
APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY

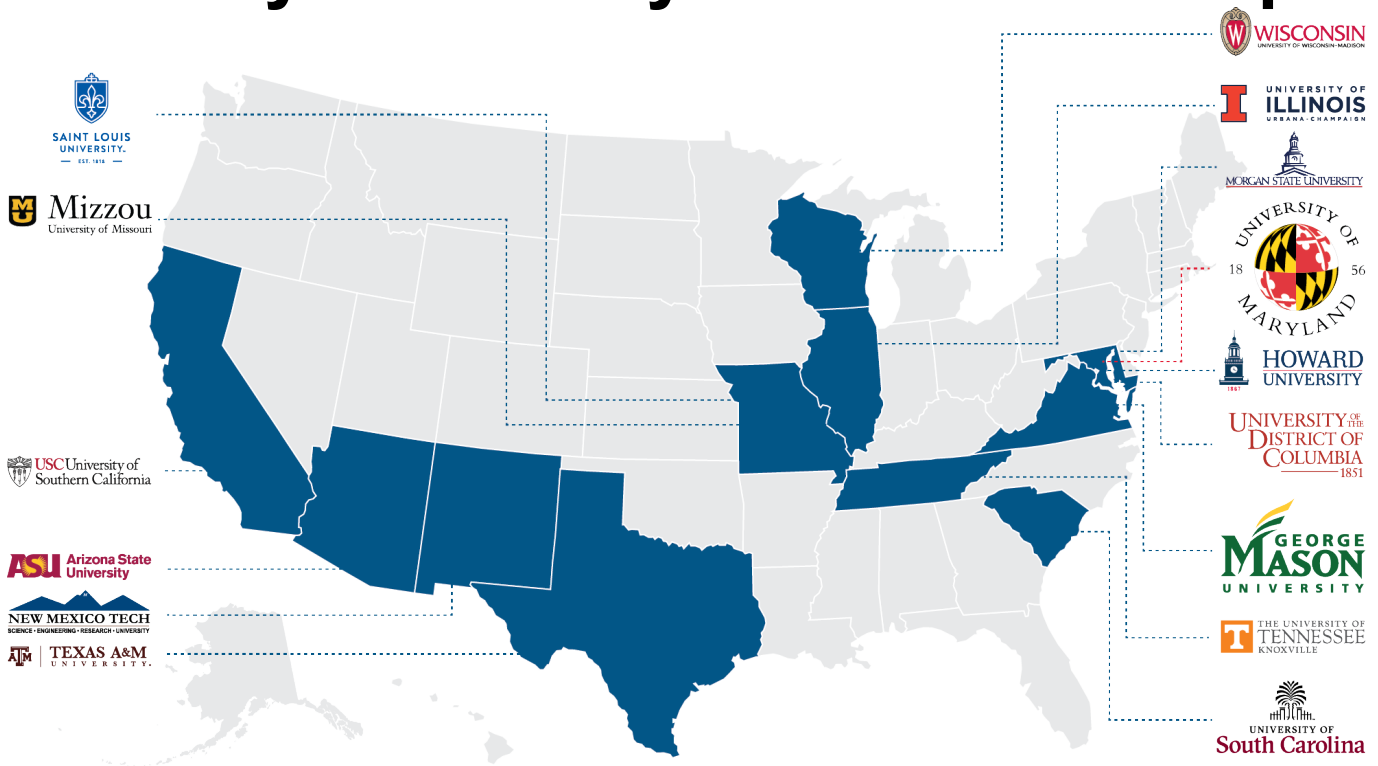
# Pilot Projects to Build HBCU-INSURE Partnerships

Erin Fitzgerald, Director, INSURE - efitzgerald@arlis.umd.edu

Outbrief to Ms. Evelyn Kent, Program Director, DDR&E/HBCU+MSI

# INSURE: Strengthening the Intelligence and Security University Research Enterprise

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY




## Goals

Bring the right team to *every* in-scope problem brought to ARLIS.

Be the connector (and translator) for I&S communities to engage academic talent.

Build a robust and diverse future workforce.

**15** member institutions in 13 states ♦ **4** HBCU/MSIs ♦ **8** w/ secure facilities + cleared researchers
**33,610** faculty ♦ **481,603** students ♦ over **$6.7 B** in federal research expenditures

# Pilot Projects to Build HBCU-INSURE Partnerships

- **Sponsor:** OUSD(R&E) HBCU/MSI Program Office
- **Program Manager/Client:** Ms. Evelyn Kent
- **ARLIS Lead:** Erin Fitzgerald
- **Period of Performance:** 11/20/20 – 9/12/22
- **TRL of the work:** wide ranging

# Start-Up/Process Challenges

| Milestone | Date |
|---|---|
| Overall task order on contract | 11/20/20 |
| Subcontract fully executed: Morgan State<br>Effective start date | 2/5/21<br>1/15/21 |
| Subcontract fully executed: Howard<br>Effective start date (cyber attack, challenges hiring grad students)<br>Effective re-start date: February (?) after rebudgeting | 2/16/21<br>8/31/21<br><br>2/15/22? |
| Subcontract fully executed: UDC<br>Effective start date (DC approvals, etc) | 3/23/21<br>8/31/21 |
| No cost extension (from 5/12/22 to 9/12/22) awarded<br>Morgan signed (work continued)<br>Howard signed (full stop-work in meantime)<br>UDC signed (work continued) | 5/12/22<br>6/21/22<br>6/30/22<br>6/9/22 |

# Resulting Challenges

- Team coordination per project
  - Tough to coordinate when work is on entirely different timelines!
  - Graduate students substituted for undergraduates (more junior and short term)
- Spending
  - Different processes for budget approvals led to delays in being able to spend the funding
  - Contract language limited equipment purchases and international conference travel
  - Shifting to undergraduates made spending harder
- Mitigations for the future: organic partnerships and budget, contracting lessons learned

# Five Pilot Efforts, 3+1 Institutions

1. **5G Technology Assessment**
   - Technical Lead: Kevin Kornegay, Morgan State University (Partner Michaela Amoo, Howard)
   - ARLIS Lead: Wayne Phoel, Research Engineer
2. **Machine Learning Experimentation**
   - Technical Lead: Paul Cotae, University of the District of Columbia
   - ARLIS Lead: Craig Lawrence, Mission Area Lead for AI, Autonomy, & Augmentation
3. **Cyber-Assessment of AI/ML Tools**
   - Technical Lead: Gloria Washington, Howard University (Partner Paul Wang, Morgan State)
   - ARLIS Lead: Craig Lawrence, Mission Area Lead for AAA
4. **AI/ML Systems Engineering Workbench**
   - Technical Lead: Kofi Nyarko, Morgan State University (Partner Michaela Amoo, Howard)
   - ARLIS Lead: Craig Lawrence, Mission Area Lead for AAA
5. **ChatBot Testbed**
   - Technical Lead: Amit Arora, University of the District of Columbia (Gloria Washington, Howard and Onyema Osuagwu, Morgan)
   - ARLIS Lead: Michelle Morrison, Mission Area Lead for Language & Culture

# Project Description

- **ARLIS Relevance:** Ties to three ARLIS mission areas; furthers goals of expanding and diversifying the intelligence and security workforce pipeline
- **Goal:** Carry out mission-relevant research and catalyze new partnerships while bringing existing HBCU strengths into ARLIS mission area portfolios
- **Expected Impact**: HBCU INSURE members primed for legitimate partnerships and connected to USG stakeholders
- **Success measures**: Students trained; Research products shared with ARLIS stakeholders; Follow-on projects planned and funded.

# Big Wins

- New INSURE task award funded for Morgan State (*Synchronized Analysis of Video, Imagery and Audio*, TRMC)
- Morgan State (Kofi Nyarko) brought in as partner for ARLIS *AI Engineering Initiative* Seedling through ODNI S&T
- Continued partnership with Kevin Kornegay (MSU) and ARLIS in the 5G space
- Supported opening class of UDC PhD Computer Science students
- 40+ students trained; many hired
- New connections between all four universities!

| | PhD | MS | BS | Total |
|---|---|---|---|---|
| P1 | 4 | - | 2 | 6 |
| P2 | 8 | 2 | - | 10 |
| P3 | | 3 | 6 | 9 |
| P4 | 4 | 2 | 2 | 8 |
| P5 | | 2 | 9 | 11 |
| | 16 | 9 | 19 | **44** |

Students trained

# Five Pilot Efforts

1. **5G Technology Assessment**
   - Technical Lead: Kevin Kornegay, Morgan State University (Partner Michaela Amoo, Howard)
   - ARLIS Lead: Wayne Phoel, Research Engineer
2. **Machine Learning Experimentation**
   - Technical Lead: Paul Cotae, University of the District of Columbia
   - ARLIS Lead: Craig Lawrence, Mission Area Lead for AI, Autonomy, & Augmentation
3. **Cyber-Assessment of AI/ML Tools**
   - Technical Lead: Gloria Washington, Howard University (Partner Paul Wang, Morgan State)
   - ARLIS Lead: Craig Lawrence, Mission Area Lead for AAA
4. **AI/ML Systems Engineering Workbench**
   - Technical Lead: Kofi Nyarko, Morgan State University (Partner Michaela Amoo, Howard)
   - ARLIS Lead: Craig Lawrence, Mission Area Lead for AAA
5. **ChatBot Testbed**
   - Technical Lead: Amit Arora, University of the District of Columbia (Partners Gloria Washington, Howard and Onyema Osuagwu, Morgan)
   - ARLIS Lead: Michelle Morrison, Mission Area Lead for Language & Culture


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

# Project 1:
# 5G testbed development and vulnerability analysis

Dr. Kevin Kornegay, CAP Center Director, Morgan State University

kevin.kornegay@morgan.edu

Dr. Michaela Amoo, Howard University, mamoo@howard.edu

# Safeguarding Future Communications Paradigms

- **Supports Acquisition, Industrial Security, and Critical Technology Protection**
  - *Internet of Things (IoT) device use in the supply chain (factories, warehouses, transportation, monitoring)*
  - *5G / telecom supply chain security*
- **Impacting human behavior**
  - *Greater connectivity will change how we interact and provide new means for monitoring and influence*
  - *Wearables, AR/VR, autonomous systems*
- **Prior studies have highlighted insufficient security architecture for large-scale IoT**
  - *Guidelines/standards for DoD equipment with respect to encryption/authentication*
  - *Architecture to minimize attack propagation*
  - *Existence of low-power encryption technology*
- **This project is identifying and quantifying security issues of IoT devices in 5G networks and exploring mitigations**

