Coastal Virginia Center for Cyber Innovation
December 31, 2020

Semi-Annual Progress Report
Research and Faculty Reports
(July 2020 – December 2020)

Brian Payne – Director
R. Michael Robinson – Deputy Director
John Costanzo – Administrative Officer/Program Manager

5115 Hampton Boulevard
Norfolk, Virginia 23529
(757) 683-4757
Email: bpayne@odu.edu

Table of Contents

Appendix 1: Cybersecurity Research Project Team Reports *4*

i. Explore Privacy-Preserving in Deep Image Retrieval Systems. Old Dominion University, William & Mary, and Hampton University *5*

ii. Encouraging Positive Changes in Cyber Hygiene Behaviors and Knowledge in the Department of Defense. Old Dominion University and MI Technical Solutions *7*

iii. Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks. William & Mary and Old Dominion University *9*

iv. Leveraging AI and Machine Learning to Develop New CPSS and Workforce Development Solutions. Old Dominion University and CivilianCyber *12*

v. Trust, Interoperability and Inclusion: A Framework for Creating Cyber-Trust in Connected Homes. William & Mary and Old Dominion University *20*

Appendix 2: Research Scientist Faculty Reports *23*

i. Tan Le, Old Dominion University *24*

i. Yan Lu, Old Dominion University *38*

ii. Rui Ning, Old Dominion University *43*

iii. Daniel Shin, College of William & Mary *49*

iv. Masiane Moeti, Norfolk State University *52*

Research Initiatives

COVA CCI Cybersecurity Research and Innovation Funding Program
The COVA CCI Cybersecurity Research and Innovation Funding program supports diverse and inclusive CPSS research efforts, with a focus on the intersection of artificial intelligence (AI), cybersecurity, and CPS technologies applied to maritime, transportation, and defense sectors.

Five research projects were awarded for COVA CCI node funding in Spring 2020. These projects are on-going and are scheduled to be completed in May 2021.
These projects are.

1. Explore Privacy-Preserving in Deep Image Retrieval Systems. Old Dominion University, William & Mary, and Hampton University
2. Encouraging Positive Changes in Cyber Hygiene Behaviors and Knowledge in the Department of Defense. Old Dominion University and MI Technical Solutions
3. Leveraging AI and Machine Learning to Develop New CPSS and Workforce Development Solutions. Old Dominion University and CivilianCyber
4. Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks. William & Mary and Old Dominion University
5. Trust, Interoperability and Inclusion: A Framework for Creating Cyber-Trust in Connected Homes. William & Mary and Old Dominion University

See the news stories from ODU News and Inside Business (May 25, 2020) for additional information regarding these projects.

See Appendix 1 for Research project reports.

Research Scientists
COVA CCI is funding a regional cluster hire of four research scientists for Norfolk State University (1), Old Dominion University (2), and William & Mary (1). A fifth research scientist was hired by ODU as a match. These scientists will conduct research in cybersecurity related projects supporting the goals of CCI.

See Appendix 2 for Research Scientist reports.

Appendix 1: Cybersecurity Research Project Team Reports

Cybersecurity Research Project Team reports

i. Explore Privacy-Preserving in Deep Image Retrieval Systems. Old Dominion University, William & Mary, and Hampton University

ii. Encouraging Positive Changes in Cyber Hygiene Behaviors and Knowledge in the Department of Defense. Old Dominion University and MI Technical Solutions

iii. Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks. William & Mary and Old Dominion University

iv. Leveraging AI and Machine Learning to Develop New CPSS and Workforce Development Solutions. Old Dominion University and CivilianCyber

v. Trust, Interoperability and Inclusion: A Framework for Creating Cyber-Trust in Connected Homes. William & Mary and Old Dominion University

i. Explore Privacy-Preserving in Deep Image Retrieval Systems. Old Dominion University, William & Mary, and Hampton University

Faculty Report: Cong Wang, Qun Li and Janet Walters-Williams
Report Date: December 22, 2020

Initiative/Project Title: Explore Privacy-Preserving in Deep Image Retrieval Systems

1. Lay Summary: This project aims to explore the security and privacy issues in deep image retrieval systems. These systems utilize content-based similarity matching that users can use image queries to search for the similar images in the database, without knowing the name of the content. An open problem is the security and privacy of these systems as service providers usually aggregate images into the database for potential queries. This project aims to: 1) design a privacy-preserving technique such that private images would not be returned even though they are gathered by the database; 2) explore the attack surface to the integrity of the system facing black-box attacks. The research builds on the known vulnerability of deep learning to utilize it as either a privacy-preserving countermeasure or an offensive attack strategy. The project will strengthen the collaboration between ODU, William & Mary and Hampton University in machine learning and security research, and advance cybersecurity education in the Hampton roads area on both undergraduate and graduate levels in the novel AI security field.

2. Project Focus (check all that apply):
_x__ Research
___ Innovation / Commercialization of IP
___ Workforce Development / Job Creation

3. Breakthroughs
We have made the following contributions and breakthroughs:
I. We have successfully developed a privacy-preserving technique to prevent private images from the users being matched and returned by the image retrieval system. We have re-designed the optimization goal to induce adversarial perturbation on the original image such that the user's image will reside at the non-retrievable regions. The work is published in: Yanru Xiao, Cong Wang and Xing Gao, Evade Deep Image Retrieval by Stashing Private Images in the Hash Space, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, 2020. (Acceptance Rate: 22%)
2. We have also successfully enhanced the success rate of the targeted black-box attack. Our mechanism leverages additive random noise to land adversarial perturbations in a more robust region, such that they are more transferrable to a heterogenous model architecture. We are now conducting more experiments to validate the effectiveness of our mechanism in traditional softmax classification networks.

4. External Grants:

Funding Agency	Project Title	Period of Performance	Funding amount
NSF	CHS: Small: AI-Human Collaboration in Autonomous Vehicles for Safety and Security	10/1/20 – 9/30/23	$500,000

5. Results of entrepreneurship
We have published the source code of the first part of the project on Github: https://github.com/sugarruy/hashstash

6. Results of workforce planning. NA

7. Collaborative partnerships and projects
Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Cong Wang	Assistant Professor	ODU	PI-Lead
Qun Li	Professor	William & Mary	PI
Janet Walters-Williams	Assistant Professor	Hampton University	Adjunct

Organizations: Other organizations involved as partners. NA

Collaborators or Contacts: Other collaborators or contacts involved. NA

8. Correlated economic outcomes. NA

9. Additional Information
The following publications are supported in part by this award:

Cong Wang, Yuanyuan Yang and Pengzhan Zhou, Towards Efficient Scheduling of Federated Mobile Devices under Computational and Statistical Heterogeneity, Accepted to Appear in the IEEE Transactions on Parallel and Distributed Systems.

Yanru Xiao, Cong Wang and Xing Gao, Evade Deep Image Retrieval by Stashing Private Images in the Hash Space, IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, 2020. (Acceptance Rate: 22%)

ii. Encouraging Positive Changes in Cyber Hygiene Behaviors and Knowledge in the Department of Defense. Old Dominion University and MI Technical Solutions

Faculty Report: Jeremiah Still, Old Dominion University
Report Date: December _31st___ 2020

Initiative/Project Title:
Encouraging Positive Changes in Cyber Hygiene Behaviors and Knowledge in the Department of Defense

1. Lay Summary:
We are developing SCORE to identify poor cyber-hygiene behavior, and to design an interface that effectively increases users' awareness of their cyber risk. The system will alert users to at-risk behaviors and creates reports. The goal is to show SCORE can raise the awareness of cybersecurity policy violations. Both the technology and user experience will be developed to increase users' cyber awareness, knowledge, and willingness to comply with cybersecurity policies.

2. Project Focus (check all that apply):
_X__ Research
___ Innovation / Commercialization of IP
___ Workforce Development / Job Creation

3. Breakthroughs
No breakthroughs yet. We are currently collecting data for three proposed studies.

4. External Grants: NA

5. Results of entrepreneurship
We plan to submit a provisional patent application to ODU during the Spring semester for CHIP.

6. Results of workforce planning
Janine Mator is being funded as a GRA. This work has influenced her research path. Janine plans to develop her dissertation around understanding the Human Factors surrounding AI and cyber hygiene.

7. Collaborative partnerships and projects
Project Objectives
MITS: Develop SCORE for Cyber Hygiene & Provide DoD Expertise
• Generate initial activities database
• Determine Cyber Hygiene recommendations
• Create interfaces for generating reports, alerts, and data visualizations
• Create interface feedback that guides how-to correct noncompliance
• Update SCORE's interface based on our human-centered design findings & proposed studies

• Staff serves as DoD content experts
• Led the way on exploring future funding options from DoD

Dr. Still's Laboratory: Determine interface requirements, complete series of studies
• Meet with stakeholders to collect interface requirements
• Complete storyboarding, task analysis, and cognitive walkthrough
• Develop prototypes following a human-centered design process
• Develop messages and interactions that help users correct cyber-hygiene issues
• Develop messages and interactions that increase Cyber Situation Awareness
• Complete IRB applications
• Collect data
• Complete statistics
• Led the way on exploring future funding options from NSF
• Compare newly developed technology to traditional solution measuring user's Cyber Situation Awareness and cyber-hygiene knowledge
• Explore the social influence of visual achievement both internally and externally to the user

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Jeremiah Still, PhD	Asst. Prof.	ODU	PI
Mike Ihrig	CEO	MI Technical Solutions	CO-PI
John Gray, DM, PMP, LSSMBB		MI Technical Solutions	

Name	Title	Home Institution	Project Role
Rachel Jarvis, PMP		MI Technical Solutions	
Michael Wandel, MS		MI Technical Solutions	
Kurtis Lyle, BS		MI Technical Solutions	
Janie Mator, BS		ODU	GRA

Collaborators or Contacts: Other collaborators or contacts involved. NA

8. Correlated economic outcomes. NA

9. Additional Information
We are currently drafting two manuscripts, but don't expect submissions until April. Further, we plan to use the data collected from this project to support an NSF EAGER or small grant proposal.

iii. Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks. William & Mary and Old Dominion University

Faculty Report: Gang Zhou, William & Mary
Report Date: December __21__ _2020__

Initiative/Project Title: Securing IoT Devices through Power Side Channel Auditing and Privacy Preserved Convolutional Neural Networks

1. Lay Summary:
In order to make IoT bot detection practical and efficient, a fine-grained, universal, non-invasive, and privacy preserving detection technique is needed. In this project, we aimed to exploit IoT devices' power side channel information to identify the compromised IoT devices. We answered the following two major research questions: (1) How to exploit the power side channel information to characterize the malicious behaviors
of compromised IoT devices? (2) How to preserve data privacy when a cloud is used to offload the computation of the IoT bot detection algorithm?
To answer the first research question. We designed a Convolutional Neural Network (CNN) and corresponding digital signal processing technologies to model IoT sensor power data for differentiating malicious bot attacks from normal IoT sensing behaviors. Then, we incorporated our processing and modeling into a universal Smart Plug design so as to work with heterogeneous IoT devices in a ubiquitous way.
To answer the second research question, we developed a distributed high-performance machine learning based IoT bot detection with privacy preservation scheme. With this scheme, the IoT sensor power data are encrypted and uploaded to the cloud through a local
data inferencer. The encrypted data are processed by the CNN in the cloud, and the bot detection result is sent back and decrypted to plaintext. When an attack is detected, users are notified and the power to corresponding IoT devices are cut off by the Smart Plug for protection.

2. Project Focus (check all that apply):
__X_ Research
___ Innovation / Commercialization of IP
___ Workforce Development / Job Creation

3. Breakthroughs
We developed new hardware called Smart Plug. We also developed new digital signal processing technologies and CNN algorithms that process IoT power streaming data obtained through Smart Plug.
The CNN algorithm was developed as a distributed algorithm with a local data inferencer and a cloud-host computing module. These two modules communicate with a newly designed privacy-preserving protocol.
Multiple graduate and undergraduate students were trained through coordinated efforts from multiple faculty members from W&M and ODU through this project.

4. External Grants:

Funding Agency	Project Title	Period of Performance	Funding amount
NSF	Tangram: Scaling into the Exascale Era with reconfigured aggregated "Virtual Chips"	7/15/20 – 7/14/23	$213,426
NSA	Developing Cyber Talents to secure DoD cyberspace	9/16/20 – 12/31/21	$75,000

5. Results of entrepreneurship

Identify any products produced, patents, inventions, licenses, and other innovation activities

The team designed and developed the Smart Plug hardware and correspond privacy-preserved distributed CNN algorithm that goes across IoT/Edge/Cloud platforms. We plan to submit a U.S. patent application based on our inventions.

The team participated in the Innovation Commercialization Assistance Program (ICAP) by GMU in fall 2020.

The team submitted a commercialization proposal to COVA CCI based on this project in 2020 but was not funded.

6. Results of workforce planning

Describe any involvement in experiential learning, training, internships, and other workforce development activities

Multiple faculty members worked together to train multiple graduate and undergraduate students from W&M and ODU through the proposed project.

We plan to incorporate research results from this project into future courses taught by the PI and Co-PIs.

7. Collaborative partnerships and projects

Short description of project objectives

The objective of this project is to secure IoT devices through power side channel auditing and privacy preserved Convolutional Neural Networks.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Gang Zhou	Professor	W&M	PI
Chunsheng Xin	Professor	ODU	Co-PI
Danella Zhao	Associate Professor	ODU	Co-PI
Woosub Jung	Graduate Student	W&M	RA
Sabbir Khan	Graduate Student	ODU	RA (Unpaid)
Yizhou Feng	Graduate Student	ODU	RA

Amanda Watson	Graduate Student	W&M	RA (Unpaid)
Andrew Lyubovsky	Undergraduate Stud.	W&M	RA (Unpaid)
Luke McDevitt	Undergraduate Stud.	Brown Univ.	RA (Unpaid)
Trey Rankin	Undergraduate Stud.	ODU	RA (Unpaid)

Organizations: Other organizations involved as partners

Type of Org	Name	Location	Partner Contrib
PiKaso	Steve Elena	VA	Supported us in research commercialization
RISE Resilience	Paul Robinson	VA	Supported us in research commercialization

Collaborators or Contacts: Other collaborators or contacts involved

Type of Collab	Name	Location	Collaborator Role
Upwork Freelancer	Jeffrey Johnston	TX	Designed Smart Plug Cutoff circuit

8. Correlated economic outcomes

Multiple faculty members and graduate students from W&M and ODU were employed to work on the proposed research.

