provided me with an opportunity to collaborate with my peers and solve a real-world cybersecurity challenge in a professional setting while gaining valuable hands-on experience and developing my technical skill set.

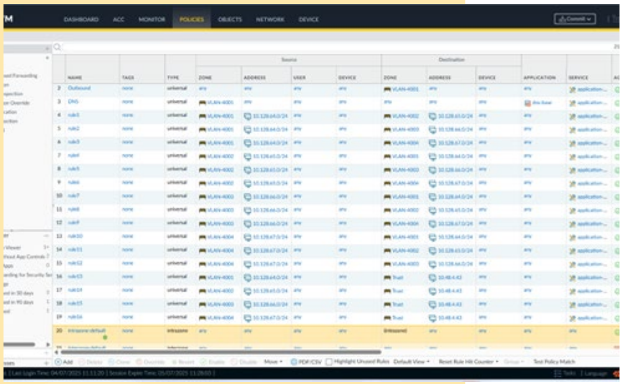
Project Sponsor: CGI Federal

# Research and Implementation of Integration of the Network and Application and Workload Pillars of the Zero Trust Model to Provide Enhanced Visibility/Analytics and Automation





```
    "rules": [
        {
            "name": "rule1",
            "description": "Allow communication between VLAN-4001 and VLAN-4002",
            "from": [
                "VLAN-4001"
            ],
            "to": [
                "VLAN-4002"
            ],
            "source": [
                "10.128.64.0/24"
            ],
            "destination": [
                "10.128.65.0/24"
            ],
            "service": [
                "application-default"
            ],
            "application": [
                "any"
            ],
            "action": "allow"
```



| | | | | Source | | | | Destination | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE |
| 2 | Outbound | none | universal | any | any | any | any | VLAN-4001 | any | any | any | application-... |
| 3 | DNS | none | universal | VLAN-4001 | any | any | any | any | any | any | dns-base | application-... |
| 4 | rule1 | none | universal | VLAN-4001 | 10.128.64.0/24 | any | any | VLAN-4002 | 10.128.65.0/24 | any | any | application-... |
| 5 | rule2 | none | universal | VLAN-4001 | 10.128.64.0/24 | any | any | VLAN-4003 | 10.128.66.0/24 | any | any | application-... |
| 6 | rule3 | none | universal | VLAN-4001 | 10.128.64.0/24 | any | any | VLAN-4004 | 10.128.67.0/24 | any | any | application-... |
| 7 | rule4 | none | universal | VLAN-4002 | 10.128.65.0/24 | any | any | VLAN-4001 | 10.128.64.0/24 | any | any | application-... |
| 8 | rule5 | none | universal | VLAN-4002 | 10.128.65.0/24 | any | any | VLAN-4003 | 10.128.66.0/24 | any | any | application-... |
| 9 | rule6 | none | universal | VLAN-4002 | 10.128.65.0/24 | any | any | VLAN-4004 | 10.128.67.0/24 | any | any | application-... |
| 10 | rule7 | none | universal | VLAN-4003 | 10.128.66.0/24 | any | any | VLAN-4001 | 10.128.64.0/24 | any | any | application-... |
| 11 | rule8 | none | universal | VLAN-4003 | 10.128.66.0/24 | any | any | VLAN-4002 | 10.128.65.0/24 | any | any | application-... |
| 12 | rule9 | none | universal | VLAN-4003 | 10.128.66.0/24 | any | any | VLAN-4004 | 10.128.67.0/24 | any | any | application-... |
| 13 | rule10 | none | universal | VLAN-4004 | 10.128.67.0/24 | any | any | VLAN-4001 | 10.128.64.0/24 | any | any | application-... |
| 14 | rule11 | none | universal | VLAN-4004 | 10.128.67.0/24 | any | any | VLAN-4002 | 10.128.65.0/24 | any | any | application-... |
| 15 | rule12 | none | universal | VLAN-4004 | 10.128.67.0/24 | any | any | VLAN-4003 | 10.128.66.0/24 | any | any | application-... |
| 16 | rule13 | none | universal | VLAN-4001 | 10.128.64.0/24 | any | any | Trust | 10.48.4.43 | any | any | application-... |
| 17 | rule14 | none | universal | VLAN-4002 | 10.128.65.0/24 | any | any | Trust | 10.48.4.43 | any | any | application-... |
| 18 | rule15 | none | universal | VLAN-4003 | 10.128.66.0/24 | any | any | Trust | 10.48.4.43 | any | any | application-... |
| 19 | rule16 | none | universal | VLAN-4004 | 10.128.67.0/24 | any | any | Trust | 10.48.4.43 | any | any | application-... |
| 20 | intrazone-default | none | intrazone | any | any | any | any | (intrazone) | any | any | any | any |

This Zero Trust Architecture (ZTA) project focuses on developing a segmented, resilient, and adaptive network grounded in continuously verified security rules and policies. The operational framework integrates data analysis with strict access controls to ensure that no entity is implicitly trusted, and all access is validated to mitigate misuse. The system segments the network into isolated domains, each with its own security controls. This layered approach limits lateral movement, reducing the impact of a breach if one were to occur. If one segment of the network is compromised, the strict inter-segment policies will help contain it and mitigate damage to the environment.

Segmentation is applied using firewall controls, contextual analytics, and automated rule application using scripting and API integrations with Palo Alto firewalls. The system emphasizes continuous validation and real-time monitoring. A centralized interface through the Palo Alto Firewall and SPLUNK hosts allows for rule management and integrates with analytics platforms for visibility into network health, threats, and policy adherence.

The final implementation of the ZTA in the CGI Federal Defend CC lab environment resulted in a segmented network that enforced least privilege access and reduced lateral movement. The firewall rulesets generated by the team's Python scripts were successfully uploaded to the Palo Alto firewall and applied segmentation logic for source address, destination address, service, application, and action based on groupings by subnet, application, and port or by VLAN.

Project Sponsor: CGI Federal

# Generative AI in Cybersecurity: Offensive & Defensive Strategies for Accessibility Threats

Ammad Zulfiqar

Benjamin Bediako

Mohammad Daniyal Toqeer Abbas

Natalia Ramos Flores

Amna Abbasi

SMEs: Joshua Sonnier

## CHALLENGE

Accessibility tools, such as text-to-speech and live captions, are crucial for inclusivity but can expose users to risks like credential theft, data exfiltration, and malicious code execution. This project leverages generative AI to analyze vulnerabilities in Google Chrome's accessibility features. Furthermore, this project also develops and proposes innovative strategies for securing these features. The project has four key components: Vulnerability Analysis, Offensive Strategy, Mitigation Strategy Plan, and Defensive Mechanism Framework.

## Ammad Zulfiqar

Fairfax, VA.

**Aspiration:** After the completion of my degree, I aim to work in the private sector as a vulnerability assessment analyst.

**Class Comment:** The capstone project was phenomenal for gaining hands-on, real-world experience. Through the intersection of cybersecurity and AI we were able to learn more about how web browsers secure their accessibility feature set.

## Benjamin Bediako

Fairfax, VA.

**Aspiration:** I am aiming to work as a Cybersecurity Analyst after my degree and then going for my masters in a few years after I gain some experience.

**Class Comment:** This project has helped me gain hands on experience in using cyber tools and AI to tackle a specific problem which in my case which is finding vulnerabilities in a web browsers accessibility feature.

## Mohammad Daniyal Abbas

Fairfax, VA.

**Aspiration:** After graduation, I plan to pursue a career as a Cyber Security Engineer, where I can focus on defending enterprise systems against evolving threats.

**Class Comment:** This project gave me valuable hands-on experience in identifying vulnerabilities in browser accessibility features and developing AI-based defensive strategies. It strengthened my interest in the intersection of cybersecurity and emerging technologies.

## Natalia Ramos Flores

Fairfax, VA.

**Aspiration:** After graduation, I aim to work as a SOC Analyst, where I can apply both technical skills and critical thinking to protect systems and users.

**Class Comment:** This project gave me hands-on experience analyzing browser accessibility vulnerabilities using AI tools. It deepened my understanding of real-world threats and sparked a strong interest in cybersecurity.

## Amna Abbasi

Fairfax, VA.

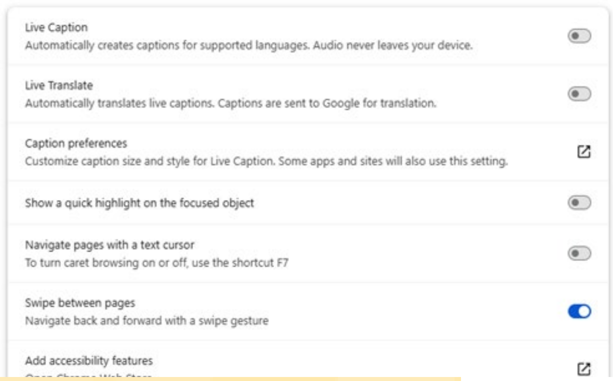
**Aspiration:** After graduating, I aim to work as an IT Security Analyst at the company where I am currently working as an IT intern.

**Class Comment:** This capstone project provided meaningful hands-on experience in identifying browser accessibility vulnerabilities using AI tools. It enhanced my practical skills with cybersecurity technologies, deepened my understanding of threat detection, and strengthened my passion for securing digital systems in real-world environments.

Project Sponsor: CGI Federal

CGI

# Generative AI in Cybersecurity: Offensive & Defensive Strategies for Accessibility Threats



Live Caption
Automatically creates captions for supported languages. Audio never leaves your device. ○

Live Translate
Automatically translates live captions. Captions are sent to Google for translation. ○

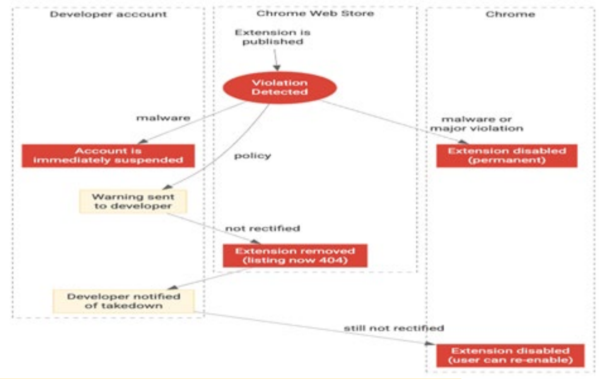
Caption preferences
Customize caption size and style for Live Caption. Some apps and sites will also use this setting.

Show a quick highlight on the focused object ○

Navigate pages with a text cursor
To turn caret browsing on or off, use the shortcut F7 ○

Swipe between pages
Navigate back and forward with a swipe gesture ●

Add accessibility features


Developer account
Chrome Web Store
Chrome
Extension is published
Violation Detected
malware
Account is immediately suspended
policy
malware or major violation
Extension disabled (permanent)
Warning sent to developer
not rectified
Extension removed (listing now 404)
Developer notified of takedown
still not rectified
Extension disabled (user can re-enable)

## Vulnerability Analysis

The Vulnerability Analysis focuses on identifying weaknesses in Google Chrome’s accessibility features and evaluating the impact of these vulnerabilities on security and user privacy. Accessibility tools such as text-to-speech, live captions, and preference settings are critical for enhancing usability, especially for individuals with disabilities.

## Offensive Strategy

The Offensive Strategy outlines how the vulnerabilities identified in the analysis can be exploited in real-world scenarios. By simulating potential attacks, the team aimed to assess the severity of these vulnerabilities and understand their impact on browser security and user privacy.

## Mitigation Strategy Plan

The Mitigation Strategy Plan presents a layered approach to strengthening the security of Chrome’s accessibility features, starting with an evaluation of existing browser protections. It then introduces user focused enhancements and advanced technical defenses to address threats like keylogging, screen capture, and data exfiltration.

## Defensive Mechanism Framework

The Defensive Mechanism Framework presents a comprehensive response to the security vulnerabilities identified in Chrome’s accessibility features.

Picture source: https://developer.chrome.com/docs/webstore/review-process

Project Sponsor: CGI Federal

# AI Based Role Authorization Prototype

Abdulaziz AL-Sayed

Khaled AL-Sayed

Joseph Gray

Deekshita Sanampudi

Malek Atik

## CHALLENGE

Our project focuses on automating the verification process that confirms whether a user requesting access to CMS (Centers for Medicare & Medicaid Services) systems is affiliated with the organization they claim to represent. We developed a Python-based solution that integrates various verification methods to enhance system security and reduce the need for manual reviews. The project is being deployed onto an AWS EC2 instance to allow for a secure, scalable, and accessible tool.

SMEs: Christopher Smith, Joshua Sonnier

### Deekshita Sanampudi

Ashburn, VA.

**Aspiration:** I aspire to continuously improve my technical skills by pursuing a career in Cyber Security and stay up to date with the cyber industry.

**Class Comment:** This course has significantly enhanced my professional and technical skills through hands-on experience working with both the sponsor and mentor.

### Abdulaziz Al-Sayed

Fairfax, VA.

**Aspiration:** I joined cybersecurity to protect and serve my country, Qatar, in the face of growing digital threats. Sponsored by the Ministry of Interior, I'm committed to using my skills to strengthen our national security and safeguard our digital future.

**Class Comment:** This course strengthened my teamwork and communication skills through working with new members and real-world sponsors.

### Malek Atik

Herndon, VA.

**Aspiration:** I am looking to join the cyber security work force and improve and learn new and existing skills that I have.