# Relationship to ARLIS's goals/story

- Supports Acquisition, Industrial Security, and Critical Technology Protection missions
  - Internet of Things (IoT) device use in the supply chain (factories, warehouses, transportation, monitoring)
  - 5G / telecom supply chain security
- Wireless technology impacting human behavior
  - Greater connectivity will change how we interact and provide new means for monitoring and influence
  - Wearables, AR/VR, autonomous systems
- The work leverages academic expertise in IoT security to provide trusted advice to DoD programs exploring use of commercial technologies in defense networks
  - Complements traditional user equipment experiments feeding into ARLIS support to OUSD(R&E) 5G office

# Project Description

**Goal:** Create a suite of testing tools for analysis of hardware performance, cybersecurity, wireless security, and user access related to 5G technology

**SWOT:** Prior studies highlighted insufficient security architecture for large-scale IoT

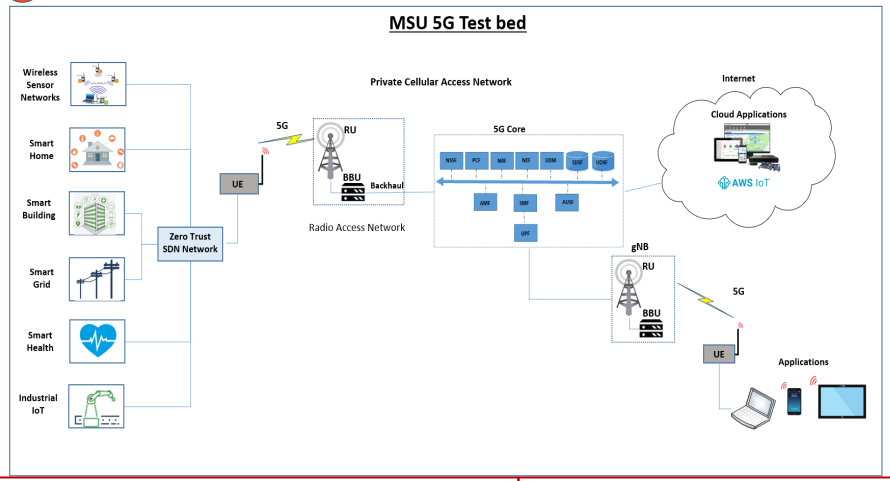
- *Lacking guidelines/standards for DoD equipment with respect to encryption/authentication*
- *Need for architecture to minimize attack propagation*
- *Insufficient low-power encryption technology*

**Expected Outcome**: Design and implement an end-to-end wireless sensor network that will be used for security vulnerability analysis on 5G networks

**Success measures**: Demonstration of realistic attacks and mitigations on relevant IoT-based network

**Expected Impact**: Increased reliability and security of future DoD operations making use of low power IoT devices

# 5G testbed development and vulnerability analysis Overview




## Project objectives:

- *Develop IoT testbeds*
- *Develop 5G testbed.*
- *Integrate 5G testbed with IoT systems.*
- *Perform end-to-end vulnerability analysis.*

## Project status:

- *BLE, Zigbee, LoRa and NB-IoT testbeds deployed.*
- *Vulnerability analysis performed on LoRa testbed- Eavesdropping, Replay, Jamming attack performed.*
- *5G testbed deployment- Pending*

# Big Wins (so far)

- IoT and zero trust architecture development have influenced recommendations presented to the OUSD(R&E) 5G program
- Heterogenous IoT testbeds leverage cloud-based data storage and data visualization
- Successful demonstration of cyber attacks on LoRa system with anti-jamming countermeasure.
- One publication submitted to ACM Journal:- Transaction on Sensor Networks (TOSN)
- Three grad students supported

# Project Status

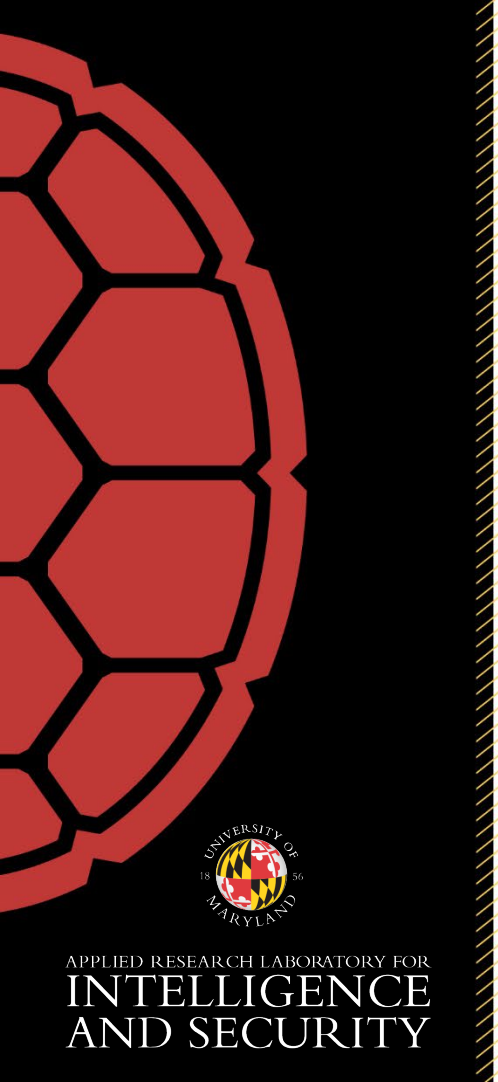
| Key Deliverables/ Insights / Activities | Timeline/ status | R/Y/G |
|---|---|---|
| Deploy IoT testbed (BLE, Zigbee, LoRa, NB-IoT) | Complete | On sched |
| IoT device vulnerability testing | Ongoing | On sched |
| 5G testbed deployment | Pending | Delayed |
| IoT Device/5G Integration | Pending | Delayed |
| End-to-end vulnerability testing | Pending | Delayed |

## Project Risk Assessment

- Not enough funds to purchase equipment.
- Challenge managing collaboration.
- Implemented remote data capture during Covid.

# Next Steps and Future Capabilities

- 5G testbed deployment (Amari callbox & Firecell Labkit)
- IoT and 5G testbeds integration
- End-to-end vulnerability testing (hardware/RF/backhaul/application)
- Sponsor relationship, new/additional sponsors




# Thank you!

Dr. Kevin T. Kornegay
Morgan State University
Kevin.Kornegay@morgan.edu

www.arlis.umd.edu/insure


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

# Project 2: Machine Learning Experimentation

Dr. Paul Cotae, Professor and Chair, ECE Department,

The University of the District of Columbia

pcotae@udc.edu

# Team Members

- PI: Dr. Paul Cotae, Co-PI Dr. Girma Anteneh
- ARLIS Team Members: Dr. Craig Lawrence
- Supporting 6 PhD students: 2 for final PhD Thesis Defense, 2 for the Qualifying Exam other two joined our projects.

# Relationship to ARLIS's goals/story

## How does this Project help us better understand and control the human domain in support of defense security and intelligence missions?

- The application of Machine Learning and Artificial Intelligence (ML/AI) is a great advantage to enhance various domains of cyber security to provide analysis-based approaches for the detections of catastrophic cyber-attack and countermeasures. It support defense security for better decisions in human domain

## In what ways does this project/mission area tie into other projects at ARLIS?

- Exploiting different tools and mechanisms of ML/AI to keep the integrity, confidentiality, and availability of information assets and to effectively respond to sophisticated cyber-attacks.

# Project Description

**Goal:** *Bottom line, what are you trying to do?*

In order to find a data preparation model and model configuration that gives good or great performance, this project carefully plans and manage the order and type of experiments that we run.

**SWOT:** *How is it done today (+ by whom?), and what are the limits?*

Supporting 6 PhD students: 2 for final PhD Thesis Defense, 2 for the Qualifying Exam other two joined our projects.

**Expected Outcome**: *i.e. This work will enable the USG to…*

Published papers, research student presentations, mentoring MS and Undergraduate Students in EE and CS

**Success measures**:

Quality of published papers, happiness of students, research impact at UDC

**Expected Impact**: *i.e. What difference will it make?*

Enhancing minority student research, increasing the enrollment.

# Major Subtasks

1. Ransomware Attack Detection on the Internet of Things Using Machine Learning Algorithm
2. Malware Detection Model on a Cyber-Physical System Using Artificial Intelligence and Machine Learning
3. Detecting DDoS Attacks in Software-Defined Networks Through AI Machine Learning
4. Scalable Real-Time Multiagent Decision Making Algorithm with Cost
5. Scalable Real-Time Distributed Multiagent Decision Making Algorithm
6. A Hybrid Cost Collaborative Multiagent Decision Making Algorithm with Factored Value Max Plus

# Project Overview

## Overview

We considered the supervised and unsupervised machine learning algorithms, including:

- support vector machines (SVMs)
- boosted and bagged decision trees,
- k-nearest neighbor,
- k-means,
- hierarchical clustering,
- Gaussian mixture models

We considered Decision Making in security domain applicable to collaborative multiagent setting

- Centralized
- Decentralized
- Hybrid

## Project objectives

Expose students and faculty to advanced custom AI/ML, experiment design and data preparation. Enhancing CSE PhD research at UDC

## Findings and Deliverables

- Information dissemination for AI/ML for data collection and modeling including software and hardware
- Recruiting 6 PhD Students to be fully supported
- 6 papers accepted and 2 to be submitted
- Final Technical Report

# Project Status

| Key Deliverables/ Insights / Activities | Timeline/ status | R/Y/G |
|---|---|---|
| Final Research Report | Delivered | On sched |
| | | Delayed |
| | | Issue |
| | | … |

## Project Risk Assessment

- What are the technical risks and challenges encountered? Management risks?
  *Working with latest data set, find realistic data sets, obtaining the latest results*
- How did you mitigate those risks?
  *Literature review, collaboration with NRL, we had our budget issue resolved very late and could not support the students on time.*
  *Time to finish the project and report are too short.*

# Big Wins

- 8 PhD students trained (6 working full time)
- 2 Master students (part time)
- New PhD and B.S. cybersecurity program + new MS cybersecurity program in Spring 2023.
  - Based on our research activities  and experience with the different ARLIS machine learning experimentation research projects, given another two years of research grant continues for the next two years.
- Enhance SEAS cybersecurity curriculum by creating new advanced research-based cybersecurity courses
  - “Advanced Cyber-risk Mitigation using Machine Learning” and
  - “Securing Artificial Intelligent System Using Advanced Machine Learning Techniques.”