A freelancer from Upwork was hired to design Smart Plug cutoff circuits.

9. Additional Information

The team are currently developing two research papers for submission based on findings from this project.

iv. Leveraging AI and Machine Learning to Develop New CPSS and Workforce Development Solutions. Old Dominion University and CivilianCyber

Faculty Report: Darryl Amason
Report Date: December 2020

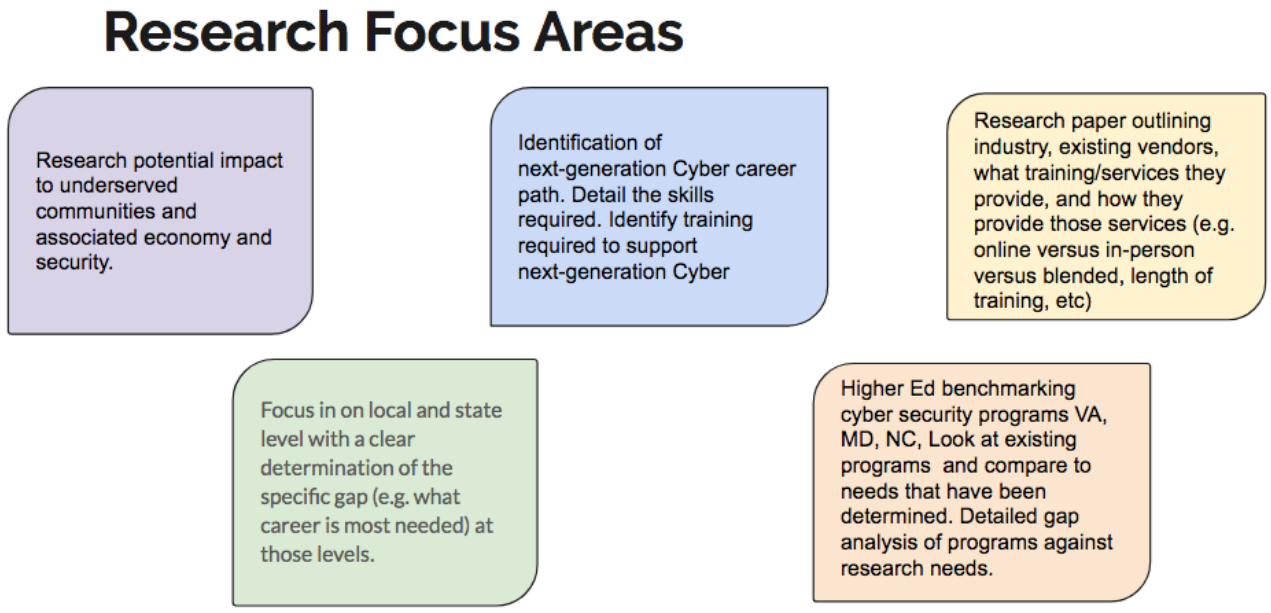
Initiative/Project Title: Leveraging AI and Machine Learning to Develop New CPSS and Workforce Development Solutions

1. Lay Summary:

This research project will seek to determine how to effectively automate the match of candidates to cyber jobs and associated training using Artificial Intelligence, analytics and novel data collection methodologies. This project leveraged crowd-sourced content and input to uncover new approaches to developing disruptive cyber-physical systems through the use of workforce assessment and experiential education via a secure prototype community on the Discovery Science Platform (iDISPLA). iDISPLA, a prototype community, provides the vehicle for talent aptitude assessments and to deliver smart training to match and develop personnel specifically for the roles for which they are best suited.

To guide our research, five integral areas focused on the foundation of this project. The five areas are depicted in figure 1.

Figure 1.

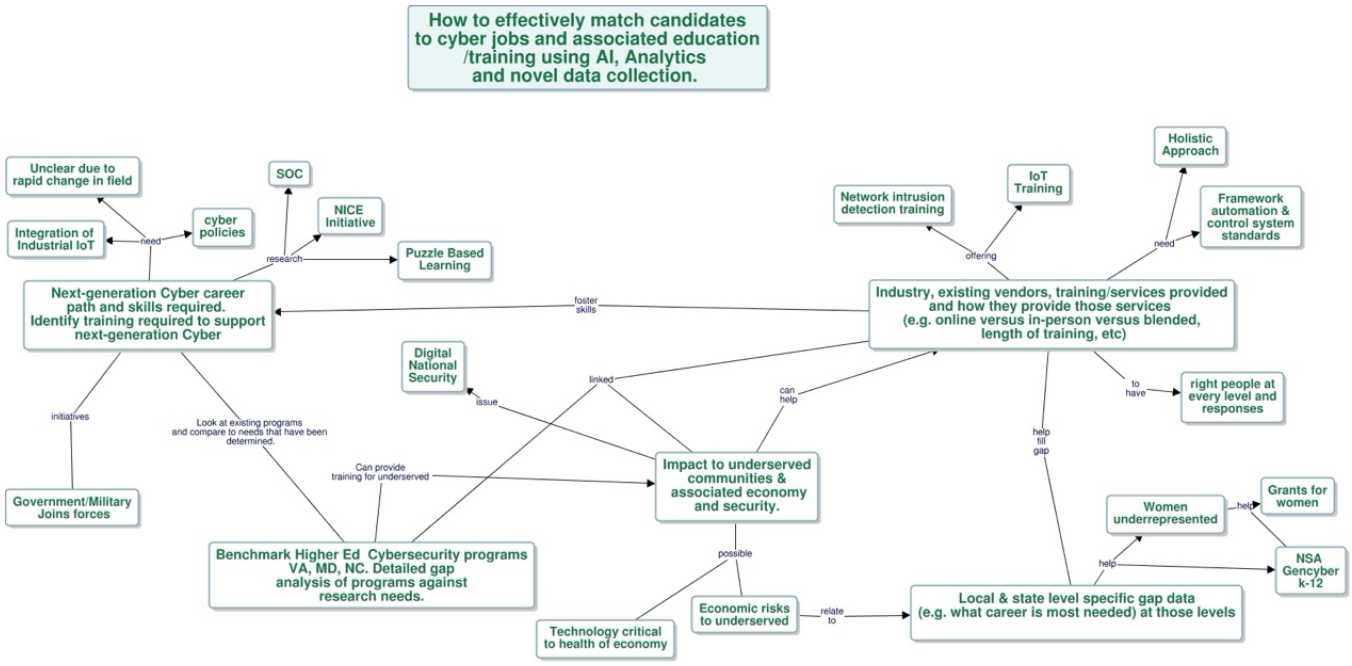


The ultimate goal is to achieve equitable access to opportunity in these fields, to positively impact transitioning Veterans, and create an awareness to prospective cyber talent as early as

middle and secondary school that would address the demand to improve the community/economy.

Figure 2 is a concept map of the five research areas:

Figure 2.



2. Project Focus (check all that apply):

X Research

X Innovation / Commercialization of IP

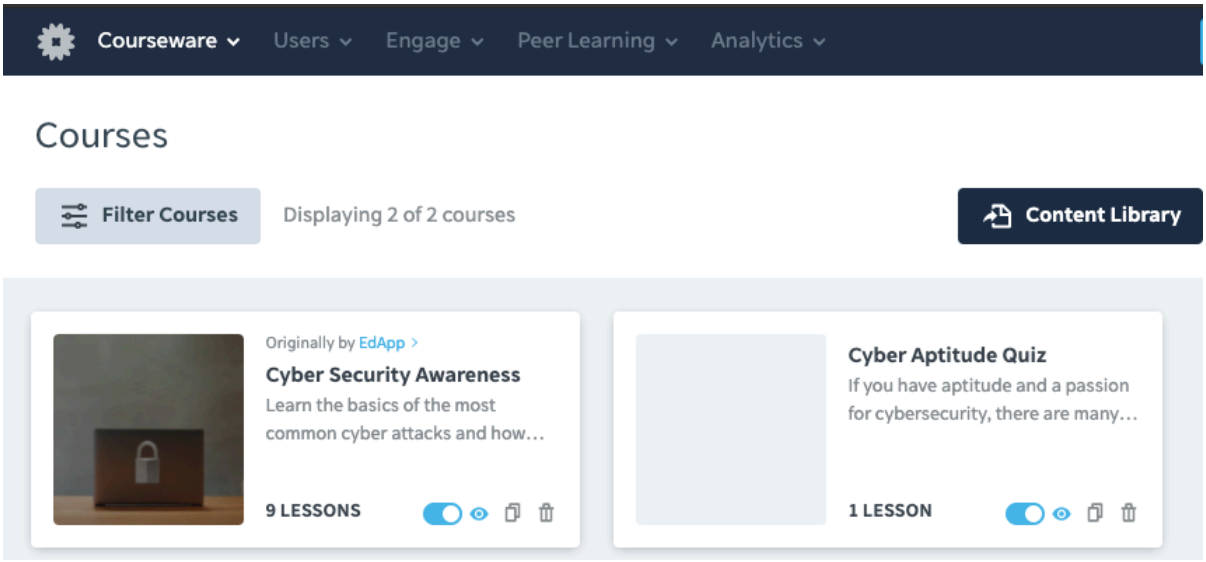
X Workforce Development / Job Creation

3. Breakthroughs

The research findings uncovered a better understanding of the barriers facing the cybersecurity profession and uncovered strategies that organizations can use to recruit, build and strengthen their cybersecurity teams.

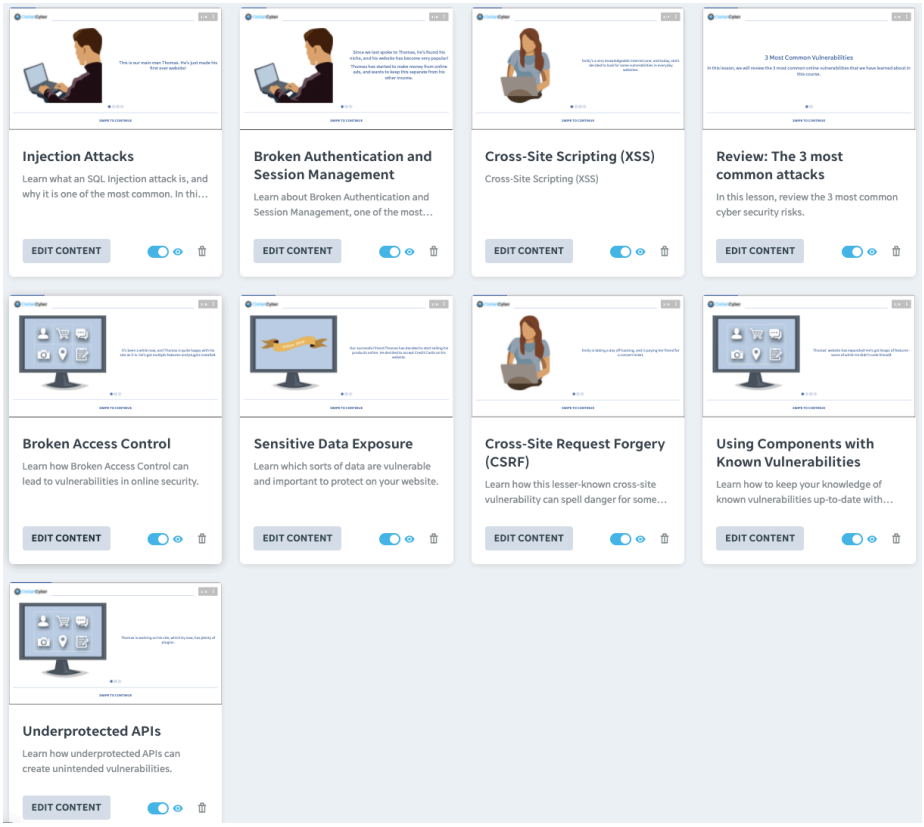
The development of nine cyber awareness courses and the cyber aptitude assessment was derived from the research findings. Below is a graphic depicting all nine modules and subject areas that are adapted for mobile, table and PC platforms.

Figure 3.



The nine modules shown below in figure 4 addresses basic cyber security principles and activities. Each module uses an innovative approach to present the content by using storytelling/gamification as a pedagogy. This platform is customizable and will lead to commercialism of this training products for workforce development.

Figure 4.



The cyber aptitude assessment is located on two platforms: the first in conjunction with the nine learning modules (figure 3), and the second in a newly developed Moodle LMS platform (figure 5 below). The cyber aptitude assessment measures the following cyber aptitudes: analytical thinking, inductive and deductive reasoning.
Figure 5.

