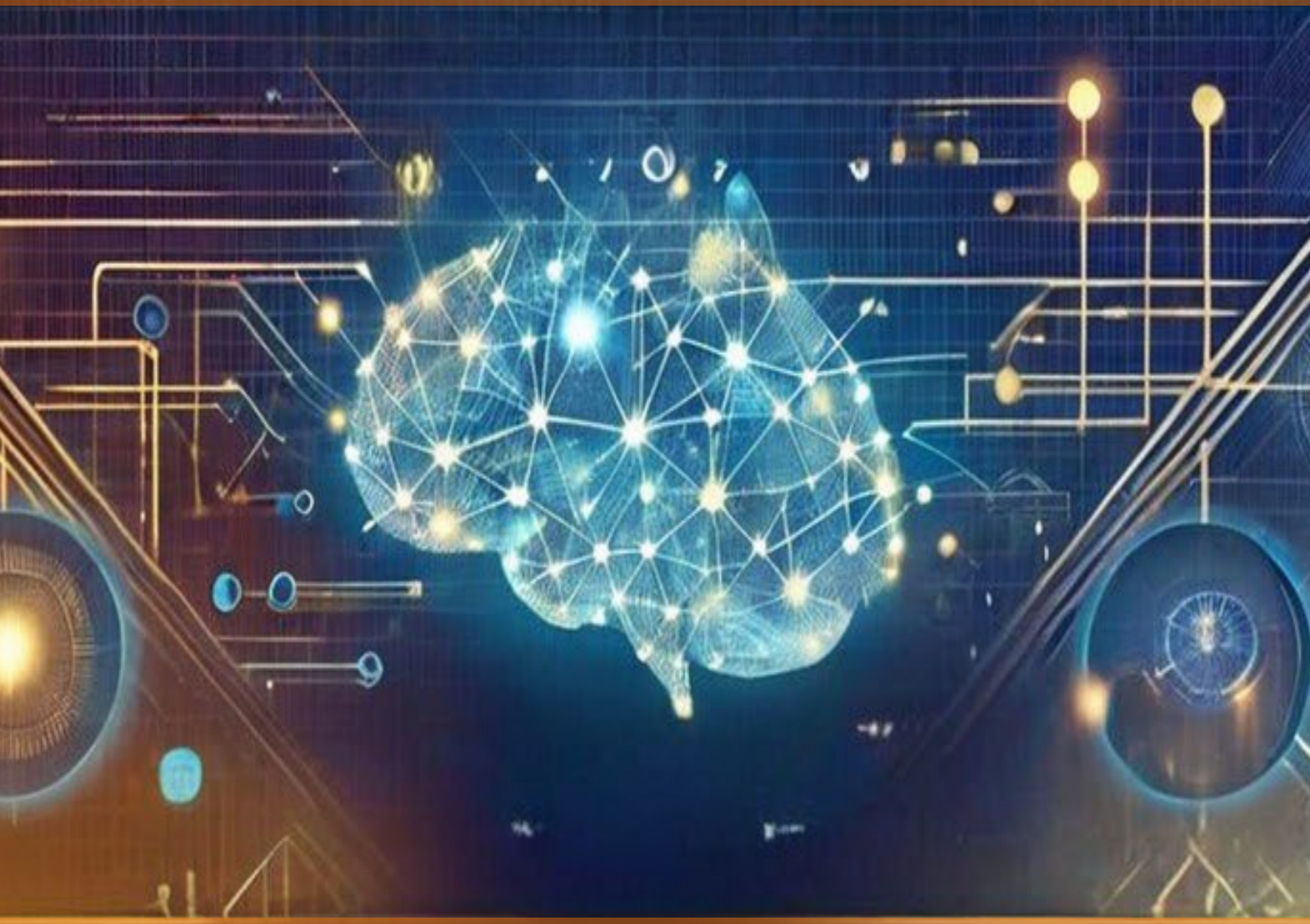
THE SYMPOSIUM ON COMPUTING AT MINORITY INSTITUTIONS

ADMI 2025: Enhancing AI Capacity of Minority Serving Institutions



March 27 – 29, 2025

Charlotte, North Carolina

President's Message

Greetings,

It is my honor and privilege to extend a warm welcome to each of you as we convene under the overarching theme of "Enhancing AI Capacity of Minority Serving Institutions" Over the next two days, we are delighted to uphold our longstanding tradition of showcasing faculty and student research at the Symposium on Computing at Minority Institutions 2025. Our symposium promises to deliver an array of high-quality technical activities, encompassing research paper sessions, poster sessions, workshops, and demonstrations. These engagements will not only facilitate learning but also provide numerous opportunities for networking and professional growth.

Continuing our emphasis on graduate education, we are proud to host a Graduate School Recruitment/Career Fair, underscoring our commitment to nurturing future leaders in academia and industry. Additionally, we invite you to observe our student competitions: the Cybersecurity Challenge and the Code-a-thon, where innovation and skill will be on full display.

I encourage you to consult the Schedule-at-a-Glance to maximize your engagement with our intellectually stimulating program. Your active participation is instrumental in fostering a vibrant and enriching symposium experience.

On behalf of the ADMI Board of Directors, I extend heartfelt gratitude to our symposium sponsors and esteemed speakers for their invaluable support. Special recognition is also due to the diligent efforts of the Symposium's program committee, led by Drs. Felicia Doswell and Timothy Holston, whose dedication has been integral to the success of this conference.

Your presence here is deeply appreciated, and we trust that you will find this conference both engaging and invigorating. Whether reconnecting with familiar faces or forging new connections, may your interactions be enriching and fulfilling.

As we embark on this collective journey of knowledge-sharing and collaboration, we eagerly anticipate your feedback, which will guide our ongoing efforts to enhance future ADMI events. We eagerly anticipate the opportunity to welcome you back for ADMI 2026.

Warm Regards,

E. Rebecca Caldwell

E. Rebecca Caldwell, Ph.D.
President, ADMI

ADMI 2025: **Enhancing AI Capacity of Minority Serving Institutions**
March 27 - 29, 2025
Charlotte, North Carolina

Thursday, March 27, 2025		
6:00 P.M. – 8:00 P.M.		Board Meeting (*ADMI Board Members only)*
Friday, March 28, 2025		
7:30A.M. – 5:00 P.M.	Grand Ballroom Prefunction	Registration
7:30 A.M. – 8:15 A.M.	Atrium	Breakfast
8:30 A.M. – 8:40 A.M.	Grand Ballroom	Opening Session/Welcome Dr. E. Rebecca Caldwell, ADMI President Associate Professor Winston Salem State University
8:40 A.M. – 9:40 A.M.	Grand Ballroom	Keynote Address Dr. Napoleon Paxton, VP of Federal Services AISquared
9:45 A.M. – 10:45 A.M.	Salon B	Student Track: Internship Roundtable Dr. Elva Jones, Computer Science Professor Emeritus Winston-Salem State University
	Salon A	Faculty Track: Faculty Papers
10:45 A.M. – 10:55 A.M.		Break
11:00 A.M. – Noon	Salon C	Student Track: Graduate School Prep Dr. Cheryl Seals, Charles W. Barkley Professor Auburn University
	Salon D	Faculty Track: NAIRR Pilot opportunities of interest to the ADMI community. Dr. Marlon Pierce, Program Director for NSF's Office of Advanced Cyberinfrastructure Moderator: Dr. Linda Bailey Hayden, SGX3 Director of Workforce Development, ADMI VP for Programs
NOON – 1:30 P.M.	Lunch Queen City Room	Graduate School and Career Networking Expo
1:30 P.M. – 3: 30 P. M.	Salon A	HPC Crash Course Dr. Elijah MacCarthy, HPC Engineer Dr. Tuguldur (Togo) Odbadrakh, HPC Engineer Oak Ridge National Laboratory
3:30 P.M. – 5:30 P.M.	Salon C	Student Competition: Code-a-thon
	Salon D	Student Competition: Cybersecurity

	Salon B	Faculty Session: AI Education Dr. Siobahn Day Grady, NCCU Prof. Yvonne Phillips Taylor, Morehouse AI in Sports
5:30 – 6: 00 P. M.	Grand Ballroom	Collaborative Undergraduate Education (CUE) Students
6:00 - 6:30 P.M.	Grand Ballroom	Dinner
Saturday, March 29, 2025		
7:30 A.M. – Noon		Registration
7:30 A.M. – 8:15 A.M.	Atrium	Breakfast
8:30 A.M. – 9:30 A.M.	Grand Ballroom	Workshop: Mr. Moyo Orekoya, CEO & Founder Shepherd
9:30 A. M. – 10:30 A.M.	Salon C	Student Session: AI Tools Dr. John Sands Dr. Kristine Christensen
	Salon B	Faculty Session: Learning Community Grant
10:30 A.M. – 10:40 A.M.		Break
10:45 A.M. – 11:45 A.M. (session immediately starts at 10:45)	Salon A	Student Session: GPU Programming Dr. Elijah MacCarthy, HPC Engineer Dr. Tuguldur (Togo) Odbadrakh, HPC Engineer Oak Ridge National Laboratory
	Salon D	Faculty Session: Dr. John Sands Dr. Kristine Christensen
Noon – 12:45 P.M.	Queen City room	Lunch(eon) Mrs. Kristen Dunlap Johnson, Principal Technical Analyst Altria
1:00 P.M. – 2:15 PM	Salon A&B	Student and Faculty Poster Session
2:30 P.M. – 5:30 P.M.	Salon C	Undergraduate Student Papers
	Salon D	Graduate Student Papers
5:30 P.M. – 6:00 P.M.		Break

6:00 P.M. – 8:00 P.M.	Queen City Room	Dinner Video Presentation When Theory Became Reality for Dr. Evelyn Boyd Granville: The World Produced its First Black Computer Scientist. Moderator: Dr. Johnny Houston, ECSU Professor Emeritus Awards Banquet - Alumni Spotlight Mr. Jerry Akoula Gampio, Leader, Technical Systems Engineering, Cisco Systems Mr. Timothy Campbell, Senior Project Manager, Duke Energy Mr. Khendr'a Reid, Principal Data and GenAI Strategist, Amazon Web Services

Keynote Speaker Biography

Dr. Napoleon Paxton

Dr. Paxton is the Vice President of Federal Technology at AI Squared and he is a senior-level technologist with over 20 years of experience as a developer and leader of product development teams. Before joining AI Squared, Dr. Paxton was a senior-level contractor for Booz Allen Hamilton where he led and served on many projects. This included being the deputy branch chief of the AI/MLOps Branch of the ADVANA analytic platform which is the largest analytic platform for the DoD.