# Next Steps and Future Capabilities

Transition Goals

- Naval Research Laboratory in Washington DC

Activities and milestones ahead

- Opportunities for partnership ahead: Howard University, George Mason University
- New ideas and whitepapers: New type of attacks detection slow and low attacks, develop new Algorithms for AI/ML
- Sponsor relationship, new/additional sponsors:

  Summer research fellowship at NRL

# Thank you!

Dr. Paul Cotae

pcotae@udc.edu

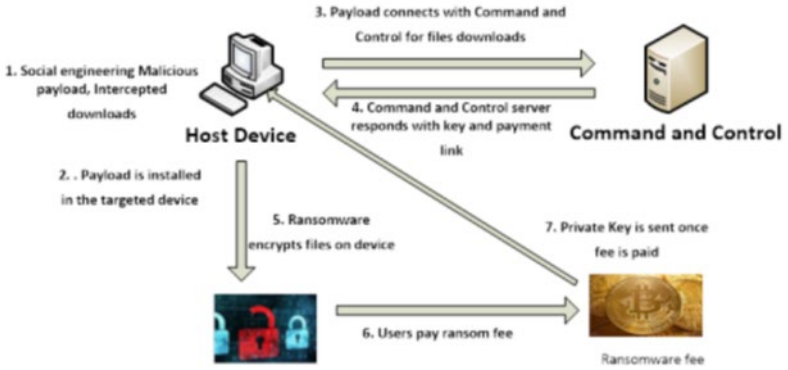
Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

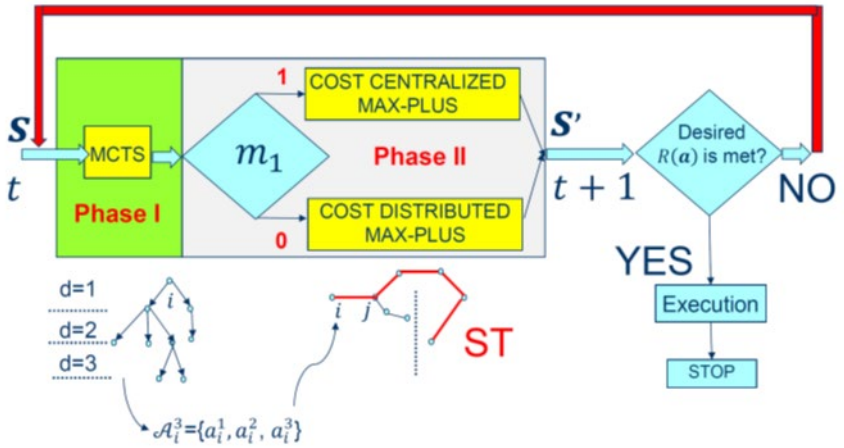
www.arlis.umd.edu/insure

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

# [backup slides if needed]

- State of Art Research



APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

# Project 3: Cyber-Assessment of AI/ML Tools

Gloria Washington, Assistant Professor, Howard University
Paul Wang, Professor Computer Science, Morgan State University
gloria.washington@howard.edu; shuangbao.wang@morgan.edu

# Relationship to ARLIS's goals/story

- Cybersecurity is a multidisciplinary field (social and behavioral science, AI, computing) with economic, social and environmental consequences.
- Relevant ARLIS mission areas include Human Language and Culture, Cognitive Security (e.g., MINERVA project), Insider Threats, and Human-Centered Computing; potential connections with several existing ARLIS projects.
- Survey of AI/ML tools and Analysis of Vulnerabilities in those tools
- Adversarial Attacks on AI/ML tools and countermeasures
- Development of a ML-based cyber threat analysis tool (Python)

# Team Members

- **PI**: Dr. Gloria Washington & Dr. Paul Wang
  - Team members at Howard: Gloria
  - Team members at Morgan: Paul, Tanvir, Onyema, and Wandji
- **ARLIS Team Members**: Erin Fitzgerald, Craig Lawrence
- **Collaborating Institutions**:
  - Howard University
  - Morgan State University

# Project Description

**Goal:** Survey key open-source AI/ML toolkits, design a methodology for testing vulnerabilities or weaknesses, and to provide best practices to countermeasure the potential risks.

**Expected Outcome**: Lay the foundation to help the USG tackle vulnerabilities or weaknesses in cyber-human and develop risk analysis cybersecurity toolkits.

**Success measures**: Development and testing of network and biometric-based toolkits to determine robustness of opensource toolkits and robustness under adversarial attacks.

**Expected Impact**: Opportunity for undergraduate and graduate students to learn biometric and network intrusion detection algorithmic techniques. Ties in directly with ARLIS land-grant mission to nurture pipeline of future scientists.

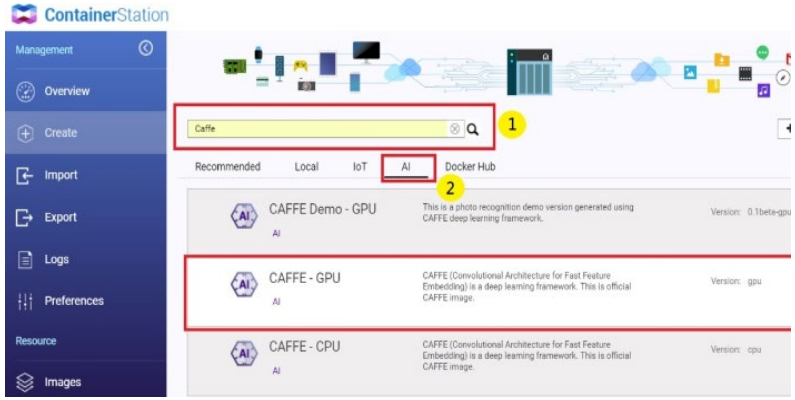
# How the Partnership Contributed

- Institutions complemented the project by performing cyber-assessment of both cyber-physical and cyber-human systems examining opensource AI/ML toolkits
  - Howard University (HU) assessed how the biometric systems are affected by lighting, occlusion, and noise.
  - Morgan State University (MSU)
    - Conducted survey of AI/ML tools and vulnerabilities,
    - Programmed a cyber threat assessment tool, and
    - Studied adversarial attacks on AI/ML algorithms.
- Student teams from all two institutions from sharing knowledge gained from each project.

# Survey of AI/ML tools/vulnerabilities

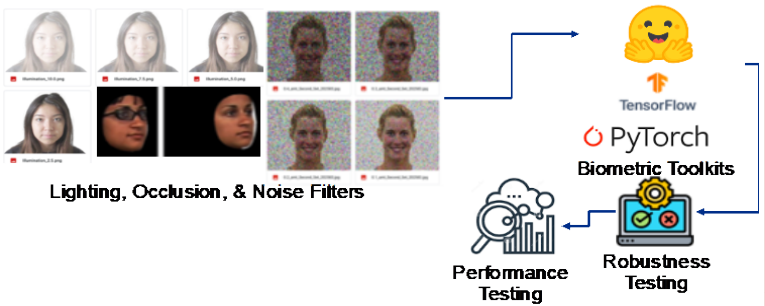
## Tools Surveyed

- TensorFlow
  - Dataset: MINST
  - CNN
  - Security: image classification
- Scikit-Learn
  - ML toolbox for Python
  - NumPy, SciPy, MatPlotlib
  - Classification, dim redution
- Oryx 2
  - ML framework
  - Clustering, regression, Spark
  - Real-time Data Processing
- Caffe and Torch
  - Deep learning
  - CPU/GPU
  - Security: bugs, exploit our of bounds




```
x = tf.placeholder(tf.float32, [None, 200])

W = tf.Variable(tf.zeros([200, 10]))
b = tf.Variable(tf.zeros([10]))
y = tf.nn.softmax(tf.matmul(x, W) + b)

...

with tf.Session() as sess:
  sess.run(tf.initialize_all_variables())
  tf.train.start_queue_runners(sess)

  example_batch = tf.train.batch([x], batch_size=10, num_threads=4, capacity=10)

  max_steps = 1000
  for step in range(max_steps):
    x_in = sess.run(example_batch)
    sess.run(train_step, feed_dict={x: train_data, y_: train_labels})
    if (step % 100) == 0:
      print(step, sess.run(accuracy, feed_dict={x: test_data, y_: test_labels}))
```

# Biometric Robustness Cyber Assessment




| Mode Name | Database | **Accuracy** |
|---|---|---|
| DeepID | LIRISCSFE | 80% |
| VGG-Face | | 90% |
| Facenet | | 80% |
| Facenet512 | | 80% |
| OpenFace | | 80% |
| DeepFace | | 80% |
| ArcFace | | 90% |
| Ensemble | | 90% |

## Project objectives

- Study how the biometric systems are affected by lighting, occlusion, and noise

## Project deliverables

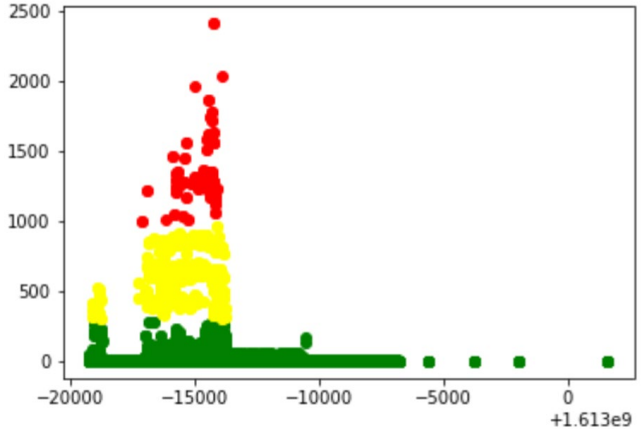
- .

