Mahmoud Nabil Mahmoud

Personal Data

Name:	Mahmoud Nabil Mahmoud
Address:	1601 E. Market Street, 219 The Martin Complex, Greensboro, NC, 27411
Cell:	+1 (931) 252-8058
Email:	mnmahmoud@ncat.edu
Skype:	mah.nabil
Website:	https://mahmoudnabil.github.io
Scholar:	https://scholar.google.com/
Publons:	https://publons.com/researcher/3021906/mahmoud-nabil/

Education

Aug. 2019 PhD
Department of Electrical & Computer Engineering, Tennessee Technological University, TN, USA.
Thesis: "Electricity Theft Detection with Privacy Preservation for Smart Grid AMI Networks Using Machine Learning".
GPA: 4.0/4.0

Jun. 2016 MSc in Electrical Engineering, Cairo University, Egypt.
Thesis: "Sentiment Analysis and Keyphrases Extraction for Arabic Language".
GPA: 3.7/4.0.

Jul 2012 BSc in Computer Engineering, Cairo University, Egypt.
Grade: 91.59% equivalent to 3.94/4.0 GPA - Distinction with honor degree.

Professional Experience

Aug. 2024 - Present **Associate Professor (Tenured)**, North Carolina A&T, Greensboro, NC, USA.
Role: Teaching graduate and undergraduate courses, conducting research, advising students, and actively participating in department services.

Jun. 2023 - Aug. 2023 **Summer Visiting Faculty**, Fermi National Accelerator Laboratory (FNAL), Batavia, IL, USA.
Role: Participated in the Department of Energy's (DOE) Visiting Faculty Program, conducting research and collaborating with FNAL scientists.

Aug. 2019 - 2024 **Assistant Professor**, North Carolina A&T, Greensboro, NC, USA.
Role: Teaching graduate and undergraduate courses, advising students, and actively doing department services.

Jan. 2017 - Aug. 2019 **Research Assistant**, Tennessee Technological University, Cookeville, TN, USA.
Role: Working on different projects including privacy preserving ride sharing, dynamic charging systems, data aggregation in smart grid, keyword search over encrypted data, intrusion detection systems for AMI networks.

Jun. 2016 - Dec. 2016 **Lecturer Assistant**, Faculy of Engineering, Cairo University, Cairo, Egypt.
Courses Assisted in: Data structure and Algorithms, Algorithms Labs, Artificial Intelligence, Computer Networks.

Sep. 2012 - Jun. 2016 **Teaching Assistant**, Faculy of Engineering, Cairo University.
Courses Assisted in: Data structure and Algorithms, Computer Architecture, Fundamentals of Multimedia, Microprocessor I, Microprocessor II, Pattern Recognition, Natural Language Processing, Computer Vision, Digital systems, VHDL labs, Image processing labs, Algorithms labs, Artificial Intelligence, Computer Networks.

Mar. 2014 - Jun. 2016	**Research Assistant**, in ITIDA's ITAC project number CFP-65 , Cairo, Egypt **Role**: Builiding tools to collect Arabic social dataset from Twitter, analyzing the data, and developing machine learning algorithms to classify the sentiment of the tweets.
Mar. 2013 - Mar. 2014	**Software Developer**, Military main software development center (MSDC), Cairo, Egypt **Role**: Implementing and maintaining web applications using C# and Microsoft SQL server.
Jun. 2011 - Aug. 2011	**Intern**, in Giza System , Cairo, Egypt **Role**: Administrating Linux based operating system (Redhat & Solaris).

Research Interests

I lead the **Wi**reless and **Se**curity **Net**working (Wise-Net) Research group at N.C. A&T. My group studies the networking, security, and privacy aspects of Cyber-Physical Systems (CPS) and the Internet of Things in general (IoT). Our research draws on theoretical tools from communication, cryptography, game theory, optimization, and machine learning, as well as practical simulation, and prototype creation techniques. Specific interests are: smart grid AMI networks, machine learning for cybersecurity, adversarial machine learning, encrypted machine learning, blockchain applications, self-driven vehicle applications, electric vehicle communications, vehicular ad hoc networks, wireless sensor networks, trust and reputation systems, and location privacy-preserving schemes.