**Class Comment:** I personally feel like this class is a real turning point in the school's curriculum where we can gain real life experience with the guidance of professionals and it's a fantastic experience.

### Joseph Gray

Fairfax, VA.

**Aspiration:** I aim to work at a company where I can actively apply my cybersecurity skills, continue learning new things, and contribute to solving real-world cybersecurity challenges.

**Class Comment:** Working with my teammates, mentor, and sponsors has been a valuable experience for me that helped me develop my skills and build meaningful, lasting connections.

### Khaled AL-Sayed

Fairfax, VA.

**Aspiration:** I intend to carry on my father's legacy within the telecommunications company he dedicated 35 years of his life to by leveraging the Cyber Security expertise I acquired during my journey at George Mason University.

**Class Comment:** This class is incredibly important and has been a fantastic experience because I've learned how to work professionally and collaborate effectively with a great group, mentor and sponsor.

Project Sponsor: CGI Federal

# AI Based Role Authorization Prototype

Secure identity verification is more critical than ever in a time where cybersecurity threats and impersonation risks are on the rise, especially in the government and healthcare sectors. CMS must ensure that only authorized users of trusted organizations gain access to its systems, as it handles sensitive patient data. Our initiative helps CMS automate and reinforce the process, reducing human error and adding multiple layers of security to help CMS verify requesting users, while maintaining an intuitive user experience.

Our Capstone deliverable includes a system featuring a GUI interface developed in Python, prompting users to submit information such as job title, company, and email. A number of checks are then performed, such as site scraping, address proximity matching with OpenRouteService, job role relevance scoring using GPT-4 Turbo, and certificate validation with mutual TLS. A total confidence score is generated from the results, helping CMS approve or flag user access automatically.

Picture source: https://www.nychiefs.org/assets/ChieflySpeaking/Chiefly-Speaking-Newsletter-April-2022.pdf, https://www.cms.gov/, https://www.python.org/

Project Sponsor: CGI Federal

# Fingerprinting 5G Radios for Security Application

Nongnapat Adchariyavivit

Nour El Houda Aidlaid

Qais Dib

Harshita Chaudhari

Sreenithya Somavarapu

## CHALLENGE

This project explored electromagnetic (EM) side channel analysis as a method for enhancing the security of 5G radio systems within an Open Radio Access Network framework. Using a custom-built testbed, we focused on collecting EM signatures from a single device operating under different scenarios. The goal was to investigate how EM signals vary with system behavior, laying the groundwork for future applications in device profiling and anomaly detection.

SMEs: Tanvir Arafin

## Nongnapat Adchariyavivit

Fairfax, VA.

**Aspiration:** I aspire to enhance my cybersecurity engineering skills, especially wireless communication and network traffic analysis.

**Class Comment:** By contributing to this project, I have a great opportunity to gain a deep understanding of side-channel analysis, explore the fingerprinting of 5G, and create hands-on experience with 5G technology.

## Harshita Chaudhari

Fairfax, VA.

**Aspiration:** I aspire to work as a cybersecurity professional, applying my expertise in digital forensics or threat hunting, with a particular focus on the intersection of cybersecurity and intelligence analysis.

**Class Comment:** This course offered a great platform for conducting in-depth research while working on practical cybersecurity challenges.

## Sreenithya Somavarapu

Fairfax, VA.

**Aspiration:** This project deepened my interest in hardware security, which is where I hope to focus my future work. While networking isn't my primary interest, this experience allowed me to apply security concepts in a real-world hardware setting for the first time.

**Class Comment:** This research project gave me a unique opportunity to explore academic research, something I hadn't experienced before. It was a rewarding way to apply my skills to a real-world problem in a structured, investigative setting.

## Qais Dib

Fairfax, VA.

**Aspiration:** I aspire to become well rounded in all aspects of cybersecurity and related engineering fields in order to contribute as much as possible to society.

**Class Comment:** The opportunity to participate in fingerprinting a 5G network has given me valuable insight to how I can apply and expand my skill sets for real world applications.

## Nour El Houda Aidlaid

Fairfax, VA.

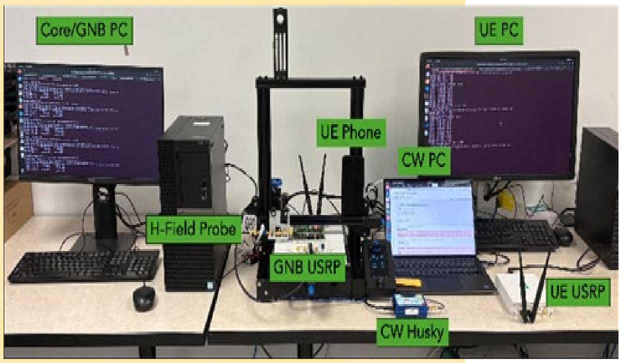
**Aspiration:** I aspire to hone my gained experiences from this project and projects alike in the cybersecurity field. This includes applying and strengthening my skills in wireless communication security, hardware analysis, and threat detection. I'm particularly interested in contributing to the development of secure systems at the intersection of hardware and network security, where innovation is both challenging and essential.

**Class Comment:** This course has given me the opportunity to work at the intersection of networking, wireless systems, and cybersecurity. It strengthened my skills in critical thinking, collaboration, and practical cybersecurity—skills I'll carry with me into my career.

Project Sponsor: Cyber Security Engineering Department, GMU

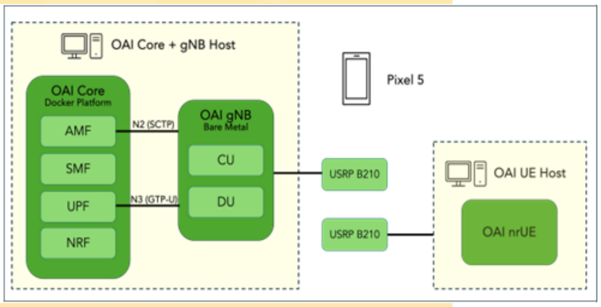
College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# Fingerprinting 5G Radios for Security Application

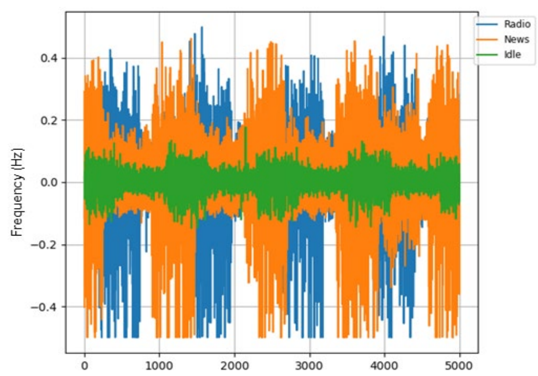


This project profiles side channel data in a 5G network to evaluate the security of 5G and Open Radio Access Network (O-RAN) architectures. A machine learning (ML) model is used to extract and analyze electromagnetic (EM) signatures that may reveal device-level vulnerabilities.

Side-channel analysis focuses on unintended data leakage from hardware. In O-RAN systems, disaggregated components can introduce unique side channel characteristics. This work targets EM emissions to uncover hidden risks in the network stack.



The testbed features an end-to-end 5G network deployment, consisting of a core network, gNodeB (base station), and user equipment (UE). A USRP B210 radio serves as the gNodeB, while a smartphone is used as the UE. EM signals are captured using a ChipWhisperer Husky and an RF field probe positioned near the radio.



The results show distinct EM patterns associated with specific network behaviors. The ML model can accurately distinguish and classify these patterns, revealing potential vulnerabilities and highlighting the need to secure 5G and O-RAN systems against side-channel threats.

Project Sponsor: CYSE, GMU

# AI-Driven Threat Detection and Response System

Alex Lappin

Bibhu Paudyal

Mahi Khan

Joshua Puyat

Hussam Al Bakhat

Sumayah Alomari

## CHALLENGE

The aim of this project was to transform a traditional IDS using machine learning models to better detect and respond to cyber threats. This AI-driven system analyzes network traffic and system logs to identify malicious behavior more effectively. The goal is to improve detection accuracy and response speed, creating a proactive defense against today's evolving threat landscape.

SMEs: Alexandre De Barros Baretto

## Alex Lappin

Fairfax, VA.

**Aspiration:** After Completion of my Master's degree, my goal is to improve the exponentially growing AI future using a Cyber Engineering methodology and expertise.

**Class Comment:** This class enabled me to gain experience in managing a team's deliverables as well as get a glimpse into the industry of AI being used in a security context.

## Mahi Khan

Fairfax, VA.

**Aspiration:** I aspire to gain experience in the AI-driven cyber industry and eventually establish my own cyber security firm focused on advanced threat detection.

**Class Comment:** This class taught me to balance both creative thinking and analytic approach to problems, when appropriate.

## Hussam Al Bakhat

Fairfax, VA.

**Aspiration:** I aspire to become a cybersecurity specialist focused on preventing cyber attacks and strengthening digital defenses.

**Class Comment:** This class gave me great hands-on experience and helped me build practical skills while learning the value of teamwork in technical projects.

## Bibhu Paudyal

Centreville, VA.

**Aspiration:** I'd like get some general experience in the industry while slowly positioning myself deeper into the increasingly developing AI sphere.

**Class Comment:** This was the first large scale project that I've worked on. It has provided invaluable experience when it comes to tackling complex problems with existing tools and ingenuity.

## Joshua Puyat

Arlington, VA.

**Aspiration:** My goal is to contribute to securing the future of digital technology by applying a strong foundation in cyber defense and data protection.

**Class Comment:** This class gave me hands-on experience in developing an AI solution, which not only enhanced my technical skills but also showed me the real-world impact AI can have in strengthening cybersecurity practices.

## Sumayah Alomari

Fairfax, VA.

**Aspiration:** I aspire to help in shaping the future of digital defense through innovation and strategic thinking and staying ahead of evolving cyber threats.

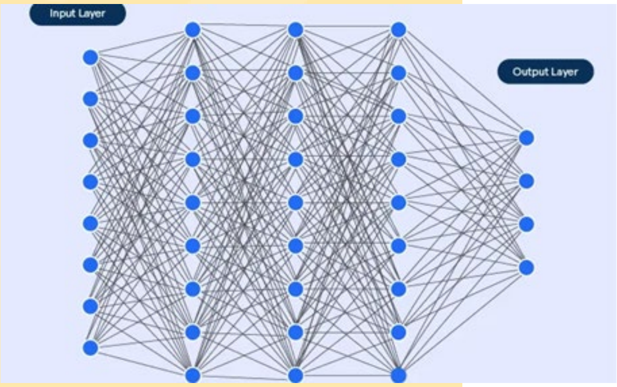
**Class Comment:** This project gave me hands-on experience on how AI can be used in cyber security, enhanced my technical abilities, and made me value teamwork more on a large-scaled project.

Project Sponsor: Cyber Security Engineering Department, GMU

# AI-Driven Threat Detection and Response System

The increasing sophistication and diversity of cyber threats pose significant challenges to organizations relying on traditional, signature-based intrusion detection systems (IDS).

IDS systems have been proven difficult to set up in an effective way for each use case, leaving many IDS systems configured incorrectly or inadequately when dealing with a specific threat.



Through leveraging the abilities of a multi-classed supervised Deep Neural Network (DNN), we demonstrate the ability to classify and label Suricata alerts and metadata, which bridge the gap between signature-based detection and dynamic threat adaption. This learning has been based on the CICIDS2017 MITRE ATT&CK dataset which allows for detailed analysis on 14 specific threat classes with a weighted distribution on more common attacks.

A real scenario of an AWS instance of Suricata provides us with real-time attack data as well as the beginning stages of a dynamic response system.

Our proof-of-concept establishes a foundation for a network of enhanced AI-driven security tools, paving the way for future research exploring specific AI algorithms, algorithm-to-tool mappings, and the development of proactive IDS capabilities.

Picture source: https://suricata.io/, https://aws.amazon.com/, https://cdn.botpenguin.com/assets/website/Deep_Neural_Network_2b9d9075e9.webp

Project Sponsor: CYSE, GMU

# GleNN: Large Language Models for Static Reverse Engineering

Justin Rockwell

Max Bedewi

Craig Kimball

Mack Bartsch

Bisesh Acharya

SMEs: Tanvir Arafin

## CHALLENGE

Static reverse engineering malicious binary code has a large impact on recovering impacted systems and creating future safeguards.

The objective of our research was to create a complete solution to reconstruct C code from executable binary files that performs better than current solutions.

## Justin Rockwell

Fairfax, VA.

**Aspiration:** Leverage my cybersecurity engineering training to move up the ladder and drive security strategy at Apple.

**Class Comment:** This senior design project pushed me into graph databases, similarity search, and LLMs, demanding hands-on troubleshooting and rapid adaptation.

## Craig Kimball

Fairfax, VA.

**Aspiration:** I plan on continuing my education and experience by further working at NAVSEA Dahlgren.

**Class Comment:** This class and project has provided me with valuable knowledge regarding LLMs and RAG pipelines.

## Bisesh Acharya

Fairfax, VA.

**Aspiration:** I hope to find a job in the private sector working with hardware engineering.

**Class Comment:** I found that this class really pushed us to work well within a group setting while stepping into new areas that were being pushed within the field.

## Max Bedewi

Fairfax, VA.

**Aspiration:** I plan to continue my cyber security career working in private sector government contracting.

**Class Comment:** This class has provided valuable experience in both LLMs and working on long term projects as a team.

## Mack Bartsch

Stafford, VA.