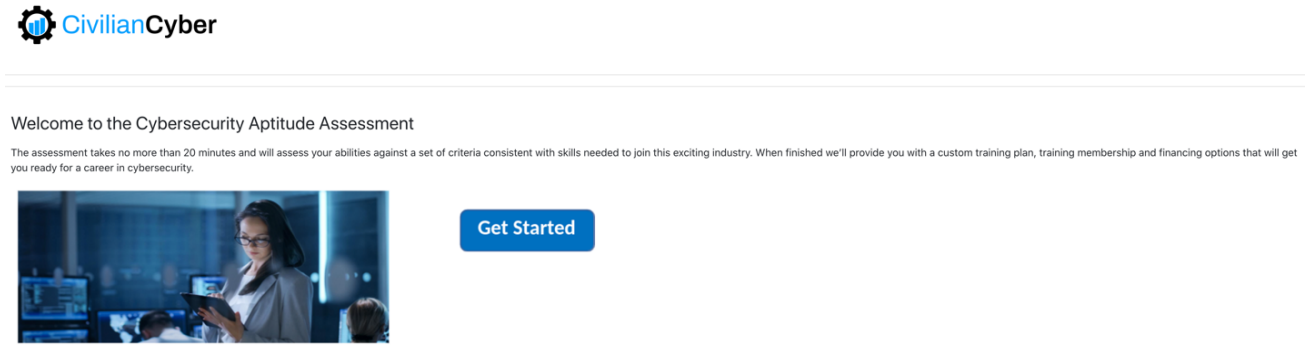
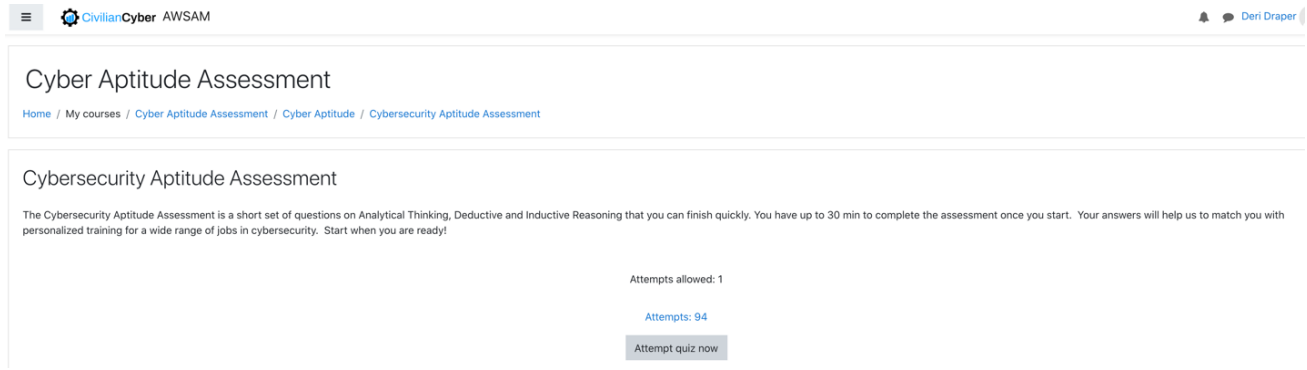


Figure 5 is the newly developed Moodle platform that can be accessed on a mobile, tablet, and PC platforms.

Cyber security competencies were derived from the NICE Framework. Each cyber aptitude question was mapped to the NICE framework and seven entry level jobs. The assessment was administered to cyber security participants in December 2020. Figure 6 below shows the number of assessment participants. The cyber awareness assessment will be further tested and administered to participants in the Q1 2021.

Figure 6



Cyber security competencies were derived from the NICE Framework. Each cyber aptitude question was mapped to the NICE framework and seven entry level jobs (see Table 1.).

Table 1.

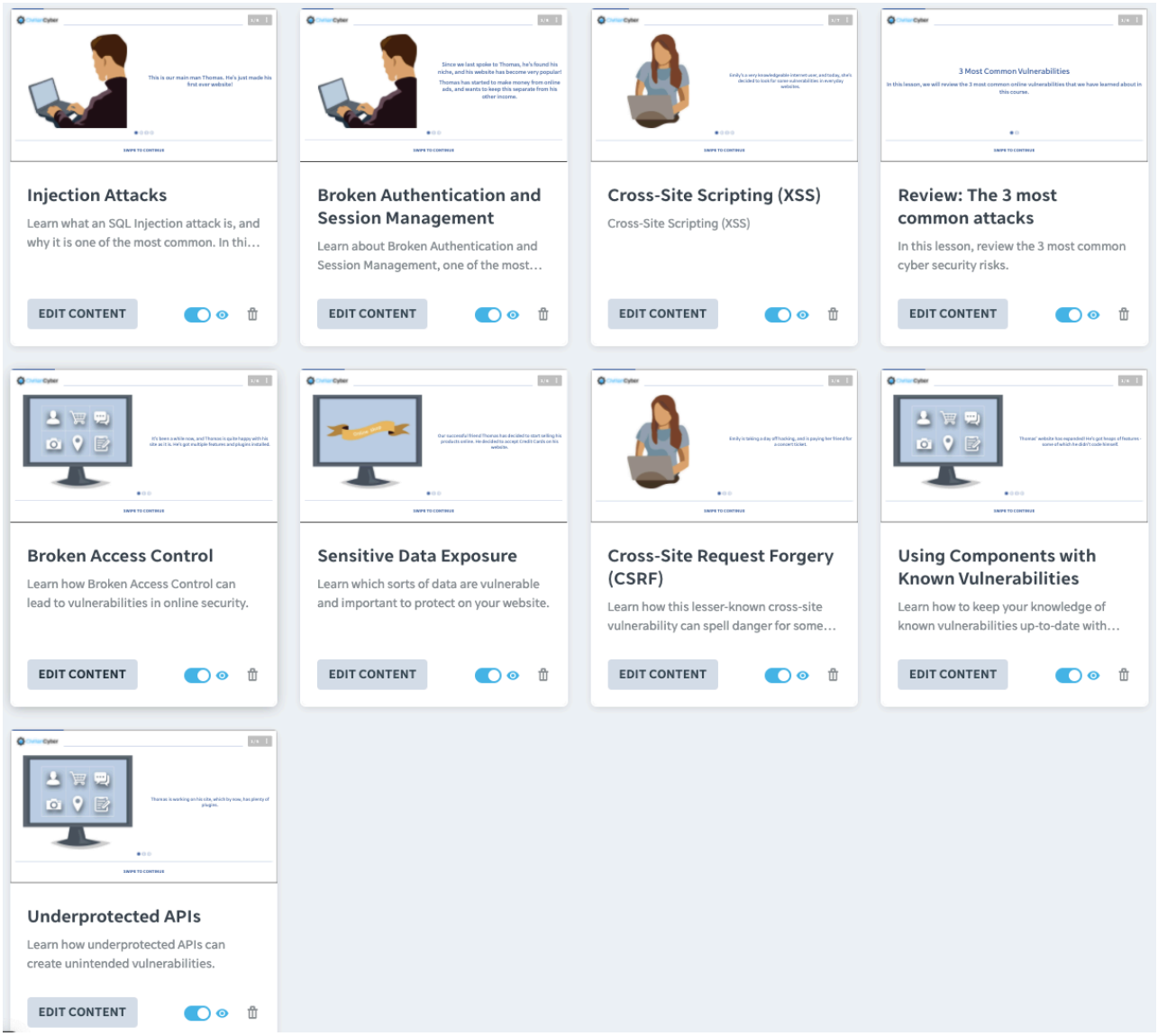
Category	Entry Level Jobs
ANALYZE	Threat Analysis (TWA), Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities;

	produces findings to help initialize or support law enforcement and counterintelligence investigations or activities., AN-TWA-001
INVESTIGATE	Digital Forensics (FOR), Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations., IN-FOR-001, IN-FOR-002
COLLECT and OPERATE	Collection Operations (CLO), Executes collection using appropriate strategies and within the priorities established through the collection management process., CO-CLO-001, CO-CLO-002
OPERATE and MAINTAIN	Customer Service and Technical Support (STS) Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty., OM-STS-001
PROTECT and DEFEND	Cybersecurity Defense Analysis (CDA), Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats., PR-CDA-001
SECURELY PROVISION	Systems Requirements Planning (SRP), Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs., SP-SRP-001
OVERSEE and GOVERN	Training, Education, and Awareness (TEA) Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate., OV-TEA-001, OV-TEA-002

4. External Grants: NA

5. Results of entrepreneurship

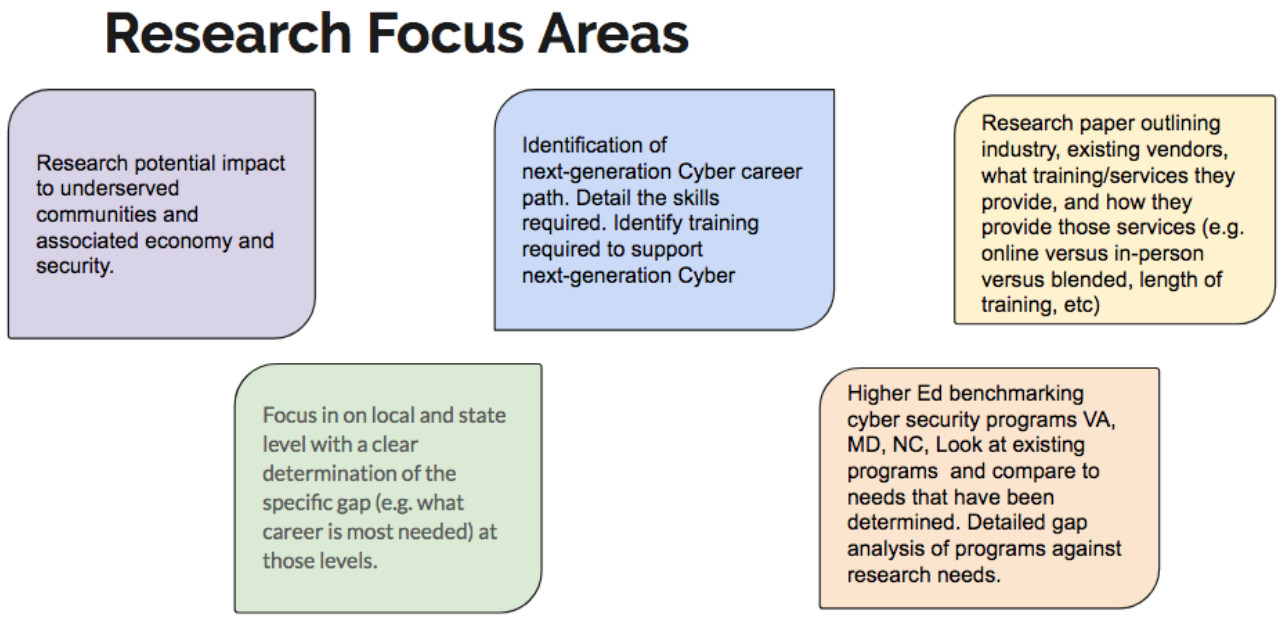
As stated previously, nine cyber awareness modules have been developed and deployed as a pilot and the Cyber Aptitude test was created and administered to over 100 participants. Findings from the pilot will provide valuable feedback for future products.



5. Results of workforce planning

The Cyber Awareness e-learning modules developed and deployed to pilot audience. Additionally, the Cyber Awareness test and modules were reviewed by 2 graduate assistants prior to release.

A survey was created for Virginia Beach Workforce Development and sent to VA Beach small and medium businesses to uncover the cyber needs for their organizations. The findings of the survey informed our five research areas:



6. Collaborative partnerships and projects

CCI Arts and Design	Develop a gamified Mobile Application for Cybersecurity Education and Assessment via User Centered Design Process	January 2021 – December 2021	$25,000

The CCI Arts and Design grant listed above will combine three courses (Moberly, Santo and Draper-Amason) during the spring semester 2021 and possibly the summer session. The three interdisciplinary courses will engage students in experiential learning. The outcome will be the development of a Minimum Viable Product (MVP) storyboard for a gamified cyber aptitude assessment that links to the NICE Framework. The funding for the MVP is considered as the initial funding of this gamified product and the team intends to submit future funding for product development and scalability. The goal is to create a cyber aptitude mobile game that all populations can benefit from the implementation of this project, younger populations in primary, secondary and higher education are already heavy users of gamified applications and will be initially targeted.

Develop a Gamified Mobile Application for Cybersecurity Education and Assessment via a User Centered Design Process

Name	Title	Home Institution	Project Role
Dr. Kevin Moberly (PI)	Associate Professor	Virginia Commonwealth University	Lead project Experiential learning
Dr. Avi Santo (co-PI)	Professor	Old Dominion University	Experiential learning

Dr. Deri Amason (co-PI)	Reach Assistant Professor	Old Dominion University (VMASC)	Experiential learning
Dr. Jeff Pittges (co-PI)	Professor	Radford University	Experiential learning
Bobby F. Keener (co-PI)	CEO CivilianCyber	CTE, Inc/CivilianCyber	Experiential learning

CCI SWVA RIW	Support for the Student Training-Engagement Program (STEP) Enhancing Virginia's Cybersecurity Workforce Pipeline with a Research, Innovation, & Workforce Development	January 2021 – December 2021	$25,000

In 2018, ODU and SWVA Higher Education Center collaborated on a Tobacco Commission grant. The objective is to create a SWVA Cyber Community that engages local community colleges and also four-year colleges a cybersecurity computer lab and "cyber playground" where participants can practice in a safe environment while building cyber skills.

Type of Org	Name	Location	Partner Contrib
Southwest Virginia Higher Education Center	David Matlock	Abington VA	Focused on Workforce Development in Southwest VA
Radford University	Jeff Pittges	Radford VA	Developed curriculum for workforce development in SWVA

7. Correlated economic outcomes

Not at this time. The team is working for venture funding and grants, as well as collaboration across the Commonwealth.

8. Additional Information

The team intends to submit separate IRBs for the Gamified Mobile Application for Cybersecurity Education and Assessment and the Student Training-Engagement Program (STEP) Enhancing Virginia's Cybersecurity Workforce Pipeline with a Research, Innovation, & Workforce Development.

v. Trust, Interoperability and Inclusion: A Framework for Creating Cyber-Trust in Connected Homes. William & Mary and Old Dominion University

Faculty Report: Dr. Stephanie J. Blackmon, Dr. Dylan Wittkower, Dr. Saikou Diallo, and Dr. Krzysztof Rechowicz

Report Date: December 2020

Initiative/Project Title: Trust, Interoperability, & Inclusion: A Framework for Creating Cyber-Trust in Connected Homes

1. Lay Summary:

Our project explores the experiences people with disabilities have with trust and inter- net-connected devices, and is rooted in universal design (UD), universal design learning (UDL), equity, and justice. Our work has three thrusts—empirical, theoretical, and technical—and each thrust informs the other. For the empirical and theoretical thrusts, we are collecting data in the form of focus groups and journal entries. That data will be used to develop a trust framework, and the framework will inform the technical thrust and result the development of a privacy-enhancing app. The app will locate all of the IoT devices in a person's home and connect people to the user agreements that correspond with those internet-connected devices in a way that is accessible for people with various types and degrees of disabilities. With this information, people can decide how/if they want to interact with internet-connected devices. The goal is to give people with disabilities greater transparency, control, and accessibility when interacting with internet-connected devices, with the understanding that the app can also be useful to people with- out disabilities. For the empirical and theoretical thrusts, we have conducted three focus groups and collected 39 journals so far. For the technical thrust, we have completed the features for detecting IoT devices in the home, mapping devices to their respective vendors, and started the initial work of connecting to the appropriate database to search for topic models based on the information provided in vendors' user agreements and privacy policies.