Dr. Paxton holds a Ph.D. in Information Technology from The University of North Carolina at Charlotte with a focus on cyber security (2011). He has a master's degree in data science from UC Berkeley, and his bachelor's degree in Computer Science from Elizabeth City State University (ECSU) in 2005. He also holds an associate degree from Campbell University, which was completed while serving in the United States Marine Corps (2003).

In addition to bringing this perspective to AI Squared he also teaches various AI/ML and Data Science courses at UC Berkeley and Stanford.

Alumni Spotlight Biographies

Khendr'a Reid

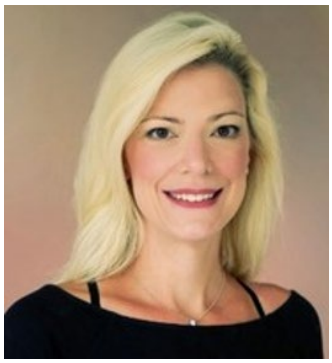
As a Principal Data and GenAI Strategy Specialist for Financial Services spanning Capital Markets, Banking, Payments, and Insurance at Amazon Web Services, Khendr'a Reid is redefining the industry. Through thought leadership and architecting purpose-built solutions that slash complexity, Reid empowers top financial services executives worldwide to harness the transformative power of cutting-edge technologies like generative AI, enabling organizations to align business objectives with data and AI, propelling them to unparalleled success. He also produces and hosts a YouTube channel, sponsored by AWS, named "Data Strategy Unravelled (DSU)" intended to provide thought leadership by interviewing worldwide leaders in the data, analytics, and AI industry.

His passion for technology enabled him to pursue a Computer Science degree from Winston Salem State University and a Master's in IT from Virginia Tech. His professional experience includes acclaimed engineering roles at tech giants like Red Hat and Microsoft, further solidifying his expertise.

In his free time, Khendr'a enjoys spending quality time and traveling with his wife Constance and kids, Kolton (5) and Carian (3), or you can find him on the golf course.

Presenter Biographies

Dr. Kristine Christensen



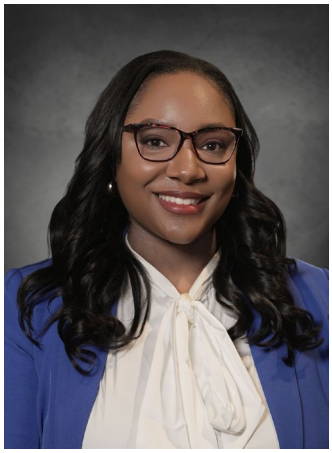
Kristine has taught and developed curriculum in website development, user interface design principles, programming, networking, robotics, and engineering technology for the past twenty years. She also serves as Moraine Valley's Director of Faculty Development and is responsible for designing, developing, and evaluating professional development programs for faculty and staff. She has been actively involved in research and curriculum development for grants awarded by the National Science Foundation, National Security Agency, and the National Centers of Academic Excellence in Cybersecurity. She holds a Bachelor of Science in Business with a double major in Human Resource Management and Industrial Psychology from Valparaiso University, a Master of Business Administration with an emphasis in Consulting from Eastern Illinois University, a Master of Science in Management Information Systems with a focus in Computer Programming and Electronic Commerce from Governors State University, a Master of Science in Teaching and Learning from St. Francis University, a graduate certificate in Online Communications and Web Design from the University of Florida, and a Ph.D. in Community College Leadership from Old Dominion University. In addition to her academic credentials, she has earned numerous professional certifications in information technology and networking, manufacturing and robotics, programming, and web development.

Dr. Siobahn Day Grady

Dr. Siobahn Grady's remarkable journey began as the first woman to earn a Ph.D. in Computer Science from North Carolina Agricultural and Technical State University in 2018. She is currently the Director of the Institute for Artificial Intelligence and Equity Research (IAIER) at North Carolina Central University, where she leads groundbreaking initiatives to foster innovation and inclusivity in artificial intelligence. Additionally, Dr. Grady serves as an assistant professor and program director of Information Science/Systems in the School of Library and Information Sciences at NCCU, heads the Laboratory for Artificial Intelligence and Equity Research (LAIER), and is an Office e-Learning Faculty Fellow.

Dr. Grady's research explores artificial intelligence, human-computer interaction, and STEM participation. She applies machine learning to combat misinformation, improve autonomous vehicle safety, and develop frameworks to eliminate bias in healthcare algorithms. She also studies public perceptions of AI and works to expand STEM education and workforce opportunities, focusing on engagement in technology fields.

Kristen Johnson

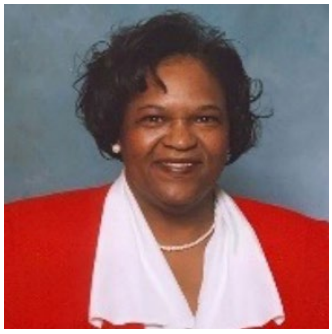


Kristen Johnson is a dedicated leader, philanthropist, and trailblazer passionate about empowering the next generation of HBCU scholars. A 2011 graduate of Winston-Salem State University with a degree in Information Technology, Kristen's potential for success was realized through her college experiences, including internships at NASA and Altria. After graduating, Kristen began working at Altria and has had a successful career at the Fortune 200 company. She also holds a Master's in Business and Global Marketing from Virginia Commonwealth University, further sharpening her leadership and business acumen.

Inspired by her HBCU experience and the university's motto, "Enter to Learn, Depart to Serve," Kristen, along with her husband Rufus, founded their nonprofit, KR Scholars in 2020. The nonprofit is dedicated to supporting current and future HBCU scholars by bridging the gap from campus to career through financial literacy, workforce, and college readiness programs. This work embodies Kristen's commitment to service as she helps equip students with the tools and resources they need to succeed in their professional lives.

Above all, Kristen is the proud wife of Rufus and mother to Nicholas, 2.

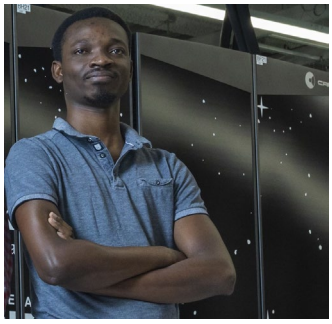
Dr. Elva J. Jones



Dr. Jones is Professor Emeritus and Founding Chair at Winston-Salem State University. She obtained a bachelor's degree from WSSU; a master's degree from the UNCG; a master's in operations research and the Ph.D. in Industrial & Systems Engineering/Computer Studies from NCSU, the first African American woman to attain a doctorate in the area from NCSU.

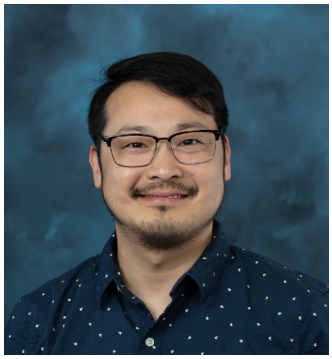
A highly accomplished teacher-scholar, Elva's accomplishments include a range of academic innovations; an active research, publication, and extramural funding record; and an exemplary record of service. The Elva J Jones Computer Science building, a $13 million academic, research, and Information Resources facility, was dedicated in her honor, September 2005. She strives to ensure continuous improvement of the department and to keep its programs cutting edge and innovative. The program is a recognized leader in graduating African American males and women in the field. Elva has committed her life to teaching excellence, mentoring, recruiting and retaining young persons in the computing field, research, and "giving back" through professional and community service.

Dr. Elijah MacCarthy



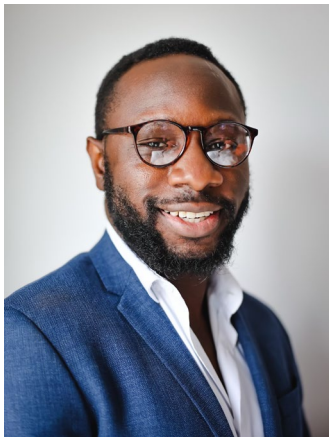
Dr. MacCarthy is an HPC Engineer with the Systems Acceptance and User Environment group at the National Center for Computational Sciences at Oak Ridge National Laboratory. He holds a Ph.D. in computational science and engineering with research interests in software containers, GPU programming, program optimization, and parallelization within HPC environments.

Dr. Tuguldur (Togo) Odbadrakh



Dr. Togo Odbadrakh is a HPC Engineer in the System Acceptance and User Environment group at the Oak Ridge Leadership Computing Facility. He received his Ph.D. in Theoretical Chemistry from the University of Pittsburgh, where he was first exposed to High Performance Computing. Upon completing a postdoctoral appointment at Furman University, Dr. Odbadrakh pivoted fully towards HPC operations. At his current post, he maintains the software stack on various OLCF machines and contributes to training events and internships.

Moyo Orekoya



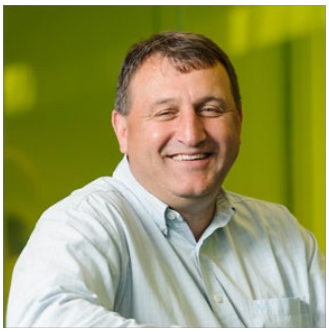
Moyo Orekoya is the founder and CEO of Shepherd, a Y Combinator-backed AI learning assistant that transforms how students access academic help globally. He's earned his Chemical Engineering degree from the Illinois Institute of Technology, a master’s in Engineering Management from Duke, and an MBA from the University of Chicago.

Prior to Shepherd, he advised Fortune 500 companies at McKinsey, driving over $100M in growth. Now, with Shepherd, he is leveraging his expertise to democratize high-quality academic support and empower Africa’s next generation of leaders.

Dr. Marlon Pierce

Dr. Marlon Pierce is a program director for the Office of Advanced Cyberinfrastructure, part of the Division of Computer and Information Science and Engineering at the National Science Foundation (NSF). He is serving as a rotating program officer, and his home institution is Indiana University, where he directed the Cyberinfrastructure Integration Research Center. Pierce's research interests are science gateways, distributed computing, scientific user environments, open-source software, and their applications to scientific computing. At the NSF, Pierce is involved in programs funding scientific and cyberinfrastructure software with a focus on their applications to the geosciences, climate research, and clean energy technologies. He leads the NSF's National Discovery Cloud for Climate initiative and supports the National Artificial Intelligence Research Resource Pilot effort. Pierce has a Ph. D. in computational condensed matter physics from Florida State University.

