Institution

: Parent Section : Institution

1. Institution Name

University of Memphis

2. President of Institution

If this information is not correct, please contact organization s CAE Tool User Access Manager to update.

David Rudd
president@memphis.edu
901.678.2234

President information is not set up. If this information is not correct, please contact organization s CAE Tool User Access Manager to update.

3. Is your institution designated a minority serving institution (MSI)? If Yes Please choose from categories below:

- □ HBCU (Historically Black Colleges and Universities)
- □ PBI (Predominantly Black Institutions)
- □ HSI (Hispanic-Serving Institutions)
- □ TCU (Tribal Colleges or Universities)
- □ NASNTI (Native American Serving Non-Tribal Institutions)
- □ ANNHI (Alaskan Native or Native Hawaiian Serving Institution
- □ AANAPISI (Asian American and Native American Pacific Islander Serving Institutions)

Institution Administration

: Parent Section : Institution Administration

Annual Report Submitter Title	Annual Report Submitter First Name
Prof.	Dipankar

Annual Report Submitter Last Name

Dasgupta

Annual Report Submitter Phone

901-678-4271

Annual Report Submitter Email

ddasgupt@memphis.edu

CAE POC

If this information is not correct, please contact organization s CAE Tool User Access Manager to update.

Professor. Prof. Dipankar Dasgupta
dasgupta@memphis.edu
9016784147

CAE Alternate POC

Alternate POC information do not exist, please contact organization s CAE Tool User Access Manager to update.

Research Expertise

: Parent Section : Research Expertise

Using the Core Area List drop-down, identify your institution s current areas of expertise. List in descending order of expertise (No more than 10).

Area of Expertise - 1

" Cryptography ▾

Area of Expertise - 2

" Identification and Auther ▾

Area of Expertise - 3

" Authorization and Acces ▾

Area of Expertise - 4

" Wireless, link, and signa ▾

Area of Expertise - 5

" Software ▾

Area of Expertise - 6

" OS/DBMS/Network mec ▾

Area of Expertise - 8

" Wireless, link, and signa ▾

Area of Expertise - 9

Select Option ▾

Area of Expertise - 10

Select Option ▾

Other

1. Intelligent tutoring systems; 2. Human-computer interaction; 3. Bio-inspired computing; 4. Cybersecurity; 5. Trustworthy AI; 6. Computer science education; 7. software engineering; 8. Biomolecular and distributed computing; 9. Data science; 10. Natural language processing; 11. Machine Learning; 12. Mobile sensor big data; 13. Behavioral privacy; 14. Socio-technical systems; 15. Computer networks; 16. Network security; 17. Multimedia communication; 18. Distributed systems; 19. Artificial intelligence/intelligent systems; 20. Internet architecture; 21. Wireless sensor networks; 22. Cyber physical systems; 23. Mobile computing; 24. Data security; 25. Blockchain; 26. Adversarial machine learning; 27. Applied cryptography

Research Funding

: Parent Section : Research Funding

Research Funding

Identify any significant funding for cyber research relevant to the current core areas/sub area of expertise (see core area list): Principles; Security Mechanisms/Functionality; Architectures; Assurance; Operations; Analysis; Non-Technical IA Issues; or Other non-identified areas.

Insert text here ...

Preparing for Next Generation Cyber Defense Workforce

Grant Name *

Preparing for Next Generation Cyber Defense Workforce

Grant Number

FEMA/DHS

Grant Period of Performance

09/01/17-03/31/22

Grant Funding Amount

$331,000

Grant Description

This project developed online training course on Examining Advanced Persistent Threat (EAPT), where different attack methods are discussed along with defense strategies.

Remove

NCAEC 2021-10 Research Award

Grant Name *

NCAEC 2021-10 Research Award

Grant Number

NSA

Grant Period of Performance

08/01/21-07/31/23

Grant Funding Amount

$499,585

Grant Description

The objective of this work is to develop a trusted system to protect malicious insiders to breach sensitive information via multi-user approval system.

Remove

NCAE Cybersecurity Education for Critical Infrastructure

Grant Name *

NCAE Cybersecurity Education for Critical Infrastructure

Grant Number

NSA

Grant Period of Performance

08/20/21-12/31/24

Grant Funding Amount

$1,014,076

Grant Description

The Center for Information Assurance (CfIA) at the University of Memphis has formed a Consortium of NCAE-C institutions with the University of West Florida, North Carolina A&T State University, and The Citadel to improve critical infrastructure cybersecurity. This multi-disciplinary consortium is designed to foster cybersecurity education and

Remove

Cybersecurity Education for Critical Infrastructure Protection in Community Development through Regional Coalition

Grant Name *

Cybersecurity Education for Critical Infrastructure Protection in Community Development throu

Grant Number

A22-0041-001

Grant Period of Performance

087/2021-07/2023

Grant Funding Amount

$1999736

Grant Description

Propose to develop a comprehensive sector-specific cybersecurity program with a regional NCAE-C Coalition to better prepare for incident response and recovery in crisis. The overall project goal is to design and develop a multidisciplinary critical infrastructure cybersecurity program to address the technical needs in energy, water

Remove

CRI: CI-EN: Collaborative Research: mResearch: A Platform for Reproducible and Extensible Mobile Sensor Big Data Research

Grant Name *

CRI: CI-EN: Collaborative Research: mResearch: A Platform for Reproducible and Extensible

Grant Number

NSF

Grant Period of Performance

10/01/18-09/30/22

Grant Funding Amount

$499,512

Grant Description

The National Science Foundation (NSF) has awarded $1.75 million to the Center of Excellence for Mobile Sensor Data-to-Knowledge (MD2K) to increase the impact of its software infrastructure by enabling and accelerating research by the scientific community in sensor design, mobile computing, privacy, data analytics and