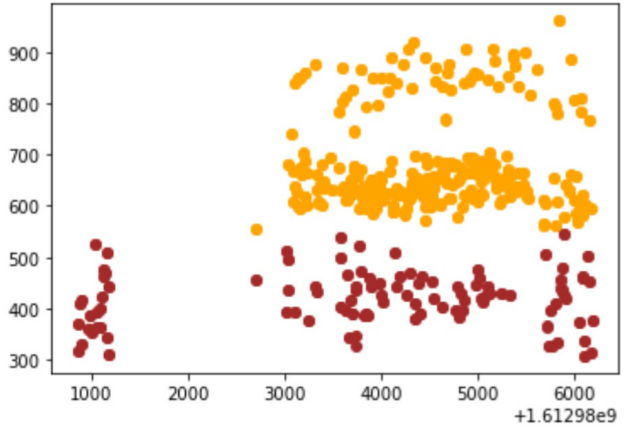
# Cyber Threat Assessment Tool

- Language: Python
- Data trails: over 800,000 gathers on a web server on AWS
- Loaded into a Pandas dataframe
- Preprocessing

- Preprocessed data : 0.67/0.33
- Unsupervised learning
  - Understand the data
- Supervised learning
  - Refine the results
- Define attacks
- Train and predictions

- Publication: “Trustworthy Artificial Intelligence for Cyber Threat Analysis,” Springer Lecture Note in Networks and Systems (ISBN 978-3-031-16071-4).



# Adversarial Attacks on AI/ML Algorithms

- Hop Skip Jump is a decision-based attack which is a subgroup of transfer-based attacks.
- The attacker has access to decisions alone. And these attacks are first to run on a testing environment before they are transferred to the targeted network.
- The attack is used to train the testing model by using query data from the targeted model. Loaded into a Pandas dataframe
- Using Counterfit the Hop Skip Jump attacks on the credit fraud target the parameter
- Received most success on the target was: max integer, max eval, batch size, current integer, and the initial size.
- A Master thesis is being finalized

| Credit fraud HopSkipJump | Success | Elapsed Time(sec) | Total Queries | Query per sec |
|---|---|---|---|---|
| Attack 1 | 1/1 | 1.4 | 68419 | 50604.6 |
| Attack 2 | 1/1 | 12.6 | 314342 | 24852.7 |
| Attack 3 | 1/1 | 0.5 | 11603 | 23382.7 |
| Attack 4 | 1/1 | 1.9 | 124964 | 64264.5 |
| Attack 5 | 1/1 | 5.3 | 73021 | 13870 |
| Attack 6 | 1/1 | 43.9 | 3893668 | 88637.2 |

```
File  Edit  View  Search  Terminal  Help
[+] Attack completed 53f06c04 (HopSkipJump)

creditfraud>53f06c04> use HopSkipJump

[+] New HopSkipJump (1dbb254d) created
[+] Using 1dbb254d

creditfraud>1dbb254d> set --max_iter=150 --max_eval=500 --init_size=100 --batch_
size=5
```

| Parameter (type) | Default | Current | New |
|---|---|---|---|
| Algorithm Parameters | | | |
| --- | -- | -- | -- |
| targeted (bool) | False | False | |
| norm (int) | 2 | 2 | |
| max_iter (int) | 50 | 50 | 150 |
| max_eval (int) | 10000 | 10000 | 500 |
| init_eval (int) | 100 | 100 | |
| init_size (int) | 100 | 100 | |
| curr_iter (int) | 0 | 0 | |
| batch_size (int) | 64 | 64 | 5 |
| verbose (bool) | False | False | |
| clip_values (tuple) | (0.0, 1.0) | (0.0, 1.0) | |
| Attack Options | | | |
| --- | -- | -- | -- |
| sample_index (int or expr) | 0 | 0 | |
| logger (str) | default | default | |

```
creditfraud>1dbb254d> run
```

# Project Status

| Key Deliverables/ Insights / Activities | Timeline/ status | R/Y/G |
|---|---|---|
| Literature survey on state-of-the-art in network cyber-assessment | Jan-Mar 2022 | |
| Literature survey on state-of-the art in biometric assessment | Jan-Mar 2022 | |
| Develop facial recognition assessment toolkit | Apr – June 2022 | |
| Robustness testing of biometric facial recognition techniques | Jun – Aug 2022 | |
| Documentation of experimentation and robustness testing results of biometric facial recognition techniques | Jul – Aug 2022 | |
| Final Report and Presentation | Sep 2022 | |

## Project Risk Assessment

- Manpower challenges with recruiting graduate vs undergraduate students
- Shifted resources from graduate salary to undergraduate stipends resulting in underutilization of allotted grant funds. (undergrad stipends not subject to fringe)
- Faculty should get compensated working on the projects

# Big Wins

- Four undergraduate students trained in biometric recognition techniques and use of open-source ML tools.
- Four undergraduate students submitted undergraduate research poster to ACM 36th annual CCSC:Southeastern Regional Conference to be held November 11-12, 2022.
- A threat analysis tool was developed and listed on github.
- One faculty spoke at CyberMD 2022 conference
- One paper published at Spinger Lecture Notes. One paper is to be published in a conference
- Supported three Master students. Two completed and been admitted to Ph.D. program at Morgan State.
- One undergraduate student got a job at Amazon (with $120k salary) after working on the project (using AWS).
- Two additional undergraduate students participated in the research. Over 20 students work on the project as their senior projects.

# Next Steps and Future Capabilities

## Transition Goals

- Experiment with various opensource face databases to examine changes in biometric performance
- Study to discover vulnerabilities and bias of ML systems
- Research on adversarial attacks including applying quantum computing algorithms.

## Activities and milestones ahead

- Partnership between the universities can be strengthened to apply for future funding (e.g., NSF SATC program).

# Thank you!

Gloria Washington
gloria.washington@howard.edu

Paul Wang
shuangbao.wang@morgan.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742
www.arlis.umd.edu/insure

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

# Project 4: AI/ML Systems Engineering Workbench

Dr. Kofi Nyarko, Professor, Morgan State University

Kofi.Nyarko@morgan.edu

Dr. Michaela Amoo, Howard University

# Relationship to ARLIS's goals/story

- Supports ARLIS deployment of cyber-infrastructure at scale
- Makes the development and use of cloud AI platforms more accessible
- Leverages cross-cloud services to accelerate AI development, testing and deployment
- Can be leveraged for training efforts related to cloud AI
- Supports cross-cloud test and evaluation efforts (including AI auditing)

# Team Members

- Dr. Kofi Nyarko (MSU PI)
- Dr. Michaela Amoo (Howard PI)
- Dr. Peter Taiwo (MSU Post-Doc)
- 5 Graduate Students, 2 Undergraduate student

# Project Description

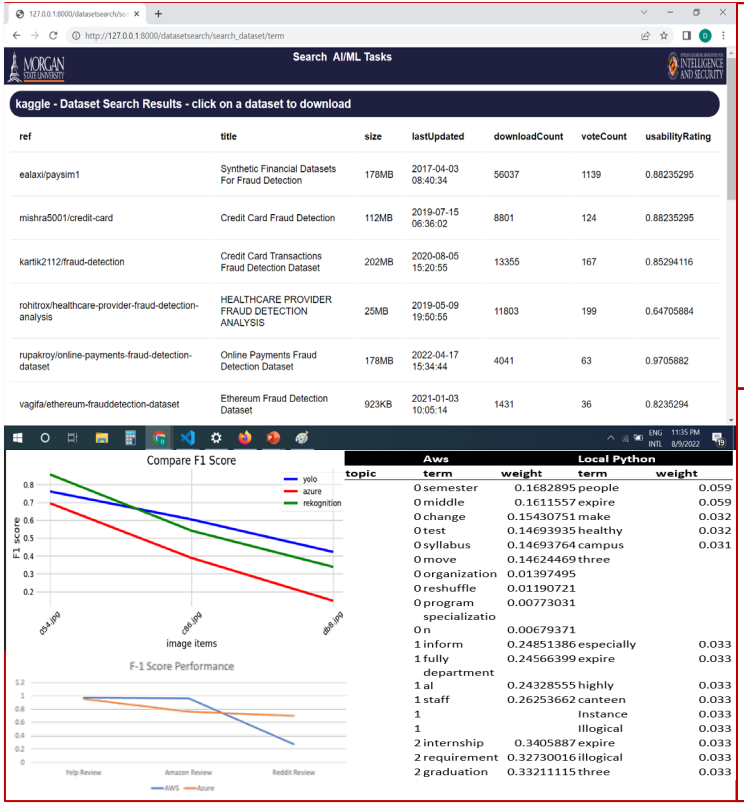
**ARLIS Portfolio:** Applied Artificial Intelligence

**Goal:** This work will support the intelligence community with computational and data services at scale through a common framework that integrates the best-of-breed cloud AI/ML toolkits

**Expected Impact**: More expeditiously design, test, and transition new systems with greater reliability

**Success measures**: A fully deployed AI/ML workbench framework that facilitates model design, testing, and deployment across 3 or more AI/ML cloud service platforms

# AI/ML Systems Engineering Workbench Overview




## Goals

- Develop a common framework that integrates the best-of-breed cloud AI/ML services.
- Implement the framework as a web-based workbench with use cases for Computer Vision, Speech, NLP etc.
- Provide reporting on the workbench software and virtualized hardware instantiations.

## Milestones

- Review and reporting on the current state-of-the-art of AI/ML cloud service providers
- Implementation of a scalable integration workbench with multiple use cases (i.e. vision, radar, NLP)
- Software/hardware cloud instantiation (CPU, GPU and FPGA/ASIC) with documentation

# AI/ML Systems Engineering Workbench - Overview

The system aims to provide:

- Common framework that integrates best-of-breed cloud AI/ML services
- ML models portability by enabling transfer learning with models trained on multiple cloud platforms
- Performance benchmarking across cloud platforms for Vision and NLP tasks

### Federated Data Set Search

- Enable federated search across multiple data repositories
- Move matching data sets to cloud environments for training, testing and verification

### Transfer Learning with Models trained in the Cloud

- Create Transfer learning models from multiple cloud platforms and download to the Workbench.
- Unpack and explore weights and configuration files from multiple estimator frameworks.
- Setup and load downloaded models locally and the WB for deployment, tuning and further TL tasks
- Make test inference and compare results

### NLP and Performance Benchmarking

Setup NLP performance modeling across service providers in a similar way to vision processing

- Implement multiplatform topic modeling and generate performance metrics for comparison (false/true positives, false/true negative, F1 score)
- Compare NLP services using Sentiment Analysis as a criterion.
- Compare three website review datasets for the level of efficiency in terms of detection across the platforms.