Funding Support

17 grants | Total amount: $16M+

1. **Source:** Department of Energy **Title:** Platform for Secure and Resilient Electric Power System for Research Testing and Demonstration (P4REST), **My role: Co-PI** Amt: $2.5M, year: 2024
2. **Source:** Department of Navy **Title:** Empowering Naval Cyberdefence through a Methodological Assessment of SOC Solutions – **My Role: Co-PI** - **Lead PI:** Ahmad Patoogy , Amt: $450,000, year: 2024
3. **Source:** NCAT-Internal **Title:** Securing Smart Grids Deep Learning Decision Making Models Against Adversarial Perturbations of Time Series Data – **My Role: Lead-PI** , Amt: $25,000, year: 2024
4. **Source:** Central Intelligence Agency **Title:** Towards Efficient and Secure Federated Learning over Heterogeneous Non-Terrestrial Networks, **My role: Lead-PI** Amt: $100k, year: 2023
5. **Source:** DoT **Title:** Center for Automated Vehicle Research with Multimodal Assured Navigation (CARMEN+) – **Lead PI:** Zak Kassas, , **My role Co-PI:** Amt: $1.5M, year: 2023
6. **Source:** NSF **Title:** Excellence in Research: Towards Secure Unmanned Aerial Vehicles-based Systems **My Role: Lead-PI** , Amt: $575,865, year: 2023
7. **Source:** NSF **Title:** CICI: RSSD: A Vulnerability Modeling Approach Toward Secure Scientific Cyber-Infrastructures – **My Role: Co-PI** - **Lead PI:** Hossien Sarafzadeh , Amt: $600,000, year: 2023
8. **Source:** Griffiss Institute **Title:** NKAT-VI: A Virtual Institute for Cyber Research and Experiential Education – **Lead PI:** Hossien Sarafzadeh , **My role Co-PI** , Amt: $1.5M, year: 2023
9. **Source:** CIA **Title:** Capstone Senior Design Projects – **My Role: Lead-PI** , Amt: $6,000, year: 2023
10. **Source:** NCAT-Internal **Title:** Securing Internet-of-Things Systems Using Evolvable Virtualization – **My Role: Co-PI** , Amt: $25,000, year: 2023
11. **Source:** Lockheed Martin **Title:** Privacy Preserving Traffic Management Systems – **My Role: Lead-PI** , Amt: $11,000, year: 2022
12. **Source:** Cisco Research **Title:** Interpretable Machine Learning for High-stack Applications Using Genetic Algorithm – **My Role: Lead-PI** , Amt: $56,191k, year: 2022
13. **Source:** Intel and NCAT College of Engineering **Title:** Smart Supply Chain Managment – **My Role: Lead-PI** – Amt: $50k, year: 2022
14. **Source:** Air Force **Title:** Air Force (AF) X20.c Small Business Technology Transfer (Sttr) Program Vehicles – **Lead PI:** Balakrishna Gokaraju , **My Role: Co-PI** – Amt: $50k, Share: $13k, year: 2021
15. **Source:** NSF Major Research Instrumentation – **Title:** MRI: Acquisition of a Testbed of Connected Autonomous MicroTransit Vehicles – **Lead PI:** Ali Karimoddini, **My Role: Co-PI** – Amt: $550k year: 2020

16. **Source:** NASA University Leadership Initiation – **Title:** Secure and Safe Assured Autonomy (S2A2) Vehicles – **Lead PI:** Abdullah Homaifar, **My Role: Co-PI** – Amt: $8M, Share: $635k, year: 2020
17. **Source:** Intel Mindshare Program – **Title:** Engineering Applications of Artificial Intelligence , **My Role: Lead-PI** – Amt: $25k, year:2020
18. **Source:** NCAT -Center of Excellence in Cybersecurity Research, Education, and Outreach (CREO) – **Title:** Converging Blockchain and Next-generation Privacy-preserving Artificial Intelligence Technologies for Intelligent Transportation Systems , **My Role: Lead-PI** – Amt: $5k, year:2020

Journal Papers

[J1] M. Mynuddin, S. U. Khan, R. Ahmari, L. Landivar, **M. Nabil**, and A. Homaifar, "Trojan attack and defense for deep learning based navigation systems of unmanned aerial vehicles," *IEEE Access*, 2024.