Remove

Navy ROTC Cybersecurity Training Program

Grant Name *

Navy ROTC Cybersecurity Training Program

Grant Number

A20-0206-001/N00014-

Grant Period of Performance

02/01/20-04/30/22

Grant Funding Amount

$318,459

Grant Description

The goal of this project is twofold: 1) develop research-driven, complex scenario-based, interactive, multi-level, technically rigorous exercises for cybersecurity curriculum primarily for university students with a focus on preparing them for the cybersecurity workforce 2) customize appropriate level instructional content to our local workforce

Remove

Advancing the Science of Learning Data Science with Adaptive Learning for Future Workforce Development

Grant Name *

Advancing the Science of Learning Data Science with Adaptive Learning for Future Workforce

Grant Number

NSF

Grant Period of Performance

01/15/20-12/31/24

Grant Funding Amount

$3,439,035

Grant Description

This project aims to serve the national interest by improving training in data science. Data scientists are needed to power the ongoing revolution in Big Data that is transforming virtually every sector of the economy. Progress in training data scientists is currently limited by a lack of understanding about how data science is learned and

Remove

RI:Small:Investigating Techniques that Couple Markov Logic and Deep Learning with Applications to Discovering Strategies to Improve STEM Learning

Grant Name *

RI:Small:Investigating Techniques that Couple Markov Logic and Deep Learning with Applicati

Grant Number

NSF

Grant Period of Performance

10/01/20-06/30/23

Grant Funding Amount

$413,482

Grant Description

The goal of this project is to develop novel techniques to integrate different but complementary approaches in artificial intelligence (AI). This research combines the strengths of Deep Neural Networks (DNNs) and Markov Logic Networks (MLNs) to address key shortcomings of those techniques when used by themselves. In particular,

Remove

CRI-New: Collaborative: Building the Core NDN Infrastructure to Advance Information-Centric Networking Research

Grant Name *

CRI-New: Collaborative: Building the Core NDN Infrastructure to Advance Information-Centric

Grant Number

NSF

Grant Period of Performance

09/01/16-08/31/22

Grant Funding Amount

$516,000

Grant Description

The goal of this project is to support the evaluation, experimentation, and further development of the Named Data Networking (NDN) architecture through building the core NDN infrastructure as a community resource, serving to advance research in the

Remove

Developing application-specific shared-trust framework for accessing sensitive information

Grant Name *

Developing application-specific shared-trust framework for accessing sensitive information

Grant Number

A22-0037-001

Grant Period of Performance

8/1/2021 7/31/2023

Grant Funding Amount

$500K ($251K awarded for yr 1)

Grant Description

The overall objective of this project is to develop a robust multi-faceted methodology (and protocol) in order to reduce insider threats by considering organizational structure, risk factors of sensitive data, access control mechanism, and work flow and access-log

Remove

Cybersecurity Impact Analysis for End Users Security and Privacy

Grant Name *

Cybersecurity Impact Analysis for End Users Security and Privacy

Grant Number

FEMA/DHS

Grant Period of Performance

9/1/2021-8/31/2024

Grant Funding Amount

$600K (Multi-University grant of $4M)

Grant Description

A FEMA Continuing Training Grant was awarded to the National Cybersecurity Preparedness Consortium of which the University of Memphis is a member. The grant lead is the University of Arkansas Criminal Justice Institute with the University of Memphis as a sub-awardee ($600,000). Dr. James McGinnis (Engineering Technology) and Dr. Dipankar Dasgupta (Computer Science) will lead the grant to develop new cybersecurity training. Accordingly, two web-based courses - Remote/Home-Office

Remove

Examining Advanced Persistent Threats Online Course Development

Grant Name *

Examining Advanced Persistent Threats Online Course Development

Grant Number

A18-0169-001

Grant Period of Performance

10/1/2017 3/31/2022

Grant Funding Amount

$331,000 (Multi-University grant of $2M)

Grant Description

Developed an web-based course on Examining Advanced Persistent Threats.(EAPT); this online course is designed to teach how to identify, avoid, and defend against complex cyberattacks, called Advanced Persistent Threats. This course is released at FEMA training site by leveraging the collaborative relationships among members of the

Remove

Overall objectives are to develop 2 web-based cybersecurity courses for FEMA cybersecurity training: Remote/Home-Office Cybersecurity Preparedness Training (RHC) and End-User Security and Privacy (ESP).(Co-PI)

Grant Name *

Overall objectives are to develop 2 web-based cybersecurity courses for FEMA cybersecurity t

Grant Number

NSF

Grant Period of Performance

12/01/2021-11/30/2024

Grant Funding Amount

$2,412,261

Grant Description

Overall objectives are to develop 2 web-based cybersecurity courses for FEMA cybersecurity training: Remote/Home-Office Cybersecurity Preparedness Training

Remove

Add New Grant

Outreach / Professional Development

: Parent Section : Outreach / Professional Development

1. Professional Development

Provide separate examples of professional development opportunities provided to faculty and students since your last annual report / application.

Evidence files can be fliers, posters, letters, attendance records, or other evidence of professional development for faculty and students (in PDF).

PDF

Choose Files No Files Selected

Name	Size	Action
Professional Development Assignments.pdf	256003	Delete

2. Outreach Activities

2a. Provide evidence of how the institution has shared cyber related curriculum and/or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge since your last annual report / application. Identify specific materials provided, to whom the material was provided, when and for what purpose. Any additional supporting documentation of this exchange, such as emails, formal meeting notes, links to material on accepting parties website, etc. is encouraged (in PDF).

Provide evidence of how the institution has shared cyber related curriculum and/or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge since your last annual report / application. Identify specific materials provided, to whom the material was provided, when and for what purpose. Any additional supporting documentation of this exchange, such as emails, formal meeting notes, links to material on accepting parties website, etc. is encouraged (in PDF).