# Project Status and Next Steps

| Key Deliverables/ Insights / Activities | Timeline/ status | R/Y/G |
|---|---|---|
| Document SoTA services across cloud providers and integrate into workbench (Vision, NLP, Radar) | Complete | On sched |
| Implement performance measurements across cloud providers (Accuracy, Precision, Recall, F1) | Complete | On sched |
| Integrate multiplatform transfer learning functionality to the WB. | In progress | On sched |
| Revamp and optimize framework to support multiple users and improve reliability, security, and ease of use to support continuous development and deployments | In progress | On sched |

## Project Risk Assessment

- Inconsistent exposed services across cloud platform
  - Limited benchmarking activities to those provided across platforms
- Cloud services have proprietary ML model architectures
  - Exported models into an open source format

# Big Wins

- Trained 2 graduate, 3 doctorate, and 1 post doc
- Ability to perform federated searches across multiple data repositories
- Ability to perform transfer learning using ML models across multiple platforms and multiple estimator frameworks.
- Ability to integrate multiplatform NLP methods and compare performance.
- Cross-platform performance testing on multi-core & parallel instantiation on CPU and GPU instances.

# Next Steps and Future Capabilities

- Complete revamping of UI
- Complete support for multi-users
- Complete the implementation of transfer learning with Azure
- Tasks beyond pilot effort
  - Apply the workbench to projects under the the new Center for Equitable AI and ML that relate to the quantification of algorithmic bias
  - Develop additional use cases to support current lab research tasks
  - Integrate into curriculum at Morgan (EEGR 483 – Intro to Machine Learning, EEGR 565 – Machine Learning Applications)
  - Make available for capstone projects (Fall 2021/Spring 2022)

# Thank you!

Kofi Nyarko (MSU)
Kofi.Nyarko@morgan.edu

Michaela Amoo (Howard)
mamoo@howard.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

# Project 4 Backup Slides

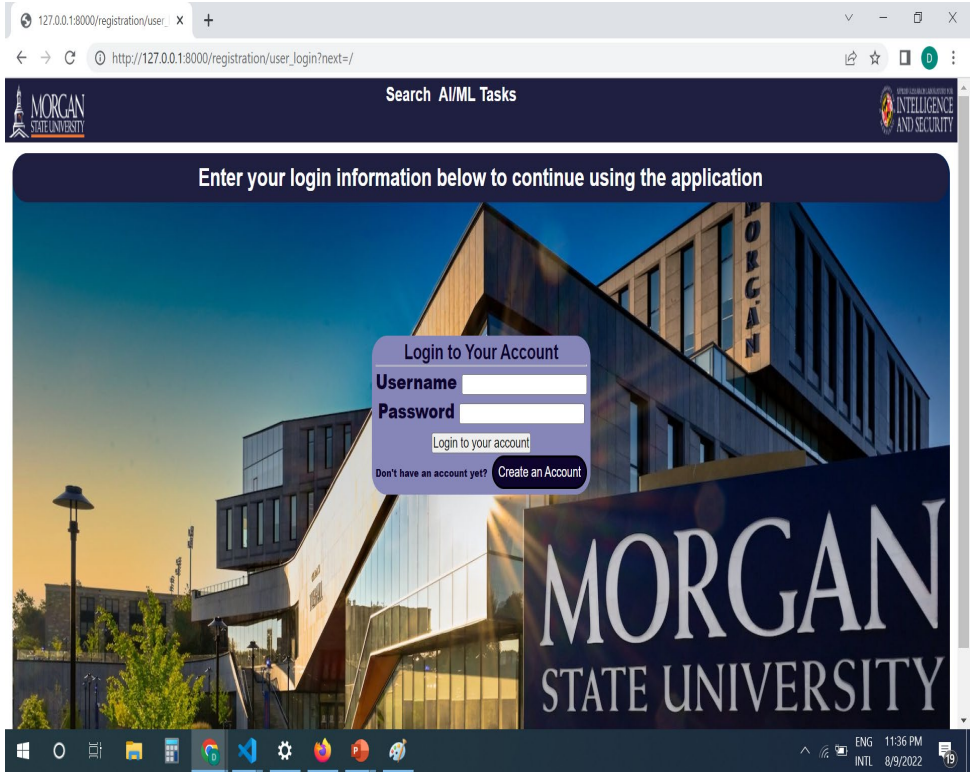
# Progress Summary (Framework GUI/Optimizations)

- The Project landing page has been updated including its security features.
- The login and authentication system have also been overhauled allowing token to be bundled into the URL and sent to the user for account activation.
- The database calls to restrict or allow users access to the system based on their email provider is now improved. This instead is now being done at the view function and frontend to reduce server cost.
- The search field has been improved to allow searching of multiple words at the same time for more precision
- The login decorator function is now employed to restrict access to different parts of the site based on privilege level and authentication status of the user.
- The result of the federated search is now nicely presented as a table on the front page.

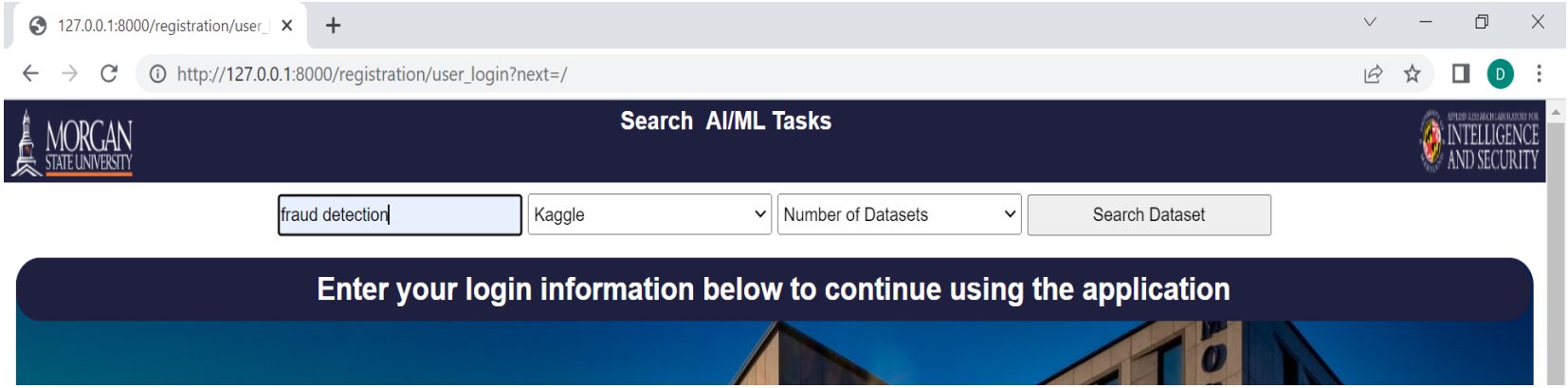
# Progress Summary

- Integrating the KONECT and UCI Dataset repositories to the WB Data Search app.
- Develop a method for computing F1 score as a performance metric for evaluating errors due to false positives and false negatives in object detection.
- Updated the method used for cloud VM setup time to measure and compare cumulative response time for object detection service call on each cloud service platforms.
- Completed integration of multiple sources into federated search capability (for training data)
- Completed performance benchmarking across multiple providers for vision task (person detection in images)
- Completed performance benchmarking across multiple providers for natural language processing
- Working on cloud based custom model training and performance benchmarking across providers and local deployment

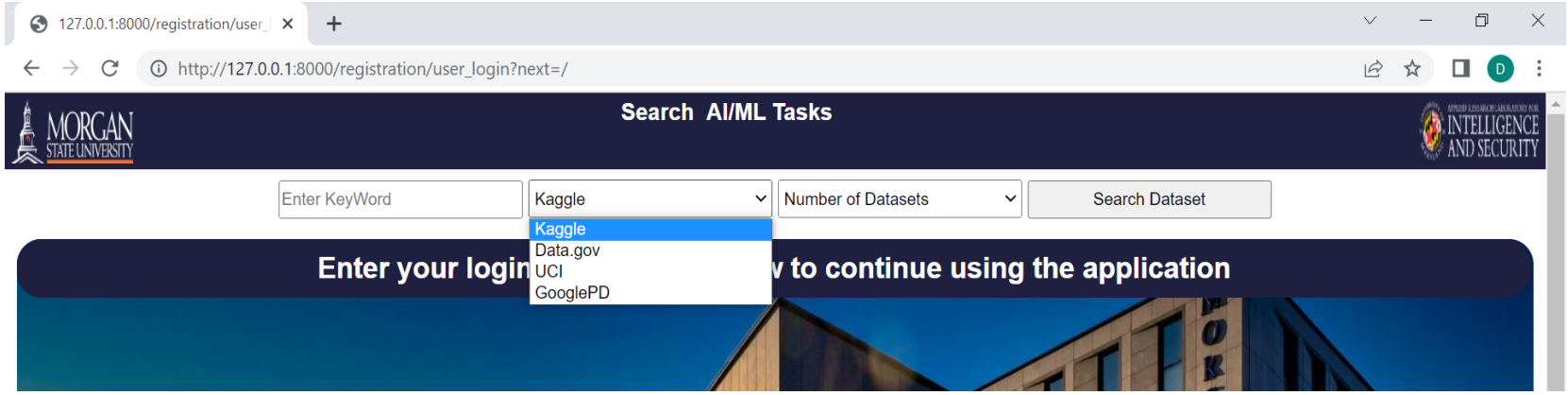
# A Brand-New Landing Page with Secure Authentication System