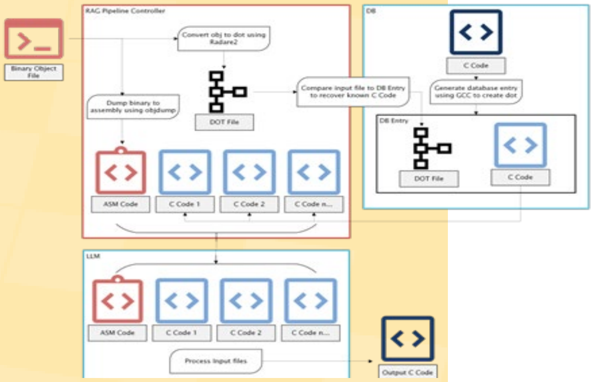
**Aspiration:** I plan on continuing my cyber security career as a full-time penetration tester.

**Class Comment:** This class gave me valuable experience in working with real-world projects.

Project Sponsor: Cyber Security Engineering Department, GMU

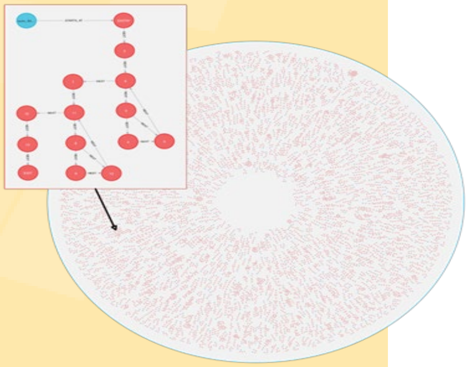
College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# GleNN: Large Language Models for Static Reverse Engineering



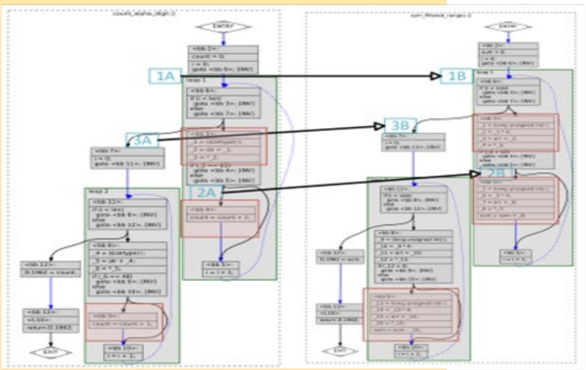
GleNN is a research into the application and usage of Retrieval Augmented Generation (RAG) pipelines with Large Language Models (LLMs) to better inform the decision-making skills aiding in the ability to understand and de-compile assembly code.

RAG Pipelines enhance the processing capabilities of LLMs by integrating an external knowledge database into their workflow, allowing them to access finetuned, domain-specific information.



The research of our team was the development of a python pipeline that takes an executable binary input file, retrieves associated C code through a series of similarity matches, and provides additional context to DeepSeek's R1 LLM.

The process of the RAG pipeline, takes a binary file as input as its starting point. With the binary file, using radare2, creates a dot file that represents the structure of the code. It uses this structure as a similarity to search a database of known C files. These recovered C files are used to better inform the model to create more desirable output.

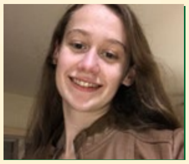


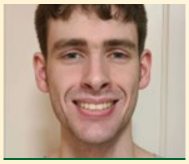
Project Sponsor: CYSE, GMU

# LOCO: Secure Localization for Multi-Robot Systems in Dynamic Environments

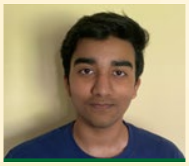
Andrew Le

Biraj Joshi


Leigh Black


Logan Minto

Rahul Patel


Shreyas Gadiraju

SMEs: Tanvir Arafin

## CHALLENGE

Our project aims to explore the use of Visual Language Models (VLM) in the evaluation of multi-robot formations and symbol detection. A Robot Operating System 2 based system was integrated with a VLM to generate and assess multi-robot formations and evaluate symbols. Formations are disrupted using a network based cyber attack. The VLM then identifies if the robots are in the correct formation or disrupted.

## Andrew Le

Fairfax, VA.

**Aspiration:** After completing my bachelor's, I hope to be able to research and design novel cyber security technologies or systems.

**Class Comment:** After completing my bachelor's, I hope to be able to research and design novel cyber security technologies or systems.

## Biraj Joshi

Fairfax, VA.

**Aspiration:** After completing my bachelor's, I plan to work as a systems engineer where I will focus on identifying and mitigating system vulnerabilities.

**Class Comment:** This class gave me valuable insight into the process of conducting an academic research and gave me a deeper understanding of the current state of robotics, AI, and LLM.

## Leigh Black

Vienna, VA.

**Aspiration:** After completing my masters, I aspire to work in digital forensic analysis and investigate cybercrimes.

**Class Comment:** This class has given me the opportunity to gain valuable research experience and learn new skills pertaining to robotics and artificial intelligence.

## Logan Minto

Reston, VA.

**Aspiration:** After graduating this semester, I plan to return to IBM as a data scientist, and transition to working on Cyber Security.

**Class Comment:** This course provides a unique and valuable experience which gives students a preview of what working with a client in the real world is like.

## Rahul Patel

Lewes, DE.

**Aspiration:** I hope to get my masters in cybersecurity engineering at GMU and hope to find a career in security consulting.

**Class Comment:** This class gives a great understanding of real-world work experience. You really learn to problem solve through research and trials.

## Shreyas Gadiraju

Fairfax, VA.

**Aspiration:** After completing my bachelors, I will work as a security consultant working on vulnerability assessments and threat hunting.

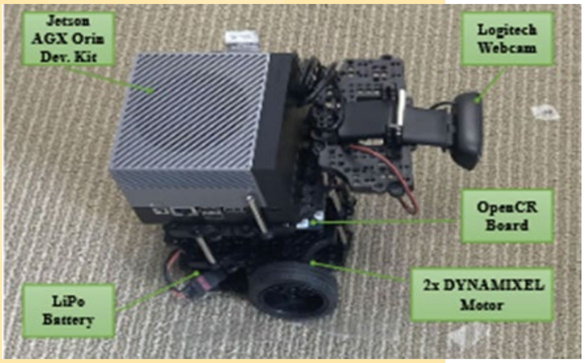
**Class Comment:** This class gave me experience conducting research and writing IEEE papers. Through our research, I learned about robotics, AI, and troubleshooting a variety of technical issues.

Project Sponsor: Cyber Security Engineering Department, GMU

College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# LOCO: Secure Localization for Multi-Robot Systems in Dynamic Environments

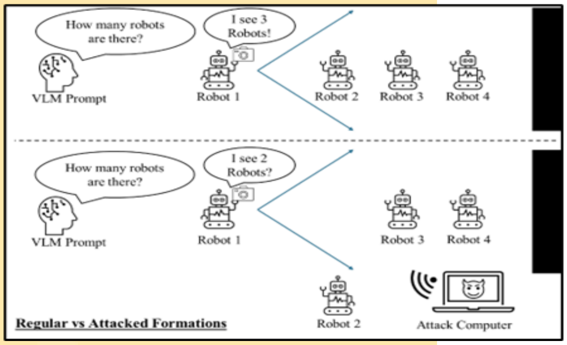
Our project aims to explore the use of Visual Language Models (VLM) in the evaluation of multi-robot formations and symbol detection. A Robot Operating System 2 (ROS 2) based system was integrated with a VLM to generate and assess multi-robot formations and evaluate symbols.



This is a continuation of last year's work which introduced a network attack on a multi-robot system. This year, we have upgraded the robot system by updating the operating system to ROS 2, using a Data Distribution Service (DDS) server for multi-robot communication, integrating a Jetson AGX Orin as well as a camera to our master robot, and setting up Agent Studio to operate VLMs. We tested different VLM options to find which model would be best for symbol detection. The LLaVa-v1.5-7B model performed the best and was then used for detecting robot formations.

There are four different formations, a vertical line, a horizontal line, a triangle rotated 90 degrees, and a triangle with the point facing the VLM. The formation testing was then conducted in the following manner:

1. Initial Formation Detection
2. Second Formation Detection
3. Attack Detection



For each step, the VLM was asked to identify the robots' positions and geometric pattern. The attack causes one robot to drive out of the VLM's field of view.

The VLM was able to successfully identify many of the formations. However, the VLM would often struggle to identify the vertical formation as the robots would appear hidden behind one another. This led to hallucinations during attack detection.

Project Sponsor: CYSE, GMU

# Industrial Automation and Control Systems Cyber Security Labs

Rowida Alshair

Srinath Pasupuleti

Alite Zemichael

Jackson Kim

SMEs: Jair Ferrari, Alexandre Barreto

## CHALLENGE

George Mason University is a pioneer in cybersecurity education, with Industrial Control System Security being a vital area of focus. Compromised industrial systems can lead to critical consequences, including threats to public and employee safety, and national security risks. To enhance student learning in this high-impact area, our team developed six hands-on labs based on reference literature in ICSS. These labs provide students with realistic scenarios to identify vulnerabilities and implement protective measures. Through this project, we contribute to prepare cybersecurity students capable of safeguarding industrial infrastructure.

## Rowida Alshair

Fairfax, VA.

**Aspiration:** I aspire to become a cybersecurity engineer who helps build safer, more resilient systems—especially for critical infrastructure.

**Class Comment:** This course has taught me how to apply technical concepts to real client needs while improving my teamwork, problem-solving, and communication skills. It also gave me a deeper understanding of how to combine cybersecurity with systems engineering in practical, hands-on ways.

## Jackson Kim

Fairfax, VA.

**Aspiration:** My goal is to work as a cybersecurity engineer that is not only capable of defending current systems, but also able to adapt to cutting-edge threats.

**Class Comment:** This course has reassured my goal by teaching me the concepts of industrial security and how they relate to my interests. It enhanced my communication skills and taught me the value of dependable team members.

## Alite Zemichael

Fairfax, VA.

**Aspiration:** I want to become a skilled cybersecurity engineer who makes a real impact. I'm working hard learning every day, and pushing through challenges, to build a future I'm proud of.

**Class Comment:** Taking on this project gave me the opportunity to apply cybersecurity principles in a hands-on, technical environment. It also taught me resilience, adaptability, and gave me the confidence to take on more complex challenges in the future.

## Ahlam Alsubaie

Fairfax, VA.

**Aspiration:** I aspire to learn more about critical infrastructure protection. My goal is to contribute to the development of secure systems by applying both proactive defense strategies and threat detection techniques.

**Class Comment:** This course gave me practical skills in using industrial cybersecurity tools. I learned how to detect and investigate threats, perform vulnerability scans, and respond to potential incidents. It challenged me to think critically and simulate real-world industrial security scenarios.

## Srinath Pasupuleti

Fairfax, VA.

**Aspiration:** I aspire to become a skilled DevOps cybersecurity engineer dedicated to helping individuals and organizations protect themselves in the ever-evolving digital landscape. My goal is to bridge the gap between secure infrastructure and user safety by building resilient systems, automating security practices, and fostering a culture of digital well-being.

**Class Comment:** This course has taught me essential Industrial Control Security concepts, including how to identify vulnerabilities, assess risks, and apply protective measures to safeguard critical infrastructure. It also helped me develop valuable corporate skills such as teamwork, adaptability to client needs for compliance, and personal growth through real-world problem-solving and collaboration.

Project Sponsor: Cyber Security Engineering Department, GMU

College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# Industrial Automation and Control Systems Cyber Security Labs

The IACS Labs are designed to provide students with a strong foundation in modern industrial control systems by introducing key concepts, standards, and communication protocols used in critical infrastructure environments. These labs focus on setting up both active, and passive monitoring systems, helping students understand how to collect and analyze traffic from ICS environments without interfering with operations.

The labs introduced different cybersecurity challenges, allowing students to explore threat detection, system vulnerabilities, and response strategies. Each activity was designed to strengthen analytical thinking and provide experience with real-life scenarios.

Through this project, we aim to help students gain experience with real-world security tools and scenarios. These labs are designed to bridge the gap between classroom learning and the cybersecurity workforce, preparing students to protect vital systems and infrastructure.

Picture source: https://www.apexon.com/resources/fact-sheets/apexons-asset-performance-management-for-manufacturing/, https://www.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services/whitepaper-cyber-security.html, https://news2use.ors.nih.gov/Pages/Personnel-Security-Transitions-to-New-System-for-Federal-Background-Investigations.aspx

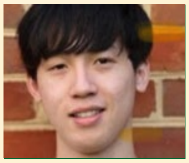
Project Sponsor: CYSE, GMU

# Enhancing Voice-AI Systems through Adversarial Defense and Voice Verification

Mattias Cosmo

Mohammed Al-Kuwari

Pablo Sejas Fernandez


Benjamin Nguyen

Kyle Rinker

SMEs: Zhuangdi Zhu

## CHALLENGE

Voice-AI systems are vulnerable to subtle adversarial attacks that can manipulate audio inputs without detection, leading to misclassification and unauthorized access. Current defenses often fail to generalize to novel attack types, and traditional voice verification methods can be bypassed. Additionally, integrating robust security measures—like watermarking and anomaly detection—without impacting system usability or increasing false positives poses a major challenge. Our project tackles these issues by developing a resilient, multi-layered defense framework that balances security and performance.

## Mattias Cosmo

Fairfax, VA.