Choose Files No Files Selected

Name	Size	Action
Outreach Activities_CAE-R.pdf	370801	Delete

2b. Provide evidence since your last annual report / application that the institution has participated in CAE events such as: CAE Community Symposium, CRRC workshops for applying institutions, CAE Tec Talk/Forum used in classroom, collaboration on grants with CAE institutions (in PDFs).

PDF1

Choose Files No Files Selected

Name	Size	Action
2020 CAE in Cybersecurity Symposium - Speaker.pdf	146791	Delete

PDF2

Choose Files No Files Selected

Name	Size	Action
CAETechTalk_15 April.pdf	79880	Delete

PDF3

Choose Files No Files Selected

Name	Size	Action
CAE-Forum - May 2021.pdf	76264	Delete

2c. Provide evidences since your last annual report / application that faculty members from the institution has contributed to the CAE community such as: served as PoS Validation and/or CAE-C Designation mentors, reviewers, members of the CAE Working Groups, presented in CAE Community Symposiums, CRRC workshops, CAE Tech Talk/Forum (in PDFs).

PDF1

Choose Files No Files Selected

Name	Size	Action
SE CAE Community Forum July 2021.pdf	370417	Delete

PDF2

Choose Files No Files Selected

Name	Size	Action
20210812_CAE-CoP-CD_GettingToKnowYourFellowCAEs (1).pdf	231109	Delete

PDF3

Choose Files No Files Selected

Name	Size	Action
2020_1104 - CAE Forum_TechTalk.pdf	107185	Delete

2d. Provide evidence since your last annual report / application of faculty members collaborating with current CAE-C institutions on research, grants, course development, etc. (in PDF).

Choose Files No Files Selected

Name	Size	Action
CfIA Press Release- 26 August 2021 NCAEC.pdf	56958	Delete

2e. Provide evidence since your last annual report / application of faculty members/employee sponsorship or oversight of students for Cyber events for the community at large. Events could include Cyber awareness and education for local schools, adult education centers, senior centers, camps, first responder training and the surrounding community (in PDF).

Choose Files   No Files Selected

Name	Size	Action
cyber-ambassador-2021-summary-report.pdf	142821	Delete

2f. Provide evidence since your last annual report / application on how the institution works with employers and students to support placement for cyber related internships and jobs, such as via institutional Career Development Services (i.e. HandShake) and industry events on-campus (in PDF).

Choose Files   No Files Selected

Name	Size	Action
Raymond James_UofM partnership.pdf	280404	Delete

2g. Provide evidence since your last annual report / application of obtaining input on curriculum to meet industry needs (in PDF).

Choose Files   No Files Selected

Name	Size	Action
IABMeeting191122.pdf	103506	Delete

Institution Reflective of the CAE Designation or POS Validation

: Parent Section : Institution Reflective of the CAE Designation or POS Validation

Institution Successes & Achievements

Since the institution s last designation application - Describe activities that represent successes and achievements of the program(s) reflective of the CAE designation / POS Validation such as scholarships, outreach, partnerships, awards, conference participation, etc.