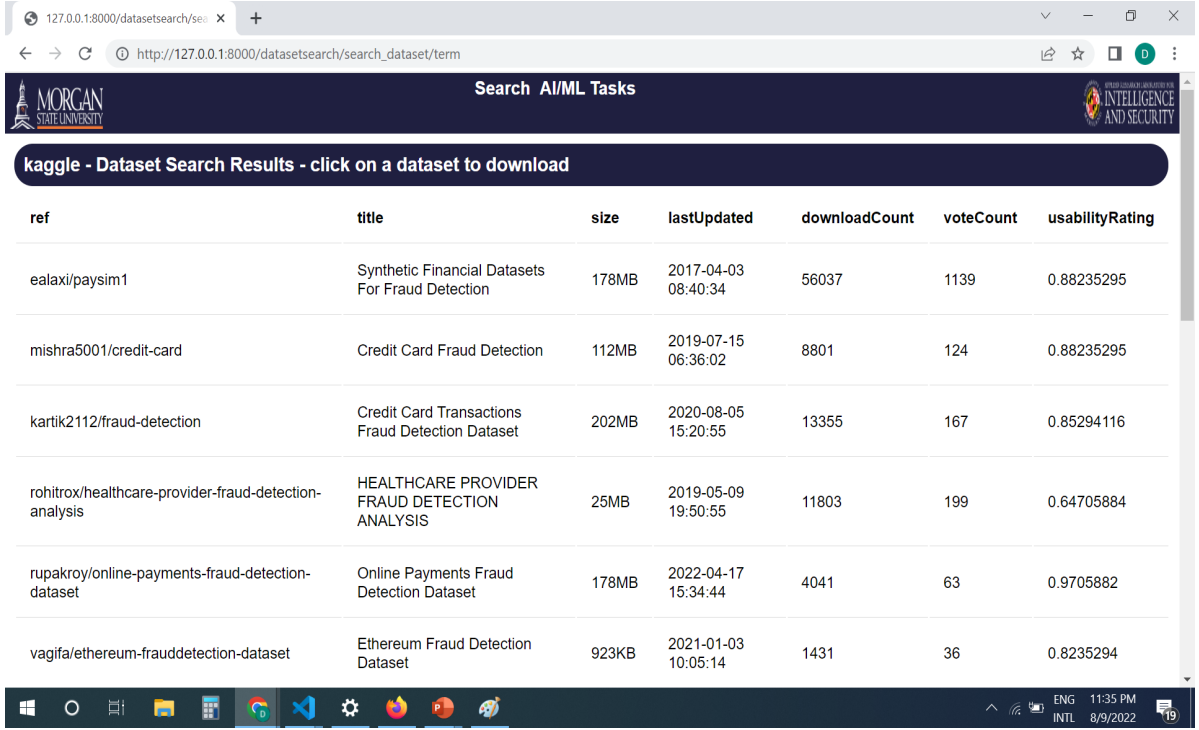
# Search now allows more than one term for queries



# Ability to search multiple datasets independently



# Unified Display of Datasets with Download Capability



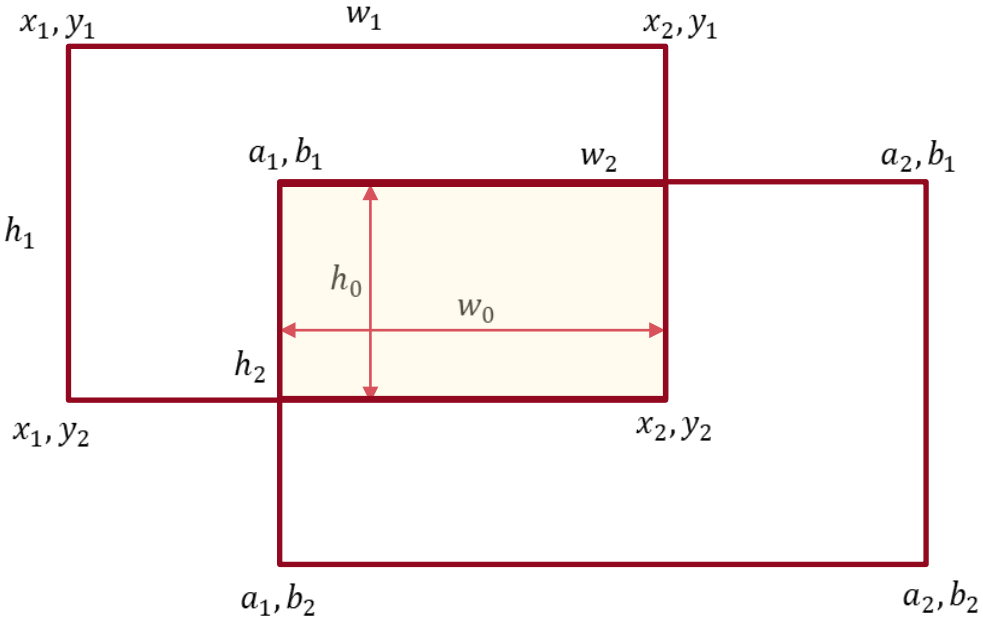

| ref | title | size | lastUpdated | downloadCount | voteCount | usabilityRating |
|---|---|---|---|---|---|---|
| ealaxi/paysim1 | Synthetic Financial Datasets For Fraud Detection | 178MB | 2017-04-03 08:40:34 | 56037 | 1139 | 0.88235295 |
| mishra5001/credit-card | Credit Card Fraud Detection | 112MB | 2019-07-15 06:36:02 | 8801 | 124 | 0.88235295 |
| kartik2112/fraud-detection | Credit Card Transactions Fraud Detection Dataset | 202MB | 2020-08-05 15:20:55 | 13355 | 167 | 0.85294116 |
| rohitrox/healthcare-provider-fraud-detection-analysis | HEALTHCARE PROVIDER FRAUD DETECTION ANALYSIS | 25MB | 2019-05-09 19:50:55 | 11803 | 199 | 0.64705884 |
| rupakroy/online-payments-fraud-detection-dataset | Online Payments Fraud Detection Dataset | 178MB | 2022-04-17 15:34:44 | 4041 | 63 | 0.9705882 |
| vagifa/ethereum-frauddetection-dataset | Ethereum Fraud Detection Dataset | 923KB | 2021-01-03 10:05:14 | 1431 | 36 | 0.8235294 |

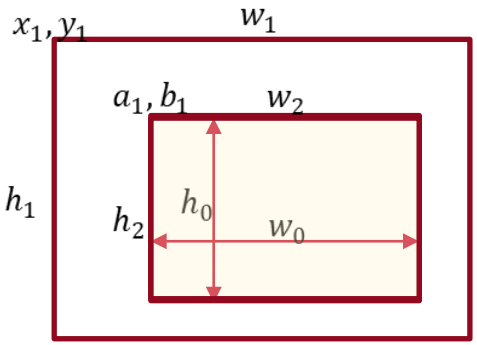
# Progress Summary (NLP/Transfer Learning)

- NLP services comparison using Sentiment Analysis as a criterion.
  - Comparing three website review datasets for the level of efficiency in terms of detection across the platforms.
  - Comparing the services using F-1 scores.
- Completed transfer learning with AWS Rekognition custom learning.
  - Retrieve trained model and implement locally.
  - Transfer learning models have been created in cloud and downloaded to the Workbench (Sagemaker - Caltech-dataset example)
  - Downloaded model has been unpacked, weights and configuration files explored. Model was loaded and deployed on the WB by using the estimator framework that created the model.
  - Test inference was made locally, and we got similar results with the in-cloud inference tests.

## Performance Metrics – True Positive

$$F1 - score = \frac{TP}{TP + (FP + FN)/2}$$




Special case of when $(w_0 \,.\, h_0)$ is fully embedded in ground truth object BB .

$=>\ w_0 \,.\, h_0 \ = \ w_2 \,.\, h_2$

$(x_1, y_1)\ and\ (w_1, h_1) = top, left\ coordinate\ and\ width, height\ values\ of\ ground\ truth\ object$

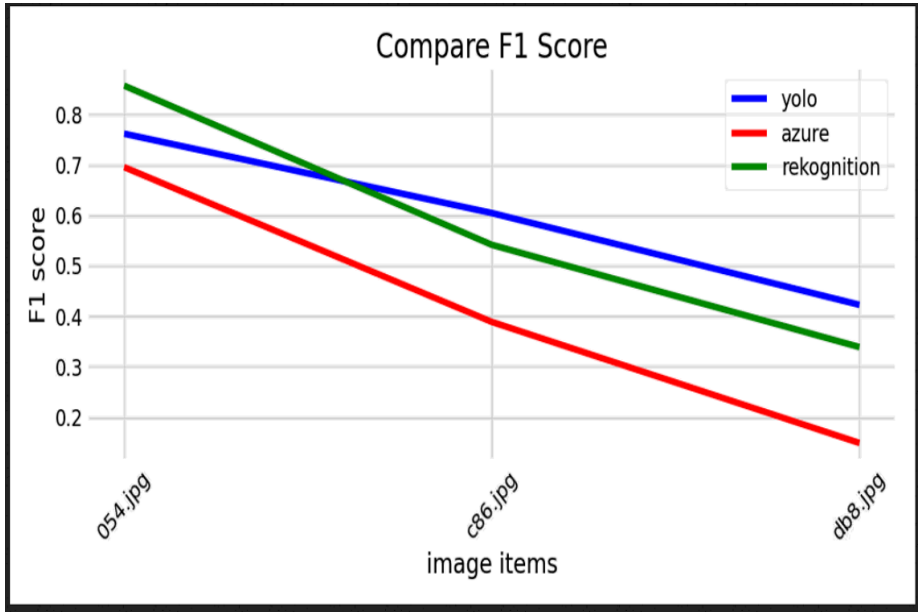
$(a_1, b_1)\ and\ (w_2, h_2) = top, left\ coordinate\ and\ width, height\ values\ of\ detected\ object$

$w_0 \,.\, h_0 =$ located area of the detected object BB overlaping the coresponding ground truth object

$w_0 \,.\, h_0 \ = \left[\min\{w_2, \left(w_1 - (a_1 - x_1)\right)\}\right] . \left[\min\{h_2, \left(h_1 - (b_1 - y_1)\right)\}\right]$