Dr. John Sands



John brings over twenty-five years of experience in information technology management and information assurance. John earned a Ph.D. for Colorado State University. As a 25-year employee of Moraine Valley Community College, Dr. Sands is currently the department chair of the Computer Integrated Technologies programs. John has also served as a Principal Investigator (PI), Co-PI and project evaluator for numerous National Science Foundation (NSF) Advance Technology Education centers and projects. John was also instrumental in establishing the Center for System Security and Information Assurance (CSSIA) NSF ATE project #9950037, one of the country's first comprehensive Centers for Advanced Technology Education.
John holds several industry certifications including: CISSP, CCIA, A+, Network+ and Security+. John served as a senior researcher for Cisco Learning Institute in technical education.

Dr. Cheryl D. Seals

Dr. Seals, the Charles E. Barkley Professor of Computer Science and Software Engineering at Auburn University, is a dynamic and accomplished academic, researcher, and educator with a career spanning more than two decades. She directs the AU Computer Human Interaction Lab, which investigates interesting solutions to Advance Learning Technology. She have published numerous journals and presented at conferences around the world in eLearning, Computational Linguistics, Engineering Grand Challenge of Enhancing Virtual Reality (VR) through projects in VR and Augmented Reality (AR) (i.e., Pharmacy, Building Science (VR), Civil Engineering Structures (VR), Communications disorders (VR) and (Osteopathic Medicine (AR). Dr. Seals is also passionate about broadening participation in computing and is a member of NSF BPC IAAMCS and the STARS Alliance. In her research, Dr. Seals has supervised over 100 graduate, undergraduate and REU students, graduated 15 PhDs and authored and/or coauthored more than 90 publications.

Paper Abstracts

1

Evaluating Topic Models for Tracing Discussion Forum Posts to Course Material in MOOCs

Saichaitanya Bondada

This research paper investigates the effectiveness of various topic models in tracing discussion forum posts back to corresponding course material in massive open online courses (MOOCs). Utilizing mean reciprocal rank (MRR) as a metric for evaluation, we compare the performance of traditional TF-IDF models against multiple topic modeling approaches, including LDA, HDP-LDA, and labeled LDA, across five different courses in computer science and software engineering. Our results demonstrate that while TF-IDF consistently outperforms topic models in terms of accuracy, the latter still significantly exceeds random chance, suggesting their potential as a feature extraction tool for educational content traceability. Additionally, we analyze off-topic discussions and their vocabulary intersections, revealing common themes and vocabulary used by students. The study underscores the importance of labeled topic models for improving traceability and discusses the implications for future research and applications in diverse educational domains. The findings contribute to the field of software engineering traceability and enhance our understanding of discourse analysis in educational settings.

2

Exploring AI in Vishing: Threats and Countermeasures

Kayla Council and Chutima Boonthum-Denecke

This study examines how artificial intelligence (AI) can help with voice phishing (vishing) attacks, with a particular emphasis on deepfake technologies and AI-driven voice synthesis. It examines the strategies used by cybercriminals, assesses the effectiveness of the present defenses, and identifies difficulties in identifying and preventing such attacks. The results show that to combat the increasing complexity of vishing strategies, there is an urgent need for sophisticated detection systems and preventive actions. Future directions include the creation of cooperative policy frameworks to control the misuse of AI and easily accessible solutions for small enterprises.

3

Continuous User Authentication: A Vital Component of Mobile Security

Sydney Johnson and Jean Muhammad

As mobile devices become increasingly integral to daily life, the need for robust security measures has intensified. Continuous user authentication (CUA) is an emerging paradigm designed to enhance security by verifying user identity throughout device usage, rather than solely at login. This study aims to explore user perceptions, experiences, and references concerning CUA methods, such as biometric scans (e.g., fingerprints, facial recognition) and behavioral analytics (e.g., typing patterns, swipe gestures).

We will investigate the importance users place on continuous authentication for safeguarding personal data, as well as the usability challenges they encounter. Specifically, we will delve into how users perceive the reliability and accuracy of biometric and behavioral authentication methods, considering factors such as the perceived invasiveness of biometric scans and concerns about data privacy. Additionally, we will examine how perceptions and preferences for CUA vary across different age groups, as younger generations may be more accustomed to biometric authentication and less concerned about privacy implications, while older generations may have different preferences and concerns.
The findings of this study will provide insights into user trust, privacy concerns, and the overall effectiveness of CUA in improving mobile security. By understanding user attitudes, this research seeks to inform the development of more intuitive and secure authentication solutions that align with user needs and expectations across various demographics.

4

AI-Driven Cybersecurity: Opportunities, Challenges, and the Future of Human-AI Collaboration

Sheyla Gyles and Chutima Boonthum

As cyber threats grow in both frequency and sophistication, traditional cybersecurity measures struggle to keep pace with evolving attack methods. Artificial Intelligence (AI) has emerged as a powerful tool for enhancing threat detection, prevention, and response. AI-driven security systems offer the ability to analyze vast amounts of data in real-time, recognize subtle patterns indicative of cyber threats, and adapt to new attack strategies more efficiently than conventional approaches. However, despite AI's potential,

challenges remain regarding its effectiveness, ethical implications, and risks of adversarial manipulation. This research investigates the strengths and limitations of AI-driven cybersecurity by comparing AI-based security tools with traditional methods, identifying key advantages and vulnerabilities, and exploring ethical considerations. Additionally, a survey of cybersecurity professionals was conducted to assess expert opinions on AI's role, effectiveness, and potential risks. By combining these insights with experimental testing and a comprehensive review of existing literature, this study provides a nuanced understanding of AI's impact on cybersecurity and offers recommendations for optimizing its integration into modern security infrastructures.

5

Cybersecurity in Smart Homes: User Awareness and Security Practices

Fayed Troy and Chutima Boonthum-Denecke

This report will discuss and analyze the risks and challenges associated with smart home devices, focusing on vulnerabilities in commonly used products such as smart speakers, security cameras, thermostats, and lighting systems. As the adoption of smart home security grows globally, it has become clear that many users remain unaware of the associated security risks, leading to data breaches and potential privacy violations. This research evaluates the security features of these devices, the frequency of breaches, and common vulnerabilities. Using a mixed-methods approach—including a user survey, analysis of past cybersecurity incidents, and a detailed review of existing literature—this study assesses the current state of smart home device security. The findings aim to highlight gaps in user awareness, evaluate manufacturers' protective measures, and provide recommendations for improving cybersecurity practices in smart home environments.

6

A Study of Public Awareness and Perceptions for Enhancing Deepfake Detection Technologies

Jericka Guy

Deepfake technology presents a significant challenge to cybersecurity. These highly sophisticated AI-generated manipulations can compromise sensitive information and erode public trust, privacy, and security. This has led to broader societal impacts, including decreased trust and confidence in digital communications. This paper will discuss public knowledge, understanding, and perception of AI-generated deepfakes,

which was obtained through an online survey that measured people's ability to identify video, audio, and images of deepfakes. The findings will highlight the public's knowledge and perception of deepfakes, the risks that deepfake media presents, and the vulnerabilities to detection and prevention. This awareness will lead to stronger defense strategies and enhanced cybersecurity measures that will ultimately enhance deepfake detection technology and strengthen overall cybersecurity measures that will effectively mitigate exploitation risks and safeguard personal and organizational interests.

7

Behavioral Biometrics for Continuous Authentication: Exploring the Challenges and Opportunities

Gabrielle Olds and Janett Walters-Williams

This paper explores behavioral biometrics, an emerging authentication method leveraging unique user behavior patterns for continuous security. This dynamic approach offers enhanced protection compared to traditional methods, yet significant challenges must be addressed. A key concern, examined herein, is accuracy; false positives and false negatives can undermine system effectiveness. User frustration arises from false positives, while false negatives create security vulnerabilities. The work emphasizes the need for careful system tuning and advanced machine learning to mitigate these errors. Data privacy and security are also paramount, given the sensitive, non-replaceable nature of the collected information. The paper highlights the importance of robust security measures, user transparency, and informed consent. Furthermore, it acknowledges that natural human behavioral variability, influenced by physical and environmental factors, can impact authentication accuracy, necessitating adaptive systems. In conclusion, addressing these technical and ethical challenges is crucial for realizing the full potential of behavioral biometrics.

8

Defending Adversarial Patches: Detect & Blur

Erick Constant, Chutima Boonthum-Denecke and Idongesit Mkpong-Ruffin

Computer Vision models have increasingly been embedded into video software to recognize and classify things in the physical world. While this can provide a useful result it also opens the door to vulnerabilities through a physical attack. Using a printed-out generated image, individuals can exploit computer visions models to disguise their true

intentions. A possible way to block and mitigate the problems is to detect and blur the entire image to try to allow the AI to inference the said image.

9

Reducing The Effects Of Adversarial Patches Using Ai-Based Inpainting

Aris Hill and Chutima Boonthum-Denecke

Adversarial patches represent a critical vulnerability in computer vision systems, as they are specifically created in order to deceive object detection algorithms, which can compromise their reliability in real-world applications. This research investigates the impact of adversarial patches on object detection models and proposes a novel mitigation strategy to address this challenge. The study's primary objective was to design a comprehensive framework that integrates adversarial patch detection with image restoration. To achieve this, a YOLOv8-based detection framework was employed, trained on a specialized dataset of adversarial patches to ensure high detection accuracy. Upon identification of patches, advanced inpainting techniques utilizing AI models were applied to mask and fill the affected areas, restoring the image with expected content. The methodology combines the precision of object detection with the generative capabilities of modern inpainting algorithms, ensuring minimal disruption to the visual integrity of the image. This work contributes to the field of adversarial robustness by providing a comprehensive approach that integrates detection, masking, and content restoration. The results highlight the potential of AI-driven solutions to enhance the resilience of object detection systems against adversarial attacks, paving the way for safer deployment of vision-based technologies in critical domains such as autonomous vehicles, surveillance, and medical imaging.

10

Comparative Evaluation and Redesign of University Websites for Enhanced Human-Computer Interaction (HCI)

Angelina Woodard, Aris Hill, Chi Martin, Kaila Roberts, Noah Green and Joseph Aneke

University websites serve as a critical gateway for prospective students, faculty, and stakeholders, offering vital information about the institution and its services. This study evaluates the websites of four (4) universities– Cambridge, Hampton, Harvard, and Spelman, through the lens of Human-Computer Interaction (HCI). Using tools such as Google Page Speed Insights, and WAVE Accessibility Evaluation Tool focusing on compliance with WCAG 2.1 AA standards, we analyzed ten usability dimensions,

including technical performance, accessibility, responsiveness, branding, and user experience. Based on our findings, we propose a comprehensive prototype that incorporates the best features of these websites. This research does not in any way rank these universities but aims to highlight the importance of user-centered design in creating accessible, engaging, and efficient university websites.