===>>>Awards/Activities Dr. Lan Wang Publication Chair: ACM Conference on Information-Centric Networking, 2020 Steering Committee Member: International Conference on Hot Information-Centric Networking (HotICN), 2020 Program Committee: IEEE International Conference on Sensing, Communication and Networking (SECON), 2021 Dr. Dipankar Dasgupta Dr. Dasgupta became a member of IEEE CIS Neural Networks Technical Committee Task Force on Secure Learning. A Patent (#10,671,747)/by Dr. Dasgupta on multi-user permission strategy to access sensitive information approved by USPTO on June 2, 2020. For details/click here. Dr. Dasgupta received summer Grant on June 1,/2020/from Idaho National Lab to conduct research on 5G Technology Security. Dr. Dasgupta received Cybersecurity Training Grant (as Co-PI) on June 1, 2020. For details:/New Cybersecurity Training Grant. Dr. Dipankar Dasgupta gave an invited talk at INNOVATE IT 2020 Conference hosted by Greater Memphis IT Council on October 8th. Event Agenda at/http://www.memphisitcouncil.com/uploads/1/2/8/1/128111718/greater_memphis_it_council_innovate_it_it-_program_agenda_-10-8-20_-_revised.pdf. As the top Innovation in Entrepreneurship award, Dr. Dasgupta s Adaptive Multi-Factor Authentication was ranked #1 by the virtual attendees of the event. Dr. Dasgupta is organizing a symposium on Computational Intelligence in Cyber Security (CICS) at the IEEE Symposium Series on Computational Intelligence (SSCI) at/Canbara, Australia (Virtual) on Dec 1 - 4, 2020. Dr. Dasgupta gave an invited talk at the Greater Memphis IT Council (GMITC) Cyber Security Roundtable quarterly meeting of 25 CISOs on July 21, 2020. Dr. Dasgupta gave a presentation at IEEE World Congress on Computational Intelligence (WCCI) entitled AI is not Magic it is Computational Logic on July 21, 2020. The presentation is available from YouTube. Dr. Dasgupta has recently been featured in news "How vulnerable are home Wi-Fi routers to cyber hackers?" on FOX13 Memphis, TN. Published on February 20, 2020. Dr. Kan Yang 2021.08 Kan was invited to serve as a TPC member in the 2021 IEEE International Conference on Blockchain (Blockchain 2021). 2021.07 Kan was invited to serve as a TPC member in the 2021 IEEE International Conference on Communications: Communication and Information Systems Security Symposium (IEEE ICC’21 - CISS). 2021.03 Kan was invited to serve as a TPC member in IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS’21). 2021.03 Kan was invited to serve as a TPC member in IEEE International Performance Computing and Communications Conference (IPCCC’21). 2020.09 Kan was interviewed by Local 24 News on the security and privacy issues on iOS/Android newly released features on COVID-19 contact tracing 2020.05 Kan was invited to serve as a TPC member in the 2020 IEEE Global Communications Conference: Communication and Information Systems Security (IEEE Globecom’20 - CISS). 2020.05 Kan was invited to serve as a TPC member in the 17th IEEE International Conference on Mobile Ad hoc and Smart Systems (IEEE MASS’20). 2020.03 Kan was invited to serve as a TPC member in the 2020 IEEE International Conference on Blockchain (Blockchain 2020). ===>>>Publications (Journals/Conferences) Dr. Bonny Banerjee Kapourchali, Masoumeh Heidari, and Bonny Banerjee. "Learning Communication Policies for Knowledge Transfer between Agents." In/CogSci. 2020. Dr. Brian Janz Totty, Stephanie, He Li, Brian Janz, and Chen Zhang. "Themes in Information Security Research in the Information Systems Discipline: A Topic Modeling Approach." (2020). Dr. Chen Zhang Totty, Stephanie, He Li, Brian Janz, and Chen Zhang. "Themes in Information Security Research in the Information Systems Discipline: A Topic Modeling Approach." (2020). Dr. Dipankar Dasgupta Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Adversarial Input Detection Using Image Processing Techniques (IPT)." In/2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0309-0315. IEEE, 2020. Poudyal, Subash, and Dipankar Dasgupta. "AI-Powered Ransomware Detection Framework." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1154-1161. IEEE, 2020. Sen, Sajib, Dipankar Dasgupta, and Kishor Datta Gupta. "An empirical study on algorithmic bias." In/2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1189-1194. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Applicability issues of evasion-based adversarial attacks and mitigation techniques." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1506-1515. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Determining sequence of image processing technique (ipt) to detect adversarial attacks."/SN Computer Science/2, no. 5 (2021): 1-20. Reddy, Bheemidi Vikram, Gutha Jaya Krishna, Vadlamani Ravi, and Dipankar Dasgupta. "Machine Learning and Feature Selection Based Ransomware Detection Using Hexacodes." In/Evolution in Computational Intelligence, pp. 583-597. Springer, Singapore, 2021. Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey."/The Journal of Defense Modeling and Simulation/(2020): 1548512920951275. Gupta, Kishor Datta, Md Lutfar Rahman, Dipankar Dasgupta, and Subash Poudyal. "Shamir's Secret Sharing for Authentication without Reconstructing Password." In/2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0958-0963. IEEE, 2020. Akhtar, Zahid, Murshida Rahman Mouree, and Dipankar Dasgupta. "Utility of Deep Learning Features for Facial Attributes Manipulation Detection." In/2020 IEEE International Conference on Humanized Computing and Communication with Artificial Intelligence (HCCAI), pp. 55-60. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Adversarial Input Detection Using Image Processing Techniques (IPT)." In/2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0309-0315. IEEE, 2020. Sen, Sajib, Dipankar Dasgupta, and Kishor Datta Gupta. "An empirical study on algorithmic bias." In/2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1189-1194. IEEE, 2020. Poudyal, Subash, and Dipankar Dasgupta. "Analysis of Crypto-Ransomware Using ML-Based Multi-Level Profiling."/IEEE Access/9 (2021): 122532-122547. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Applicability issues of evasion-based adversarial attacks and mitigation techniques." In/2020 IEEE Symposium Series on Computational