2. Project Focus (check all that apply):

_X Research
_X_ Innovation / Commercialization of IP
____ Workforce Development / Job Creation

3. Breakthroughs

Our project was selected for the Innovation Commercialization Assistance Program (ICAP), so two of our team members (Blackmon and Wittkower) are currently participating in that training. ICAP requires teams to complete 20 market research interviews, so we have been collecting research data for the project and market research for ICAP. We have completed the 20 market research interviews. The work with ICAP has been a major breakthrough for our

project because it has allowed us to explore potential partner- ships for the commercial component of our work and has further validated the importance of the research component of our work.

4. External Grants: N/A

5. Results of entrepreneurship

As a result of our work with ICAP, we have developed a business thesis that is clear and consistent with the core tenets of our research, we have defined our customer segment, and we have built relationships with local and national organizations that can serve as potential partners for our work. Also, as noted previously, the app we are creating is partially developed.

6. Results of workforce planning N/A

Describe any involvement in experiential learning, training, internships, and other work-force development activities

7. Collaborative partnerships and projects

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Stephanie J. Blackmon	Associate Professor	William & Mary	Lead PI
Dylan Wittkower	Associate Professor & Department Chair	ODU	Co-PI
Saikou Diallo	Research Associate Professor	VMASC/ ODU	Co-PI
Krzysztof Rechowicz	Research Assistant Professor	VMASC/ ODU	Co-PI

Organizations: Other organizations involved as partners. NA

Collaborators or Contacts: Other collaborators or contacts involved. NA

8. Correlated economic outcomes

Our venture will not function as a start-up, but we are using the principles of a lean start- up (via ICAP) to produce a prototype. We plan to seek additional funding to shift from prototype to market-ready app.

9. Additional Information

We have completed one invited conference presentation, have one peer-reviewed publication under review, one peer-reviewed conference proposal under review, and two papers in progress. We anticipate having more conferences and papers in the spring as we collect and analyze more data. We are also working on securing external funding.

Unfortunately, due to COVID-19, we will not be able to complete the in-person components we planned for the technical thrust in the spring. To account for that data, we will increase our data collection components related to the other key aspect of the technical thrust, the app.

Appendix 2: Research Scientist Faculty Reports

i. Tan Le, Old Dominion University

ii. Yan Lu, Old Dominion University

iii. Rui Ning, Old Dominion University

iv. Daniel Shin, College of William & Mary

v. Masiane Moeti, Norfolk State University

i. Tan Le, Old Dominion University

Faculty Report: Tan Thanh Le
Report Date: July 25 – December 30, 2020

Initiative/Project Title: Secure and privacy preserving 5G network for connected vehicles
Program: CCI Program
Funding Agency: CCI
Status: Awarded
Period: Jan 2021-Dec 2021
Funding amount: $200K- matching: $200K
1. Lay Summary: 250 Words
Describe the project, including objectives, impact, and results, to a general audience.
Brief Description - Old Dominion University and collaborators George Mason University, University of Virginia and Virginia Tech develop a "Secure and privacy preserving 5G network for connected vehicles" as an innovative 5G security enhancement prototype for maritime and transportation industries. This project effort will result in a new multi-node CCI capability: a comprehensive vehicular 5G security and privacy-preserving prototype. This prototype will provide a unique research infrastructure attraction for the CCI node members pursuing future opportunities with Department of Transportation and Department of Defense. Furthermore, our collaboration with Maritime Industrial Base Ecosystem will recommend our prototype to local stakeholders to enhance their modernization capabilities. The benefits for 5G empowered vehicular network for maritime and transportation industries will have a direct impact on tracking of connected and autonomous vehicles. For example, Port of Virginia has a critical need for truck tracking capability to provide insights into a) location of trucks and drivers in the terminals, b) optimal assignment of trucks to terminal areas to maximize throughput of container loading/unloading, c) dynamic route planning for trucks based on dynamic conditions. There is a need to ensure that the critical and valuable information carried by this 5G network is secure and private. Under observations of unique challenges, the research objective of this proposal is to develop an integrated secure and privacy preserving 5G-empowered connected-vehicle platform that addresses 1) machine learning aided mobility-aware security; 2) privacy preservation of drivers while tracking locations; 3) artificial intelligence assisted trust management system; 4) real-time controller area network bus intrusion detection.

2. Project Focus (check all that apply):
_X__ Research
_X__ Innovation / Commercialization of IP
_X__ Workforce Development / Job Creation

3. Breakthroughs
Identify any research, innovation, or workforce development breakthroughs as a result of the project, program, or initiative.

Overview-Vehicular communication technologies must provide reliable wireless connectivity to realize intelligent transportation systems. The 3rd Generation Partnership Project (3GPP) has developed a roadmap for supporting 5G-empowered vehicle-to-everything (V2X) services by leveraging extreme high bandwidth, ultra-low latency and high-density connections. However, practical deployments of 5G-enabled vehicular networks must also address security, trust and privacy challenges. Several academic and commercial organizations, including many in Virginia, are conducting research and development to support this vision provided by 3GPP. Researchers have investigated security, privacy and trust management challenges in vehicular ad hoc networks (VANETs) and privacy and data integrity issues of autonomous vehicles. However, security and privacy challenges in the context of 5G applied to connected and autonomous vehicles have received little attention. The research objective of this proposal is to develop an integrated secure and privacy preserving 5G-empowered connected-vehicle platform that addresses secure mobility management, intrusion detection on the controller area network, privacy preserving data sharing and trust management.

Impact on the Commonwealth:

Commercialization-The proposed prototype will comprise of enhancements to the 5G's security software stack that will be beneficial to industry verticals, in areas such as cyber security, wireless communications, transportation, and maritime shipping. Partnerships with companies in these industries will help sustain the project beyond the project period. We will collaborate with Raytheon, Perspecta Labs, Viventum (all companies with a Virginia presence) to additional commercialization opportunities with vertical industries such as the transportation and maritime industries. We will apply for IP protection with the respective Technology Transfer Offices at ODU, UVA, VT and GMU. The PI has received two CRCF grants for commercialization of cybersecurity technologies. The PI will submit a proposal to the Commonwealth Research Commercialization Fund (CRCF) Matching Funds program from the Center for Innovative Technology (CIT) to support commercialization of the proposed prototype. In addition, the team will explore SBIR/STTR funds from NSF, DoD and DoE.

Workforce Development-5G, security, privacy and vehicular networks represent diverse areas. However, these areas do share several fundamental core concepts in Electrical Computer Engineering, Computer Science and Modeling and Simulation. The faculty research team members teach courses in security, privacy, cyber physical systems, and model engineering. These courses could benefit from the tools created by research at intersection of 5G, security, privacy and vehicular networks. We propose the introduction of hands-on learning modules, based on the developed research tools, to support laboratory experiments in courses taught by participating faculty. These modules would provide students insights into new attack surfaces in 5G empowered vehicular networks and security and privacy mechanisms to mitigate such attacks.

Economic Development and Impact-Our collaboration with Maritime Industrial Base Ecosystem (MIBE) provides opportunities to present our prototype to regional stakeholders in Hampton Roads area to enhance their maritime sustainment and modernization capabilities. We will pilot a prototype at Virginia Port Authority (VPA) who have been working on deploying a private 5G network infrastructure for tracking vehicles across the Norfolk International Terminal (NIT). NIT is VPA's largest terminal and has a capacity of 1.22 million containers, with 63 % of the

containers handled by trucks. The proposed prototype will enhance the security of their deployed 5G network and will ensure the protection of their logistics applications from cyber-attacks. VPA is a member of MIBE, and through collaboration with MIBE, we will work to deploy the proposed 5G security and privacy preserving enhancement prototype.

4. External Grants:
Awarded Projects:

Funding Agency	Project Title	Period of Performance	Funding amount
Deloitte Inc	Top-down 5G Networks Security Design and Implementation in Zero-Trust Network Architecture	Dec 2020 - Apr 2021	$200k, ODU team: $50k
Office of the Under Secretary of Defense, DoD	Distributed Secure Live, Virtual, and Constructive (LVC) Air Combat System Training Environment (SLATE)	2020 - 2022	$320k

Pending/Submitted Projects:

Funding Agency	Project Title	Period of Performance	Funding amount
BIRD Energy Center, Israel - U.S. Binational Industrial R&D Foundation	Cyber Twin: Business Risk Simulation and Analysis in Energy Systems	2021 - 2023	
DoD	Resilient 5G-IoT Platform for Mobile Edge Computing	2020 - 2024	
Space and Naval Warfare Systems Center Atlantic	Naval Station Norfolk 5G Architecture Ashore and Afloat	6/1/2021 – 5/30/2024	

Projects in preparation (almost done and ready to be submitted):

Funding Agency	Project Title	Period of Performance	Funding amount

NSF	Artificial intelligence-based intrusion-detection systems for resilient distributed control architecture of power grid	2021 - 2025	NA
Accenture Inc	Fair and Privacy-Preserving Deep Federated Learning for Edge Computing and Attack Detection	NA	NA

Not Awarded Projects (Prepared and Submitted but Failed):

Funding Agency	Project Title	Period of Performance	Funding amount
NSF	Developing Artificial Intelligence Assurance Learning Modules for Healthcare Professionals	NA	NA
Army Research Laboratory (ARL), DoD	Center of Excellence: Robust Cross-layer Digital Forensics for Internet-of-Things	NA	NA

5. Results of entrepreneurship

Identify any products produced, patents, inventions, licenses, and other innovation activities
NA

6. Results of workforce planning

Describe any involvement in experiential learning, training, internships, and other workforce development activities
NA

7. Collaborative partnerships and projects

7.1 Secure and privacy preserving 5G network for connected vehicles

Short description of project objectives

Old Dominion University and collaborators George Mason University, University of Virginia and Virginia Tech develop a “Secure and privacy preserving 5G network for connected vehicles” as an innovative 5G security enhancement prototype for maritime and transportation industries. This project effort will result in a new multi-node CCI capability: a comprehensive vehicular 5G security and privacy-preserving prototype. This prototype will provide a unique research infrastructure attraction for the CCI node members pursuing future opportunities with Department of Transportation and Department of Defense. Furthermore, our collaboration with Maritime Industrial Base Ecosystem will recommend our prototype to local stakeholders to enhance their modernization capabilities. The benefits for 5G empowered vehicular network for maritime and transportation industries will have a direct impact on tracking of connected and autonomous vehicles. For example, Port of Virginia has a critical need for truck tracking capability to provide insights into a) location of trucks and drivers in the terminals, b) optimal assignment of trucks to terminal areas to maximize throughput of container loading/unloading, c) dynamic route planning for trucks based on dynamic conditions. There is a need to ensure that the critical and valuable information carried by this 5G network is secure and private. Under observations of unique challenges, the research objective of this proposal is to develop an integrated secure and privacy preserving 5G-empowered connected-vehicle platform that addresses 1) machine learning aided mobility-aware security; 2) privacy preservation of drivers while tracking locations; 3) artificial intelligence assisted trust management system; 4) real-time controller area network bus intrusion detection.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Sachin Shetty	CCI Fellow	Old Dominion University	PI
Tan Le	CCI Research Faculty	Old Dominion University	Co-PI
Jeff Reed	CCI Fellow	Virginia Tech	Co-PI
Cong Shen	CCI Fellow	University of Virginia	Co-PI
Duminda Wijesekera	CCI Fellow	George Mason University	Co-PI
Kai Zeng	CCI Fellow	George Mason University	Co-PI

Organizations: Other organizations involved as partners

Type of Org	Name	Location	Partner Contrib
Industry	Raytheon	Headquarters: Waltham, MA	Equipments
Industry	Perspecta Labs	Headquarters: Basking Ridge, NJ	Equipments
Government	Virginia Port Authority	VA	Facilities

Government	Maritime Industrial Base Ecosystem	VA	Economic Development

7.2 Top-down 5G Networks Security Design and Implementation in Zero-Trust Network Architecture

Short description of project objectives

The fifth generation of wireless cellular networks (5G) is expected to fulfill various requirements from a wide range of industries/verticals so that many use-cases such as enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine-type communications (mMTC) are supported. Besides, 5G networks are expected to serve as the communications infrastructure for some emergency service, natural disaster rescue, public safety, and military communications. Cyber attacks to 5G networks pose severe risks to public communication services. In this proposal, we aim to provide a top-down approach of scalable 5G network security design and implementation, which accomplishes node-to-node security protection in distributed zero-trust network (ZTN) architecture. In our proposed cross-layer security design, we study the intra- and inter-cell aspects of 5G connectivity to provide distributed ZTN security for 5G networks. Four major tasks are included in the proposal: (1) an intelligent physical layer vulnerability assessment system for universal jamming and interference detection and classification; (2) fuzzy testing for network and protocol vulnerability assessment; (3) 5G attack graphs for rapid identification of attacks and exploitation across multiple layers; (4) a blockchain-based ZTN architecture to ensure identification and authentication of nodes, components, entities, and users, and to guarantee that traffic behavior is continuously monitored and tracked.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Sachin Shetty	Associate Professor	Old Dominion University	Co-PI
Tan Le	Research Assistant Professor	Old Dominion University	Co-PI
Eranga Herath	Sr. Project Scientist	Old Dominion University	Co-PI
Jeff Reed	Professor	Virginia Tech	PI
Ying Wang	Lead 5G Engineer	Virginia Tech	Co-PI

7.3 Distributed Secure Live, Virtual, and Constructive (LVC) Air Combat System Training Environment (SLATE)

Short description of project objectives

Note: This project is a large project with the teams from different organizations. Our team at Old Dominion University works on one task of this project.