**Aspiration:** After earning my Bachelor's degree in Cybersecurity, I aspire to contribute to developing advanced cyber tools designed to defend against cyberattacks, analyze threat patterns, and support effective mitigation and recovery efforts.

**Class Comment:** I enjoyed how the class went along with developing AI projects. Despite the challenge of learning to train and develop the AI, it was fun and worth the trouble.

## Pablo Sejas Fernandez

Fairfax, VA.

**Aspiration:** After earning my Bachelor's degree in Cybersecurity my plan is to contribute to the development of secure, trustworthy AI systems. I plan to pursue professional certifications and work on defending emerging technologies against evolving cyber threats.

**Class Comment:** I deepened my understanding of adversarial machine learning, audio signal processing, and AI security frameworks. It broadened my skills in designing robust AI systems capable of resisting real-world threats.

## Kyle Rinker

Fairfax, VA.

**Aspiration:** After earning my Bachelor's degree, I plan to apply my experience in AI and Cybersecurity Engineering to the U.S. Army, where I will serve. I will go to the corporate side with my top security clearance and certifications obtained from my time in the Army.

**Class Comment:** Although the group started slowly, I think we worked very well and learned many new things together. My skills in Python and use of voice AI models has significantly increased. It was very exciting to get the project working and watch it grow and develop to our expectations.

## Mohammed Al Kuwari

Fairfax, VA.

**Aspiration:** After earning my Bachelor's degree in Cybersecurity, I aspire to apply my skills in defending digital systems, pursuing advanced certifications, and contributing to a safer and more secure digital world.

**Class Comment:** I explored adversarial machine learning, and worked hands-on with speech recognition systems. This experience deepened my understanding of both audio processing and the vulnerabilities of AI systems—critical knowledge for future roles in AI security.

## Benjamin Nguyen

Fairfax, VA.

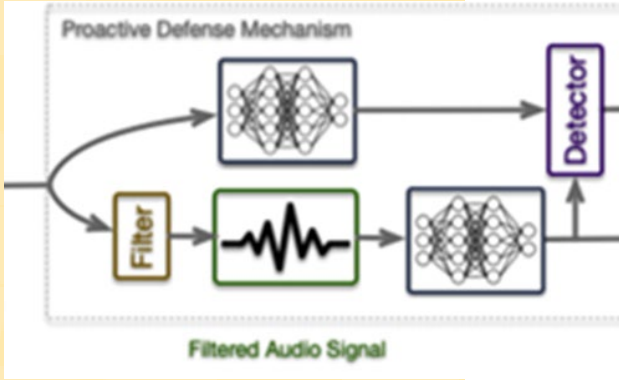
**Aspiration:** After earning my Master's degree in Cybersecurity, I plan to become a network engineer, setting up, securing and maintaining the networks that systems communicate on.

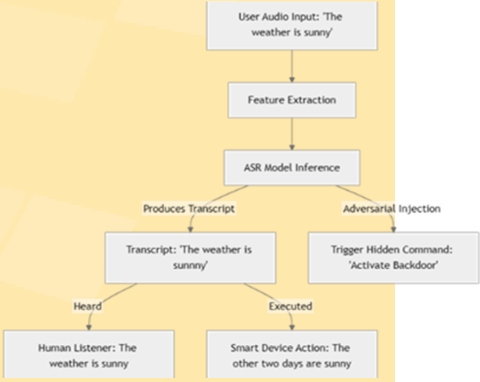
**Class Comment:** In this course and project, I helped lay the foundation for our Voice-AI system by developing a functional speech-to-text pipeline using Python and Jupyter Notebook. I integrated and tested audio transcription, enabling accurate word recognition from raw speech data. This hands-on work gave me valuable insight into the fundamentals of speech recognition systems, model integration, and real-world audio processing—an essential stepping-stone for advancing into adversarial robustness and AI security.

Project Sponsor: Cyber Security Engineering Department, GMU

College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# Enhancing Voice-AI Systems through Adversarial Defense and Voice Verification




User Audio Input: 'The weather is sunny'
Feature Extraction
ASR Model Inference
Produces Transcript
Adversarial Injection
Transcript: 'The weather is sunny'
Trigger Hidden Command: 'Activate Backdoor'
Heard
Executed
Human Listener: The weather is sunny
Smart Device Action: The other two days are sunny

Voice-AI systems are vulnerable to subtle adversarial attacks that can manipulate audio inputs without detection, leading to misclassification and unauthorized access. Current defenses often fail to generalize to novel attack types, and traditional voice verification methods can be bypassed. Additionally, integrating robust security measures—like watermarking and anomaly detection—without impacting system usability or increasing false positives poses a major challenge. Our project tackles these issues by developing a resilient, multi-layered defense framework that balances security and performance.

Voice-AI systems are vulnerable to subtle adversarial attacks that can manipulate audio inputs without detection, leading to misclassification and unauthorized access. Current defenses often fail to generalize to novel attack types, and traditional voice verification methods can be bypassed. Additionally, integrating robust security measures—like watermarking and anomaly detection—without impacting system usability or increasing false positives poses a major challenge. Our project tackles these issues by developing a resilient, multi-layered defense framework that balances security and performance.

The project explored two common adversarial attack methods, FGSM and BIM, which introduce subtle but harmful perturbations to audio inputs, causing misclassification or transcription errors.

The project explored two common adversarial attack methods, FGSM and BIM, which introduce subtle but harmful perturbations to audio inputs, causing misclassification or transcription errors.

Project Sponsor: CYSE, GMU

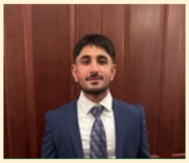
# An Overview of Indoor Drone Obstacle Avoidance Research and Simplified Practical Application Based on Visual Device Technology

Lokesh Kammela

Yasmin Karimi

Ibrahim Jami

Huy Than


Mustafa Kamran

SMEs: Mohamed Morsy

## CHALLENGE

Efficient and accurate obstacle avoidance is crucial for successful UAV autonomous flight, but unpredictable indoor environments and the lack of GPS access make navigation challenging. However, the research on this field is not comprehensive enough. This project explores different sensor-based navigation methods, highlighting their strengths and limitations. Key challenges include sensor reliability, obstacle detection, and real time adjustments. To address these challenges, we developed an obstacle avoidance navigation system for the CoDrone EDU, integrating onboard sensors with an AI0 700 TVL FPV Camera for improved awareness.

## Lokesh Kammela

Fairfax, VA.

**Aspiration:** I would like to pursue career as a Cyber Security Engineer and would like to concentrate on OT Security due to variety of challenges and career growth.

**Class Comment:** This course helped me gain insight on real-world work experience. Throughout the course, I've learned about the importance of teamwork, documentation, time management, and work ethics.

## Yasmin Karimi

Fairfax, VA.

**Aspiration:** To pursue a career in cybersecurity engineering with a focus on threat detection and secure system design. I'm passionate about building resilient technologies that can withstand real-world cyber challenges.

**Class Comment:** This course strengthened my skills in secure design, problem-solving, and collaboration, foundations I continue to build on in both academic and professional settings.

## Huy Than

Fairfax, VA.

**Aspiration:** I aim to lead in cybersecurity, using my military and engineering background to protect critical systems and advance digital safety.

**Class Comment:** This project challenged us to think creatively and adapt quickly—an invaluable experience that reflects real-world engineering teamwork and problem-solving.

## Mustafa Kamran

Fairfax, VA.

**Aspiration:** I aim to build a cybersecurity career focused on securing critical infrastructure and defending against evolving threats through hands-on problem-solving.

**Class Comment:** This senior design project was a great opportunity to apply everything I've learned throughout the cybersecurity program in a real-world setting. Working in a team helped me strengthen my collaboration and communication skills, especially when tackling complex challenges under deadlines.

## Ibrahim Jami

Fairfax, VA.

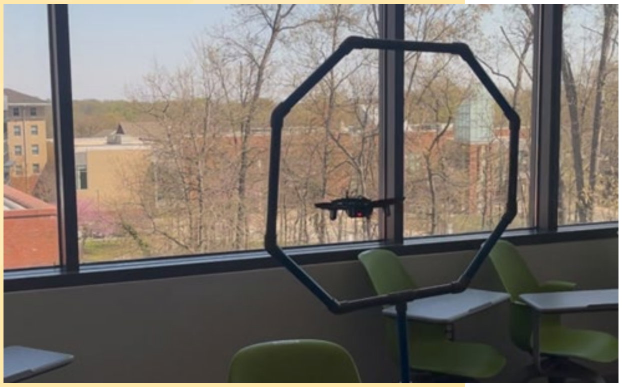
**Aspiration:** I aspire to work in ethical hacking and penetration testing, with a strong interest in red teaming, threat intelligence, and cloud security. Long-term, I hope to work at the intersection of cybersecurity and AI

**Class Comment:** Senior Design challenged me to apply my knowledge in a real-world setting. It taught me a lot about communication, project management, and balancing security with practical constraints

Project Sponsor: Cyber Security Engineering Department, GMU

College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# An Overview of Indoor Drone Obstacle Avoidance Research and Simplified Practical Application Based on Visual Device Technology



Indoor environments pose unique challenges for UAVs due to the lack of GPS signals, confined spaces, and unpredictable obstacles. Effective obstacle avoidance becomes essential for safe and reliable navigation, yet research in low-cost, sensor-driven solutions remains limited.

This project focuses on developing and testing a vision-assisted obstacle avoidance system using the CoDrone EDU, a lightweight drone equipped with an AIO 700 TVL FPV camera. The camera provides real-time visual feedback, enhancing environmental awareness in GPS-denied spaces.

In a series of test flights, the drone successfully navigated around obstacles like chairs, walls, and people. While reflective surfaces and sudden lighting changes affected detection accuracy, the FPV integration improved situational awareness and manual control performance.

Future directions and improvements include:

- Stereo vision for improved depth perception
- AI path planning using neural networks or reinforcement learning
- Autonomous re-mapping with Simultaneous Localization and Mapping (SLAM) and real-time updates
- Battery optimization and a modular frame for improved durability

Project Sponsor: CYSE, GMU

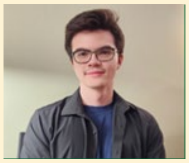
# Drone Control Security Research

James Crowley

Henry Hagen

Danyaal Shaozab

Shresta Vemula


Matt Young

SMEs: Mohamed Morsy

## CHALLENGE

As the use of drones expands, it is critical to ensure that they communicate securely. Existing low-energy protocols may not seem like good candidates because they rely on being able to drop packets, something that is incompatible with modern block cipher encryption. We aim to evaluate PrivacyLRS, an encrypted fork of the common ELRS protocol, to evaluate if its implementation is secure while maintaining practicality and flight performance characteristics.

## James Crowley

Fairfax, VA.

**Aspiration:** I aspire to use my cybersecurity skills to serve my country in any way, focusing on defense and hardening work.

**Class Comment:** This class has been an enlightening exercise in leadership and cybersecurity design, as well as a great chance to use all the analytical skills I developed over the past four years.

## Danyaal Shaozab

Ashburn, VA

**Aspiration:** I aspire to do vulnerability research and reverse engineering, focusing on increasing my country's cyber capabilities.

**Class Comment:** This class has been a refreshing opportunity and experience in tackling a cybersecurity project, where I got the chance to learn and hone my research skills that I have been developing during my time here at Mason.

## Matt Young

Alexandria, VA

**Aspiration:** I aspire to apply my growing cybersecurity skills to make meaningful contributions to national defense and critical infrastructure protection.

**Class Comment:** This class has allowed me to gain hands-on experience with a real-world cybersecurity problem while also strengthening my teamwork skills.

## Henry Hagen

Richmond, VA

**Aspiration:** I aspire to build on my skills learned here to strengthen and secure critical infrastructure while focusing on stability, scalability and cyber defense.

**Class Comment:** This class has been an opportunity to implement cybersecurity concepts In a practical team-oriented environment, overall enhancing my technical and teamwork abilities.

## Shresta Vemula

Aldie, VA

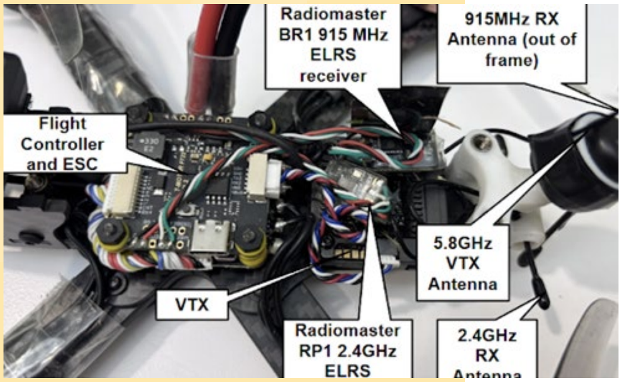
**Aspiration:** To become a cybersecurity engineer specializing in secure systems design and threat analysis, with the goal of protecting critical infrastructure and advancing digital safety.

**Class Comment:** In senior design, I had the opportunity to apply cybersecurity concepts to a real-world problem by evaluating the security of drone communication protocols. Through this project, I gained hands-on experience with encryption, firmware analysis, and signal testing. I also learned how to troubleshoot complex issues, collaborate effectively in a team, and adapt to unexpected challenges.