Intelligence (SSCI), pp. 1506-1515. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Determining sequence of image processing technique (ipt) to detect adversarial attacks."/SN Computer Science/2, no. 5 (2021): 1-20. Reddy, Bheemidi Vikram, Gutha Jaya Krishna, Vadlamani Ravi, and Dipankar Dasgupta. "Machine Learning and Feature Selection Based Ransomware Detection Using Hexacodes." In/Evolution in Computational Intelligence, pp. 583-597. Springer, Singapore, 2021. Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey."/The Journal of Defense Modeling and Simulation/(2020): 1548512920951275. Dasgupta, Dipankar, Arunava Roy, and Debasis Ghosh. "Multi-user permission strategy to access sensitive information." U.S. Patent 10,671,747, issued June 2, 2020. Datta Gupta, Kishor, and Dipankar Dasgupta. "Negative Selection Algorithm Research and Applications in the last decade: A Review."/arXiv e-prints/(2021): arXiv-2105. Basnet, Manoj, Subash Poudyal, Mohd Ali, and Dipankar Dasgupta. "Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station."/arXiv preprint arXiv:2104.07409/(2021). Gupta, Kishor Datta, Md Lutfar Rahman, Dipankar Dasgupta, and Subash Poudyal. "Shamir’s Secret Sharing for Authentication without Reconstructing Password." In/2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0958-0963. IEEE, 2020. Nguyen, Christopher, Walt Williams, Brandon Didlake, Donte Mitchell, James McGinnis, and Dipankar Dasgupta. "Social Engineering Attacks in Healthcare Systems: A Survey." In/National Cyber Summit, pp. 141-150. Springer, Cham, 2021. Akhtar, Zahid, Murshida Rahman Mouree, and Dipankar Dasgupta. "Utility of Deep Learning Features for Facial Attributes Manipulation Detection." In/2020 IEEE International Conference on Humanized Computing and Communication with Artificial Intelligence (HCCAI), pp. 55-60. IEEE, 2020. Basnet, Manoj, Subash Poudyal, Mohd Ali, and Dipankar Dasgupta. "Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station."/arXiv preprint arXiv:2104.07409/(2021). Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Adversarial Input Detection Using Image Processing Techniques (IPT)." In/2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0309-0315. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Applicability issues of evasion-based adversarial attacks and mitigation techniques." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1506-1515. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Determining sequence of image processing technique (ipt) to detect adversarial attacks."/SN Computer Science/2, no. 5 (2021): 1-20. Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey."/The Journal of Defense Modeling and Simulation/(2020): 1548512920951275. Akhtar, Zahid, Murshida Rahman Mouree, and Dipankar Dasgupta. "Utility of Deep Learning Features for Facial Attributes Manipulation Detection." In/2020 IEEE International Conference on Humanized Computing and Communication with Artificial Intelligence (HCCAI), pp. 55-60. IEEE, 2020. Abderrahmane, Herbadji, Guermat Noubeil, Ziet Lahcene, Zahid Akhtar, and Dipankar Dasgupta. "Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems."/IET Biometrics/9, no. 3 (2020): 91-99. Abderrahmane, Herbadji, Guermat Noubeil, Ziet Lahcene, Zahid Akhtar, and Dipankar Dasgupta. "Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems."/IET Biometrics/9, no. 3 (2020): 91-99. Dr. Christos/Papadopoulos Gharaibeh, Manaf, Christos Papadopoulos, John Heidemann, and Craig Partridge. "Delay-based Identification of Internet Block Movement." (2020). Fan, Chengyu, Susmit Shannigrahi, Christos Papadopoulos, and Craig Partridge. "Discovering in-network caching policies in ndn networks from a measurement perspective." In/Proceedings of the 7th ACM Conference on Information-Centric Networking, pp. 106-116. 2020. Fan, Chengyu, Susmit Shannigrahi, Christos Papadopoulos, and Craig Partridge. "Discovering in-network caching policies in ndn networks from a measurement perspective." In/Proceedings of the 7th ACM Conference on Information-Centric Networking, pp. 106-116. 2020. Dr. Deepak Venugopal Mahfouz, Ahmed M., Abdullah Abuhussein, Deepak Venugopal, and Sajjan G. Shiva. "Network Intrusion Detection Model Using One-Class Support Vector Machine." In/Advances in Machine Learning and Computational Intelligence, pp. 79-86. Springer, Singapore, 2021. Mahfouz, Ahmed, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. "Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset."/Future Internet/12, no. 11 (2020): 180. Das, Saikat, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. "Empirical evaluation of the ensemble framework for feature selection in ddos attack." In/2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 56-61. IEEE, 2020. Das, Saikat, Deepak Venugopal, and Sajjan Shiva. "A holistic approach for detecting ddos attacks by using ensemble unsupervised machine learning." In/Future of Information and Communication Conference, pp. 721-738. Springer, Cham, 2020. Mahfouz, Ahmed M., Deepak Venugopal, and Sajjan G. Shiva. "Comparative analysis of ML classifiers for network intrusion detection." In/Fourth international congress on information and communication technology, pp. 193-207. Springer, Singapore, 2020. Mahfouz, Ahmed M., Deepak Venugopal, and Sajjan G. Shiva. "Comparative analysis of ML classifiers for network intrusion detection." In/Fourth international congress on information and communication technology, pp. 193-207. Springer, Singapore, 2020. Das, Saikat, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. "Empirical evaluation of the ensemble framework for feature selection in ddos attack." In/2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 56-61. IEEE, 2020. Mahfouz, Ahmed, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. "Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset."/Future Internet/12, no. 11 (2020): 180. Mahfouz, Ahmed M., Abdullah Abuhussein, Deepak Venugopal, and Sajjan G. Shiva. "Network Intrusion Detection Model Using One-Class Support Vector Machine."