Our proposal will conduct independent validation and verification of spectrum risk in the 1780-1850 MHz compressed band for air instrumentation implementations. The main challenges of

the implementations are that the environments would suffer the congested and contested issues whenever the new systems are relocated within this band. In particular, multiple systems and their associated waveforms are relocated into the aforementioned band, as reported in the AWS-3 auction. So we have to evaluate the cohabitation capability of these waveforms in the compressed band under testing, training and operational conditions as well as to provide the suggestions for performance enhancement. It implies that we need to maximize the system performance in 5G-ATW applied to LVC environment. To address this challenge, our goal is to establish technical definition and terms of references for both Dynamic Spectrum Access (DSA) and cohabitation, which can benefit to performance enhancement. In this paper, we provide the analytical model for DSA and cohabitation for waveforms in congested spectrum space. The metrics derived from the mathematical model can be compared with the EMANE model results to quantify the quality of service in the congested band. We will first provide the system model considered for the DSA and cohabitation model. Next, we will formulate problems and their possible solutions. Finally, we will provide the quantitative metrics for shared spectrum performance.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Sachin Shetty	Associate Professor	Old Dominion University	PI
Tan Le	Research Assistant Professor	Old Dominion University	Co-PI
Sarada Prasad	Postdoc	Old Dominion University	Co-PI

7.4 Cyber Twin: Business Risk Simulation and Analysis in Energy Systems

Short description of project objectives

Note: This project is a large project with the teams from more than ten organizations and Prof. David Malcolm Nicol, University of Illinois at Urbana-Champaign lead the project. Our team at Old Dominion University works on Task 10 of this project.

The system behavior will be characterized as normal behavior and/or abnormal behavior based on the network activities analyzed from network traces and device logs. An example scenario is monitoring the network traffic in the highly interconnected network with massive number of components. In this scenario, the malicious actor can target stepping stones to laterally propagate or cause disruption through changes in network traffic. There is a need to characterize system behavior to identify opportunities available in the system for adversaries to cause disruption. The major task in this section is to understand the system behaviors from full-packet captured raw network traffic flows and OT logs are by 1) identifying the system components that could be victim of targeted attacks based on their role in supporting business process; 2) determining the operability level expected of OT devices to ensure smooth operation of the business processes; classifying and ranking these nodes and OT devices with the order of the criticality and/or stepping stone targets; 3) identifying the potential exploitable configuration parameters on OT devices that could be targeted by attackers.

To response this challenge, we develop suite of machine learning algorithms for learning several behavior groups according to the network activities. Specifically, we will employ transfer learning as there is a potential for correlation between network activities across multiple scenarios and network environments.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Sachin Shetty	Associate Professor	Old Dominion University	PI
Tan Le	Research Assistant Professor	Old Dominion University	Co-PI
Yan Lu	Research Assistant Professor	Old Dominion University	Co-PI

7.5 Resilient 5G-IoT Platform for Mobile Edge Computing

Short description of project objectives

5G and Internet of Things (IoT) have recently emerged as technologies tailored to realize massive, low-latency and resilient infrastructure that would benefit large number of DoD mission-supporting devices. A team of researchers at Old Dominion University's College of Engineering are engaged in developing techniques that would realize the aforementioned properties for a 5G-IoT infrastructure. The team has developed techniques in the 5G User Equipment (UE), Radio Access Network and Core layers. Specifically, the techniques in the 5G UE layer focus on improving resilience by reducing interference in beamforming techniques in mmWave links by adjusting the transmission time for all UEs traffic, subject to the power budget of base stations (BS), number of beamformers of BSs, UE traffic loads, and the required minimum signal to interference ratio for each UE. We have developed secure network slicing techniques that would allow the 5G core to provide resilient allocation of resources. Finally, we have developed a technique to realize a Blockchain platform that would provide a trusted framework for the Iot devices to communicate. The requested 5G research instrumentation is a UE emulator that will complement existing resources in BCET at ODU with specialized equipment for signal generation and measurement, wireless network activity visualization, and performance monitoring. The equipment will be set up for experimentation by a team of faculty in the Computational Modeling, Simulation Engineering (CMSE), Electrical and Computer Engineering (ECE), and departments, with complementary expertise at all layers of the networking stack as well as in measurements and instrumentation, and will enable the PIs to use the latest wireless technologies to study specific problems of interest to DoD in the area of resilient and scalable5G-IoT platform.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Sachin Shetty	Associate Professor	Old Dominion University	PI
Chunsheng Xin	Professor	Old Dominion University	Co-PI

Hongyi Wu	Professor	Old Dominion University	Co-PI
Tan Le	Research Assistant Professor	Old Dominion University	Co-PI
Sarada Prasad	Postdoc	Old Dominion University	Co-PI

7.6 Naval Station Norfolk 5G Architecture Ashore and Afloat

Short description of project objectives

The integration of 5G and IoT results in increased efficiency, throughput, response time and reliability for Shipboard Radio Access Network (SRAN) and Shore Core Network (SCN). However, the 5G network architecture, which primarily comprises 5G User Equipment, 5G Radio Access Network and 5G Core layers have numerous attack surfaces that need to be mitigated prior to deploying in a SRAN and SCN responsible for delivering mission-critical naval operations. The "security-by-design" principle needs to be adopted during the design and implementation of the 5G network. This principle needs to consider the unique security related opportunities and challenges in the SRAN and SCN during the design of the aforementioned layers. Our project goal is to develop foundational security techniques and end-to-end security architectures, conduct vulnerability assessment, develop5G threat mitigation techniques and generate 5G cyber threat intelligence database to enable security and resilience at scale in SRAN and SCN. The specific objectives of the project are to create countermeasures to mitigate attack surfaces in the 5G physical, network, and core layers within the SRAN and SCN. The proposed platform creates a secure and privacy-preserving infrastructure environment that protects various heterogeneous user equipment (UEs) and diverse network environments in SRAN and SCN. The benefits of the architecture outlined within this paper is the flexibility and interoperability inherent within the design to support a range of use cases for the U.S. Navy, to include, but not limited to voice communication, streaming video, C2/ISR, emergency communications, etc. within ship-to-ship and ship-to-shore communication.

Virginia Tech Applied Research Corp (VT-ARC), in partnership with Industry partners, Intelligent Automation Inc. (IAI), Interdigital(ID), Radisys, Keysight (KS) and Kitco Fiber Optics (KF) with the academic institutions in the Commonwealth Cyber Initiative (CCI) faculty research team propose to create next-generation secure, privacy-preserving and resilient 5G networks for SRAN and SCN. We develop an Artificial Intelligence (AI)-aided end-to-end security solution that leverages innovation in physical layer authentication, anti-jamming, covert communications, network slice trust management, SDN based privacy-preserving and secure key management. The aforementioned capabilities are implemented across the three layers in a 5G security system prototype for detecting the presence of threats and resilience ensured through rigorous testing. In addition, the architecture provides continuous vulnerability assessment and generates a catalog of 5G cyber threat intelligence that would be updated on a regular basis. We demonstrate all of the security innovations in a testbed compatible with 3GPP release 15 standards and interfaces. This research and development shall ensure a trusted and highly efficient SRAN and SCN. The integrated solution's end result will address several exploitable attack surfaces in the ship-ship and ship-shore environment for both the physical layer, the RAN

network and the 5G core. The motivation for developing the secure 5G reference architecture for SRAN and SCN is to address the various threats that could exploit the 5G physical, RAN and Core layers. We describe these threats in the following that our proposed 5G secure architecture aids in mitigation.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Sachin Shetty	Associate Professor	Old Dominion University	PI
Chunsheng Xin	Professor	Old Dominion University	Co-PI
Tan Le	Research Assistant Professor	Old Dominion University	Co-PI
Christopher J. Lynch	Lead Project Scientist	Old Dominion University	Co-PI
Duminda Wijesekera	Professor	George Mason University	Co-PI
Kai Zeng	Associate Professor	George Mason University	Co-PI
Brian L. Mark	Professor	George Mason University	Co-PI
Cong Shen	Assistant Professor	University of Virginia	Co-PI
Tamer Nadeem	Associate Professor	Virginia Commonwealth University	Co-PI
Jeff Reed	Professor	Virginia Tech	Co-PI
Aloizio P. Da Silva	5G Testbed Director	CCI	Co-PI
Michael Miller	Program Manager	Virginia Tech - Applied Research Corporation	PI
Mike DiFrancisco	Director of the Engineering Test & Evaluation Division	Virginia Tech - Applied Research Corporation	Co-PI
Mike Smith	Wireless Communications Expert	Virginia Tech - Applied Research Corporation	Co-PI
Edward Colbert	Technical Director	Intelligent Automation, Inc.	Co-PI
Yalin Sagduyu	Director of the Networks and Security Division	Intelligent Automation, Inc.	Co-PI

Sean Zhou	Lead Research Scientist	Intelligent Automation, Inc.	Co-PI
Sudhir B Pattar	Scientist	Interdigital	Co-PI
Phil Pietraski	Scientist	Interdigital	Co-PI
William Hackett	Director of Engineering	Interdigital	Co-PI
Ganesh Shenbagaraman	VP Integrated Products and Ecosystems	Radisys	Co-PI
Marc Steiner	VP of Defense Programs	KITCO Fiber Optic	Co-PI
Bart Barton	Director of Technical Services	Radisys	Co-PI
Shane Baker	Engineering and Quality Manager	Radisys	Co-PI
Bart Barton	Director of Technical Services	Radisys	Co-PI
Raymond Shen	Director of 5G and Spectrum Govt Test Solutions	Keysight	Co-PI

7.7 Artificial intelligence-based intrusion-detection systems for resilient distributed control architecture of power grid

Short description of project objectives

Meeting the profound growth of energy demand requires to find the range of promising alternative energy sources and to make the radical changes in the structure of electric power system, which bring the emerging enormous challenges. In particular, the innovative energy grid is developed by integrating higher shares of more distributed and renewable energy resources and technologies such as wind and solar (or photovoltaic) electrics as well as by building significantly enhanced communications infrastructure for timely and reliable data exchanges between the control center and various grid control and monitoring points. Moreover, the successful utilization and development of cyber-physical systems are recently reported in such diverse industrial automation systems including automotive, energy production, power electronics and consumer electronics. Smartgrid is an example of the cyber-physical system that integrates different communications, control and computing technologies to build the massive number of communication and complex networks, which enable to support many critical grid control, monitoring and management operations and emerging smartgrid applications. Along with these impressive creations, the modernized energy grid with these advents of novel technologies will also be exposed directly to a larger number of cyber/physical attacks, which are reported as increasing in both frequency and severity of attacks. For instance, the software program failure due to attackers compromising the controllers in the power system on August 14, 2003 caused the power blackout in North America and affected 50million people, while on August 2019, malicious actors exploited zero-

day vulnerabilities to modify sensors at the smart building controller for the heating, ventilation and air conditioning (HVAC) and caused the adverse impact on HVAC systems. Therefore, it is essential to develop the effective and quick detection for the potential cyber-security attacks to dynamically optimize reliable grid operations of the modernized power system as well as to maximize the quality of the electrical power supply.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Sachin Shetty	Associate Professor	Old Dominion University	PI
Tan Le	Research Assistant Professor	Old Dominion University	Co-PI
Yan Lu	Research Assistant Professor	Old Dominion University	Co-PI
Md Touhiduzzaman	Energy Cyber-physical Security Researcher	National Renewable Energy Laboratory	Co-PI

7.8 Fair and Privacy-Preserving Deep Federated Learning for Edge Computing and Attack Detection

Short description of project objectives

We have a discussion with Dr. Amin Hassanzadeh, Senior Research Principal at Accenture Inc. to propose the proposal entitled “Fair and Privacy-Preserving Deep Federated Learning for Edge Computing and Attack Detection”. In particular, we develop practical collaborative deep learning to balance tradeoff between accuracy and privacy, where selective parameter sharing is effective because stochastic gradient descent algorithms can be parallelized and run asynchronously. Moreover, controlling parameter sharing amount allows each participant to avoid local minima but reduce information exchange. To complete our design, we integrate the AI assisted model with our Blockchain design to create the fully distributed model.

7.9 Developing Artificial Intelligence Assurance Learning Modules for Healthcare Professionals

Note: This is rejected project.

Short description of project objectives

As the recent Covid-19 pandemic has illustrated, Artificial intelligence (AI) has not been widely leveraged to understand the spread of Covid-19 or the impact of various intervention strategies. The lack of such wide uses is due to the dependencies of the AI solutions on labeled datasets, the need to account for dynamic changes in healthcare complex environments, and the difficulty of AI models customized to the domain. Specifically, in order for AI to make a meaningful impact in providing patient care in an efficient fashion, there is a need to train healthcare professionals on incorporating trust in their use of AI solutions. Different from undergraduate/graduate student training, developing training modules for healthcare professionals will require addressing several challenges, such as a) understanding of healthcare operational policies and procedures, b) security and privacy aspects specific to handling healthcare data, and c) adherence to compliance requirements. It will require tackling the

collaboration barrier and risk between faculty and healthcare professionals. This project aims to break the barrier through co-development of learning modules that will be used as a model for future long-term collaboration in training. Specifically, the goals of this two-year project are to build innovative experiential learning modules that will greatly enhance educational programs to teach Sentara professionals engaged in health information systems to (1) identify the dangers of using untrusted AI software, (2) understand the impact of vulnerabilities in AI system operations, (3) learn the secure AI workflow for healthcare, (4) identify best practices of using secure AI in healthcare, and (5) augment health security standards with trustworthy AI. The resulting feedback from the learning modules will be used to continuously update learning modules. The experts from Old Dominion University (ODU) and University of South Florida (USF)will achieve the above project goals with Sentara by leveraging their respective strengths and experiences in AI cybersecurity and education. While ODU is designated as NSA's CAE-CO, USF is designated as NSA's CAE-CDE and CAE-R. Sentara offers services in 12 hospitals with more than 3800 medical staff (see https://www.sentara.com/aboutus.aspx).