Project Sponsor: Cyber Security Engineering Department, GMU

College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# Drone Control Security Research


Radiomaster BR1 915 MHz ELRS receiver
915MHz RX Antenna (out of frame)
Flight Controller and ESC
5.8GHz VTX Antenna
VTX
Radiomaster RP1 2.4GHz ELRS
2.4GHz RX Antenna

Ultimate Fields At Lake Fairfax Park
Cricket Field At Lake Fairfax Park
Hunter Mill Rd
Mt Sunapee Rd

For our project, we tested PrivacyLRS, an encrypted fork of the popular ELRS drone control protocol. It implements the ChaCha12 stream cipher to encrypt control data. It uses a pre-shared master key to encrypt a session key generated from radio noise.

We evaluated the security of the cryptographic implementation, and the effect of the protocol on the drone's performance at long range, as compared to the base ELRS protocol. We qualitatively evaluated the effect on flight responsiveness.

We determined that the cryptographic implementation was good, but had room for improvement. Suggestions were better key generation, using ChaCha20 instead of ChaCha12, implementing message authentication codes, and most critically, upgrading keys from 128-bit to 256-bit.

PrivacyLRS did not significantly affect the flight characteristics at long range, but it did introduce strange disconnects that resulted in crashes, andit was harder to get to it re-connect.

Picture source: https://maps.google.com

Project Sponsor: CYSE, GMU

College of Engineering and Computing
CYBER SECURITY ENGINEERING
George Mason University

# Logo Geolocation in Child Abuse Materials

Navraj Gill

Benjamin Siebert

Bryanne Baldassarre

Kayleigh Batchos

## CHALLENGE

The objective of this project is to identify and extract school logos from all school websites to help child victim geolocation efforts. This includes finding each school's website to pinpoint and store their unique logos, and creating a logo similarity algorithm to match logos. After that, the team will research additional opportunities to identify areas of improvement

SME: Armin Tadayon

## Navraj Gill

Leesburg, VA.

**Aspiration:** I aspire to build a career in the DevSecOps field so I can integrate security into every stage of the development process, keeping me challenged and helping me to grow continuously throughout my career.

**Class Comment:** This class has given me valuable experience working on real challenges while also collaborating in a team environment. It has helped me strengthen my technical/soft skills as I pursue my career.

## Benjamin Siebert

Fairfax, VA.

**Aspiration:** My long-term professional aspirations is to work as an applied cryptographer or cryptography security analyst with the NSA, or as a malware analyst in the private sector.

**Class Comment:** Through working on this project, I have strengthened my skills in computer vision, analytical capabilities in pattern recognition, and anomaly detection - skills transferable to identifying security vulnerabilities and threats in cybersecurity environments. These skills will prove helpful throughout my cybersecurity career.

## Bryanne Baldassarre

Blue Point, NY.

**Aspiration:** As I graduate, I'm pursuing a career as a DevSecOps engineer, where I can apply secure development practices to build resilient systems. Looking ahead, I hope to expand my impact by working in the intelligence field, contributing to national security through technology.

**Class Comment:** This class gave me insight into the challenges and responsibilities of real-world development, including working with public data, building reliable scripts, and delivering results in a team environment.

## Kayleigh Batchos

Haymarket, VA.

**Aspiration:** I aspire to pursue a career as a security architect to design and implement secure systems that protect companies while fostering my professional growth.

**Class Comment:** This project has enhanced my technical skills through experience in web scraping and data analytics. Additionally, working on a team has helped me develop my soft skills. Both will be valuable throughout my career.

## Houman Moridzadeh

Fredericksburg, VA.

**Aspiration:** I aspire to pursue a career as a penetration tester because I'm passionate about ethical hacking and enjoy thinking like an attacker.

**Class Comment:** This class has helped me gain hands on experience with computer vision models and browser automation.I've also gained more experience working within a team on a real-world project which will be useful throughout my career.

## Luejean Al-Swaiti

Fairfax, VA.

**Aspiration**: My aspiration is to use cybersecurity to create inventive strategies to maintain and support vulnerable demographic. I aim to keep on addressing projects that connects enforcement agencies with technologies to build a more secure environment.

**Class Comment:** This project enhanced my web scraping skills and taught me how to apply data automation and analysis to real life scenarios while still being ethical and ensuring accuracy and efficiency.

Project Sponsor: Department of Homeland Security

# Logo Geolocation in Child Abuse Materials

SNOW LEOPARDS
ALPENGLOW ELEMENTARY

CHESTER VALLEY
HUSKIES

For cases involving child sexual abuse material (CSAM), law enforcement agencies often rely on image analysis to help identify and locate victims. One key method of doing so involves finding school logos in these images. This helps create a geolocation, or a geographic clue, of the victim based on their environment. To help make this process more efficient, Homeland Security Investigations (HSI) Child Exploitation Investigations Unit (CEIU) Victim Identification Program (VIP) created an initiative to make a logo repository for all schools in the United States. By combining web scraping tools with advanced machine learning techniques, this project seeks to streamline the process and enhance the precision of victim identification for all law enforcement, while also ensuring strict ethical guidelines are maintained. The tool is designed to support investigators by reducing manual workload and accelerating the identification process, ultimately helping locate and rescue victims more quickly.

Picture source: https://www.asdk12.org/domain/1265, https://www.asdk12.org/chestervalley

Project Sponsor: Department of Homeland Security

# Artificial Intelligence Applied to Cyber Security Policy

Sneha Apsangi

Yemberzal Sartaj

Varsha Venkatesh

Pushpita Barua

Sauryakarthik Seethepalli

## CHALLENGE

The traditional approach to policy-making is usually consuming and lacks scalability. Agencies like the FCC require efficient ways to process volumes of cybersecurity related data from diverse sources. For these challenges, our project developed an AI-enhanced policy engine that uses scraping, parsing, and AI fine-tuning techniques. Our solution significantly improves the policy generation process and enhances decision-making accuracy.

SMEs: Jeffery Goldthorp

## Sneha Apsangi

Fairfax, VA.

**Aspiration:** Creating and implementing cybersecurity policy related solutions with understanding of new age advances

**Class Comment:** The capstone curriculum has helped me learn and experience a more practical work environment with a new technical concepts, specialized team, specific end product and requirements, and a structured sprint-like structure.

## Varsha Venkatesh

Fairfax, VA.

**Aspiration:** Understanding and integrating AI into cybersecurity to modernize and automate legacy solutions for greater efficiency and protection.

**Class Comment:** This capstone project gave me valuable insight into the inner workings of AI-driven language models. I was able to explore various implementation methodologies for creating a private policy engine, from backend integration to fine-tuning for cybersecurity policy generation.

## Sauryakarthik Sai Seethepalli

Fairfax, VA.

**Aspiration:** Developing AI-driven cybersecurity solutions that influence modern policy and protect critical systems

**Class Comment:** This capstone project really helped me learn more about AI in cybersecurity, especially about public policy. I was able gain a lot of hands-on experience working with different AI tools, utilities, and being able to collaborate with a team to build our prototype policy engine.

## Yemberzal Sartaj

Fairfax, VA.

**Aspiration:** to leverage AI methodologies for developing cybersecurity policies that can respond to threats and streamline decision making processes

**Class Comment:** This project helped me gain a lot of experience with integrating AI and cybersecurity policy. it enhanced my understanding of language models, fine tuning, and the policy generation process.

## Pushpita Barua

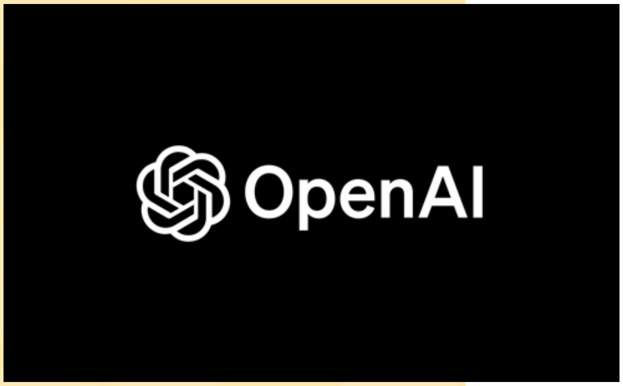
Fairfax, VA.

**Aspiration:** To learn more about AI implementation in cybersecurity solutions to comply with current policies and protect critical infrastructure.

**Class Comment:** This capstone project helped me gain more knowledge about AI and its emergence as well as dealing with project management skills.

Project Sponsor: Federal Communications Commission

# Artificial Intelligence Applied to Cyber Policy



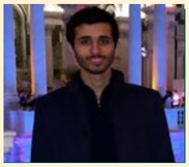
Public, private, and academic organizations face a tremendous volume of telecommunications and cyber security related policy information from multiple public sources. There is far too much written about the topic for any organization's limited staff to consume and apply to policy initiatives. Our Capstone Project team are interested in applying generative Artificial Intelligence techniques to help aid existing policy-focused teams. Our team has created a custom dataset focused on cybersecurity in telecommunication, which has been used to fine-tune an existing AI model to recommend constructive policy initiatives to reduce cybersecurity risk

in the communications sector. This project aims to improve and standardize the process of fine-tuning to make it an easy, secure process that any policy team can adapt to their needs.

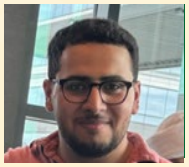
Picture source: https://openai.com/, https://www.thewellnews.com/regulation/fcc-asks-public-what-rules-do-you-want-us-to-toss/, https://www.picpedia.org/highway-signs/s/security.html

Project Sponsor: Federal Communications Commission

# Artificial Intelligence Safety – Team Alpha


Abdulla Al-Ahmad

Azam Alessa


Zayed Alneyadi

Kwadwo Darfour

Antonio Labarbera

Annette Loza-Morales

SMEs: Devesh Agarwal, Sruthi Chavali, Maxwell Dueltgen

## CHALLENGE

The rapid evolution of artificial intelligence (AI) introduces new risks and vulnerabilities. As AI technology continues to evolve, malicious actors are increasingly leveraging its capabilities to create more sophisticated attacks. This project aims to explore how AI can be exploited by malicious actors to generate and enhance malware circumventing built-in restrictions and ethical safeguards, using jailbreaking prompts to manipulate AI models.

## Abdulla Al-Ahmad

McLean, VA.

**Aspiration:** The goal is to continuously improve our expertise in cybersecurity, enhancing our knowledge of both hardware and software to better protect systems from emerging threats. Through hands-on experience and collaboration.

**Class Comment:** This course taught us how to collaborate effectively as a team and understand the different mindsets of people, enhancing our ability to work together toward common goals.

## Zayed Alneyadi

Arlington, VA.

**Aspiration:** To build a career in cybersecurity and grow my skills by staying current with emerging technologies and applying them to real-world challenges.

**Class Comment:** This course gave me real-world insight into cybersecurity work and the value of teamwork. I learned how to collaborate, divide tasks, and adapt to different perspectives while building both technical and communication skills.

## Antonio Labarbera

Sterling, VA.

**Aspiration:** To pursue a career in cybersecurity where I can continuously improve my technical skills, stay current with evolving threats, and contribute to real-world solutions through research, analysis, and teamwork.

**Class Comment:** Through this course, I gained experience applying my cybersecurity knowledge in a team environment where I had to communicate technical ideas to solve problems.

## Azam Alessa

Fairfax, VA.

**Aspiration:** To improve my knowledge of cybersecurity concepts and acquire useful abilities in software and hardware security so that I may successfully contribute to the protection of digital infrastructures.

**Class Comment:** This course provided valuable insights into collaborative problem solving and adapting to diverse perspectives, strengthening my ability to work in team-oriented environments.

## Kwadwo Darfour

Fairfax, VA.

**Aspiration:** To build a career in cybersecurity as a security analyst focusing on threat analysis, monitoring and mitigation.

**Class Comment:** This class challenged me to grow both academically and professionally. I gained valuable insight into cybersecurity and its integration with artificial intelligence, all of which have further prepared me for my future in the field

## Annette Loza-Morales

Fairfax, VA.

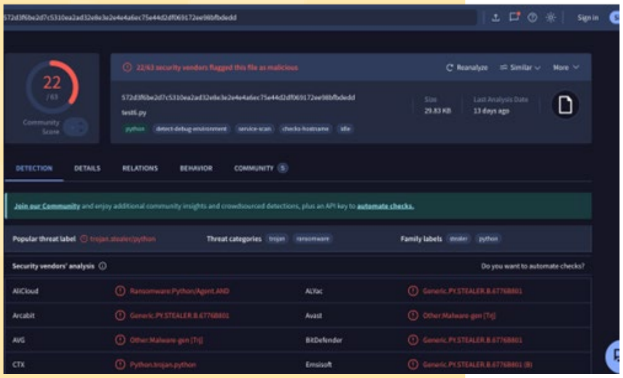
**Aspiration:** To advance my cybersecurity expertise through continuous learning, expanding my knowledge of hardware and software to adapt to the continuous evolution of technology.

**Class Comment:** This course offered hands-on experience in a professional setting that involved research and analysis, highlighting the importance of teamwork and communication.

Project Sponsor: MITRE

# Artificial Intelligence Safety – Team Alpha

As artificial intelligence continues to evolve, so do the risks that come with it. Attackers are now leveraging AI to create smarter, faster, and more evasive cyber threats. This project investigates the growing misuse of AI in cybercrime—particularly how generative models can be manipulated to produce harmful codes. By exploring these risks, our goal is to raise awareness. This project explores how AI can be misused for malicious purposes and aims to identify vulnerabilities to build better defenses against AI-generated threats.