11

Study of AI Object Detection: Patterns on Animals with YOLO and Adversarial Patches

Aniya Hopson and Chutima Boonthum-Denecke

In this paper, we documented our findings from previous research and literature related to adversarial examples and object detection. Artificial Intelligence (AI) is an increasingly powerful tool in various fields, particularly in image classification and object detection. As AI becomes more advanced, new methods to deceive machine learning models, such as adversarial perturbations, have emerged. These subtle modifications to images can cause AI models to misclassify objects, posing a significant challenge to their reliability. This research builds upon our earlier work by investigating how small perturbations affect object detection on YOLOv8. Last year, we explored patterns within images and their impact on model accuracy. This study will extend that by testing how adversarial perturbations, particularly those targeting animal patterns, affect YOLO v8's ability to accurately detect objects. We will also explore how untrained patterns influence the model’s performance, aiming to identify weaknesses and improve the robustness of object detection systems.

12

The Role of AI Machine Learning in Perpetuating Minority Bias

Angelina Woodard and Jean Muhammad

Concern about Artificial Intelligence (AI) and machine learning systems perpetuating societal biases has been growing rapidly along with the recent advancements of these systems. This study investigates how these biases are products of human prejudice reflected in training data. Very often, marginalized communities and demographics experience disproportionate negative effects from these biased systems due to the extensive integration of AI in law enforcement, government agencies, and other highly impactful organizations. The research to explore this concept will involve a type of Convolutional Neural Networks (CNNs) called residual networks, feature engineering,

and a deep understanding of classification science. By highlighting misidentification and discrepancies in accuracy, this research will illustrate the need for inclusive and diverse datasets to mitigate bias and ensure ethical fairness in these deeply integrated AI systems.

13

Navigating the Algorithm: A Study of User Behavior Patterns in the Age of Social Media

Micaiah Steplight and Jean Muhammad

Social media and entertainment application algorithms are meticulously designed with the intent of having users stay on the application. This research paper will explore how social media, and other applications algorithms influence user behavior by personalizing content and shaping engagement patterns. The study aims to investigate the mechanism behind algorithm-driven content recommendations and how systems adapt based on user behavior ultimately shaping user online habits. Through in-depth literary analysis and a variety of research methods including analyzing application data metrics, constructed interviews, and simulated algorithms, this paper will examine the connection between algorithmic personalization and the way users interact with those applications. Previous research has suggested that algorithm recommendations strengthen existing preferences leading to an increase in screen time and user retention while also profiting off monetization. This research aims to provide insight on the ethical consideration of algorithmic influence while better understanding how these algorithms shape user behavior, reinforce engagement patterns, and potentially manipulate users decision making impacting their well-being.

14

A Novel Approach to Detect Deepfakes Using LIME

Sandra Delancy and Lily Liang

The proliferation of deepfake images and videos has progressed exponentially in the past decade. Detecting deepfakes is more important than ever because of the potential damage these images can cause in medical, political, and social settings. Deepfake detectors typically flag an image or video as fake, but they may not explain how the prediction was achieved, which is important to establish trust in the prediction. This paper studies the feasibility of using LIME, an open-source object classification explainer for facial deepfake detection. We configured LIME with nine distinct combinations of

classification and segmentation algorithms, fine-tuning hyperparameters to optimize performance. By evaluating highlighted super pixels and conducting a quantitative analysis of confidence and magnitude metrics, we demonstrate that LIME can significantly enhance the interpretability and reliability of deepfake detection systems.

15

Deep Learning-Driven Predictive Frame Generation

Carlos Sac Mendoza and Lily Liang

This paper investigates and compares two different approaches for video frame interpolation using Google's FILM (Frame Interpolation for Large Motion) model to enhance the quality of low frame rate videos. We evaluated a full-frame approach, which prioritizes visual quality but is computationally intensive, and a motion-focused approach, designed for faster processing but with potential minor artifacts. While the model is designed to be used with pairs of images, its high-quality frame-generation capabilities have been adapted to work with videos. Both approaches divide videos into frames and use the FILM model to generate new intermediate frames, which can significantly improve the smoothness and responsiveness of low frame rate videos. Frame interpolation can make videos feel smoother and more responsive.

16

Deep Reinforcement Learning for Optimized Network Mapping and Vulnerability Detection

Jaden Johnson, Thaddeus White and Felicia Doswell

Network mapping is important for cybersecurity, providing a comprehensive view of network structures, identifying vulnerabilities, and detecting attack vectors. This project explores deep reinforcement learning (DRL) to enhance autonomous network mapping, enabling software agents to optimize their performance dynamically. The goal is to explore and evaluate DRL algorithms that improve the efficiency and accuracy of network discovery. Autonomous network mapping has significant societal benefits, particularly in cybersecurity, where DRL-equipped agents can continuously analyze vulnerabilities, enhance security, and improve resource allocation. Research highlights DLR's potential in cybersecurity and network resilience, emphasizing the need for adaptive learning models. Challenges such as model complexity, scalability, and cooperative decision-making remain areas of ongoing study.

This project includes a literature review on network mapping techniques, their limitations, and DRL's role in cybersecurity. Network data from sources like the Internet Topology Zoo is simulated using Mininet. The DRL approach is compared to traditional tools like Nmap and traceroute, focusing on accuracy, efficiency, and scalability. Visualization tools like NetworkX and Matplotlib illustrate network graphs, demonstrating infrastructure interconnectivity. Incorporating real-time data and state representation enhances network resilience. Findings indicate that DRL-based network mapping improves security, optimizes performance, and enables intelligent network management. By addressing real-time data collection, state representation, and efficient exploration, this research highlights DRL's potential in managing complex network environments and advancing autonomous cybersecurity.

Faculty Paper Abstracts

1

Artificial Intelligence Powered iOS Mobile App for Weed Identification

Biswajit Biswal and Jackson Edwards

Weeds are major burden in small and local farming communities in the United States due to the lack of technology, awareness, and education. Weed control is one of the greatest factors affecting crop production. Manual weeding provides the most precise management of weeds in the field. However, manual weeding is high labor intensity and high labor costs. This makes weed management hard for small and local farmers in the state of South Carolina, resulting in loss of crop yield and poor-quality production. In this work, Artificial Intelligence (AI) based iOS mobile app is used to identify the weed plants. In our work, we have successfully implemented an iOS mobile app to capture a weed image and identify weed-type using CNN, CreateML, Xcode and Swift programming language. Our model tested our weed plant database with an accuracy of 96%. Our results show that the developed iOS mobile app successfully identifies the weed plant. Our future work will include testing the iOS mobile app with more weed plant data for precise weed identification.

2

Leveraging Big Data for Sleep Health: A Preliminary Report of OSA Risk and Sleep Quality among HBCU Students

Ayodele Akinremi, Joseph Aneke, Graham Chakafana, Tafadzwa Machipisa and Elizabeth Locke

Obstructive Sleep Apnea (OSA) is a prevalent but underdiagnosed sleep disorder that disproportionately affects historically marginalized populations. Despite its known impact on cardiovascular and metabolic health, limited research has examined OSA risk and sleep quality among young Black adults, particularly those attending Historically Black Colleges and Universities (HBCUs). This study explores the association between OSA risk and sleep health among 64 HBCU students (39M, 24F), revealing that 7% had a high risk, 25% had an intermediate risk, and 68% had a low risk for OSA. Participants at high risk exhibited significantly higher BMI, waist circumference, and systolic and diastolic blood pressure, underscoring potential early health risks. Poor sleep quality emerged as an independent predictor of high OSA risk (OR: 1.17; 95% CI: 1.09 – 1.42). To advance this research, we propose leveraging big data and health informatics to enhance sleep health insights among young Black adults. By integrating large-scale datasets such as

the All of Us Research Program, machine learning models, and predictive analytics, we aim to develop personalized risk profiles, analyze social determinants of sleep disparities, and assess cardiovascular and metabolic health implications. Wearable technology and mHealth applications will enable real-time monitoring, facilitating targeted interventions to improve sleep hygiene and mitigate long-term health risks. This interdisciplinary approach underscores the transformative potential of AI and big data in sleep health research, offering scalable solutions to address health disparities and advance precision medicine in underrepresented communities."

3

Expanding AI and Machine Learning Education at Morehouse College: A Case for HBCU Integration

Ashley Scruse and Alfred Watkins

The artificial intelligence (AI) industry faces a dual challenge: a persistent diversity crisis and a growing skills gap. Black students remain underrepresented in AI and machine learning (ML), limiting both industry innovation and equitable representation in AI development [2, 21]. Historically Black Colleges and Universities (HBCUs) have the potential to address these disparities by expanding access to AI and ML education [5, 22]. This paper focuses on the need for AI and ML courses at HBCUs, with specific emphasis on implementing an introductory ML course at Morehouse College. The course is built using Google's Intro to Machine Learning materials [3] and teaches industry-standard tools like TensorFlow and NumPy, ensuring practical exposure to key ML workflows. A key aspect of this course is the integration of culturally relevant pedagogy, which has been shown to enhance student engagement and success [4, 14, 18]. By incorporating real-world applications that address issues relevant to Black communities, the course seeks to foster interest, improve retention, and prepare students for future opportunities in AI and ML. This initiative represents a critical step in bridging the AI education gap at HBCUs. By implementing structured AI and ML courses at Morehouse College, this effort aims to create a sustainable framework for increasing Black student participation in AI, ultimately leading to a more equitable and representative field [9, 16].

Poster Abstracts

1

Enhancing Personalised Book Recommendations Using Machine Learning

Oreoluwa Ala
Claflin University

Abstract

This project represents a vital step in addressing the problem of choice paralysis in readership. It seeks to use the potential of machine learning to provide a means to filter through the vast sea of book content available today.

The discovery process for new books is refined and made more accessible using various data processing, analytical tools, and machine learning methods. Instead of using one mode of generating recommendations, multiple methods are merged. Using clustering techniques such as K-means with SBERT's sentence transformer and cosine similarity and the power of semantic embedding, the developed recommendation system filters through book content to generate specific suggestions that resonate with each user's unique blend of tastes.

By bettering the process of discovering the next book, this research aspires to open the doors of literature to those who may not have found their way to it otherwise and those who have lost their way for many reasons.