Name	Title	Home Institution	Project Role
Kaiqi Xiong	Professor	USF	PI
Tan Le	Research Assistant Professor	Old Dominion University	PI
Marino Alvarez	Professor	Tennessee State University	PI
Daniel Bowden	Vice President Assistant Professor	Sentara	PI

7.10 Center of Excellence: Robust Cross-layer Digital Forensics for Internet-of-Things
Note: This is rejected project.
Short description of project objectives
Although use of handheld networked devices allows to take right actions timely by gathering real time information from the environment, it is also attracting malicious users to take advantage of the loosely secured Internet-of-Things (IoT) ecosystem. Given devices exchange proliferated critical sensed data among many heterogeneous devices around, malicious access to the devices may serve as a stepping-stone for reaching other critical networked assets. In such scenarios, reconstruction of crime scenes by pin pointing evidences from a disparate set of devices deployed at various locations, is a crucial challenge. Since the manufactures of IoT devices put significant emphasis on size, cost and usability, forensics features are generally overlooked. Albeit no standard IoT forensics process has been established to complete the evidence life cycle that could serve solving fundamental legal issues caused by IoT applications, it is important to address the unique challenges associated to (1) evidence identification and acquisition, (2) preservation and analysis of digital evidences and (3) attribution of attacks via evidence presentation. By building a principled process to tackle these phases, we can provide deeper knowledge of reconstructed criminal scenes and allow sharing processed tamper-proof forensics evidences to appropriate legal authorities. Therefore, this proposal aims to establish a

Center of Excellence to investigate challenges of digital forensics in densely connected IoT environments and develop efficient approaches for evidence acquisition, processing to generate authentic intelligence information and sharing forensics information securely among investigators to protect the networked systems being abused by malicious actors. In this line, we will address the following grand challenges to realize a scalable yet robust forensics platform for large and dense networked systems: 1) Cross-layer Evidence Collection, 2) Enabling Authenticity using AI and Provenance and 3) Efficient Evidence Processing and Sharing.

Name	Title	Home Institution	Project Role
Deepak Tosh	Assistant Professor	University of Texas at El Paso	PI
Sachin Shetty	Associate Professor	Old Dominion University	Co-PI
Tan Le	Research Assistant Professor	Old Dominion University	Co-PI

8. Correlated economic outcomes

Identify industry investment/production, entrepreneur start-ups created, jobs created, Venture Capital interest/investment, and any other economic impact on the Commonwealth and the nation.

NA

9. Additional Information

Peer-reviewed publications, white papers, and any additional information that you feel is useful to appreciate the contribution and impact achieved in CCI, through this project.

NA

i. Yan Lu, Old Dominion University

Faculty Report: Yan Lu

Report Date: December _31, 2020___

Initiative/Project Title: Trustworthy AI

1. Lay Summary: My current research focus on artificial intelligence, deep learning, and reliable/trustworthy AI. With AI and deep learning technologies continuing to gain strength and broaden its scope, the reliability of AI technology has become an undeniable rising security issue. To better support the sustainability of the growth of AI/ML, my current research/collaborated research are as follows:

    1. Research projects/proposals currently contributing and supporting:
        - On-going internal research on verifiable/trustworthy AI on: 1) identifying the potential cyber-risks and address the security challenges at every stage of life-cycle of AI applications, 2) combating the abuse of AI technology and establish reliable and trustworthy AI models and procedures, 3) integrating the data-driven and machine learning model-based to establish a reliable secure ecosystem for AI applications.
        - On-going collaborated research and proposal in preparation with National Renewable Energy Lab (NREL) on integrating physics-based models in machine learning for intrusion detection in energy delivery system (EDS). This project aims at detection and mitigation of cyberattacks initialed on EDS operations by: 1) establishing physics-based augmented AI models for effective detection, 2) quantifying the reliability of AI models, 3) improving risk mitigation strategies for effective remediation solutions.
        - On-going collaborated research and proposal in preparation with Accenture in machine learning related research from perspective of security and privacy. This project is aiming for strengthening and aiding regulatory compliance by quantifying the privacy risks of machine learning/deep learning models used in intrusion detection systems.
        - On-going collaborated research with Vanderbilt University on data-driven models and analysis. This research aims for building fairness and trustworthy AI in precision medicine and healthcare.
    2. Research proposals submitted:
        - Collaborated research with Dept. of art of Virginia Commonwealth University on the project of “Building the Bridges between CCI and Arts and Design Community. This research aims to develop an AI algorithms-driven deep learning framework to detect, identify, extract, and cover-up the dancers in collected choreography images and videos for privacy preservation purpose.

- Collaborated research with Dept. of Computational Modeling and Simulation Engineering at ODU on "Detection and Mitigation of the Adversarial Attacks in Autonomous Vehicles and Assistive Driving by Deep Learning Models". This research aims to exploring the vulnerabilities of the sensor-based perception modules such as the on-board cameras, especially the RADAR/LiDAR sensors in autonomous vehicles and develop mitigation strategies.
- Collaborated research with Dept. of Computer Science at Howard university on "Robustness to Adversarial Deception in Learning Enabled Systems". This proposal is targeting the challenges in verifying and validating AI model in learning enabled cyber-physical system through 1) exploring the model training/testing consistency by adversarial training and, 2) model verification by temporal/semantic/spatial data coherences and data benchmarking.
- Collaborated research on proposal with 13 members/8 organizations headed by University of Illinois at Urbana-Champaign on proposal of "Power System Cyber Risk Platform". This project aims to develop outcome-based approaches, tools and frameworks that enable companies to explore and define their risk and tolerance to cyber security, compliance and privacy for the critical infrastructures. Our tasks in this research focusing on: 1) developing risk definition and calculation models and metrics, 2) attacks detection deep learning models.

3. Publication and research papers in preparation:

- Research paper on "Adversarial attacks on LSTM model" aimed for simulation conference in March/April 2021.
- Research paper on "An end-to-end GAN data augmentation solution to adversarial attacks" aimed for a tire-1 conference or journal in June/July 2021 is in preparation.
- Abstract for book chapters on "AI Assurance towards valid, explainable, fair and ethical AI" is in preparation.

2. Project Focus (check all that apply):

_x Research
___ Innovation / Commercialization of IP
___ Workforce Development / Job Creation

3. Breakthroughs

(Identify any research, innovation, or workforce development breakthroughs as a result of the project, program, or initiative)

- White paper "Center of Excellence for Robustness to Adversarial Deception in Learning Enabled Systems" collaborated with Dept. of Computer Science at Howard university was submitted to Army

HBCU/MI Research centers of excellence.

- Research Proposal "Advanced Detection and Mitigation of Adversarial Attacks to Perception Sensors in Autonomous Vehicles and Assistive Driving" collaborated with Dept. of Computational Modeling and Simulation Engineering at Old Dominion University was submitted to CCI.
- Research Proposal "Building Bridges between CCI and Arts and Design Communities" collaborated with Dept. of Art at Virginia Commonwealth University was submitted to CCI and funded.
- Research proposal "Power System Cyber Risk Platform" collaborated with 13 members/8 organizations headed by University of Illinois at Urbana-Champaign was submitted to US-Israel Center of Excellence in Energy, Engineering and Water Technology (The Energy Center).

4. External Grants: NA

5. Results of entrepreneurship

Identify any products produced, patents, inventions, licenses, and other innovation activities

6. Results of workforce planning

Describe any involvement in experiential learning, training, internships, and other workforce development activities

7. Collaborative partnerships and projects

Individuals working on the initiative

Name	Title	Home Institution	Project Role
Yan Lu	Research Assistant Professor	Virginia Modeling, Analysis, and Simulation Center	Co-PI
Sachin Shetty	Associate Director and Associate Professor	Virginia Modeling, Analysis, and Simulation Center	Co-PI
Tan Le	Research Assistant Professor	Virginia Modeling, Analysis, and Simulation Center	Co-PI
Touhiduzzaman, MD	Research Scientist	National Renewable Energy Lab (NREL)	Co-PI

Amin Hassanzadeh	Technology Research Senior Manager	Accenture	Co-PI
Juan Zhao	Research Assistant Professor	Vanderbilt University	Co-PI
Hong Yang	Assistant Professor	Dept. of CMSE at ODU	CO-PI
Kate Sicchio	Assistant Professor	Dept. of Art at VCU	CO-PI

Organizations: Other organizations involved as partners

Type of Org	Name	Location	Partner Contrib
Higher Education	VMASC, ODU	Suffolk, VA	
Higher Education	VCU	Richmond, VA	
National Lab	NREL	Golden, CO	
Industry	Accenture	Arlington, VA	
Higher Education	Vanderbilt	Nashville, Tennessee	
Higher Education	ODU	Norfolk, VA	

Collaborators or Contacts: NA

8. Correlated economic outcomes

Identify industry investment/production, entrepreneur start-ups created, jobs created, Venture Capital interest/investment, and any other economic impact on the Commonwealth and the nation.

9. Additional Information

Peer-reviewed publications, white papers, and any additional information that you feel is useful to appreciate the contribution and impact achieved in CCI, through this project.

1. Generally, through CCI collaborated research: 1) we successfully conducted/ being conducting cyber security research with researchers and organizations from organizations ranged from industry (Accenture), National Labs (NERL), and academia (VCU, ODU, Vanderbilt, Howard, & UIUC) on important yet interesting cyber related research topics encompassing broad and various research fields in power grid, energy system, healthcare, art/choreography, and autonomous driving. 2) CCI collaborated research bridges the gap between these research fields and raise the awareness that the cyber security and reliability of AI technology has become an undeniable rising issue and provide solutions. 3) Through CCI collaborated research, we push the forefront lines of what's possible in cyber security research in different research fields

and expands the boundary of cyber security technologies itself as well.

2. Specifically, through the CCI collaborated research "Center of Excellence for Robustness to Adversarial Deception in Learning Enabled Systems", we collaborated with Dept. of Computer Science at Howard university on research targeting the critical challenges on verifying and validating AI model in learning enabled cyber-physical system, this research aims at transforming the learning- enabled autonomous systems from tools into trusted and collaborative partners and develop competency-aware mechanism and framework by: 1) exploring the model training/testing consistency and, 2) model verification by temporal/semantic/spatial data coherences and data benchmarking.

3. Specifically, through the CCI collaborated research "Advanced Detection and Mitigation of Adversarial Attacks to Perception Sensors in Autonomous Vehicles and Assistive Driving" with Dept. of Computational Modeling and Simulation Engineering at Old Dominion University, the research aims at exploring the vulnerabilities of sensor-based perception modules on Autonomous Vehicles (AVs) such as on-board camera, RADAR and LiDAR to a variety of adversarial attacks and developing mitigation strategies and technologies for robust sensing. In this research, we will implement and complete the research for thorough understanding the AV perception systems under sensor-based adversarial attacks and provide a hybrid testbed for evaluating the built-in black-box AI algorithms in assisting driving by incorporating both simulated and actual attacking data.

4. Specifically, through CCI collaborated research "Building Bridges between CCI and Arts and Design Communities" collaborated with Dept. of Art at Virginia Commonwealth University, we aim develop an AI algorithms-driven deep learning to detect, identify, extract, and cover-up the dancers in collected choreography images and videos for privacy preservation purpose. In this research, we bridge the gap between technologies and art, and provide new ideas and concepts for creating new form of art and dance presentation by integrating technology elements.

5. Specifically, through CCI collaborated research "Power System Cyber Risk Platform" collaborated with University of Illinois at Urbana-Champaign(leading), we aim to develop outcome-based approaches, tools and frameworks that enable companies to explore and define their risk and tolerance to cyber security, compliance and privacy for their critical infrastructures. Through this research, we combine different standards and guidelines across security, compliance and privacy through a layered top-down model into a single, unified view of enterprise cyber risk framework.

ii. Rui Ning, Old Dominion University

Faculty Report: Rui Ning
Report Date: December 2020

My research focuses on the intersection of Cybersecurity and Machine Learning. One the one hand, I use machine learning as a tool to discover possible vulnerabilities in cyber physical systems and develop countermeasures. On the other hand, the machine learning model itself, as a sophisticated cyber system, also surfers from adversarial and backdoor attacks. My research aims at achieving secure and privacy-preserving AI by exploring its vulnerabilities and building defense mechanisms.
Below is a summary of a currently funded project carried out between 07/01 – 12/31/2020.
Initiative/Project Title: BlockFL: A Blockchain-based Fully Distributed Federated Learning Framework

1. Lay Summary:
Deep Learning (DL) has achieved proven success and has been adopted in a variety of intelligent systems. It is data-driven, requiring a tremendous amount of training data to gain competitive performance. Under a centralized learning framework, users upload their data to a global server to perform training. This approach triggers privacy concerns as the training data may contain private, valuable, or even safety-critical information. There is an urgent need to develop privacy-preserving learning techniques. Among a handful of options investigated by the research community, the federated learning (FL) is a promising approach adopted by the industry. FL is a data parallelism approach. It employs multiple machines (see Fig. 1), where each of them maintains a copy of the DL model and uses its private data for training. The locally trained model weights are uploaded to the server, which are subsequently used to update the global learning model. Since a node does not upload its data but only the training parameters, FL is effective in protecting participants' privacy. Despite the demonstrated promise, FL has several limitations. For instance, it is vulnerable to a malfunctioned server, lacks an incentive mechanism to encourage participants, and vulnerable to model poison attacks. In this project, we tackle this issue by developing a novel framework based on Blockchain to achieve secure, privacy-preserved, and fully decentralized deep learning. We are teaming with an industry partner, named InterDigtal, to develop and standardize the proposed BlockFL system. The work is partially funded by InterDigtal.