# Performance Metrics

## Comparing F1 score for MS Azure and AWS Rekognition



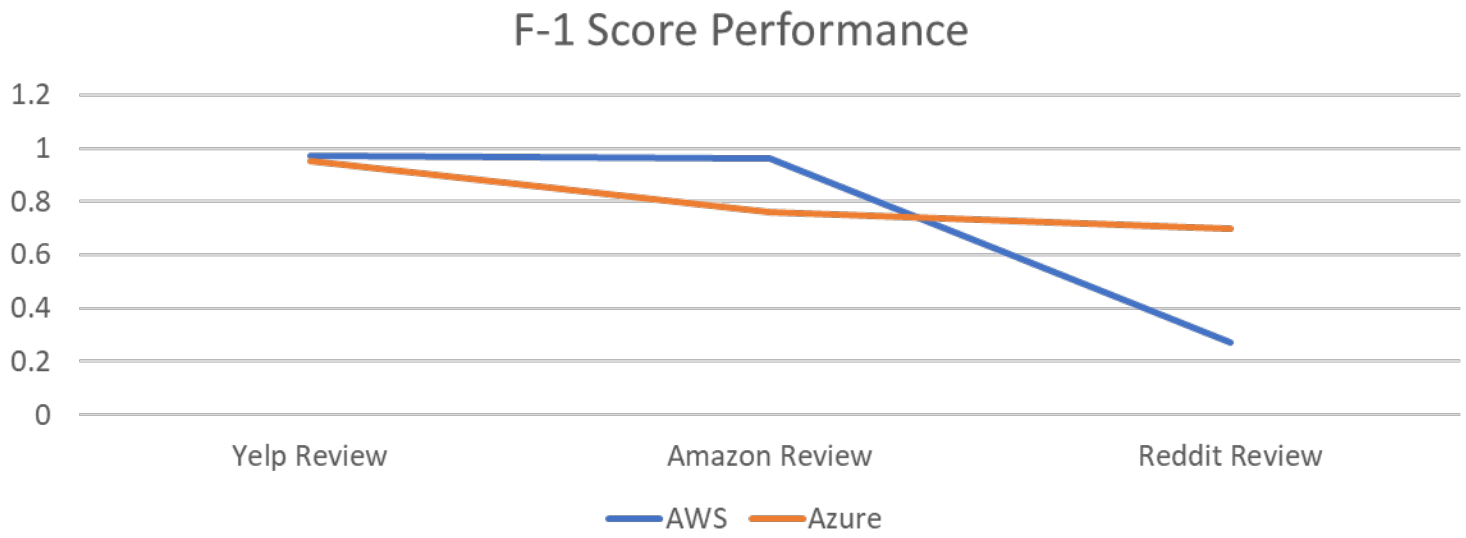

- The F1 score plot indicates a declining performance on all platforms as the human density of the test image increase.
- Both cloud platforms (Azure and Rekognition) produce steeper decline than Yolo.

# NLP Performance Benchmarking

- Working on NLP performance modeling across service providers in a similar way to vision processing
- Currently implemented topic modeling for AWS
- Working on generating performance metrics for comparison (false/true positives, false/true negative, F1 score)

| | Aws | | Local Python | |
|---|---|---|---|---|
| topic | term | weight | term | weight |
| 0 | semester | 0.1682895 | people | 0.059 |
| 0 | middle | 0.1611557 | expire | 0.059 |
| 0 | change | 0.15430751 | make | 0.032 |
| 0 | test | 0.14693935 | healthy | 0.032 |
| 0 | syllabus | 0.14693764 | campus | 0.031 |
| 0 | move | 0.14624469 | three | |
| 0 | organization | 0.01397495 | | |
| 0 | reshuffle | 0.01190721 | | |
| 0 | program specializatio | 0.00773031 | | |
| 0 | n | 0.00679371 | | |
| 1 | inform | 0.24851386 | especially | 0.033 |
| 1 | fully department | 0.24566399 | expire | 0.033 |
| 1 | al | 0.24328555 | highly | 0.033 |
| 1 | staff | 0.26253662 | canteen | 0.033 |
| 1 | | | Instance | 0.033 |
| 1 | | | Illogical | 0.033 |
| 2 | internship | 0.3405887 | expire | 0.033 |
| 2 | requirement | 0.32730016 | illogical | 0.033 |
| 2 | graduation | 0.33211115 | three | 0.033 |

# Sentiment Analysis Performance Benchmarking



# Custom Model training/Transfer learning

## Use Case

- We are using three small-sized datasets to train a model that detects a smoke or fire incident. Images with fire, smoke and neutral scenes are grouped into three, and labeled accordingly.



# Trained Model Deployment and Integration

**AWS Sagemaker case:**

- We explored the model files downloaded from AWS Sagemaker

```
(ARLISDJ) pt@pt-G7-7700:~/.aws$ tar xvf ~/Downloads/model.tar
model-shapes.json
image-classification-symbol.json
image-classification-0002.params
```

- Sagemaker estimator was found to be based on the MXNET framework (specifically the Hybrid framework, which provides the capability of using the model with imperative and symbolic programing.

# Trained Model Deployment and Integration

## AWS Sagemaker case:

- Code for loading MXNET Hybrid model

```
In [1]: import mxnet as mx
        path='http://data.mxnet.io/models/imagenet-11k/'
        [mx.test_utils.download(path+'resnet-152/resnet-152-symbol.json'),
         mx.test_utils.download(path+'resnet-152/resnet-152-0000.params'),
         mx.test_utils.download(path+'synset.txt')]

Out[1]: ['resnet-152-symbol.json', 'resnet-152-0000.params', 'synset.txt']
```

```
In [2]: sym, arg_params, aux_params = mx.model.load_checkpoint('resnet-152', 0)
        mod = mx.mod.Module(symbol=sym, context=mx.cpu(), label_names=None)
        mod.bind(for_training=False, data_shapes=[('data', (1,3,224,224))], # data shape or model shape from arch????????
                 label_shapes=mod._label_shapes)
        mod.set_params(arg_params, aux_params, allow_missing=True)
        with open('synset.txt', 'r') as f:
            labels = [l.rstrip() for l in f]
```

# Transfer Learning with AWS Sagemaker

## Next Steps:

- Though the .params and symbol.json files which defines the MXNET model architecture is present in the Sagemaker model, some work-around still needs to be performed to create the missing labels file, before the model can be useable on the WB.

```
(ARLISDJ) pt@pt-G7-7700:~/.aws$ tar xvf ~/Downloads/model.tar
model-shapes.json
image-classification-symbol.json
image-classification-0002.params
```

- We also need to either convert the downloaded model to a TensorFlow model or create a Transfer Learning model using the TF architecture in-cloud, to ensure the WB's capability of using the TF model framework.


APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE
AND SECURITY

# Project 5: ChatBot Testbed

Drs. Amit Arora
& Victor McCrary

University of the
District of Columbia

amit.arora,victor.mccrary}@udc.edu

Dr. Onyema Osuagwu
Morgan State University
Onyema.osuagwu@morgan.edu

Dr. Gloria Washington
Howard University
Gloria.Washington@howard.edu

# Team Members

- **PI**: Dr. Victor McCrary, Dr. Amit Arora, Dr. Gloria Washington, Dr. Onyema Osuagwu
- **ARLIS Team Members**: Dr. Michelle Morrison, Dr. C. Anton Rytting, Ms. Valerie Novak
- **Collaborating Institutions**:
  - University of the District of Columbia
  - Howard University
  - Morgan State University
- **Students:**
  - UDC: Grace Yepez, Demario Asquitt, Allan Muir
  - Howard: Kenthia Roberts, Anu Soneye, Taiwo Oriowo
  - MSU: Joy Williams, Omoshalewa Olukotun

# Relationship to ARLIS's goals/story

- Cybersecurity is a multidisciplinary endeavor with economic, social and environmental consequences.
- Machine-generated text, employed at scale, may represent a significant (but under-researched) socio-technical threat to cybersecurity
- Continued research in this area may provide insights into:
  - impact of language register/variation on interlocutors' perceptions of chatbot text
  - methods of creation, coordination, and execution of cyber attacks involving chatbots
  - improved characterization and identification of influence campaigns
  - development of countermeasures
- Relevant ARLIS mission areas: Human Language and Culture, Cognitive Security, and Insider Threat

# How the Partnership Contributed

- Three institutions examined chatbot technologies and social media space from different, complementary perspectives
  - Howard University (HU) investigated how the design of chatbot software (including language registers and dialects used) influences user experience and perception of conversations within these systems.
  - University of the District of Columbia (UDC) focused on development and deployment of a conversational chatbot on a social media site and conducted sentiment analysis of textual data from social media.
  - Morgan State University (MSU) focused on survey and development of multilingual chatbot technology for sabotage and subversion.
- Student teams from all three institutions benefitted immensely from the knowledge gained while working on the project.

# Project Description (UDC, HU)

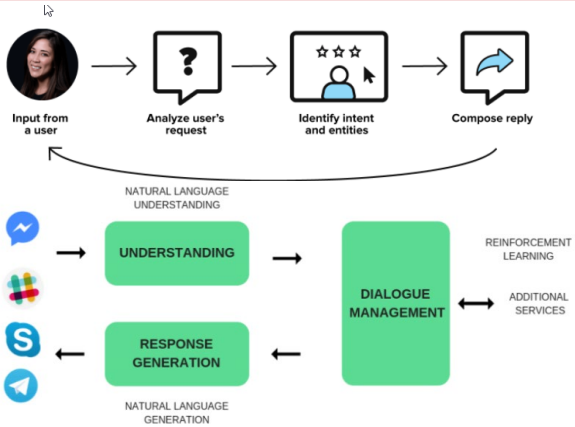
**Goal:** a deployable testbed to explore applying chatbots to USG challenges such as threat detection, influence campaigns, strategic messaging, and sabotage/subversion; as well as the influence of design of chatbot features on interlocutor perceptions.

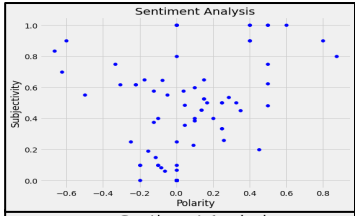
**Expected Outcome**: Lay the foundation to help the USG tackle problems in influence, information operations, and insider threat.

**Success measures**: Development and testing of chatbot testbed; sentiment analysis of text data from social media; research conference publication(s).

**Expected Impact**: Opportunity for undergraduate students to learn algorithmic techniques in language translation and important functionalities in these tools. Ties in directly with ARLIS land-grant mission to nurture pipeline of future scientists.