[J2] S. U. Khan, M. Mynuddin, and **M. Nabil**, "Adaptedge: Targeted universal adversarial attacks on time series data in smart grids," *IEEE Transactions on Smart Grid*, 2024.

[J3] I. Elgarhy, M. M. Badr, M. Mahmoud, **M.Nabil**, M. Alsabaan, and M. I. Ibrahem, "Securing smart grid false data detectors against white-box evasion attacks without sacrificing accuracy," *IEEE Internet of Things Journal*, 2024.

[J4] N. K. Gyimah, R. Akinie, X. Yan, **M. Nabil**, K. D. Gupta, A. Homaifar, V. Hemmati, and D. Opoku, "Ncat12-det: A new benchmark dataset for surface defect detection and a comparative study," *IEEE Access*, 2024.

[J5] A. A. S. AlQahtani, T. Alshayeb, **M. Nabil**, and A. Patooghy, "Leveraging machine learning for wi-fi-based environmental continuous two-factor authentication," *IEEE Access*, 2024.

[J6] **M. Nabil**, A. Sherif, M. Mahmoud, W. Alsmary, and M. Alsabaan, "Accurate and privacy-preserving person localization using federated-learning and the camera surveillance systems of public places," *IEEE Access*, 2022.

[J7] **M. Nabil**, "Putting proof of work to work," *Nature Energy*, pp. 1–2, 2022.

[J8] B. Gebru, L. Zeleke, D. Blankson, **M. Nabil**, S. Nateghi, A. Homaifar, and E. Tunstel, "A review on human–machine trust evaluation: Human-centric and machine-centric perspectives," *IEEE Transactions on Human-Machine Systems*, 2022.

[J9] **M. Nabil**, A. Sherif, M. Mahmoud, W. Alsmary, and M. Alsabaan, "Privacy-preserving non-participatory surveillance system for covid-19-like pandemics," *IEEE Access*, 2021.

[J10] N. Bahadori, **M. Nabil**, B. Kelley, and A. Homaifar, "Enabling content-centric device-to-device communication in the millimeter-wave band," *IEEE Transactions on Mobile Computing*, pp. 1–1, apr 2021.

[J11] N. Bahadori, **M. Nabil**, and A. Homaifar, "Antenna beamwidth optimization in directional device-to-device communication using multi-agent deep reinforcement learning," *IEEE Access*, 2021.

[J12] M. Baza, M. Pazos-Revilla, A. Sherif, **M. Nabil**, M. Mahmoud, and W. Alasmary, "Privacy-preserving and collusion-resistant charging coordination schemes for smart grid," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2021.

[J13] M. I. Ibrahem, **M. Nabil**, M. M. Fouda, M. M. E. A. Mahmoud, W. Alasmary, and F. Alsolami, "Efficient privacy-preserving electricity theft detection with dynamic billing and load monitoring for ami networks," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1243–1258, 2021.

[J14] M. Alsabaan, W. Alsmary, A. Alquniah, M. Mahmoud, and **M. Nabil**, "A distributed surveillance system with full coverage guarantee using positive orthogonal codes," *IEEE Access*, 2021.

[J15] A. Takiddin, M. Ismail, **M. Nabil**, M. M. Mahmoud, and E. Serpedin, "Detecting electricity theft cyber-attacks in ami networks using deep vector embeddings," *IEEE Systems Journal*, 2020.

[J16] A. Girma, N. Bahadori, M. Sarkar, T. Tadewos, M. Behniapoor, **M. Nabil**, A. Karimoddini, and A. Homaifar, "IoT-enabled autonomous system collaboration for disaster-area management," *IEEE/CAA Journal of Automatica Sinica*, 2020. Under Review.

[J17] M. Baza, **M. Nabil**, N. Bewermeier, K. Fidan, M. Mahmoud, and M. Abdallah, "Detecting sybil attacks using proofs of work and location in VANETs," *IEEE Transactions on Secure and Dependable Computing*. Under Review.

[J18] A. Alsharif, **M. Nabil**, A. Sherif, M. Mahmoud, and M. Songa, "MDMS: efficient and privacy-preserving multi-dimension and multi-subset data collection for ami networks," *IEEE Journal on Internet of Things*, vol. 6, pp. 10363 – 10374, 2019.