2. Project Focus (check all that apply):
_X_ Research
___ Innovation / Commercialization of IP
___ Workforce Development / Job Creation

3. Breakthroughs

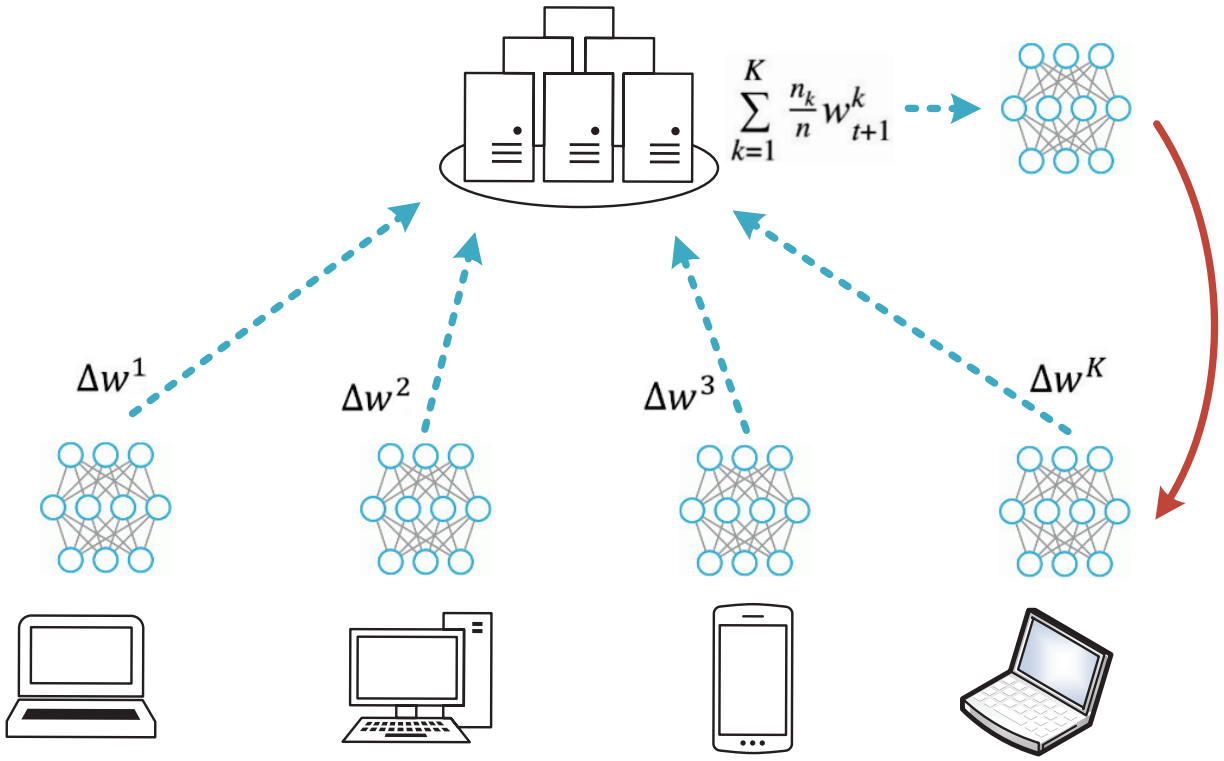


Figure 1: Federated learning.

The aforementioned limitations of the existing FL paradigm have motivated us to investigate a blockchain-based framework that enables a secure network over untrusted parties to support privacy-preserved, scalable, and fully decentralized deep learning. In particular, the decentralization supports secure sharing of model weights among all the member nodes, overcoming many-to-one traffic flows and central control dependency. Consequently, it eliminates the problem of malicious server and also reduces the communication delay. Besides, the immutable distributed ledger securely maintains information of all the member nodes in the form of blocks, which are controlled by all member nodes in a cryptographic manner. This feature prevents malicious tampering of the model, which, in turn, responds very well to backdoor attacks in neural networks. In addition, its consensus protocol and incentive mechanism encourage parties to jointly contribute to model training and local gradients sharing.

BlockFL System Overview.

An overview of the proposed framework is illustrated in Fig. 2. In the beginning, a randomly initialized model is placed into Block 0. All nodes can access the current model and perform local training. Once a node finishes training, it packs the updated model weights into a new block and requests to write the block into the current chain. Three algorithms must be devised and implemented here. (a) First, a consensus protocol is employed to decide which block should be included into the chain if multiple requests are generated around the same time. (b) Second, a validation algorithm is required to ensure the newly generated block represents a valid update

but not from tampered or malicious nodes. (c) Third, an incentive algorithm should be implemented to reward the individual nodes (that contribute their data and training power) and the validators (that provide validation service). The updated blockchain will be broadcast to the entire network, such that the new model becomes the base version of future training.

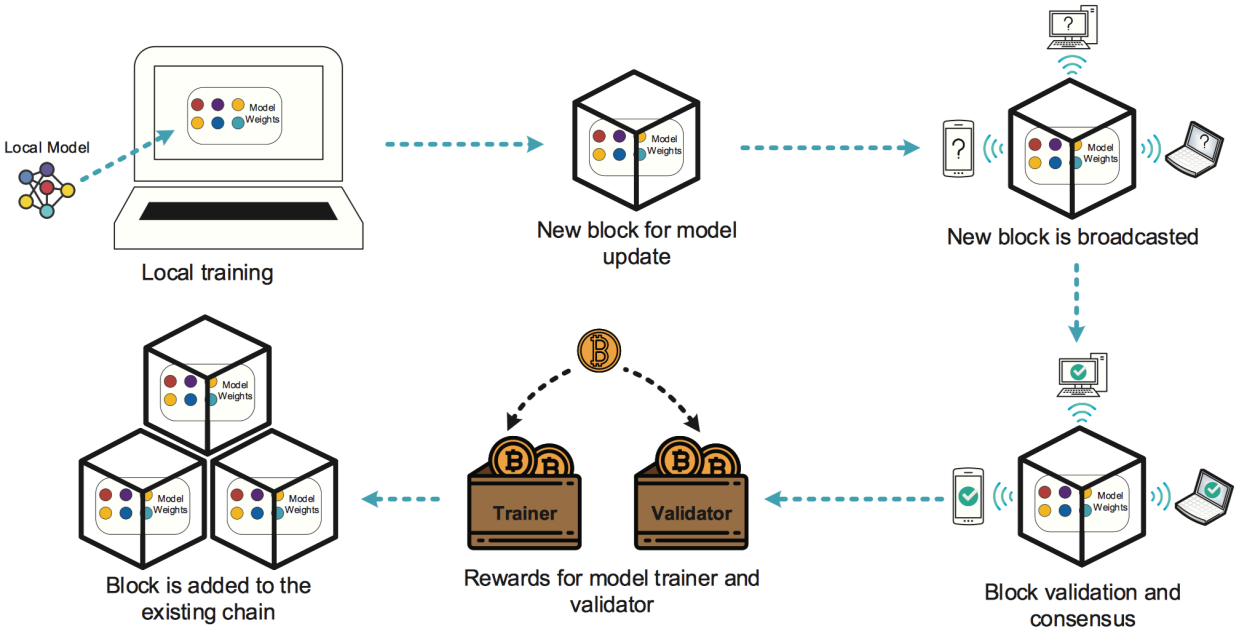


Figure 2: An overview of the proposed blockchain-based fully distributed federated learning (BlockFL) framework.

Research Innovations.

(1) Efficient Consensus Protocol.

There are a wide variety of consensus protocols, such as proof of work (PoW), proof of stake (PoS), byzantine fault tolerance (BFT)-based protocol, and hybrid protocols. In this project, we will develop a new consensus protocol that is tailored for the proposed system, by considering five design options: (a) leader selection, i.e., how to select a new block leader in each round; (b) network model, such as asynchronous, synchronous and semi-synchronous message communications; (c) system model, i.e., permissioned or permission-less system model, regulating whether a party can join the system freely; (d) communication complexity, reflecting the communication cost to propagate a new block to all parties in the system in each round; (e) adversary assumption, defining the probability of tolerating fault parties in the system.

(2) Validation of the Updated Model.

We consider that participants may have malicious behaviors during training. In particular, they may manipulate the model weights, aiming to disrupt or mislead the training process. Therefore, each model must be validated in terms of legitimacy and correctness before it is added to the blockchain. In this project, we will explore the following approaches. (a) Compare with the base model. The malicious participants intentionally modify the model weights, usually resulting in a model significantly deviated from the base version. In contrast, the regularly trained models are similar to the base version with minor updates. (b) Majority vote. A validator may compare the contribution of a given node to the updates of other nodes in the same round. If it differs

dramatically from the majority of the others, the outlier is considered malicious. (c) Local testing. The updated model should perform well on the validator's local data. Thus, a malicious model can be identified if it performs poorly on local samples. If a node receives an updated model for validation while itself is still training, it should decide whether an interruption of the current job is necessary. The first strategy is profit-oriented, where it stops if the validation reward is higher than the training reward. Another method is performance-oriented, e.g., if the updated model is from a reputed node, it pauses local training to validate the updates.

(3) Incentive Mechanism.

The deep learning model is jointly trained and owned by all nodes in the network. After training, the deep learning model will be provided as a Machine Learning As A Service (MLaaS) to the end users. The profit will be divided among the nodes according to their contributions. To this end, a cryptocurrency system will be embedded into the BlockFL framework to represent the nodes' share of the MLaaS system. We will explore three approaches to achieve fairness among the participants. i.e., data-based, training-based, and performance-based approaches. Namely, the data-based protocol rewards the nodes proportional to the number of data samples used during training. The training-based approach considers the dataset size and number of training iterations jointly for the final reward. The performance-based method aims to calculate the compensation by testing the performance of the updated model. The incentive mechanism will also reward credits to the validators that provide validation service to the network.

(4) Privacy Leakage.

Although each party in FL only uploads its local gradients to the parameter server, adversaries still can infer important information about the party’s local data through those gradients by initiating an inference attack or membership attack. On the other hand, based on the gradients, adversaries may launch parameter inferring attack to obtain sensitive information of the model. To this end, we plan to tackle the challenge by uploading the top k updated weights instead of all weights. A research challenge is how to determine the top k weights in a decentralized manner. Alternatively, we may adopt the differential privacy approach to add randomness to the weights for privacy protection.

(5) Revoke Mechanism.

Considering that if an attacker has already caused damage to the shared model, i.e., planted a backdoor. It is crucial to develop a mechanism to revoke it in an efficient way. The most straightforward method is to retrain the whole model, which is extremely costly and unrealistic. To this end, we will explore a new approach to recover the malicious data based on the poisoned model stored in the blockchain. More specifically, we will train a Generative Adversarial Network (GAN) to approximate the distribution of malicious data and recover them to finetune the model for correction purposes.

4. External Grants:

Funding Agency	Project Title	Period of Performance	Funding amount
InterDigital Communications, Inc.	BlockFL	01/01/2021 – 01/01/2022	$84,129

5. Results of entrepreneurship

The project will create unique opportunities to engage industrial and academic stakeholders in the emerging field of blockchain-enabled federated machine learning. In particular, the ODU research team will work closely with InterDigital researchers. Monthly online meetings will be scheduled to review research progress and brainstorm ideas. The ODU research team will give research talks on the blockchain and federated learning technologies as well as the new findings from this project. The ODU research team will host site visit for the InterDigital researchers to visit ODU's research labs and have face-to-face discussions.

Joint Publications. It is anticipated that this project will lead to high-quality joint publications in premium conferences and journals.

Standardization. The BlockFL is planned for ETSI standardization by ODU and InterDigital. ETSI is a leading standardization organization for Information and Communication Technology (ICT) standards fulfilling European and global market needs.

6. Results of workforce planning

The PIs will involve and train two graduate students to prepare them with advanced secure AI and blockchain skills to succeed in cutting-edge research and development projects.

7. Collaborative partnerships and projects

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
Rui Ning		ODU	PI
Hongyi Wu		ODU	Co-PI

Organizations: Other organizations involved as partners

Type of Org	Name	Location	Partner Contrib
Industry	InterDigital	New Jersey	

Collaborators or Contacts: Other collaborators or contacts involved. NA

In addition to BlockFL, I am also working with Dr. Jiang Li and Dr. Chunsheng Xin (ECE professors) and industry partners from Peregrine Technical Solutions on neural backdoor research, which has been recently funded by the CII collaborative research program. We are developing an NSF proposal based on this work.

8. Correlated economic outcomes

No economic outcome yet. But I anticipate potential commercialization based on the BlockFL and neural backdoor research.

9. Additional Information

R. Ning, J. Li, C. Xin, and H. Wu, "Hibernated Backdoor: A Mutual Information Empowered Backdoor Attack to Deep Neural Networks", under review for possible publication in Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition (CVPR), 2021

L. Zhu, R. Ning, C. Xin, and H. Wu, "CLEAR: Clean-up Trigger-Free Backdoor in Neural Networks", under review for possible publication in Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition (CVPR), 2021

R. Ning, J. Li, C. Xin, and H. Wu, "Invisible Poison: A Blackbox Clean Label Backdoor Attack to Deep Neural Networks", accepted for publication in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2021. (Acceptance ratio: 19.9%).

L. Zhu, R. Ning, C. Wang, C. Xin, and H. Wu, "GangSweep: Sweep out Neural Backdoors by GAN", in Proceedings of ACM International Conference on Multimedia (MM), Seattle, WA, October 12-16, 2020. (Acceptance ratio: 27.8%).

iii. Daniel Shin, College of William & Mary

Faculty Report: Daniel Shin
Report Date: December 2020

Initiative/Project Title: COVA CCI Research Scientist
1. Lay Summary:
Researching smart contract applications to maritime supply chain security via blockchain. Based on the development of smart contracts in the Decentralized Finance field, the research focuses on smart contract features that can automate and govern supply chain matters within a private or federated blockchain network.
Developing a paper focusing on Internet-of-Things lifecycle management practice to manage cybersecurity risks. The paper puts forward a novel Internet-of-Things lifecycle management framework, where both technical and legal risks are evaluated on networked systems.
Authoring the new CLCT Cybersecurity and Information Security Newsletter, which is an ongoing monthly newsletter with cybersecurity-related news stories and legal analysis. This has been very well received, especially by non-lawyers interested in understanding some of the legal implications arising out of cybersecurity issues.
Completed activities
Supervised and edited student papers focusing on the legal issues arising from emerging technologies that were published on the CLCT's website.
In addition, assisted with multiple COVA CCI curriculum development tasks:

- COVA CCI Curricula Development for Cyber Range and Coursework: Fundamentals of Cybersecurity for Local Government and small to medium business leaders (submitted on August 14, 2020); and
- COVA CCI Curriculum Project TCC & W&M, Part I: Core Legal Concepts for Cybersecurity Professionals (submitted on December 15, 2020) and Part II: Cybersecurity and the Law (forthcoming Spring 2021).