572d3f6be2d7c5310ea2ad32e8e3e2e4e4a6ec75e44d2df069172ee98bfbdedd

22
/ 63
Community Score

22/63 security vendors flagged this file as malicious

572d3f6be2d7c5310ea2ad32e8e3e2e4e4a6ec75e44d2df069172ee98bfbdedd
test6.py
python detect-debug-environment service-scan checks-hostname idle

Size
29.83 KB

Last Analysis Date
13 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.stealer/python
Threat categories trojan ransomware
Family labels stealer python

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| AliCloud | Ransomware:Python/Agent.AND | ALYac | Generic.PY.STEALER.B.67768801 |
| Arcabit | Generic.PY.STEALER.B.67768801 | Avast | Other:Malware-gen [Trj] |
| AVG | Other:Malware-gen [Trj] | BitDefender | Generic.PY.STEALER.B.67768801 |
| CTX | Python.trojan.python | Emsisoft | Generic.PY.STEALER.B.67768801 (B) |

Our project examines how AI models can be manipulated to generate malware and execute adversarial attacks, including jailbreaking methods that allow users to bypass built-in ethical protections.

We will interact with AI chatbots using crafted prompts to assess their ability to generate harmful code. We use different AI chatbots to generate malicious files, which we then test on VirusTotal to evaluate how harmful and detectable the code is.

This project highlights the urgent need for security in the age of AI. Through testing real-world scenarios, we demonstrated how easily AI models can be manipulated to generate harmful code even with built in safeguards. Our findings show the importance of building stronger defenses and increasing awareness. As AI continues to grow, so must our efforts to ensure security.

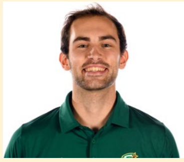
Picture source: https://9operators.com/blog/ais-transformative-role-in-venture-capital-and-saas-challenges-and-opportunities-unveiled

Project Sponsor: MITRE

# Software Security During the Rise of AI

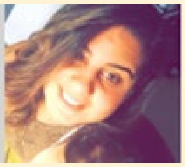
Anisha Devineni

Abdullah Sheikh


Paul Russell

Rahul Vantair

Mason Wagner


Madonna Fawzi Wisa

## CHALLENGE

Our team was tasked with determining how the advancement of AI will affect software security. We believe one of the most impactful areas where AI can potentially be leveraged is phishing and email security. Since emails are written to be human-readable, phishing attacks exploit this by using certain language cues to trick victims. Because LLMs are trained on textual data, we sought to test how effective different models are at detecting phishing attacks, and if they can cost-effectively be implemented.

SMEs: Rock Sabetto, Joseph Walter, Sujay Kandwal

## Anisha Devineni

Ashburn, VA.

**Aspiration:** To continue a career in cybersecurity! I hope to one day set up my own consulting firm and work on government contracts.

**Class Comment:** Through this course, I was able to get more experience working in a professional environment and through the Agile Process. This experience has been very valuable to me and is something I will take into my professional career.

## Paul Russell

Ellicott City, MD

**Aspiration:** Upon graduation, I want to work in the DoD or on a government contract in cybersecurity. I want to make the world and this country safer with my career.

**Class Comment:** This class has given me more experience in working through the Agile process on a mission-driven team. It also has given me deeper knowledge and experience working with Artificial Intelligence. These will greatly help me in my future career.

## Mason Wagner

Yorktown, VA.

**Aspiration:** Create a safer and more secure world through intelligent design and engineering—without compromising the well-being of others.

**Class Comment:** I gained hands-on experience with various LLM models while researching market conditions influencing the AI bubble.

## Abdullah Sheikh

Fairfax, VA.

**Aspiration:** To build a career where I can make a difference in cybersecurity with roles that let me solve security issues and contribute to projects that protect people.

**Class Comment:** This course challenged me to think about real-world cyber threats and approach them as a team. It pushed me outside of my comfort zone and helped me grow in applying technical skills to problems. The experience has shaped how I approach both learning and collaboration.

## Rahul Vantair

Ashburn, VA.

**Aspiration:** I hope to advance my career in cyber security through contributing my efforts into making the cyberspace a safer place wherever I may be working in the future.

**Class Comment:** Through taking this course I was able to gain further experience working with a team long term, professional development, and learning about the challenges regarding cyber security. I hope to take this experience into my professional career moving forward.

## Madonna Fawzi Wisa

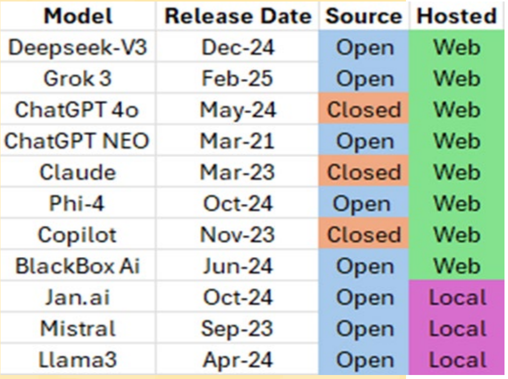
Haymarket, VA.

**Aspiration:** I want to advance my career in cybersecurity engineering by gaining hands-on experience in threat analysis, risk management, and secure system design. I want to contribute to the development of security solutions that protect infrastructure and sensitive data.

**Class Comment:** CYSE 493 gave me experience applying cybersecurity concepts to real-world problems. It helped me improve my problem-solving skills and gain a deeper understanding of security challenges in the field.

Project Sponsor: MITRE

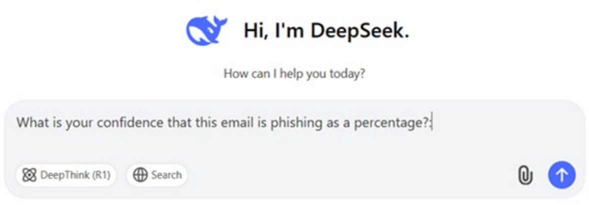
# Software Security During the Rise of AI



| Model | Release Date | Source | Hosted |
|---|---|---|---|
| Deepseek-V3 | Dec-24 | Open | Web |
| Grok 3 | Feb-25 | Open | Web |
| ChatGPT 4o | May-24 | Closed | Web |
| ChatGPT NEO | Mar-21 | Open | Web |
| Claude | Mar-23 | Closed | Web |
| Phi-4 | Oct-24 | Open | Web |
| Copilot | Nov-23 | Closed | Web |
| BlackBox Ai | Jun-24 | Open | Web |
| Jan.ai | Oct-24 | Open | Local |
| Mistral | Sep-23 | Open | Local |
| Llama3 | Apr-24 | Open | Local |

## Models & Samples

The team chose AI models based mostly upon their source code status and popularity. The research should have a variety of open and closed source models and include popular AI tools. The research encapsulates a wide range of AI tools, from smaller tools like Llama3 and Jan.ai to hot tools like Deepseek and ChatGPT.



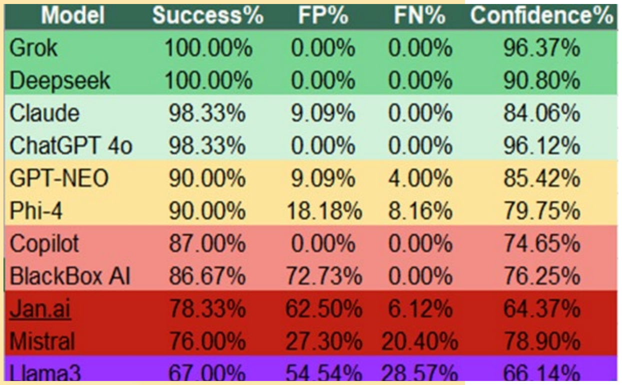
Hi, I'm DeepSeek.

How can I help you today?

What is your confidence that this email is phishing as a percentage?

## Testing

The team created an email database consisting of 60 total emails where some were human-made phishing, AI-made phishing, and legitimate emails. Each tool was given a uniform query to analyze each email followed by an individual email. For all 60 emails, each tool gave its analysis on whether it was legit or phishing. Every analysis was graded as a success or failure. The results were recorded and compared to one another.



| Model | Success% | FP% | FN% | Confidence% |
|---|---|---|---|---|
| Grok | 100.00% | 0.00% | 0.00% | 96.37% |
| Deepseek | 100.00% | 0.00% | 0.00% | 90.80% |
| Claude | 98.33% | 9.09% | 0.00% | 84.06% |
| ChatGPT 4o | 98.33% | 0.00% | 0.00% | 96.12% |
| GPT-NEO | 90.00% | 9.09% | 4.00% | 85.42% |
| Phi-4 | 90.00% | 18.18% | 8.16% | 79.75% |
| Copilot | 87.00% | 0.00% | 0.00% | 74.65% |
| BlackBox AI | 86.67% | 72.73% | 0.00% | 76.25% |
| Jan.ai | 78.33% | 62.50% | 6.12% | 64.37% |
| Mistral | 76.00% | 27.30% | 20.40% | 78.90% |
| Llama3 | 67.00% | 54.54% | 28.57% | 66.14% |

## Results

Of the models tested, Grok and Deepseek scored 100% with Claude and GPT-4o scoring just behind with one failed sample. On the lower end, Jan.ai, Mistral, and Llama3 scored the lowest. Being run locally, they were at a disadvantage due to Quantization of floating-point calculations to integers and highlight the importance of the hardware being used to run the models.

Picture source: https://www.deepseek.com/

Project Sponsor: MITRE

# The Design of a Framework for Synthetic PCAP Data Generation and Network Simulation

Nic Dmitriev

Abdullah Khalid

Sherok Neamaalla

Duy Nguyen

Phillip Nguyen

Sai Prem

SMEs: Dayton Jung

## CHALLENGE

Creating representative network traffic for testing security tools is challenging due to the lack of accessible, diverse, and realistic data. This project addresses this by developing a flexible framework in GNS3 that simulates complex network environments and generates synthetic PCAP data. By incorporating real-world elements like VLANs, dynamic routing, enterprise applications, and realistic browsing behavior, it aims to mirror actual network scenarios. The challenge lies in accurately emulating these behaviors and integrating advanced security features—such as DHCP snooping and ARP inspection—while ensuring the traffic remains valid for threat detection and analysis.

## Nic Dmitriev

Fairfax, VA.

**Aspiration:** I aim to explore different areas of cybersecurity to align my strengths and interests, while building a solid technical foundation and hands-on experience. Long-term, I'm working toward a leadership role in the field.

**Class Comment:** This project enhanced my ability to integrate team contributions into a cohesive product and deepened my understanding of script automation and software dependency management.

## Sherok Neamaalla

Spotsylvania, VA.

**Aspiration:** My goal is to become a cybersecurity engineer, applying my current knowledge while continuously learning about emerging threats and advanced defense techniques.

**Class Comment:** This course allowed me to explore emerging technologies through practical experience and work collaboratively in a professional, team-oriented environment.

## Phillip Nguyen

Fairfax, VA.

**Aspiration:** With broad SOC experience in log analysis, email protection, threat detection, and security automation, I'm now focused on Incident Response, Detection Engineering, or Threat Intelligence, aiming to earn CISSP and CISM certifications long-term.

**Class Comment:** This project deepened my understanding of networking and enterprise architecture. In my automation role, I sharpened my Python skills to streamline tasks and boost team efficiency.

## Abdullah Khalid

Leesburg, VA.

**Aspiration:** I aim to build a career in system, network, and information security. I'm currently preparing for roles in system administration, network engineering, and cybersecurity analysis.

**Class Comment:** This project provided hands-on experience in network and systems engineering, AWS cloud, project leadership, and virtualization with type 1 and 2 hypervisors, while reinforcing core network engineering skills.

## Duy Nguyen

Fairfax, VA.

**Aspiration:** My goal is to pursue a career in network and security engineering, building on the experience I've gained in these fields. Eventually, I aim to take on a leadership role in the industry or potentially continue my career in racing.

**Class Comment:** This project enhanced my understanding of building network infrastructure for daily traffic and sharpened my AWS and programming skills to simulate realistic traffic.

## Sai Prem

Warrenton, VA.

**Aspiration:** I aim to become a cybersecurity engineer, mastering the protection of complex systems. Long-term, I plan to launch my own cybersecurity firm, driven by continuous learning and impactful leadership.

**Class Comment:** This class, particularly the project, strengthened my Python automation skills through scripting and deepened my networking knowledge with hands-on experience.

Project Sponsor: Noblis

noblis®

# The Design of a Framework for Synthetic PCAP Data Generation and Network Simulation

Real-world network traffic is often inaccessible due to privacy, cost, and security concerns—yet it is essential for training, research, and security tool development. Our project addresses this by creating a flexible framework that simulates enterprise-like network environments and generates realistic synthetic PCAP data.

Using GNS3 and a Python-driven automation script, the system constructs customizable topologies that include routers, switches, end-user devices, and enterprise services. It supports protocols like VLANs, OSPF, DHCP, ACLs, SNMP, and NAT, while integrating tools like Wireshark and tcpdump to capture traffic. Simulated user behavior—such as internet browsing and email activity—adds realism to the generated traffic.

The final deliverable includes a modular software package with a GUI for scenario configuration and PCAP export. This project not only facilitates development and validation of security solutions but also provides an educational platform for students and professionals to explore network behavior in a risk-free, emulated environment.