In/Advances in Machine Learning and Computational Intelligence, pp. 79-86. Springer, Singapore, 2021. Mahfouz, Ahmed M., Deepak Venugopal, and Sajjan G. Shiva. "Comparative analysis of ML classifiers for network intrusion detection." In/Fourth international congress on information and communication technology, pp. 193-207. Springer, Singapore, 2020. Das, Saikat, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. "Empirical evaluation of the ensemble framework for feature selection in ddos attack." In/2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 56-61. IEEE, 2020. Mahfouz, Ahmed, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. "Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset."/Future Internet/12, no. 11 (2020): 180. Das, Saikat, Namita Agarwal, Deepak Venugopal, Frederick T. Sheldon, and Sajjan Shiva. "Taxonomy and Survey of Interpretable Machine Learning Method." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 670-677. IEEE, 2020. Dr. Hasan Ali Basnet, Manoj, Subash Poudyal, Mohd Ali, and Dipankar Dasgupta. "Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station."/arXiv preprint arXiv:2104.07409/(2021). Alam, SM Mahfuz, and Mohd Hasan Ali. "A New Fuzzy Logic Based Method For Residential Loads Forecasting." In/2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pp. 1-5. IEEE, 2020. Basnet, Manoj, and Mohd Hasan Ali. "Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station." In/2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES), pp. 408-413. IEEE, 2020. Keshavarzi, Morteza Daviran, and Mohd Hasan Ali. "Disturbance Resilience Enhancement of Islanded Hybrid Microgrid Under High Penetration of Renewable Energy Resources by BESS." In/2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pp. 1-5. IEEE, 2020. Basnet, Manoj, and M. Hasan Ali. "Exploring Cybersecurity Issues in 5G Enabled Electric Vehicle Charging Station with Deep Learning."/arXiv preprint arXiv:2104.08553/(2021). Basnet, Manoj, Subash Poudyal, Mohd Ali, and Dipankar Dasgupta. "Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station."/arXiv preprint arXiv:2104.07409/(2021). Dr. Huigang Liang Bu, Fei, Nengmin Wang, Bin Jiang, and Huigang Liang. " Privacy by Design implementation: Information system engineers perspective."/International Journal of Information Management/53 (2020): 102124. Liu, Chenhui, Huigang Liang, Nengmin Wang, and Yajiong Xue. "Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender."/Information Technology & People/(2021). Liu, Chenhui, Nengmin Wang, and Huigang Liang. "Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment."/International Journal of Information Management/54 (2020): 102152.5 Dr. Kan Yang L. Yan,/K. Yang, S. Yang and Z. Han, "A Trust-aware Fog Offloading Game with Long-term Trustworthiness of Users". To appear on/Proc. of 2021 IEEE Global Communications Conference (Globecom'21), Madrid, Spain, 7-11 December 2021. Zhao, Bin, Kai Fan, Wei You, Kan Yang, Zilong Wang, and Hui Li. "A Weight-based k-prototypes Algorithm for Anomaly Detection in Smart Grid." In/ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020. Zhao, Bin, Kai Fan, Kan Yang, Zilong Wang, Hui Li, and Yintang Yang. "Anonymous and Privacy-preserving Federated Learning with Industrial Big Data."/IEEE Transactions on Industrial Informatics/(2021). Yang, Anjia, Jian Weng, Kan Yang, Cheng Huang, and Xuemin Shen. "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks."/IEEE Transactions on Intelligent Transportation Systems/(2020). Yang, Hanzhe, Ruidan Su, Pei Huang, Yuhan Bai, Kai Fan, Kan Yang, Hui Li, and Yintang Yang. "PMAB: A Public Mutual Audit Blockchain for Outsourced Data in Cloud Storage."/Security and Communication Networks/2021 (2021). Zhang, Yuan, Chunxiang Xu, Hongwei Li, Kan Yang, Nan Cheng, and Xuemin Shen. "PROTECT: efficient password-based threshold single-sign-on authentication for mobile users against perpetual leakage."/IEEE Transactions on Mobile Computing/20, no. 6 (2020): 2297-2312. Yan, Lei, Kan Yang, and Shouyi Yang. "Reputation-based Truth Discovery with Long-term Quality of Source in Internet of Things."/IEEE Internet of Things Journal/(2021). Yang, Kan, and Senjuti Dutta. "Secure and Efficient Task Matching with Multi-keyword in Multi-requester and Multi-worker Crowdsourcing." In/2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS), pp. 1-6. IEEE, 2021. Xu, Guowen, Hongwei Li, Hao Ren, Jianfei Sun, Shengmin Xu, Jianting Ning, Haomiao Yang, Kan Yang, and Robert H. Deng. "Secure and Verifiable Inference in Deep Neural Networks." In/Annual Computer Security Applications Conference, pp. 784-797. 2020. Dr. Md Yeasin Alam, Shahinur, Md Sultan Mahmud, and Mohammed Yeasin. "SafeNet: An Assistive Solution to Assess Incoming Threats for Premises."/arXiv preprint arXiv:2002.04405/(2020). Alam, Shahinur, Md Sultan Mahmud, and Mohammed Yeasin. "Toward Building Safer Smart Homes for the People with Disabilities."/arXiv preprint arXiv:2006.05907/(2020). Dr. Mohammad S. Najjar Najjar, Mohammad S., Laila Dahabiyeh, and Raed Salah Algharabat. "Users' affect and satisfaction in a privacy calculus context."/Online Information Review/(2021). Dr. Myounggyu Won Won, Myounggyu, Wei Zhang, Chien-An Chen, and Radu Stoleru. "GROLL: Geographic Routing for Low Power and Lossy IoT Networks."/Internet of Things/9 (2020): 100152. Dr. Sajjan Shiva Mahfouz, Ahmed M., Abdullah Abuhussein, Deepak Venugopal, and Sajjan G. Shiva. "Network Intrusion Detection Model Using One-Class Support Vector Machine." In/Advances in Machine Learning and Computational Intelligence, pp. 79-86. Springer, Singapore, 2021. Mahfouz, Ahmed, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. "Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset."/Future Internet/12, no. 11 (2020): 180. Das, Saikat, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. "Empirical evaluation of the ensemble framework for feature selection in ddos attack." In/2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 56-61. IEEE, 2020. Das, Saikat, Deepak Venugopal, and Sajjan Shiva. "A holistic approach for detecting ddos attacks by using ensemble unsupervised machine learning." In/Future of Information and Communication Conference, pp. 721-738. Springer, Cham, 2020. Mahfouz, Ahmed M., Deepak Venugopal, and Sajjan G. Shiva. "Comparative analysis of ML classifiers for network intrusion detection." In/Fourth international congress on information and communication technology, pp. 193-207. Springer, Singapore, 2020. Al-Rousan, Suhaib, Abdullah Abuhussein, Faisal Alsubaei, Lynn Collen, and Sajjan Shiva. "Ads-Guard: Detecting Scammers in Online Classified Ads." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1492-1498. IEEE, 2020. Mahfouz, Ahmed M., Deepak Venugopal, and Sajjan G. Shiva. "Comparative analysis of ML classifiers for network intrusion detection." In/Fourth international congress on information and communication technology, pp. 193-207. Springer, Singapore, 2020. Ashrafuzzaman, Mohammad, Saikat Das, Yacine Chakhchoukh, Sajjan Shiva, and Frederick T. Sheldon. "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning."/Computers & Security/97 (2020): 101994. Das, Saikat, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. "Empirical evaluation of the ensemble framework for feature selection in ddos attack." In/2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 56-61. IEEE, 2020. Mahfouz, Ahmed, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. "Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset."/Future Internet/12, no. 11 (2020): 180. Mahfouz, Ahmed M., Abdullah Abuhussein, Deepak Venugopal, and Sajjan G. Shiva. "Network Intrusion Detection Model Using One-Class Support Vector Machine." In/Advances in Machine Learning and Computational Intelligence, pp. 79-86. Springer, Singapore, 2021. Das, Saikat, Mohammad Ashrafuzzaman, Frederick T. Sheldon, and Sajjan Shiva. "Network Intrusion Detection using Natural Language Processing and Ensemble Machine Learning." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 829-835. IEEE, 2020. Putta, Swapnika Reddy, Abdullah Abuhussein, Faisal Alsubaei, Sajjan Shiva, and Saleh Atiewi. "Security benchmarks for wearable medical things: stakeholders-centric approach." In/Fourth International Congress on Information and Communication Technology, pp. 405-418. Springer, Singapore, 2020. Al-Rousan, Suhaib, Abdullah Abuhussein, Faisal Alsubaei, Ozkan Kahveci, Hazem Farra, and Sajjan Shiva. "Social-Guard: Detecting Scammers in Online Dating." In/2020 IEEE International Conference on Electro Information Technology (EIT), pp. 416-422. IEEE, 2020. Ashrafuzzaman, Mohammad, Saikat Das, Yacine Chakhchoukh, Salahaldeen Duraibi, Sajjan Shiva, and Frederick T. Sheldon. "Supervised Learning for Detecting Stealthy False Data Injection Attacks in the Smart Grid." In/Advances in Security, Networks, and Internet of Things, pp. 291-305. Springer, Cham, 2021. Mahfouz, Ahmed M., Deepak Venugopal, and Sajjan G. Shiva. "Comparative analysis of ML classifiers for network intrusion detection." In/Fourth international congress on information and communication technology, pp. 193-207. Springer, Singapore, 2020. Ashrafuzzaman, Mohammad, Saikat Das, Yacine Chakhchoukh, Sajjan Shiva, and Frederick T. Sheldon. "Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning."/Computers & Security/97 (2020): 101994. Das, Saikat, Deepak Venugopal, Sajjan Shiva, and Frederick T. Sheldon. "Empirical evaluation of the ensemble framework for feature selection in ddos attack." In/2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 56-61. IEEE, 2020. Mahfouz, Ahmed, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. "Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset."/Future Internet/12, no. 11 (2020): 180. Putta, Swapnika Reddy, Abdullah Abuhussein, Faisal Alsubaei, Sajjan Shiva, and Saleh Atiewi. "Security benchmarks for wearable medical things: stakeholders-centric approach." In/Fourth International Congress on Information and Communication Technology, pp. 405-418. Springer, Singapore, 2020. Al-Rousan, Suhaib, Abdullah Abuhussein, Faisal Alsubaei, Ozkan Kahveci, Hazem Farra, and Sajjan Shiva. "Social-Guard: Detecting Scammers in Online Dating." In/2020 IEEE International Conference on Electro Information Technology (EIT), pp. 416-422. IEEE, 2020. Das, Saikat, Namita Agarwal, Deepak Venugopal, Frederick T. Sheldon, and Sajjan Shiva. "Taxonomy and Survey of Interpretable Machine Learning Method." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 670-677. IEEE, 2020. Abuhussein, Abdullah, Faisal Alsubaei, and Sajjan Shiva. "Toward an effective requirement engineering approach for cloud applications." In/Software Engineering in the Era of Cloud Computing, pp. 29-50. Springer, Cham, 2020. Dr. Zahid Akhtar Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Adversarial Input Detection Using Image Processing Techniques (IPT)." In/2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0309-0315. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Applicability issues of evasion-based adversarial attacks and mitigation techniques." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1506-1515. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Determining sequence of image processing technique (ipt) to detect adversarial attacks."/SN Computer Science/2, no. 5 (2021): 1-20. Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey."/The Journal of Defense Modeling and Simulation/(2020): 1548512920951275. Akhtar, Zahid, Murshida Rahman Mouree, and Dipankar Dasgupta. "Utility of Deep Learning Features for Facial Attributes Manipulation Detection." In/2020 IEEE International Conference on Humanized Computing and Communication with Artificial Intelligence (HCCAI), pp. 55-60. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Adversarial Input Detection Using Image Processing Techniques (IPT)." In/2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0309-0315. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Applicability issues of evasion-based adversarial attacks and mitigation techniques." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1506-1515. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Determining sequence of image processing technique (ipt) to detect adversarial attacks."/SN Computer Science/2, no. 5 (2021): 1-20. Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey."/The Journal of Defense Modeling and Simulation/(2020): 1548512920951275. Akhtar, Zahid, Murshida Rahman Mouree, and Dipankar Dasgupta. "Utility of Deep Learning Features for Facial Attributes Manipulation Detection." In/2020 IEEE International Conference on Humanized Computing and Communication with Artificial Intelligence (HCCAI), pp. 55-60. IEEE, 2020. Chaa, Mourad, and Zahid Akhtar. "3D Palmprint recognition using Tan and Triggs normalization technique and GIST descriptors."/Multimedia Tools and Applications/80, no. 2 (2021): 2263-2277. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Adversarial Input Detection Using Image Processing Techniques (IPT)." In/2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0309-0315. IEEE, 2020. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Applicability issues of evasion-based adversarial attacks and mitigation techniques." In/2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1506-1515. IEEE, 2020. Herbadji, Abderrahmane, Zahid Akhtar, Kamran Siddique, Noubeil Guermat, Lahcene Ziet, Mohamed Cheniti, and Khan Muhammad. "Combining multiple biometric traits using asymmetric aggregation operators for improved person recognition."/Symmetry/12, no. 3 (2020): 444. Attia, Abdelouahab, Zahid Akhtar, Nour Elhouda Chalabi, Sofiane Maza, and Youssef Chahir. "Deep rule-based classifier for finger knuckle pattern recognition system."/Evolving Systems/(2020): 1-15. Gupta, Kishor Datta, Dipankar Dasgupta, and Zahid Akhtar. "Determining sequence of image processing technique (ipt) to detect adversarial attacks."/SN Computer Science/2, no. 5 (2021): 1-20. Attia, Abdelouahab, Zahid Akhtar, and Youssef Chahir. "Feature-level fusion of major and minor dorsal finger knuckle patterns for person authentication."/Signal, Image and Video Processing/15, no. 4 (2021): 851-859. Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey."/The Journal of Defense Modeling and Simulation/(2020): 1548512920951275. Akhtar, Zahid, Murshida Rahman Mouree, and Dipankar Dasgupta. "Utility of Deep Learning Features for Facial Attributes Manipulation Detection." In/2020 IEEE International Conference on Humanized Computing and Communication with Artificial Intelligence (HCCAI), pp. 55-60. IEEE, 2020. Abderrahmane, Herbadji, Guermat Noubeil, Ziet Lahcene, Zahid Akhtar, and Dipankar Dasgupta. "Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems."/IET Biometrics/9, no. 3 (2020): 91-99. Li, Yifan, Yuchun Fang, and Zahid Akhtar. "Accelerating deep reinforcement learning model for game strategy."/Neurocomputing/408 (2020): 157-168. Sadou, Besma, Atidel Lahoulou, Toufik Bouden, Anderson R. Avila, Tiago H. Falk, and Zahid Akhtar. "FREE-REFERENCE IMAGE QUALITY ASSESSMENT FRAMEWORK USING METRICS FUSION AND DIMENSIONALITY REDUCTION." Sajjad, Muhammad, Sana Zahir, Amin Ullah, Zahid Akhtar, and Khan Muhammad. "Human behavior understanding in big multimedia data using CNN based facial expression recognition."/Mobile networks and applications/25, no. 4 (2020): 1611-1621. Akhtar, Zahid, and Attaullah Buriro. "Multitrait Selfie: Low-Cost Multimodal Smartphone User Authentication." In/Biometric Identification Technologies Based on Modern Data Mining Methods, pp. 159-175. Springer, Cham, 2021. Abderrahmane, Herbadji, Guermat Noubeil, Ziet Lahcene, Zahid Akhtar, and Dipankar Dasgupta. "Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems."/IET Biometrics/9, no. 3 (2020): 91-99. ===>>>Student Dissertations Alsubaei, Faisal S. "Security Assessment Framework for the Internet of Medical Things Solutions." Order No. 27964282, The University of Memphis, 2020. Poudyal, Subash. "Multi-Level Analysis of Malware using Machine Learning." Order No. 28645891, The University of Memphis, 2021. Solatikia, Farnaz. "Design a System of Secure Random Number Generators by Random Coupling with the Future." Order No. 28646047, The University of Memphis, 2021. Gupta, Kishor Datta. "Robust Filtering Schemes for Machine Learning Systems to Defend Adversarial Attack." Order No. 28650214, The University of Memphis, 2021. ===>>>Student Theses Enabling Efficient and Privacy-Preserving Task Matching For Cloud-Based Crowdsourcing, Senjuti Dutta, University of Memphis (2020) L. Fan and L. Wang, "Secure Sharing of Spatio-Temporal Data through Name-based Access Control,"/IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2021, pp. 1-7, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484557. Dulal, Saurab, "NDNSD: Service Publishing and Discovery in NDN" (2020)./Electronic Theses and Dissertations. 2140. Shorna, Sabira Khanam, "Performance Analysis of 5G DDoS Attack Using Machine Learning" (2021). Electronic Theses and Dissertations. 2201. Solatikia, Farnaz, "DESIGN A SYSTEM OF SECURE RANDOM NUMBER GENERATORS BY RANDOM COUPLING WITH THE FUTURE" (2021)./Electronic Theses and Dissertations. 2316. Hossain, Mazharul, "Instance Segmentation of Public Safety Objects in RGB Image from Indoor Scene to Build Rich Interior Hazard Maps" (2021). Electronic Theses and Dissertations. 2200. Gupta, Kishor Datta, "Robust filtering schemes for machine learning systems to defend Adversarial Attacks" (2021). Electronic Theses and Dissertations. 2203. Ryan Patrcik Wickman. "LRN: Limitless Routing Networks for Effective Multi-task Learning." In/Submitted to The Tenth International Conference on Learning Representations/.2022.