2

ML Solutions for Land Cover Classification by Using Hyperspectral Images

Adrian Lockwood and Carlos Theran
Claflin University
Florida A & M University

Abstract

Land Cover classification is important for tracking how land is used and changes over time. This is essential for the environment, city planning, and farming. Hyperspectral images (HSI) are especially useful because they capture more information than regular photos, giving us a lot more detail. This helps us better identify different types of land and materials, like plants, water, and buildings. This not only saves time and resources but also offers a better understanding of land use and environmental changes.

3

Artificial Intelligence Powered Android Mobile App for Weed Identification

Jackson Edwards and Biswajit Biswal
South Carolina State University

Abstract

Weed control is one of the greatest factors affecting crop production. Manual weeding is high labor intensity and high labor costs. This makes weed management hard for small and local farmers in the state of South Carolina, resulting in loss of crop yield and poor-quality production. However, with smart intelligent systems weeding methods are not costly and thus, weed management is ease through AI and mobile app allowing ease data collection, create new weed datasets, link various existing weed datasets, automatic feature extraction, and precise weed identification while reducing labor and increasing product yield and quality. In this work, Artificial Intelligence (AI) powered android mobile app is used to identify the weed. In our initial work, we have successfully implemented an android mobile app using android studio and Kotlin programming language to capture a weed image, store into the device, select and classify the weed image using a pretrained AI model. Weed plant images are collected from our 1890 research and demonstration farm as well as from local farms through participating farmers in this project. Our implemented AI method is a CNN architecture which is trained, validated, and tested in our collected data. Our initial result showed that our model identified weed plants with an accuracy of 97%. Our developed android app integrated with our model successfully and was able to identify weed plant categories with classification probability scores. Our future work will be to test our developed custom AI model with newly collected weed data.

4

Evaluating the Effectiveness of Adversarial Patch Detection Methods: Key Metrics and Considerations

Shamon Sharpe, Rebecca Caldwell and Elva Jones
Winston-Salem State University

Abstract

Deep learning models, especially those used in security-critical applications like autonomous systems and biometric authentication, are significantly threatened by adversarial patches. To ensure reliability, robustness, and real-time applicability, a comprehensive set of metrics is required to evaluate the effectiveness of adversarial patch detection methods. Key performance indicators include Detection Rate (True Positive Rate, TPR) to measure the accuracy of identifying adversarial patches, and False Positive Rate (FPR) to minimize the misclassification of clean inputs.

Additionally, Precision and F1-Score provide insights into the balance between correct detections and false alarms, while the AUC-ROC Score offers a holistic measure of the model's ability to distinguish adversarial inputs. Given the real-time constraints of many applications, Detection Latency is crucial for assessing practical deployment viability. Moreover, Robustness Against Adaptive Attacks is essential to evaluate the resilience of detection methods against sophisticated evasion strategies. This study systematically analyzes these metrics to establish a comprehensive evaluation framework, guiding the development of more effective adversarial patch detection techniques.

5

The Impact of Lighting on Eyeglass-Based Cyber Attacks

Josiah Johnson, E. Rebecca Caldwell and Elva Jones
Winston-Salem State University

Abstract

Printed eyeglass-based adversarial attacks have emerged as a novel method for deceiving facial recognition systems, raising significant concerns about the robustness of biometric security in real-world applications. While numerous studies have demonstrated the effectiveness of these attacks under control conditions, the impact of ambient lighting on their performance has not been thoroughly explored.

This study investigates how different lighting environments—specifically indoor versus outdoor conditions—affect the success rate of printed eyeglass-based adversarial attacks. Our literature review included systematic experiments using state-of-the-art facial recognition models and varying lighting parameters such as intensity, angle, and spectral composition.

Our findings indicate that while the attacks remain highly effective under uniform indoor lighting, their performance declines in outdoor environments due to variable lighting conditions and reflections that pose significant challenges. These results emphasize the importance of considering environmental factors when developing and evaluating adversarial attack methodologies. They also highlight potential avenues for improving the resilience of biometric systems against such threats.

Collision Course: Elevating Concussion Awareness Through Immersive Virtual Reality

Michael Adeleke and Naja Mack
Morgan State University

Abstract

Concussions are a critical issue in the NFL, with over 149 players sustaining such injuries in a recent season. In response to historical skepticism regarding the neurological impact of the sport, notably highlighted by Dr. Julian Bailes' seminal work in 2007, Collision Course was developed to enhance awareness of sports-related concussions. Unlike existing VR platforms such as SyncThink, VRHealth, and Pre-Game Prep, which focus on diagnostics and rehabilitation, Collision Course is uniquely designed for immersive concussion education. Built in Unity and optimized for the Meta Quest 2, Collision Course integrates Convai's AI-driven NPCs to deliver a profound simulation of both the physiological and cognitive consequences of sustaining a concussion during an NFL game. This experience features interactive concussion scenarios, symptom visualization, educational elements, and gamified progressive difficulty levels. Users must recognize and respond to symptoms such as dizziness, tinnitus, and photosensitivity while being tested on their knowledge of concussion signs through interactive challenges. A usability study was conducted to analyze user interactions, identify pain points, and refine the experience based on participant feedback. This study explores two key research questions: (1) How effectively does Collision Course raise awareness of concussion risks? (2) Can participants accurately identify and describe concussion symptoms after completing the experience? By seamlessly combining immersive VR technology with educational awareness, Collision Course represents a significant stride in addressing the complex issue of concussions in sports. The findings from this research will inform further improvements, ensuring alignment with user needs and contributing to player safety and concussion prevention—not only in the NFL but across the broader sports community.

7

Transferability Of Adversarial Examples In Image Classification

Christian Henry, Elva Jones and E. Rebecca Caldwell
Winston-Salem State University

Abstract

Adversarial examples create a significant threat to deep learning-based image classification systems, challenging the stability of modern neural networks. This research analyzes whether adversarial examples created for one model can effectively deceive another model with a similar architecture. Through a review of recent studies, we analyze how attack methods such as Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD) contribute to adversarial transferability.

Findings from the research indicate that models with similar architectures and training datasets are particularly susceptible to shared adversarial attacks. This review emphasizes the shortcomings of current defense strategies and stresses the need for enhanced adversarial resilience in security-sensitive applications such as facial recognition and autonomous navigation.

8

Human Factors and Cybersecurity Breaches: Emphasizing Managerial and Supervisory Contributions

Miles Walker, Davina Pruitt-Mentle and Joseph Aneke
Hampton University

Abstract

This study explores the critical influence of human factors, specifically managerial and supervisory contributions, on cybersecurity breaches. By employing the Human Factors Analysis and Classification System (HFACS) framework—originally developed to reduce aviation accidents in the U.S. Navy. The framework has four levels–Unsafe Acts, Preconditions for Unsafe Acts, Supervisory Factors, and Organizational Influences. In this research, we focus on Supervisory Factors, identifying specific supervisory failures that exacerbate cybersecurity vulnerabilities. The study then connects the findings to the Systems Security Management work role, as defined in the NICE Workforce Framework for Cybersecurity, aiming to highlight actionable insights for workforce development and improved cybersecurity training.

Preparing Early CS Majors for Technical Interviews with Group-Based Whiteboarding

Destiny Bertier and Naja Mack
Morgan State University

Abstract

The increasing demand for skilled computer science (CS) graduates has highlighted the importance of structured technical interview preparation, as many students, particularly those from underrepresented backgrounds, struggle due to a lack of exposure and formal training. Technical interviews are a critical component of the hiring process in the tech industry, requiring candidates to demonstrate problem-solving abilities, programming proficiency, and the ability to articulate their thought processes effectively. However, many early CS majors lack experience with these interviews, leading to performance anxiety and missed career opportunities. This study examines the impact of group-based whiteboard problem-solving activities on early CS majors at a Mid-Atlantic Historically Black College or University (HBCU), to improve their problem-solving skills, communication abilities, and overall confidence in technical interview settings. Conducted over multiple semesters in CS2 and Object-Oriented Programming (OOP) courses, the study engaged students in collaborative problem-solving sessions where they were required to articulate their approaches, think critically, and implement solutions using a virtual whiteboard. Students participated in pre-and post-assessments to evaluate their progression, while surveys captured their perceptions, comfort levels, and anxiety before and after each session. The results indicate that most students successfully completed their assigned tasks, with improvements in confidence and problem-solving proficiency over time. Their initial perceptions of the experience were largely positive, and these favorable attitudes increased as they became more familiar with the format. Comfort levels also improved after repeated exposure, though many students continued to experience performance anxiety, particularly when implementing code. While problem conceptualization and peer communication were generally perceived as easier aspects of the exercise, the actual coding process was identified as the most challenging component, highlighting a gap in student preparation. These findings suggest that while structured exposure to technical interview practices can significantly enhance student readiness, additional support, such as individualized coaching, targeted programming exercises, and extended practice sessions, may be necessary to address persistent difficulties. By integrating these activities into the CS curriculum, institutions can better prepare students for technical interviews, improving their confidence and competitiveness in the job market.

10

Comparison of Patch Size in Adversarial Patch Detection Approaches

Damone Washington, Rebecca Caldwell and Elva Jones
Winston-Salem State University

Abstract

Adversarial patches were first introduced in 2018 by Brown et al., demonstrating their ability to mislead image classifiers using round stickers (Wei et al., 2022). This concept was further developed for object detection in 2019 with the introduction of Dpatch, although initial tests were limited to digital environments.

Adversarial attacks have become a significant vulnerability for modern object detection systems, which are increasingly used in real-world applications like autonomous vehicles, surveillance, and robotics. This poster examines the critical question: "What is the minimum size of adversarial stickers required to substantially disrupt object detection systems?"

By reviewing the existing literature on adversarial patch attacks and analyzing state-of-the-art object detectors, we identify key factors that influence the effectiveness of these perturbations. Our study investigates how sticker dimensions relate to attack success rates and explores the trade-offs between sticker size and detection robustness.

The findings offer important insights into both the limitations of current object detection frameworks and potential strategies for enhancing their resistance to adversarial manipulation. This work establishes a foundation for developing more secure AI systems and informs future research on adversarial defense strategies.