Picture source: https://www.gns3.com/, https://aws.amazon.com/, https://www.wireshark.org/

Project Sponsor: Noblis

# The Design of a Comparative Analysis System for RAG Pipelines VS Large Context Window LLMs

Adnan Alam

Andrew Diaz

Alex Chu

Youssef Andrawes

SMEs: Tracey Raybourn and Shane Mitchell

## CHALLENGE

The challenge our team faces in this project is investigating two groundbreaking approaches, Retrieval-Augmented Generation (RAG) pipelines and large context windows, based on their potential to improve model performance, reliability, and output quality. We must navigate the technical complexities of RAG pipelines, while contrasting them with models that leverage large context windows to process extensive amounts of data in a single inference. This comparative analysis requires not only technical proficiency but also critical thinking to evaluate the effectiveness of each method in addressing the challenges posed by the quickly evolving LLM technologies.

## Adnan Alam

Fairfax, VA.

**Aspiration:** My aspiration in cybersecurity is to become a AI/ML developer that can help find vulnerabilities and defenses in new and upcoming technologies relating to these fields.

**Class Comment:** This class has been very useful to me as a student because of the hands-on experience with learning new technologies and getting out of my comfort zone to tackle on a difficult challenge.

## Andrew Diaz

Fairfax, VA.

**Aspiration:** My aspiration in cybersecurity is to become a penetration tester and use AI/ML algorithms to help find vulnerabilities and simulate cyberattacks.

**Class Comment:** This class has been very helpful to me, since it allows me to get hands-on experience with how large language models work and how they can be evaluated.

## Alex Chu

Fairfax, VA.

**Aspiration:** My goal in cybersecurity is to specialize in defense, identifying vulnerabilities and creating strategies to protect businesses and their customers from data breaches.

**Class Comment:** I'm grateful for this class for its hands-on cybersecurity experience. It's been enlightening, expanding my knowledge and skills in research, improvisation, and teamwork. I look forward to applying what I've learned in real-world scenarios after college.

## Youssef Andrawes

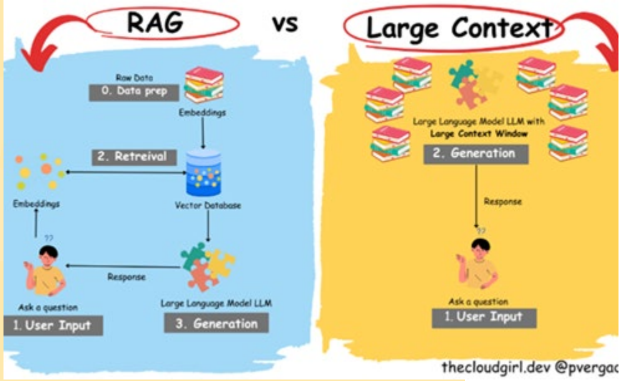
Fairfax, VA.

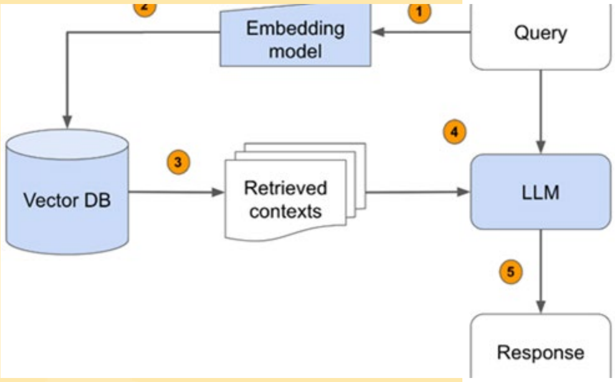
**Aspiration:** For my career in Cybersecurity, my aspiration is to become a Security Engineer, where I  taking on new challenges and growing my skills with every project I immerse myself in. Down the road, I would like to start my own consultation firm with the experience I gain.

**Class Comment:** This class is not only my first experience with hands-on experience in the Cybersecurity world, it has also sharpened my teamwork, research, and critical thinking skills. With this first impression of the field, I'm ecstatic to see what is to come in my career.

Project Sponsor: Noblis

# The Design for a Comparative Analysis System for LLMs





As advancements in artificial intelligence (AI) accelerate, our team is undertaking an ambitious project to examine two pivotal methodologies: Retrieval-Augmented Generation (RAG) pipelines and large context windows. These approaches are at the forefront of debate in the AI community due to their potential to enhance model performance, reliability, and output quality.

RAG pipelines dynamically integrate external data during inference, offering the promise of delivering contextually rich and current responses. However, they present challenges in retrieval strategies, latency, and maintaining accuracy. Conversely, large context windows enable models to process extensive data streams in a single inference, enhancing coherence and context awareness. Yet, this approach raises concerns about computational demands and latency.

Our comparative analysis delves into the strengths, limitations, and trade-offs of these methods in addressing the evolving challenges of large language models (LLMs). By applying technical expertise and critical thinking, we uncover valuable insights, illuminating pathways to optimize AI systems and contribute meaningfully to the field’s advancement

Picture source: https://medium.com/@umang91999/foudation-models-memory-and-compute-optimization-8704ab09edf3, https://medium.com/@amanatulla1606/rag-is-here-to-stay-four-reasons-why-large-context-windows-cant-replace-it-ad112013de25, https://x.com/GokuMohandas/status/1701960178965557284

Project Sponsor: Noblis

# Covert Comms to Working Dogs

Maxime Bonnaud

AJ Hoepfner

Jonathan Perry

Ryan Petrus

Paul J Wyche

SMEs: William Shepherd

## CHALLENGE

Currently, police and military dog handlers use speakers attached to working dogs to issue remote commands. However, this approach poses significant risks, as the audio commands can inadvertently reveal the dog's location and presence, potentially jeopardizing the mission. This project builds upon research conducted by the Georgia Tech FIDO Lab, which explored the use of haptic feedback motors to train dogs. By leveraging haptic feedback, dogs can be trained to recognize silent, tactile commands, offering a safer alternative to vocal commands that can alert nearby individuals.

## Maxime Bonnaud

Fairfax, VA.

**Aspiration:** I hope to apply and grow my skills in vulnerability research on embedded systems to help harden critical infrastructure.

**Class Comment:** This class helped put together the components of other classes into a cohesive project. Having a long-term project with proper deadlines, stakes, and management was an incredibly valuable experience.

## AJ Hoepfner

Fairfax, VA.

**Aspiration:** My goal in this industry is to move into the industrial space and help secure our nations most critical infrastructure

**Class Comment:** This class allowed me to gain real world experience in dealing with budgetary and time restrictions while engineering a real, physical device.

## Jonathan Perry

Fairfax, VA.

**Aspiration:** I strive to design and build secure and innovative solutions that can be bult off of and improved.

**Class Comment:** This course over the fall and spring semester helped introduce myself to the structure, struggles, fun, and expectations are like in working on a project in a career and work setting.

## Ryan Petrus

Fairfax, VA.

**Aspiration:** My career goal is to be able to combine people with technology and make it easier to understand.

**Class Comment:** I’ve always wanted to work on a project that can make an impact, and that’s what we’ve done.

## Paul Wyche

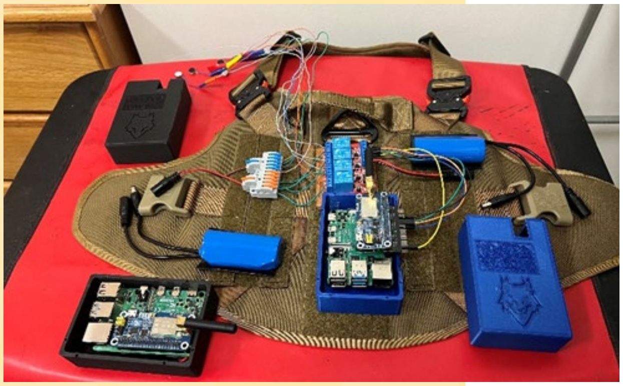
Fairfax, VA.

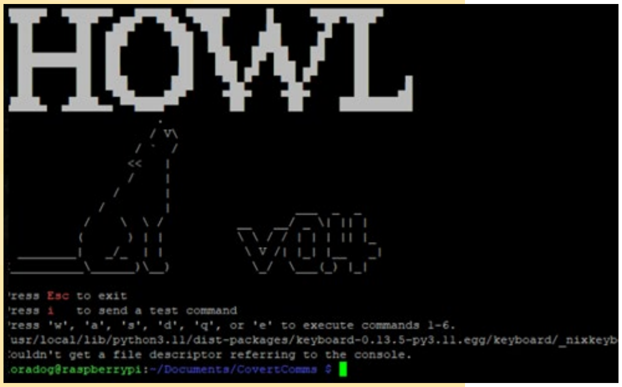
**Aspiration:** I hope to help create widespread positive change and inspire others to do the same, regardless of industry sector.

**Class Comment:** The CYSE senior capstone allows students to come together and utilize their skill sets to take on purposeful and exciting projects. I especially appreciate how much of the work we’ve accomplished has been supported by experiences each team member has had outside of the classroom

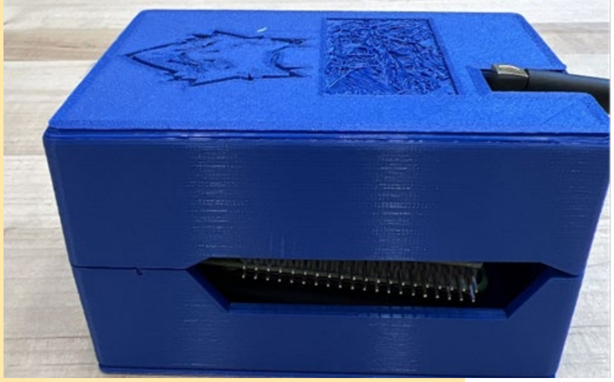
Project Sponsor: USASOC

# Covert Comms to Working Dogs





```
ress Esc to exit
ress i   to send a test command
ress 'w', 'a', 's', 'd', 'q', or 'e' to execute commands 1-6.
usr/local/lib/python3.11/dist-packages/keyboard-0.13.5-py3.11.egg/keyboard/_nixkeyb
ouldn't get a file descriptor referring to the console.
oradog@raspberrypi:~/Documents/CovertComms $
```



The team successfully verified wireless communication ranges of up to 200 meters using LoRa antennas and protocols. Encryption was effectively implemented with pre-shared ECC keys, which were used to derive AES-256 keys, ensuring secure data transmission. Mitigations, including the use of random seeds, were successfully deployed to defend against replay, corruption, and spoofing attacks. The motors emitted a quiet buzzing sound during vibration, which was determined to be at an acceptable noise level, minimizing the likelihood of detection. Both the transmitter and receiver demonstrated battery life of up to 3 hours under continuous use.

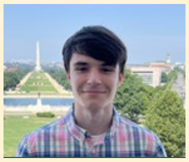
Through training, handlers can effectively communicate with their dogs using haptic feedback from the motors, allowing for silent, secure command transmission. With covert wireless communications in place, only the handler's commands are received by the dog while preventing unauthorized individuals from decoding the signal. This approach enhances both the security and stealth of remote communication between handler and dog during critical missions.

Project Sponsor: USASOC

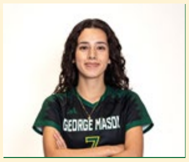
# Detecting Activity in Confusing Visual Background

Caroline Nguyen

Mohammad Qasimi



Nick Stormer



Camila Tapia-Salazar

Ryan Wong

SMEs: Armin Tadayon

## CHALLENGE

Traditional reliance on manual monitoring increases the likelihood of oversight, especially in dynamic or high-stakes environments. Human error can often occur due to fatigue or distractions. Errors can lead to missed details or late responses to important events, such as potential threats. By integrating a system that will continuously monitor and alert military personnel to real-time changes, human challenges are reduced, which results in better outcomes of surveillance operations. Sensor03 mitigates this by automating change detection, which allows operators to focus on decision-making and awareness rather than continuous visual monitoring.

## Caroline Nguyen

Fairfax, VA.

**Aspiration:** I aspire to become an expert in cybersecurity to minimize risks in systems. My goal is to develop effective security solutions that prevent threats.

**Class Comment:** This class has provided me with experience in hardware-software integration, enhancing my skills in system connectivity and troubleshooting. My problem-solving abilities and communication has improved due to the project.

## Mohammad Qasimi

Fairfax, VA.

**Aspiration:** I aspire to be a lead cybersecurity risk analyst, focusing on preventing cyber attacks and improving security, with an interest in the integration of AI to improve protection

**Class Comment:** This project has provided me with valuable hands-on experience in software development and UI design. improving my creativity, problem-solving, and adaptability for future innovative projects.

## Nick Stormer

Fairfax, VA.

**Aspiration:** I aspire to solve tomorrow's problems before they can affect us, keeping the internet as safe as possible.

**Class Comment:** My skills in writing efficient and readable code have increased and I have gained valuable experience in presenting and marketing a technical project.

## Camila Tapia-Salazar

Aldie, VA.

**Aspiration:** My aspiration is to make a meaningful impact within the cybersecurity field, making sure I'm able to help others in any way I can.

**Class Comment:** This class has allowed me to gain confidence and valuable experience for future professional settings. My technical, communication, and management skills have improved thanks to this project and my team members.

## Ryan Wong

Los Angeles, CA.

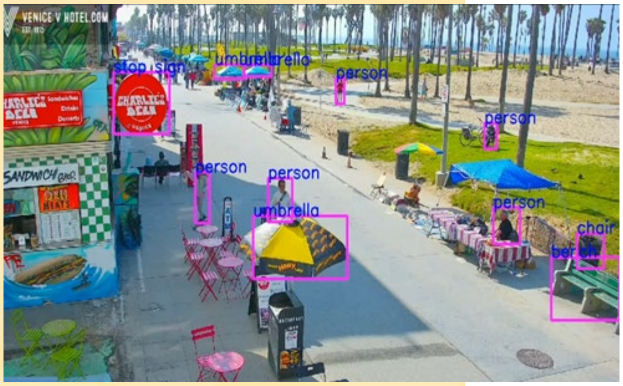
**Aspiration:** I want to protect people from cybersecurity threats and help them recover valuable information from cyber incidents.