Delivered multiple lectures on blockchain, cryptocurrencies, and deepfakes, including:

- Blockchain and Cryptocurrencies lecture for the Artificial Intelligence, Emerging Technologies, and Their Effects on the Legal Landscape course at William & Mary Law School (presented on March 24, 2020);
- Lip Manipulation and Live Deepfake demonstration for the Court Affiliates conference (Court Affiliates is a network of judges, court administrators, and other judicial officers from state and federal courts, and other adjudicative agencies) (presented on June 2, 2020); and
- Blockchain, Cryptocurrencies, and other Applications webinar for William & Mary IT client service team (presented on July 29, 2020), and for the Virginia Alliance for Secure Computing and Networking conference (presented on October 1, 2020).

Participated in COVA CCI Research Project Mentorship program supervising Diana Garcia (Christopher Newport University), who presented her research paper Data and Artificial Intelligence: Mismatch between expectations and uses (Mentorship period between August 23, 2020, and December 16, 2020).
2. Project Focus (check all that apply):
_X_ Research
___ Innovation / Commercialization of IP
_X_ Workforce Development / Job Creation

3. Breakthroughs
The curriculum materials for CCI COVA Curriculum Project TCC & W&M Part I: Core Legal Concepts for Cybersecurity Professionals, which is being developed by Professors Iria Giuffrida (W&M) and Kimberly Perez (TCC), is one of the most comprehensive and up-to-date academic teaching materials on the fundamentals of law, aimed towards high school and college students pursuing cybersecurity fields. Participating in this project has been very interesting and thought-provoking.

4. External Grants: None.

5. Results of entrepreneurship. Not applicable.

6. Results of workforce planning
Participated in COVA CCI Research Project Mentorship program supervising Diana Garcia (Christopher Newport University). Through weekly Zoom meetings, Diana learned various aspects of privacy law and the fundamentals of machine learning technologies. Later on, Diana researched a topic intersecting data ownership and machine learning data processing under my guidance. Finally, Diana wrote her research paper Data and Artificial Intelligence: Mismatch between expectations and uses and presented her findings at the COVA CCI Undergraduate Cyber Research Showcase. According to Diana, this was her first academic research experience, and she valued the mentorship program.
Invited to be a guest lecturer on cryptocurrencies and deepfakes in the Spring semester for the Law School AI course at William & Mary, mentioned above.

7. Collaborative partnerships and projects
Participants: Individuals working on the initiative. NA
Organizations: Other organizations involved as partners. NA
Collaborators or Contacts: Other collaborators or contacts involved. NA

8. Correlated economic outcomes. Not Applicable.
9. Additional Information
Forthcoming paper on Internet-of-Things lifecycle management framework that incorporates both the technical and legal perspectives to measure and manage cyber risks. Anticipated to be published on CLCT's website.

Coastal Virginia

5115 Hampton Boulevard
Norfolk, Virginia 23529

CLCT Cybersecurity and Information Security Newsletter is a monthly publication that highlights cybersecurity-related stories with additional legal analysis. This newsletter aims to explain complex cybersecurity incidents and provide the relevant legal context for all audience levels. Since its first issue, the newsletter has gained additional subscribers from around the world.

iv. Masiane Moeti, Norfolk State University

Faculty Report: Moeti Masiane
Report Date: December _x__ June _____ 2020

Initiative/Project Title: Human centered Advanced Persistent Threat (APT) Analytics

1. Lay Summary:

Humans have been treated as an afterthought in cyber security and other applications of data analytics. They are shown to be the weakest link in the cyber security chain. In an effort to bring the human to the front and center of cyber defense, this work models the human-in-the-loop (HITL) of APT data analytics. Our ultimate goal is to use this model of the HITL to assist humans to do a more effective job in cyber defense, especially in APT detection and response which are increasingly relying on advanced data analytics, machine learning, and artificial intelligence to deal with extremely high volume and high dimensional data. These techniques and tools are necessary, and they need to be guided by human insights in their development and the deployed solutions need to provide insights/actionable intelligence to the cyber security practitioners. To accomplish our goal, we break this work down into six sub-tasks that include:
ST1) Implementing and leveraging big data processing and high-performance computing (HPC) environments to provide the needed computational power.
ST2) Implementing a cyber security testbed based on the Elastic Stack.
ST3) Implementing big data visualization capabilities using a high-resolution tiled display wall.
ST4) Quantifying human cognitive insight levels using in-person and crowd studies.
ST5) Modeling HITL cognitive insight levels using machine learning.
ST6) Integrating our model of the HITL into a cyber security testbed.

2. Project Focus (check all that apply):
_x_ Research
___ Innovation / Commercialization of IP
___ Workforce Development / Job Creation

3. Breakthroughs

We have completed the design and implementation of the initial operational capability of the new high-performance computing (HPC) cluster as a part of ST1. This HPC is a part of the Cyber Analysis, Simulation and Experimentation (CASE-V) Testbed at NSU. It is running on Ubuntu OS with the Slurm job scheduler, GPUs for compute intensive processing, and Docker containers for providing varied custom environments for different use cases. We are currently working on expanding and integrating the capabilities of the HPC cluster and the CASE-V Testbed as described in ST1, ST2 and ST3.

4. External Grants: NA

5. Results of entrepreneurship

I have written and distributed a white paper that details the idea of using the concept insight driven sampling to quantify human cognitive insights in a Cyber security context.

6. Results of workforce planning
I took part in the Tracer FIRE 9 Workshop at the 2020 Annual Computer Security Applications Conference (ACSAC) on December 7-8, 2020. This forensic and incident response exercise system is developed by Sandia National Labs (SNL). The system is being incorporated into the CASE-V Testbed so it can be used to support experiential learning, training, internships, and other workforce development activities.

7. Collaborative partnerships and projects
This research contributes to the CCI's vision of "Enabl(ing) the development and commercialization of human-centered, trustworthy AI". Particularly through a focus on "trustworthy AI". The approach of this research is based on the understanding that producing reliable, rational high quality AI results will increase trust in AI and lead to a wider and faster deployment of AI. This research directs its attention to the quality of AI models. We aim to provide high quality results and in cases where our models do not provide such high quality, our models should provide the rationale for providing poor results. This is known as the explanation principle of Explainable AI (XAI). Insights need to be extracted by humans during the entire data science, AI, and Machine Learning (ML) life cycles. For this reason, we use an insight-based metric to explain the effects of model inputs on the model quality. Objective measures like data error will not work for this purpose because they neglect the impact of the human on the final result. An insight measure makes this research human-centered in that it revolves around a measure of how well the human understands the underlying data. This research works to provide visibility into black box models through leveraging the partnership between human and machine that exists in AI and ML.
The quality of (AI) and machine learning (ML) models depends on the quality of the model input. This is widely referred to as the 'Garbage In, Garbage Out' (GIGO) principle. However, an analysis of the data science pipeline that consists of data engineering, machine learning and operations components, shows that humans provide additional input to the training data input. Humans wrangle, clean and prepare the data, validate the models, and utilize the deployed models and visualizations. This means that understanding and management of human factors is important for the delivery of accurate data mining of large data sets including cybersecurity data analytics. We have started collaborations within and without Norfolk State University to learn and model the human factors involved in ML. Particularly, we are collaborating with others to learn and model the Human-in-the-Loop in the three stages of the data science pipeline. Our collaborations include the following:

Data Engineering

C1: Human Centered Ground Truth Analytics Collaboration with the Army Research Lab (ARL)

This research contributes to the CCI AI Testbed by contributing to the DataViz capability in addition to providing the platform for human factor studies that are needed for our human insight quantification and modeling.

During the data engineering stage of the data science pipeline, an understanding of the raw data is required in order to provide high quality data input for model building. An understanding of the ground truth is required in order to determine if the data input for the model is garbage or not. For example, ML practitioners need to know if the data has missing values, bad data, redundant data, etc. in order to correct any issues with the data before using it to train a model. Due to the high dimensionality of such data, information visualization is often employed to gain insights about the data. However due to the large volumes of data involved, a visualization system with a high resolution and high back-end processing power is required. We are collaborating with ARL to implement a tiled wall display powered by SAGE2 (Scalable Adaptive Graphics Environment), modeled on the collaborative space at the ARL. This space will allow us to run experiments on human factors impacting the three stages of the data science pipeline using a large display system.

Machine Learning

C2: Insight Driven Sampling in Machine Learning Collaboration with Prairie View A&M University (PVAMU)
This research contributes to the CCI vision of "Enabl(ing) the development and commercialization of human-centered, trustworthy AI" by collaborating with PVAMU to submit a joint NSF proposal focusing on human-centered explainable AI research and prototype development. The current plan is to target NSF 21-533 (CISE-MSI Program) program solicitation which has a deadline of April 15, 2021.

During the machine learning stage of the data analytics pipeline, resource management is often prioritized. For example, dimension reduction, feature selection, optimization of the learning rate, batch size and number of epochs are approaches that can be used to allow the machine learning practitioner to extend his or her available resources to larger higher dimensional data sets. Taking time as an example of a resource that is often managed and viewing it as the dependent variable while taking batch size as the independent variable, one can learn a simple relationship mapping batch size to training time. Granted that the primary role of such hyperparameters is not to manage resources like training time, but time is a resource that humans are highly cognizant of. If humans are factoring such decisions like the impact of hyperparameter values on training time into hyperparameter value selection, how do we help humans make a more informed decision when making such selections? Our collaboration aims to answer such questions. Using models developed at PVAMU and NSU, we will quantify the relationship between model accuracy and hyperparameter value selection. We will proceed to conduct experiments that provide insights on the motivation for hyperparameter value selection.

C3: Insight Quantification in Cyber Security Data Mining Collaboration with Sandia National Laboratory, Old Dominion University (ODU), Loyola University and NSU Psychology Department

This research contributes to the CCI mission of interdisciplinary research by collaborating between Computer Science and Psychology departments and it contributes to the vision of "leverag(ing) and cultivat(ing) the breadth of academic talent in the Commonwealth of Virginia" through the collaboration between ODU and NSU.

The goal of this collaboration is to provide human centered speedup for Advanced Persistent Threat (APT) cybersecurity data analytics and training. Given the time constraints involved in analyzing the big data associated with Cyber security in an attempt to find a needle-in-the-haystack breadcrumb clue pointing to a cyber attack, a speedup of such workflows is of the essence. This need for speed is exacerbated in scenarios of cybersecurity training where such analysis needs to be conducted within a couple of days. Data reduction is an approach that is used to reduce the data into a size that can be analyzed within the available time frame. The challenge with data reduction is that it can leave important data out. This leads to a trade-off between run time and accuracy. Using sampling as our form of data reduction because it is widely used in data analytics, we will learn and build a machine learning (ML) model of the relationship between sample size and the level of human cognitive insights gained from the analysis of sampled Cybersecurity data. The particular collaborations are as follows:

1. Integration of the sense-making loop in our crowd studies - Loyola University Chicago
2. Human insight quantification - NSU Psychology Department
3. Cybersecurity insight modeling - ODU
4. Human Insight Feedback for Speedup of big data security data analytics - Sandia

Operations

C4: Human Centered Cybersecurity Analytics and Training Collaboration with Sandia National Laboratory

This research contributes to the CCI mission of "develop(ing), and rigorously test(ing) artificial intelligence technologies" through the development of an Advanced Persistent Threat (APT) data analysis and training suite of applications implemented as an expert system that uses ML to identify and compliment human shortcomings in the search and mitigation of APTs.

In the entire data science pipeline, information visualization is used as an interface between high dimensional complex data and the human. Data is transformed from a textual to graphic forms that humans can process pre-attentively and in parallel. However, due to differences in human cognitive abilities and the introduction of human biases and artifacts into the final visualizations, error is introduced into the pipeline. This means that the final system used for data analysis and cyber security training has to take into consideration multiple models of human factors when delivering the final visualization of the data to the end user. Using the

various models of human cognitive insight that we learn in our research of the data science pipeline, we will provide an expert cyber security analytics and training testbed powered by the Elastic Stack that provides interactive feedback and assists end users to manage and maximize insight levels when making informed decisions on arbitrary sample sizes.

C5: High Performance Cluster (HPC) Collaboration with ODU
This research contributes to the CCI AI Testbed and the CCI “Al Commons” vision by contributing to the Decentralized Storage capability by providing additional big data storage and HPC big data processing located in NSU, closer to the NSU end users. It also contributes to the CCI mission of interdisciplinary research by collaborating between Computer Science and Psychology departments and it contributes to the vision of "leverag(ing) and cultivat(ing) the breadth of academic talent in the Commonwealth of Virginia" through the collaboration between ODU and NSU.

Our studies of the human factors involved in the entire data science pipeline will depend on our ability to process big data in order to generate interactive data analyses and visualizations of such data. Our HPC cluster will allow us to do this. In addition to the HPC’s ability to schedule data and process data intensive jobs is the ability to provide custom computing environments for different use cases. We have implemented these initial capabilities through the combination of the Slurm job scheduler and Docker containers that leverage Nvidia GPUs and containers containing ML environments and libraries. We are in the process of sharing our experiences and contributing to the CCI “AI Commons” efforts.

Participants: Individuals working on the initiative

Name	Title	Home Institution	Project Role
George Hsieh	Professor	NSU	Co PI
Simon Su	Computer Scientist	Army CCDC ARL	Co PI: C1
Lijun Qian	Professor	PVAMU	Co PI: C2
Kevin Nauer	Principal Technical Staff	Sandia National Labs	Co PI: C3 & C4
Sachin Shetty	Assoc. Professor	ODU	Co PI: C3 & C5
Jose Padilla	Research Assoc. Prof	ODU	Co PI: C3 & C5
Tianyi Li	Assistant Professor	Loyola University Chicago	Co PI: C3
Scott Debb	Assoc. Professor	NSU	Co P3
Mary Ann Hoppa	Assoc. Professor	NSU	Co PI: C3

Organizations: Other organizations involved as partners. NA
Collaborators or Contacts: Other collaborators or contacts involved. NA

8. Correlated economic outcomes
N/A

9. Additional Information

Peer-reviewed publications, white papers, and any additional information that you feel is useful to appreciate the contribution and impact achieved in CCI, through this project.

N/A