11

CodeBears+: Transforming Summer Coding Camps into Year-Round STEM Adventures

Amyra Harry and Naja Mack
Morgan State University

Abstract

A lack of exposure to computer science (CS) topics and accessible role models can diminish student engagement, leading to fewer enrollments in CS programs and a less diverse tech industry. Research suggests continuous engagement in coding and technology is critical for fostering long-term interest and proficiency in CS. CodeBears+ addresses this challenge by inspiring underrepresented students to explore STEM careers while enhancing engagement and confidence in computing skills. The program

provides technology-rich learning opportunities for underrepresented K-12 students to develop computational thinking and computer science concepts through an engaging, culturally relevant, and hands-on learning experience. Originally launched as a two-week summer camp, CodeBears Summer Camp enables youth-led teams to learn, build, and program interactive technologies with the guidance of graduate and undergraduate student instructors. The camp culminates in a showcase event, where students present their projects to family and friends. Due to its success and overwhelming positive feedback, CodeBears+ expanded to include a Saturday Academy, offering year-round engagement with advanced topics like game development and music production. More than 50% of original participants returned, reinforcing the program's impact. The Saturday Academy allows students to stay involved in computing while building rapport and strengthening their computing identity. By providing consistent exposure to STEM concepts, CodeBears+ improves problem-solving skills, fosters self-confidence, and builds a strong technical foundation for future academic and career success. Through this experience, students gain collaborative, coding, and technical skills while developing a lasting interest in computing. Future research will explore strategies for maintaining year-round involvement and incorporating culturally relevant education to expand CodeBears+'s impact on underrepresented communities.

12

FinPro: Bridging the Financial Literacy Gap in Baltimore with Artificial Intelligence

Osita Odunze and Naja Mack
Morgan State University

Abstract

Financial literacy among Baltimore's youth is a significant concern with long-term implications for their economic well-being. According to a 2021 study by the Council for Economic Education, only 34% of Baltimore high school students possess basic financial literacy skills, compared to the national average of 48%. This disparity is particularly pronounced in economically disadvantaged areas. Data from the Free and Reduced-Price Meal Statistics indicate that over 75% of students in Baltimore City Public Schools qualify for free or reduced-price meals, highlighting the socioeconomic challenges that many students face. These statistics underscore the urgent need for targeted interventions to bridge the financial literacy gap. To address this issue, the FinPro project was developed as an AI-powered application designed to enhance financial education among Baltimore's youth. By leveraging large language models and modern cloud-based tools, FinPro delivers personalized financial education through an interactive conversational agent tailored to users' diverse backgrounds. The agent provides context-aware advice and culturally relevant examples, ensuring that financial lessons resonate with the unique experiences of its users. Additionally, FinPro incorporates gamified

financial simulations that engage users in practical financial management scenarios, fostering improved budgeting skills and smarter spending habits. FinPro contributes to the growing field of AI-enhanced educational tools by demonstrating how artificial intelligence can be harnessed to deliver personalized and culturally responsive financial education. It explores the potential of AI-driven interventions to bridge educational gaps and promote economic empowerment among underserved communities. However, further research is necessary to fully understand its impact and refine its features for optimal user engagement. Future work will focus on conducting comprehensive usability studies to evaluate FinPro's effectiveness. These studies will involve detailed observations of user interactions, structured interviews, and surveys to assess usability, engagement, and educational outcomes. Specific attention will be given to identifying areas where users may experience difficulties or confusion. The insights gained from these studies will guide the iterative development of FinPro, ensuring that the application effectively meets the financial education needs and preferences of Baltimore's underserved youth.

13

Effectiveness of Adversarial Patch Detection Models Across Different Datasets

Christian Griffin, E. Rebecca Caldwell and Elva Jones
Winston-Salem State University

Abstract

Adversarial patch attacks pose significant challenges to deep learning models, particularly in object detection tasks. Recent studies have explored the creation of naturalistic adversarial patches using generative adversarial networks to produce more realistic and less conspicuous confusion. However, the relevancy of adversarial patch detection models across different datasets remains underexplored.

This study investigates the effectiveness of adversarial path detection models trained on one dataset when applied to one another, generalization, including dataset characteristics, model architectures, and training methodologies. Our finding aims to provide insights into the limitations of current adversarial patch detection approaches and suggest directions for developing more adaptable and robust detection mechanisms to enhance security in real-world applications.

Quantum Computing and Cybersecurity: Opportunities and Threats

Prairie View University Viceroy
Prairie View A & M University

Abstract

Quantum Key Distribution (QKD) uses the quantum properties of photons to establish a secure key between a sender and receiver. The BB84 protocol encodes bits into photon polarization states and is transmitted through a quantum channel. Any interception disturbs the photons, increasing error rates, which can be detected. This ensures secure key exchange, as eavesdropping alters the quantum states.

Quantum computers are reshaping cybersecurity by breaking traditional encryption and enabling unhackable communication. Most secure online communications rely on RSA encryption, which classical computers would take millions of years to crack. However, a quantum computer running Shor's Algorithm could break it in minutes to hours, prompting the development of post-quantum cryptography (PQC) by tech giants like Google, IBM, and the NSA. Quantum advancements offer a solution through QKD and quantum entanglement, making eavesdropping physically impossible by altering data upon interception. This was demonstrated in 2017 when China's Micius Satellite enabled a quantum-encrypted video call between China and Austria, proving that quantum-secure communication is already a reality. As quantum technology progresses, it presents both a threat to existing security and a pathway to future protection, making it one of the most urgent topics in cybersecurity today.

A crucial component of "cyber quantum computing" is the Quantum Random Number Generator (QRNG). Traditional pseudo-random number generators rely on algorithms running on classical hardware and can be vulnerable if their internal states are compromised or predicted. QRNGs exploit inherently unpredictable quantum phenomena to produce truly random numbers. In cybersecurity, high-quality randomness is essential for generating cryptographic keys that cannot be guessed or reverse-engineered. By integrating QRNGs into cryptographic systems, organizations can significantly enhance the security of key generation, ensuring that keys remain robust against both classical and future quantum-enabled attacks.

15

Revolutionizing and Pioneering Culturally Relevant Math Education Through Artificial Intelligence and Co-Designing Strategies

Clyde Tandjong and Naja Mack
Morgan State University

Abstract

In 2023, Baltimore City Public Schools reported a staggering statistic, none of the 1,736 students from 13 schools achieved proficiency on the Maryland state math exam. This crisis, persistent since 2017, highlights a deep-rooted systemic failure in math education. To confront this challenge, we introduce MathWiz, a groundbreaking web-based intelligent tutoring system designed to revolutionize math learning through culturally responsive teaching, mastery learning, and artificial intelligence. At the core of MathWiz is a dynamic 3D avatar math companion that delivers personalized, adaptive instruction, aligning with students' individual learning needs and cultural backgrounds. Our research hypothesizes that integrating culturally relevant content with mastery learning will drive higher math proficiency, increased engagement, and positive attitudes toward math education. Methods include a three-phase approach: (1) Co-design workshops with students and teachers to refine features and strategies, (2) usability studies to evaluate system interface and logic, and (3) pilot testing to assess preliminary effectiveness. Participants will include 50–200 middle and high school students, math teachers, and parents from Baltimore City Public Schools. Data collection will involve pre-and post-assessments, user interactions, interactive lessons, and surveys to measure impact. While results are forthcoming, anticipated outcomes include enhanced math proficiency, stronger critical thinking, and improved digital literacy skills. By fostering culturally inclusive and engaging learning environments, MathWiz aims to provide a scalable, AI-driven solution to long-standing educational inequities. Future research will explore long-term impacts, scalability, and applications in underserved communities, demonstrating how AI-powered tools can be co-designed to tackle systemic educational challenges and create equitable learning opportunities.

16

Ethical Considerations in Adversarial Patch Detection for Sensitive Domains

Tayah Lewter, Elva Jones and E. Rebecca Caldwell
Winston-Salem State University

Abstract

Adversarial patch detection is an emerging security measure designed to counteract adversarial attacks that manipulate AI models into making incorrect predictions. While

this technology enhances security in fields like surveillance and healthcare by improving anomaly detection and diagnostic accuracy, its deployment raises ethical concerns.
Key challenges include potential privacy violations, risks of over-reliance on automated systems, and the continuous need for resource allocation to keep pace with evolving threats. This presentation explores the ethical implications of implementing adversarial patch detection in sensitive domains, balancing security benefits against the societal and ethical risks associated with AI-driven decision-making.

17

Protecting the Skies and Roads: Addressing Digital Vulnerabilities in Automotive and Aviation Industries

Shemar Stewart and Shemarjstewart Hasnain
Voorhees University

Abstract

This presentation explores the increasing cybersecurity risks in vehicle manufacturing and the digitization of transportation systems, including cars and planes. As automotive and aerospace industries embrace advanced technologies like artificial intelligence (AI) and Internet of Things (IoT) systems, they become more vulnerable to cyber threats. The integration of connected systems in modern vehicles has exposed critical cybersecurity vulnerabilities, ranging from hacking autonomous vehicles to compromising aircraft systems. This presentation will examine real-world case studies, including high-profile hacking attempts in the automotive and aviation sectors, to underscore the urgent need for enhanced cybersecurity measures in safeguarding the future of transportation.

18

The Road Forward: Highways, Racial Disparities, and Inclusive Development.

Myles Ndiritu and Kyshan Nichols-Smith
Morehouse College

Abstract

How does highway development affect change? This study examines how highway access impacts inclusive economic development and racial economic disparities in Georgia. Using geospatial data from ArcGIS and socioeconomic metrics from the American Community Survey, integrated with Mastercard Inclusive Growth Scores, linear regression models reveal that highway access correlates with higher Inclusive Growth Scores statewide, indicating economic benefits. However, in Fulton County, highway proximity is linked to increased racial poverty disparities, underscoring the uneven effects of infrastructure. The findings highlight highways as both economic enablers and potential

drivers of inequality. Policy recommendations stress the need for inclusive highway development strategies that address racial disparities while promoting equitable growth.

19

Comparing the Speed of Adversarial Patch Detection Approaches

William Johnson, Elva Jones and Rebecca Caldwell
Winston-Salem State University

Abstract

Adversarial patches pose a significant threat to the reliability of machine learning systems, prompting extensive research into various detection methodologies. This poster presents a comprehensive literature review focused on comparing the speed of different adversarial patch detection approaches. Although accuracy has been the primary focus in many studies, our review highlights that detection speed is crucial for real-time applications, such as autonomous driving and surveillance.

This study analyzes and synthesizes findings from a range of methodologies—from classical statistical methods to modern deep learning frameworks—to evaluate reported processing times and computational efficiencies. The review identifies key trends and trade-offs between detection accuracy and speed and underscores the need for further research to develop faster and more scalable detection algorithms. This poster serves as a foundational resource for understanding the current landscape and guiding future advancements in adversarial patch detection.