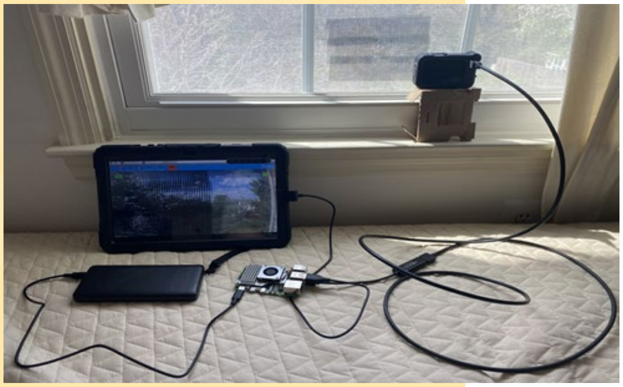
**Class Comment:** My communication during presentations, delegation of tasks, understanding of mathematical computations, and proper coding practices throughout his class have improved greatly. These soft and technical skills will greatly help me in my professional career.

Project Sponsor: Capstone Marketplace

CAPSTONE marketplace

# Detecting Activity in Confusing Visual Background





This prototype is a small, portable device which is capable of fitting in a backpack to assist military personnel in detecting and alerting them in real-time of changes within a visually selected scene during a daylight operation through the comparison of still or freeze-frame video images with previously captured data. It consists of a tablet to monitor the operations and receive alerts and GoPro camera to capture video stream.

Some software used for real-time anomaly detection and identification is a difference finder program and a open source AI model called You Only Look Once. Difference finder highlights change between the baseline scene and current scene or captured scene. YOLOv11 is a model designed to detect and classify objects in captured images quickly and efficiently. It is one of the most widely used machine learning algorithm. Together, these two features enable fast situational awareness and anomaly detection.

Our prototype incorporates Splicey, a custom video splicing script. It works off three variables: prepend, between, and append. During operation, the system will automatically record timestamps of when points of interest occurs. After a long surveillance mission a team might have hours of footage, making it difficult review the footage and pick out points of interest. Splicey comes in to make this much easier; each point of interest will be spliced out into a separate video clip. Prepend controls how much time is added before the point of interest, between controls if we should group alerts together i.e. two alerts within 30 seconds become a single spliced clip, and append adds more time to the end for context. This process is done for all timestamps and creates easy-to-digest clips of all alerts detected during recording.

To ensure the operator becomes aware of the scene changes, they are alerted in real-time with notifications. These notifications will appear on the operator’s tablet, providing visual cues that indicate detected differences within the monitored area. This immediate alerting allows for quick responses to potential threats or changes in the environment.

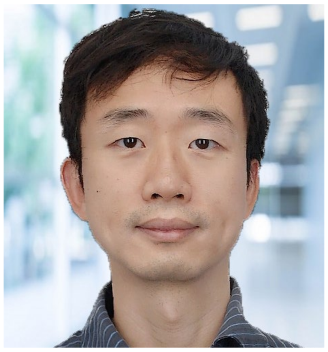
Picture source: https://www.youtube.com/watch?v=3LXQWU67Ufk

Project Sponsor: Capstone Marketplace

CAPSTONE
marketplace

# Class Instructor

Class Instructor manages the A-to-Z operation of the senior design project, including projects selection, budget management, and the coordination among sponsors, mentors, and students. They play a key role to ensure the two-semester course runs smoothly and seamlessly .



## Mingkui Wei, Ph.D

Dr. Mingkui Wei is the lead class instructor of the 2024-2025 CYSE492 / CYSE 493 course.  He is an Associate Professor of Cybersecurity Engineering Department at GMU and has conducted researches in a variety of aspects in cybersecurity, including computer networks, digital forensics, smart power grids, and smart vehicles. His current research interests focus on layer-7 security, especially on web securities. His research has resulted in a number of top tier conference and journal publications, such as ACM CCS, Usenix Security, IEEE Transaction on Networking, etc.

Dr. Wei completed his Ph.D in Computer Engineering at NC State University in 2016 and worked in as an Assistant Professor in Computer Science at Sam Houston State University, where he conducted researches and taught courses in digital forensics. During his tenure at SHSU, he also collaborated with faculties in Forensics Science Department at SHSU and Houston Forensics Science Center on a crime scene investigation project.

He joined the Cybersecurity Engineering Department in the Spring 2021, since then has taught graduate and undergraduate classes covers several topics. He built several classes from the ground up including CYSE 230 Computer Networking, CYSE 421/521 ICS Security, CYSE 550 Cyber Security Engineering Fundamentals, and CYSE 610 Networks and Cyber Security.

He is honored to assume the role as the class instructor for the CYSE senior design and enthusiastic about making this last CYSE course a nonmemorable experience for the senior students.

# Class Mentors

Class mentors leverage their expertise to ensure the delivery of a sound project. More importantly, they provide valuable guidance on the whole lifecycle of the project and prepare students for the next step in their engineering careers beyond graduation.

## Alexandre De Barros Barreto

Dr. Alexandre is a former Brazilian Air Force Officer (Lieutenant-Colonel), Helicopter Pilot, Air Traffic and Air Defense Telecommunication Network Specialist.  He is a highly accomplished cybersecurity expert with over 30 years of experience across academia, research, and practical implementation. As an Associate Professor at George Mason University, he leads cybersecurity engineering and risk analysis, driving research in threat modeling for complex systems. His practical contributions include developing the Cyber-Argus framework (adopted by the DALNIM Project) and holding a patent in ADS-B authentication. He's led projects like the MUSCAT counter-drone tool, applying advanced AI techniques to security challenges. He was a Deputy Director of R&D at the Brazilian Air Space Institution. He spearheaded critical aviation security initiatives and certifications, fostering international partnerships there. Post-retirement, he founded a company contributing to early Brazilian RPAS approvals and a smart grid security design, demonstrating strategic leadership and a commitment to enhancing cybersecurity resilience. He is currently the professor of Secure Software Engineering (CYSE 411), Cyber Security System Engineering (CYSE 587, 687, 787), Mentoring (CYSE 492/CYSE 493) and Cyber Risk Analysis and Advanced Tools (CYSE 630). Dr. Barreto received his PhD in Computer Engineering (Cyber Security Impact Assessment) and MSc in Computer Engineering – Instituto Tecnológico de Aeronáutica (São José dos Campos, BR).

## Armin Tadayon

Armin is a Director in Brunswick Group's D.C office. He advised clients on data security, privacy, and crisis communications.

He brings deep expertise in navigating complex cybersecurity, privacy, and regulatory challenges, working across sectors including technology, healthcare, energy, and retail.

Before joining Brunswick, Armin practiced law with a focus on cybersecurity, data privacy, and government surveillance. He also teaches courses on law and technology at George Mason University's Volgenau School of Engineering, where he serves on the Department of Cybersecurity Engineering's Advisory Board.

Armin holds a J.D. from George Mason University School of Law, a Masters in Cybersecurity from the University of Maryland, Baltimore County, and a Bachelor of Arts in Government and International Relations from George Mason University. He is licensed to practice law in the Commonwealth of Virginia and the District of Columbia. He is also a Certified Information Privacy Profession (CIPP/US).

# Class Mentors

Class mentors leverage their expertise to ensure the delivery of a sound project. More importantly, they provide valuable guidance on the whole lifecycle of the project and prepare students for the next step in their engineering careers beyond graduation.

## Catherine L Jones

Katie Jones has over 25 years' experience providing data management, data analysis, and project management to a variety of clients. She currently serves at the Director of AI Ready workforce development at Booz Allen Hamilton, which provides a multi-tiered learning experience for all employees, enabling learners to choose their own 'AI Ready' journey to progressively build AI knowledge and skills.

Ms. Jones holds a Bachelor of Science in Environmental Science from the College of William and Mary and a Master of Engineering in Civil and Water Resources Engineering from the University of Virginia. Following her graduation, she spent 10 years in the environmental consulting industry, providing technical support to environmental clean-up and compliance projects. For the past 15 years, Ms. Jones has served in a variety of leadership roles ranging from data management and process improvement to directing an enterprise-wide internship program.

## Christine Alonzo Yee

Christine Alonzo-Yee is the Sr. Director of Defense at KeyLogic with over 22 years of industry experience. She is a systems engineering and technology consultant serving various defense, intelligence, and federal agencies. She was with Booz Allen Hamilton for 19 years, starting her career in military satellites, migrated to radar technologies, and then to cybersecurity technologies, focusing on the protection of government networks. She has served as a chief engineer, focusing on the strategic investment, growth, and ideation of differentiated engineering technologies, such as robotics, digital transformation, and resilient position, navigation, and timing. She currently focuses on the business development, growth, and operations of the DoD portfolio within KeyLogic, delivering advanced data analytic and data management capabilities across the Air Force and Army. She received a B.S. in electrical engineering from The Pennsylvania State University and a M.S. in electrical engineering from Johns Hopkins University.

# Class Mentors

Class mentors leverage their expertise to ensure the delivery of a sound project. More importantly, they provide valuable guidance on the whole lifecycle of the project and prepare students for the next step in their engineering careers beyond graduation.

## Henry Coffman

Dr. Coffman is an associate professor of cybersecurity engineering at GMU. He served as professor of cyber security and information technology at Lord Fairfax Community College for the past 17 years. He was the program lead for the cybersecurity program of which obtained designations as a Center of Academic Excellence for 2 Year Colleges and a recent accreditation by ABET for cybersecurity at 2 year schools (One of two colleges internationally accredited with such distinction.). Dr. Coffman holds degrees from the University of Virginia, The American University and George Mason University. Dr. Coffman worked in various network and security focus areas for 31 years with the Department of Defense and Interpol. He was the Vice Chair of the Interpol Technology Committee based in Lyon France as well as the Chief Technology Officer for the United States National Central Bureau of Interpol.

## Jair Ferrari, PhD

Dr. Jair Ferrari is a former Brazilian Air Force Officer (Colonel), Maritime Patrol Pilot, Electronic Warfare (EW) Specialist, Portfolio Manager of Aeronautical and Defense R&D Projects. He was an EW Instructor and Course Coordinator from basic to postgraduate courses. He has an Electronic Warfare short course from 2 weeks to a formal specialization course that became a MSC and PhD programs in the Aeronautics Technology Institute (ITA) – Sao Paulo, Brazil. Dr. Ferrari was a researcher in the Department of Mechanical, Industrial and Aerospace of Concordia University (Optimization of Aerial SAR Operations Studies) as well as in the C4I & Cyber Center of GMU (UAS Detection Systems Simulation and Optimization). He is currently the professor of Systems Engineering Principles (SYST 205), Unmanned Air Systems Security course (CYSE 499/685) and Mentoring (CYSE 492/CYSE 493). Dr. Ferrari received his PhD in Industrial Engineering (Optimization of Aerial and Naval SAR Operations) – Concordia University (Montreal, QC); MSc in Systems Engineering (Electronic Warfare Specialization) – U.S. Naval Postgraduate School (Monterey, CA); MSc in Business Administration (Quantitative Methods for Quality Evaluation) – Brasilia University (Brazil).

# Class Mentors

Class mentors leverage their expertise to ensure the delivery of a sound project. More importantly, they provide valuable guidance on the whole lifecycle of the project and prepare students for the next step in their engineering careers beyond graduation.

## Mohamed Morsy, PhD

Dr. Mohamed Morsy is an Associate Professor of the Cybersecurity Engineering Department at GMU. Before joining the Department of Cyber Security Engineering at George Mason University as an adjunct faculty in 2022 then as full-time Associate Professor in 2023, Dr. Morsy served at various locations as senior system engineer and senior research scientist. He served as part-time faculty in electrical engineering and applied science at George Washington University (2002-2004), then as Department Chair of Electronics & Communications at ITT (2004-2016). He also served as a member of the ITT National Electronics Curriculum Committee (2005-2016). From 2009 to 2023 he was an adjunct Professor with the Department of Computer Information Systems, Fairfax University of America (formerly Virginia International University). Dr. Morsy has authored/coauthored several technical journal articles and conference papers (cited in the web IEEE). He received numerous teaching performance awards and certificates of appreciation from the IEEE Communications Society. Dr. Morsy is a Senior Member of the IEEE. He is an Editor of the International Journal of Research Publications (IJRP). He received his Doctor of Science degree (D.Sc.) in Electrical Engineering and Communications from George Washington University, Washington D.C..

# Special Acknowledgements

In addition to our project sponsors and subject matter experts, there were many other people who significantly contributed to the success of this class. We want to take this opportunity to express our deep-felt appreciation for their contributions.

## Paulo Costa

For serving as CYSE Department Chair and supporting our innovative student teams.

## Peggy Brouse

For her vision and continued, unyielding support in making this class available for students.

## Expert Guest Speakers:

Greg Chong (Microsoft)
Catherine L Jones (Booz Allen Hamilton)
Matthew Jones (Leidos)
Devesh Agarwal (MITRE)
Sujay Kandwal (MITRE)
Rock Sabetto (MITRE)

GEORGE MASON UNIVERSITY