[J19] **M. Nabil**, A. Sherif, A. Alsharif, and M. Mahmoud, "Efficient privacy-preserving ride sharing organization scheme for transferable and non-transferable services," *IEEE Transactions on Secure and Dependable Computing*.

[J20] **M. Nabil**, M. Ismail, M. Mahmoud, W. Alasmary, and E. Serpedin, "PPETD: privacy-preserving electricity theft detection scheme with load monitoring and billing for AMI networks," *IEEE Access*, vol. 7, pp. 96334–96348, 2019.

[J21] A. Alsharif, **M. Nabil**, and M. Mahmoud, "EPDA: Efficient and privacy-preserving data collection and access control scheme for multi-recipient AMI networks," *IEEE Access 2019*, vol. 7, pp. 27829–27845.

[J22] A. Alsharif, **M. Nabil**, S. Tonyali, H. Mohamed, M. Mahmoud, and K. Akkaya, "EPIC: efficient privacy-preserving scheme with e2e data integrity and authenticity for ami networks," *IEEE Journal on Internet of Things*, vol. 6, no. 2, pp. 3309–3321, 2019.

[J23] M. Nawar, **M. Nabil**, and D. A. El-Reedy, "Bel-arabi: Advanced arabic grammar analyzer," *International Journal of Social Science and Humanity*, vol. 6, no. 5.

Book Chapters

[B1] **M. Nabil**, M. Bima, A. Alsharif, W. Johnson, S. Gunukula, M. Mahmoud, and M. Abdallah, *Smart Cities Cybersecurity and Privacy*, ch. Priority-based and Privacy-preserving Electric Vehicle Dynamic Charging System with Divisible E-Payment. Elsevier, 2018.

[B2] **M. Nabil**, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe, and E. Serpedin, *Deep Learning Applications for Cyber Security*, ch. Deep Learning-based detection of electricity theft cyber-attacks in smart grid AMI networks. Springer, 2018.

[B3] M. Baza, M. Fouda, **M. Nabil**, A. Eldien, H. Mansour, and M. Mahmoud, *Combating Security Challenges in the Age of Big Data*, ch. Blockchain-based Distributed Key Management Approach Tailored for Smart Grid. Springer, 2019.

Conference Papers

[C1] M. Srewa, M. F. Winfree, M. I. Ibrahem, **M. Nabil**, R. Lu, and A. Alsharif, "Poisoning attack mitigation for privacy-preserving federated learning-based energy theft detection," in *ICC 2024-IEEE International Conference on Communications*, pp. 3962–3968, IEEE, 2024.

[C2] M. Mynuddin, S. U. Khan, and **M. Nabil**, "Trojan triggers for poisoning unmanned aerial vehicles navigation: A deep learning approach," in *IEEE International Conference on Cyber Security and Resilience*, 2023.

[C3] A. Eroglu, T. Walpita, and **M. Nabil**, "Rf power amplifier control system with dynamic load conditions," in *IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2023.

[C4] A. Eroglu and **M. Nabil**, "Artificial intelligence based high power calibration method for rf pulse amplifiers," in *2024 IEEE 42nd VLSI Test Symposium (VTS)*, pp. 1–5, IEEE, 2024.

[C5] I. Adom and t. Mahmoud, "Rb-xai: Relevance-based explainable ai for traffic detection in autonomous systems," in *SoutheastCon 2024*, pp. 1358–1367, IEEE, 2024.

[C6] F. Olagunju, I. Adom, and t. Mahmoud, "Privacy-preserving backdoor attacks mitigation in federated learning using functional encryption," in *SoutheastCon 2024*, pp. 531–539, IEEE, 2024.

[C7] S. U. Khan, M. Mynuddin, I. Adom, , and **M. Nabil**, "Mitigating targeted universal adversarial attacks on time series power quality disturbances models," in *2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pp. 91–100, IEEE, 2023.

[C8] A.-R. Nuhu, **M. Nabil**, Y. Ayalew, V. Hemmati, A. Homaifar, and E. Tunstel, "Local (per-input) robustness based guided adversarial training of deep neural networks," in *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0182–0191, IEEE, 2023.

[C9] M. Mynuddin, S. U. Khan, **M. Nabil**, and A. Alsharif, "Adversarial attacks on deep learning-based uav navigation systems," in *2023 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–6, IEEE, 2023.