20

Transforming Perspectives, One Story at a Time: Have a Heart

Elijah Ballou and Naja Mack
Morgan State University

Abstract

Have a Heart is a groundbreaking virtual reality (VR) experience designed to immerse users in the harsh realities of homelessness, fostering empathy, awareness, and action. The United States has one of the highest homelessness rates among developed nations, with 6.2% of Americans experiencing homelessness in their lifetime, compared to 2.4% in Germany and 4.0% in Italy [1]. Between 2007 and 2019, over 500,000 individuals were unsheltered on any given night, particularly in urban centers [13]. Those facing homelessness endure challenges such as hunger, violence, poor health, and extreme weather, yet societal responses often lack urgency and empathy. By integrating VR with interactive storytelling and game mechanics, Have a Heart provides an open-world experience where users explore urban environments, interact with non-playable

characters (NPCs), and make critical choices that affect their survival. Players must navigate real-life struggles, including securing shelter, finding food, managing health, and seeking employment, all while facing systemic barriers. Through action-based gameplay and branching narratives, the experience offers a deeper, more personal understanding of homelessness. Beyond raising awareness, Have a Heart enhances engagement, increases information retention, and challenges misconceptions. More than an educational tool, it is a call to action encouraging advocacy and policy change by transforming passive observation into active empathy. By leveraging VR's immersive power, Have a Heart fosters meaningful conversations and drives real-world impact, inspiring users to rethink homelessness and their role in addressing it.

21

Mind Mastery: Advancing Gaming Accessibility Through Brain-Computer Interfaces

Andrew Kelly and Naja Mack
Morgan State University

Abstract

The gaming industry continues to evolve, yet accessibility barriers persist, affecting 91% of gamers with disabilities. Mind Mastery, a Brain-Computer Interface (BCI) game developed in Unity 3D, addresses these challenges by enabling hands-free gameplay through electroencephalography (EEG) signals, gyroscopic head movements, and blink detection. Utilizing the Muse 2 EEG headset, the system reduces hair-related interference and optimizes signal filtering for improved accuracy. EEG data is streamed in real-time via MuseLSL and integrated into Unity 3D using LSL4Unity, ensuring responsive and adaptive gameplay. Players interact through gyroscopic head tilts, blink detection, and concentration-based controls, enabling actions such as jumping, shrinking, growing, and force-falling without traditional input devices. Developed with an emphasis on real-time signal processing and adaptive feedback, Mind Mastery incorporates gyroscopic calibration, blink detection, and dynamic difficulty adjustment to enhance user experience. A usability study with 22 participants highlighted areas for improvement, including error handling, blink calibration, and increased challenge variability. In response, levels have been refined, and enhancements to blink calibration and error handling are in progress. Future development aims to integrate motor imagery detection as the primary control mechanism, allowing players to interact solely through thought-based commands. By advancing EEG-based interaction and real-time BCI integration, Mind Mastery demonstrates the potential of neurotechnology in gaming accessibility, breaking traditional barriers and fostering inclusivity in interactive experiences.

22

Securing Financial Transactions: Evolution, Innovations, and Future Challenges

Ashley Chambers
Voorhees University

Abstract

The expansion of online banking, digital transactions, and cryptocurrencies has revolutionized the financial industry, necessitating advanced security measures. This research examines the evolution of online banking security, the development of credit card technology, and the impact of digital currencies like Bitcoin on global finance. Additionally, it explores vulnerabilities in current financial systems and investigates emerging technologies such as blockchain, multi-factor authentication, biometric security, and AI-driven fraud detection for improving the security of online banking and cryptocurrency transactions. By analyzing these innovations, this study aims to contribute to the development of more secure and resilient financial infrastructures in the digital era.

23

AI & Sports: Analyzing NBA Key Player Impacts

Derrick Tilford
Morehouse College

Abstract

This research focuses on and demonstrates the National Basketball Association's player statistics from the 2020-2021 season. The research question examined is, “What were the stats for key players during the 2020-2021 season?” This critical information is essential to determine the team's outcome for that season and how their key players contributed to these outcomes. The data will be stored in the API keys and manipulated with Python, creating a chat box for basketball fans to ask questions about players and get insights into their stats from that season. Big data from API key and machine learning are used to understand how many games players played, their average points, rebounds, assists, steals, free throw percentage, and field goal percentage. The data gathered from the API key will be put into Python and coded for the AI assistant to sort through when asked about a particular player from the data. The research finds that the teams with more key players with higher stats in each category tended to have a better season outcome. This is significant for coaches and team general managers because it shows them where players are thriving and where they need to improve, helping their team succeed in the future. It is also significant for the fans because if they want to know

statistical information about players, they can ask the chatbot, and the AI assistant will provide the information.

24

Advancements in Word Embeddings for Natural Language Processing: Improving AI-Driven Language Understanding

Wendon Doswell, Clay Jones and Tonya Fields
Norfolk State University

Abstract

Natural Language Processing (NLP), a branch of Artificial Intelligence (AI), enables machines to interpret, generate, and manipulate human language. Since raw text is not inherently understandable by machines, it must be transformed into numerical representations for processing. This transformation is achieved through word vectors and word embeddings, which serve as mathematical representations of words, allowing machine learning (ML) models to derive meaning from language.

Traditional NLP techniques, such as one-hot encoding, bag of words, and term frequency-inverse document frequency (TF-IDF), provided initial methods for representing words numerically. However, these approaches struggled to capture relationships between words and often resulted in sparse, high-dimensional representations that lacked semantic understanding. To address these limitations, word embeddings, such as Word2Vec, GloVe, and FastText, were introduced as more advanced techniques. Unlike earlier methods, word embeddings generate dense vector representations of words, capturing their semantic relationships by positioning similar words closer together in a multi-dimensional space. These embeddings leverage neural networks and statistical models to understand word meanings based on their contextual usage in large text corpora. For example, trained word embeddings can effectively capture relationships such as "king" and "queen" or "Paris" and "France."

A comprehensive literature review was conducted to examine the evolution of NLP techniques and assess the effectiveness of various word embedding algorithms. Additionally, experimentation with different algorithms was performed to analyze their performance in capturing semantic relationships and improving text-based ML applications. The findings indicate that Word2Vec and FastText performed well in capturing word similarities and contextual relationships, with FastText demonstrating superiority in handling previously unseen words due to its subword-based approach. GloVe, while effective in capturing global word co-occurrence, showed limitations in real-time learning applications where adaptability is required. Overall, word embedding enhanced NLP tasks compared to traditional techniques, improving model performance in sentiment analysis, machine translation, and chatbot development.

The integration of word embeddings has significantly advanced NLP applications by enhancing language understanding and contextual accuracy in AI-driven systems. The transition from traditional numerical representations to word embeddings has improved ML model performance, enabling more sophisticated and context-aware NLP applications. Findings from this study emphasize the need for continued research and optimization of embedding techniques to further refine AI-driven language understanding.

25

Reinforcement Learning for Network Intrusion Detection: A Deep Q-Learning Approach

Benedict Frimpong, Antione Searcy and Briana Wellman
University of the District of Columbia

Abstract

In today's fast-evolving digital landscape, where cyber threats are becoming more sophisticated by the day, embracing advanced and intelligent defense strategies is of utmost importance. THis work introduces an innovative reinforcement learning (RL) agent, crafted with the purpose of autonomously detecting and responding to possible network intrusions.

We have analyzed, established and tested tailored simulations in an environment utilizing existing robust frameworks that faithfully replicate network traffic patterns. Within this carefully constructed setting, the agent learns to make crucial binary choices about whether to approve or deny incoming network packets, all by scrutinizing key attributes, including source IP addresses and the sizes of the packets.

The focus of this RL approach is to enable the agent to learn from rewards. The RL reward structure incentivizes the agent to successfully block anomalous traffic while imposing penalties for erroneous blocking, thereby facilitating the continual improvement of its decision-making processes. Preliminary findings from our simulation indicate promising effectiveness, and we are actively engaged in further validating our methodology with real-world network datasets like CTU-13, utilizing Scapy. This investigation aims to enhance our comprehension of how modifications to the reward function may impact detection accuracy.

As extremely challenging adversaries become ever more prevalent and advanced, ensuring the stability and sustainability of networks grows increasingly trying. A plethora of threats plague modern networks, from dynamic Distributed Denial of Service (DDoS) attacks to intrusive worms. Deep Reinforcement Learning (DRL) is proposed as a versatile tool in the cybersecurity arsenal, expanding its potential to address key

cybersecurity challenges and explore emerging attack types, while emphasizing future application opportunities.This work demonstrates the ability of DRL, particularly in the form of Deep Q-Learning (DQN), to enhance cybersecurity, especially in addressing modern network threats like DDoS attacks and botnets. Preliminary results, including cumulative reward and accuracy, demonstrate the potential of DRL to evolve as a powerful tool for network defense.

26

Enhancing Autonomous Network Mapping Using Deep Reinforcement Learning

Jaden Johnson, Thaddeus White and Felicia Doswell
Norfolk State University

Abstract

Effective network mapping is essential for cybersecurity, as it enables a comprehensive view of network structures, identifies vulnerabilities, and detects potential attack vectors. This project explores deep reinforcement learning (DRL) to enhance autonomous network mapping, allowing software agents to dynamically learn and adapt for improved accuracy and efficiency in network discovery. By addressing limitations in traditional methods, DLR offers a more intelligent and adaptive approach to network analysis.

Autonomous network mapping plays a major role in cybersecurity, where advanced threats require adaptive defense mechanisms. DRL-equipped agents can continuously analyze network vulnerabilities, enhance security measures, and optimize resource allocation for improved network performance. Existing research highlights the potential of DRL in cybersecurity and network resilience, emphasizing the need for adaptive learning models that evolve with changing data and threats. However, challenges such as model complexity, scalability, and cooperative decision-making remain areas of ongoing study.

This research follows a structured methodology, beginning with a literature review of network mapping techniques, their limitations, and DRL's potential in cybersecurity. Network topology data is collected from sources like the Internet Topology Zoo and simulated using tools such as Mininet and NS-3. The DRL-based approach is evaluated against traditional network mapping methods like Nmap and traceroute, focusing on accuracy, efficiency, and scalability. Visualization tools like NetworkX and Matplotlib demonstrate the interconnected nature of modern infrastructures and the need for advanced mapping techniques. By integrating real-time data collection and state representation, this approach enhances network resilience.

Results show that DRL-based network mapping improves security, increases efficiency, and enables intelligent network management, outperforming traditional methods in

performance metrics. This research highlights DRL's role in handling complex network environments and underscores the importance of continued innovation in autonomous cybersecurity. Future work should explore multi-agent DRL models and real-time adaptive mapping to further strengthen network security.