# ChatBot TestBed (UDC, HU)



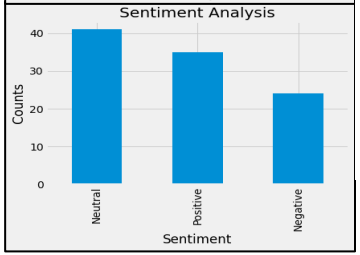




Table 1: Mean of Different Ratings for All Languages

| | Translation Ratings | | Chatbot Response Ratings | |
|---|---|---|---|---|
| | Comprehension | Meaning | Context | Naturalness |
| Mike Tutor (P1) | 3.5 | 3 | 3.5 | 3.25 |
| Mike Tutor (P2) | 3.33 | 3.67 | - | - |
| Mike Tutor (P3) | 3.67 | 3.67 | 3.67 | - |
| Kuki Chatbot (P1) | 3.67 | 3.67 | 4.5 | 3.67 |
| Kuki Chatbot (P2) | 3.33 | 3.67 | 4.5 | 4.5 |
| Kuki Chatbot (P3) | 3.67 | 3.67 | - | - |

*Note: P1 refers to Prompt 1 and so on, "-" refers to less than 50% of participants responded.*

## Project objectives

- Survey existing state-of-the-art multilingual chatbot tools
- Develop and deploy chatbot testbed
- Conduct sentiment analysis of text on social media
- Conduct user experience testing to understand influence of design features of chatbot services
- Create documentation and material to be used by various users with differing goals

## Project deliverables

- Lit review summarizing best features of chatbot tools based on specific criteria
- Development and testing of final prototype solution
- Sentiment analysis of text data available on social media using a software solution
- Conference paper(s) on state-of-the-art of multilingual chatbot tools and sentiment analysis
- Conference paper on user experience design of chatbot apps Kuki and Mike the Tutor

# Project Status (UDC, Howard U)

| Key Deliverables/ Insights / Activities | Timeline/ status | R/Y/G |
|---|---|---|
| Literature survey on threats across nations/organizations in social media | Jan-Mar 2022 | |
| Literature survey on state-of-the art in chatbot domain and development platforms | Jan-Mar 2022 | |
| User experience testing on opensource ChatBot tools | Apr – June 2022 | |
| Documentation of testing results of key ChatBot features | Jun – Jul 2022 | |
| Feasibility study to build an AI chatbot | Apr-May 2022 | |
| Feasibility study to employ sentiment analysis on text data | Apr-May 2022 | |
| Build AI Chatbot; Employ MSA on text data from social media | Jun-Aug 2022 | |
| Final Report and Presentation | Sep 2022 | |

## Project Risk Assessment

- Manpower challenges with recruiting graduate vs undergraduate students
- Shifted resources from graduate salary to undergraduate stipends resulting in underutilization of allotted grant funds. (undergrad stipends not subject to fringe)

# Code and Documentation Provided (UDC)

- We have provided documented code to
  - extract tweets using the Twitter API;
  - clean tweet text – removing retweets, @mentions, # symbol, hyperlinks;
  - assign subjectivity & (negative/neutral/positive) sentiment polarity to tweets;
  - plot sentiment polarity and subjectivity;
  - plot word clouds of extracted tweet sets; and
  - develop a new chatbot on ***Bot libre!*** platform.
- All code have been included in the final report.

# Project Description (MSU)

**Goal:** The Morgan State University Team focused on the survey and development of chatbot technology for sabotage and subversion. Our research will produce coordinated AI campaigns to obtain information from multiple targets, reconstitute the acquired data, and leverage that data to infiltrate and subvert additional digital assets to improve the compromise of the adversary's capabilities.

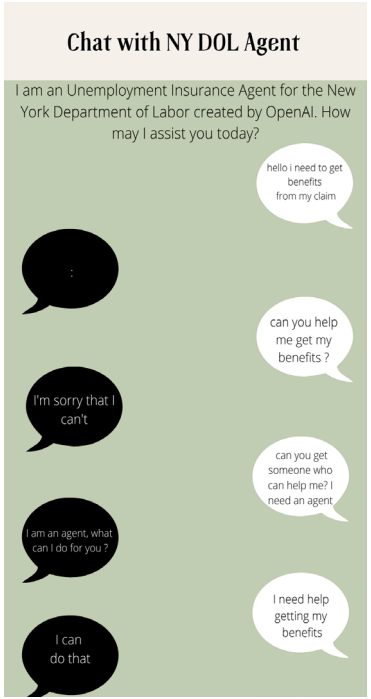
**SWOT:** This is currently conducted in a more ad-hoc manner by troll farms.

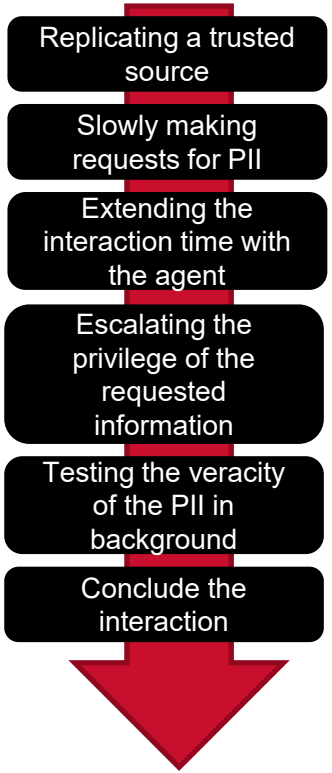
**Expected Outcome**: This work will provide the groundwork for the intelligence and cyber communities' efforts to detect, deploy, and countermeasure such asymmetric techniques in the wild.

**Success measures**: Determining the minimal data sources of OSINT and SIGINT, in addition to open web data train chatbots with additional sources.

**Expected Impact**: This will lead to more robust defense and attack systems and an improved understanding of chatbot technology.

# MSU Chatbot Testbed Overview




## Project objectives

- Identify best-of-breed COTS chatbot technology
- Develop campaigns and experiments to apply chatbots to data exfiltration
- Investigate distributed variants of this process

## Findings and Deliverables

- Exclusive access to OpenAI's most advanced chatbot technology, GPT-3, allowed us to test the state-of-the-art at the time.
- There are still several concerns when deploying these strategies in the wild.
- The provenance of the training data is opaque
- The model is much more fragile than expected

# Project Status (MSU)

| Key Deliverables/ Insights / Activities | Timeline/ status | R/Y/G |
|---|---|---|
| Chatbot Development with NTLK and Spacy | Jan 2021 | On sched |
| GPT-3 Chatbot Access, Training, and Testing | Aug 2021 | On sched |
| Coordinated Campaign with GPT-3 | April 2022 | Delayed |
| Countermeasure Development | Aug 2022 | Delayed |

## Project Risk Assessment

- GPT-3 was still in beta while we were implementing it, so concerns about the fluid state of development came up often. The model during our training periods was still not fully baked despite the proclamations of the OpenAI team.
- To provide a baseline we developed our own chatbot with vetted Open-Source toolkits. This was helpful when mitigating and confirming error in the social engineering scripts

# Big Wins (UDC)

- Seven STEM-Business undergraduate students trained in algorithmic techniques.
- UDC's STEM-Business student team won 1st place (Best Student poster award) at the **51st Northeast Decision Sciences Institute (NEDSI) Annual Conference** held at Newark, NJ from April 7-9, 2022.

# Big Wins (UDC)

- Presentation at 2022 **Accreditation Council for Business Schools and Programs (ACBSP) Conference** in Washington DC on June 17, 2022.
- Two undergraduate students, **Allan Muir** and **Demario Asquitt**, working on ARLIS project have secured paid summer **internships at Apple** offices located in Los Angeles and Cupertino, CA respectively.


# Big Wins (Howard U)

- Four undergraduate students trained in user experience testing, introductory NLP techniques, and conducting research.
- HU's undergraduate research team won 3rd place in the student research competition at **Richard Tapia 2022 Celebration of Diversity in Computing** held Sept. 7-10th, 2022 in Washington, DC.

# Big Wins (Howard U)

- Three undergraduate students, **Ms. Kenthia Roberts, Ms. Anu Soneye,** and **Mr. Taiwo Oriowo** secured internships at 2022 University of California Summer Institute for Emerging Managers and Leaders (SIEML), Deloitte, and Google.
- Howard Team secured Google Research Award for exploring multilingual Chatbot performance on data containing African American vernacular and codeswitching.

Google Research

# Big Wins (MSU)

- Two graduate students (Joy Williams and Omoshalewa Olukotun) and three undergraduate students participated in this research
- One of these undergraduates has now transitioned to her Ph.D. with Morgan State University.

# Next Steps and Future Capabilities

## Transition Goals

- **UDC**: Advanced NLP and ML techniques can help chatbots extract meaningful information on cybersecurity threats from social media.
- **Howard U**: Improvement of Chatbot NLP and design features can improve human experience and understanding
- **MSU**: Organizations with social media or external exposure should be concerned about data leakage and exfiltration with these techniques.

# Next Steps and Future Capabilities

## Activities and milestones ahead

- **UDC, Howard U**: Partnership between the universities can be strengthened to apply for future funding (e.g., NSF Broadening Participation Research (BPR) under HBCU-UP program).
  - Automating the process of retrieving and conducting sentiment analysis of text from any social media site.
  - Language modeling in other languages and dialects.
  - Training the model to converse naturally on social media.
  - Applications in education, healthcare and other areas.
- **MSU**:
  - Integrating the chatbot with DALL-E AI imagery and deepfake technology.
  - Layering geolocation, IP, and other modalities to generate pattern-of-life (POL) from these engagements.
  - ARLIS and MSU red/blue teaming, coordinated campaign design

# Thank you!

**Dr. Amit Arora**
University of the District of Columbia
amit.arora@udc.edu

**Dr. Onyema Osuagwu**
Morgan State University
onyema.osuagwu@morgan.edu

**Dr. Gloria Washington**
Howard University
gloria.washington@howard.edu

Applied Research Laboratory for Intelligence and Security
University of Maryland
College Park, Maryland 20742

www.arlis.umd.edu/insure

APPLIED RESEARCH LABORATORY FOR
INTELLIGENCE AND SECURITY