Designation Return on Investment

Identify any opportunities, successes and/or achievements, grants specifically resulting from the institution s designation as a CAE.

1. Developing application-specific shared-trust framework for accessing sensitive information, DoD/NSA, $500K ($251K awarded for yr 1), 8/1/2021 7/31/2023. 2. Multidisciplinary cybersecurity program for Critical Infrastructure Protection, DoD/NSA, $2M (Multi-University), 8/20/2021 12/31/2023. 3. Cybersecurity Impact Analysis for End Users Security and Privacy (Co-PI), FEMA/DHS, $600K (Multi-University grant of $4M), 9/1/2021-8/31/2024. 4. Examining Advanced Persistent Threats (APTs), FEMA/DHS, $331,000 (Multi-University grant of $2M), 10/1/2017 3/31/2022. 5. Navy ROTC Cybersecurity Training Program, DoD, $318K, 5/1/2020-4/30/2022. 6. Cyber Security Workforce Development, NSA, $206,085, 09/01/2017-8/31/2019. 7. Scholarship for Services (SFS) (Co-PI), NSF, $2.9M, 12/01/2021 -11/30/2024.

CAE Community Contributions

Check all that apply to the institution s specific contributions to the CAE Community:

☑ Attendance at CAE Community Meetings
□ CAE Mentor / Reviewer
☑ Participation in CAE Working Groups (name working group)
□ CAE Research Collaborations (state collaboration information)
☑ CAE Forum / Tech Talk contributor (date presented / topic)
□ CAE Regional Hub (CRH) or CAE National Resource Center (CNRC)
□ Participation in KU development and refinement
□ Other (provide contribution information)

Additional Information

Institution may use this section to provide any additional information not previously mentioned in this report pertinent to the CAE program.

President of Institution: Dr. David Rudd CAE Alternate POC: Dr. James A. McGinnis (jmcgnnis@memphis.edu) CAE Working Group: SE NCAE-C K12 Pipeline Working Group SE CAE Community Forum: July 16, 2021 (Guest Speaker - Dr. Dipankar Dasgupta) CAE CoP Cyber Defense: August 12, 2021 (Dr. Dipankar Dasgupta - University of Memphis)