27

Comparison of Accuracy in Adversarial Patch Detection Approaches

Joshua Cooke, Rebecca Caldwell and Elva Jones
Winston-Salem State University

Abstract

Adversarial patch detection has emerged as a crucial field in securing deep learning models against localized adversarial attacks. This literature review examines and compares various adversarial patch detection approaches with a focus on accuracy. We analyze traditional machine learning methods, deep learning-based techniques, and hybrid models, highlighting their detection effectiveness across different datasets and attack scenarios. By synthesizing findings from recent studies, we identify key factors influencing detection accuracy, including model architecture, feature extraction techniques, and robustness to adaptive attacks. Our review provides insights into the strengths and limitations of existing approaches, offering guidance for future research and the development of more reliable adversarial patch detection systems.

28

Bridging the Gap: An Alumni, Student and Professors Engagement Platform for Career Opportunities

Anthony Nwafor and Marcus Golden
Mississippi Valley State University

Abstract

The transition from academia to the professional realm or vice versa can be a formidable challenge for students, alumni, and professors alike. Securing internships or jobs that align with career aspirations and fostering meaningful connections within professional networks can be particularly daunting. Recognizing these challenges, we propose an alumni engagement platform that assists seamless interactions between alumni, students, and professors, cultivating a supportive network that opens doors to a wide spectrum of professional opportunities.

The platform will incorporate a user-friendly interface, and a messaging system. These features empower alumni, students, and professors to navigate the job market effectively, fostering a culture of knowledge sharing and professional growth. To streamline the application process, the platform will incorporate a user-friendly interface that allows

applicants to submit their resumes and cover letters directly to the provided application link posted by the opportunity poster. To foster effective communication between job seekers and employers, a private messaging system will be integrated, enabling direct and confidential exchanges. For opportunity posters, the platform will provide a dedicated dashboard to manage job postings, review or track applicants for the specific opportunity. By bridging the gap between these three key stakeholders, we aim to empower the next generation of professionals.

29

PeerConnect

Teniola Oluwaseyitan
Mississippi Valley State University

Abstract

PeerConnect is a tutoring platform developed to enhance academic support among students at Mississippi Valley State University. This app allows students to seamlessly switch between roles as tutors and learners, empowering them to either seek assistance in challenging subjects or offer their expertise in areas they excel. By enabling students to specify their academic strengths and areas for growth, PeerConnect provides a flexible, role-switching system that fosters a collaborative learning community. Core features include user registration, session scheduling, and an intuitive search function to connect students with compatible study partners.

30

Analyzing Network Traffic for Virus Detection Based on Destination and C2 Command Variability

Ayomide Olasupo and Eyimofe Ajagunna
Mississippi Valley State University

Abstract

The detection of potential viruses and malware can be enhanced by analyzing network traffic patterns, particularly through changes in destination addresses and Command and Control (C2) commands. Malware often communicates with specific destinations or C2 servers, and deviations from these patterns may indicate suspicious behavior. This paper discusses how monitoring destination changes and C2 command anomalies can aid in early virus detection, improving the accuracy and efficiency of network monitoring systems.

31

Smart Integrated Shopping System App

Ledarius Robinson and Adin Lindsey
Mississippi Valley State University

Abstract

The Smart Integrated Shopping System App transforms grocery shopping with advanced technology to improve efficiency and convenience. This app assists shoppers from planning to checkout, featuring real-time pricing, product availability, and store-specific promotions. Its key features include a navigational store map, a self-driven cart for visually impaired users, and automatic reminders for frequently purchased items. By reducing the need for in-store assistance and enhancing customer experience through efficient service, the app sets new retail standards. Functionalities include a comprehensive product database, automatic bill generation, and the ability to update product details, ensuring a seamless shopping journey for all users.

32

AI Threat Detection and Prevention

Takejah O'Neal and Khaleah Jackson
North Carolina Central University

Abstract

Artificial Intelligence (AI) is transforming the way cybersecurity professionals detect and prevent threats, offering faster, more accurate, and flexible solutions to handle today's complex cyber challenges. This poster explores the different ways AI helps to find, evaluate, and address security risks, focusing on techniques like machine learning (ML), deep learning, and behavioral analytics. By analyzing vast amounts of data, AI can spot unusual patterns and behaviors, which often go unnoticed by traditional security systems and human analysts.

In threat detection, AI-powered tools can monitor network traffic in real-time and quickly flag unusual activities, making it easier to respond to incidents rapidly. This is especially important for identifying advanced threats, like zero-day vulnerabilities and advanced persistent threats (APTs), which are becoming more sophisticated and difficult to detect. AI models, including neural networks and decision trees, enhance predictive accuracy, giving organizations the chance to respond proactively.

For threat prevention, AI supports proactive defense strategies by analyzing potential threats and simulating attack scenarios, helping cybersecurity teams build stronger defenses. AI can also adapt to new threats by learning from past incidents, evolving continuously with the shifting threat landscape.

This project also looks at challenges, such as AI's potential risks from adversarial attacks and privacy concerns in data handling. Through this study, we aim to demonstrate how AI can be a powerful tool for those in cybersecurity, equipping them to take on critical roles in defending against cyber threats and inspiring others to enter this innovative and impactful field.

33

The Effectiveness of Basic Image Processing Methods in Filtering Out Adversarial Patches

Michael Hall, Rebecca Caldwell, and Elva Jones
Winston-Salem State University

Abstract

Based on an extensive literature review, this research poster explores the effectiveness of basic image processing methods in filtering out adversarial patches. Adversarial patches are manipulated pixel regions designed to mislead machine learning models, presenting a significant challenge in the field of image classification. Various basic image processing techniques, such as color-depth reduction, spatial smoothing, and total variance minimization, have been studied as potential defenses against these attacks. By synthesizing findings from existing research, this study examines how these methods impact the robustness and accuracy of image classification models. The review highlights that while these techniques can mitigate some adversarial effects, they often result in a trade-off with reduced accuracy for clean images. The findings underscore the need for further exploration of more advanced and integrated defense mechanisms to achieve a balance between robustness and accuracy. This poster aims to provide a foundational understanding for researchers and encourage future investigations into effective adversarial patch defenses.

34

Enhancing Virus Detection with RTT, TTL, and Network Hop Analysis

Bakri Diyaolu, Teniola Oluwaseyitan, Sofiyah Afolabi
Mississippi Valley State University

Abstract

Effective detection of potential viruses on a machine requires analyzing both traditional indicators, such as file signatures, and network-level attributes like Round Trip Time (RTT), Time-to-Live (TTL), and hop counts. Abnormalities in these metrics can indicate malware communication attempts. Variations in TTL values may suggest that a virus is attempting to disguise its traffic or avoid detection through proxy servers. Additionally, missing or unnecessary hops in network routes can signal malware attempting to

obscure communication with external servers. This paper explores how RTT, TTL, and hop-based analysis improve the accuracy of virus detection and discusses the effectiveness of anomaly detection in identifying malware activity.

Faculty Poster Abstract

Empowering Health Informatics Research at an HBCU: Leveraging AI and the All of Us Database for Health Equity

Graham Chakafana[1], Joseph Aneke[1], Ayodele Akinrem[1] & Tafadzwa Machipisa[2]
[1]Hampton University & [2]University of Pennsylvania

Abstract

Historically Black Colleges and Universities (HBCUs) play a pivotal role in addressing healthcare disparities by fostering diversity in research participation and promoting culturally competent healthcare solutions. The All of Us Research Program, a National Institutes of Health (NIH) initiative, provides a transformative resource for advancing precision medicine and health equity. At Hampton University, we are integrating Artificial Intelligence (AI) and data science into health informatics research to enhance institutional research capacity and prepare the next generation of data-driven healthcare professionals.

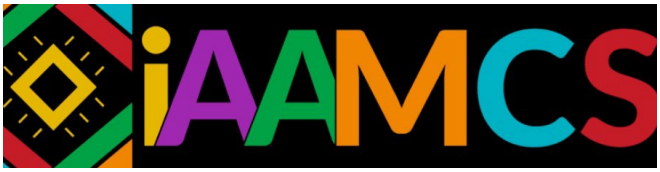
This study presents a structured approach to incorporating AI-driven analytics into the utilization of the All of Us database at Hampton University. Our initiative trains undergraduates in Biochemistry, Computer Science, and Physical therapy to apply machine learning (ML), natural language processing (NLP), and predictive modeling in clinical research. Using AI, we explore early detection models for lung infections and cardiovascular disease, particularly in underrepresented populations, by identifying novel risk factors and predictive biomarkers.

Faculty engagement has been strengthened through interdisciplinary collaborations, bridging the gap between computational sciences and biomedical research. AI-powered data mining techniques are employed to extract meaningful insights from structured and unstructured health records, enabling more precise investigations into genetic factors, social determinants of health, and epidemiological trends. Additionally, AI-based explainable models are used to ensure transparency and fairness in health disparity research.

The impact of this initiative was assessed through structured surveys, data utilization metrics, and student research output. Our findings demonstrate that integrating AI with the All of Us database significantly enhances research productivity, fosters innovative student-led projects, and broadens participation in biomedical data science at an HBCU. Community engagement further amplifies research outreach, fostering trust in AI-driven healthcare solutions. By combining AI methodologies with large-scale, diverse datasets, we hope to revolutionize health informatics research at Hampton University. This initiative will not only strengthen HBCU research capacity but also advance precision medicine and health equity investigations, ensuring that AI-driven innovations benefit underrepresented communities.

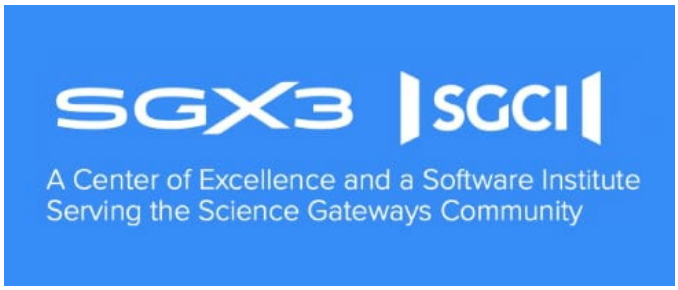
Thank you to all sponsors!

Institute for African American Mentoring in Computer Sciences (IAAMCS)



AUC Data Science Initiative

SGX3



NcyTE

Texas A&M Cybersecurity Center

Stats LLC

AI Squared

Auburn University