[C10] C. Shelton, A. Eroglu, and **M. Nabil**, "Artificial neural networks for modeling of gan devices," in *2022 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, pp. 1–1, IEEE, 2022.

[C11] N. K. Gyimah, K. D. Gupta, **M. Nabil**, X. Yan, A. Girma, A. Homaifar, and D. Opoku, "A discriminative deeplab model (ddlm) for surface anomaly detection and localization," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1137–1144, IEEE, 2023.

[C12] H. Shittu and **M. Nabil**, "Smart supply chain management with attribute-based encryption access control," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0198–0204, IEEE, 2023.

[C13] E. Lobachev, **M. Nabil**, and A. Patooghy, "Blockchain-based smart supply chain management," in *International Conference on Dependable Systems and Their Applications (DSA)*, 2022.

[C14] **M. Nabil**, A. Sherif, M. Mahmoud, W. Alsmary, and M. Alsabaan, "Person localization using machine learning in multi-source camera surveillance system," in *SoutheastCon*, 2022.

[C15] M. Forney, X. Yan, K. D. Gupta, **M. Nabil**, and A. Homaifar, "Identifying anomalous flight trajectories by leveraging ensembled outlier detection framework," in *2022 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, 2022.

[C16] A.-R. Nuhu, K. D. Gupta, W. B. Bedada, **M. Nabil**, L. A. Zeleke, A. Homaifar, and E. Tunstel, "Negative selection approach to support formal verification and validation of blackbox models' input constraints," in *2022 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 413–420, IEEE, 2022.

[C17] R. A. Agyapong, **M. Nabil**, A.-R. Nuhu, M. I. Rasul, and A. Homaifar, "Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning," in *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 01–08, IEEE, 2021.

[C18] C. Shelton, A. Eroglu, and **M. Nabil**, "Application of genetic algorithm for planar transmission lines," in *2021 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, pp. 394–394, IEEE, 2021.

[C19] M. Hataba, A. Sherif, M. Elsersy, **M. Nabil**, M. Mahmoud, and K. H. Almotairi, "Privacy-preserving biometric-based authentication scheme for electric vehicles charging system," in *2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pp. 86–91, IEEE, 2021.

[C20] B. Hamoui, A. Alashaikh, A. Sherif, E. Alanazi, **M. Nabil**, and W. Alsmary, "Google searches and covid-19 cases in saudi arabia: A correlation study," in *2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pp. 104–108, IEEE, 2021.

[C21] S. Alqurashi, A. Alashaikh, **M. Nabil**, E. Alanazi, A. Sherif, and W. Alsmary, "Identifying information superspreaders of covid-19 from arabic tweets," in *2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, pp. 109–114, IEEE, 2021.

[C22] A. Girma, A. Homaifar, **M. Nabil**, X. Yan, and M. SARKAR, "Da-2-net: Diverse adaptive attention convolutional neural network," in *IEEE International Conference on Systems, Man, and Cybernetics* **(SMC)**, (Melbourne, Australia), Oct 2021.

[C23] N. K. Gyimah, A. Girma, **M. Nabil**, S. Nateghiboroujeni, A. Homaifar, and D. Opoku, "A robust completed local binary pattern (rclbp) for surface defect detection," in *IEEE International Conference on Systems, Man, and Cybernetics* **(SMC)**, (Melbourne, Australia), Oct 2021.

[C24] A. Alsharif and **M. Nabil**, "A blockchain-based medical data marketplace with trustless fair exchange and access control," in *2020 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2020.

[C25] A. Shafee, M. Baza, D. Talbert, M. Fouda, **M. Nabil**, and M. Mahmoud, "Mimic learning to generate a shareable network intrusion detection model," in *IEEE Consumer Communications and Networking Conference* **ICNC**, (Las Vegas, USA), Jan 2020.

[C26] **M. Nabil**, M. Ismail, M. Mahmoud, and E. Serpedin, "Deep recurrent electricity theft detection in AMI networks with evolutionary hyper-parameter tuning," in *In Proceedings of the IEEE International Conference on Internet of Things 2019* **iThings**, (Atlanta, USA), July 2019.

[C27] A. Alsharif, A. Shafee, **M. Nabil**, M. Mahmoud, and W. S. Alasmary, "A multi-authority attribute-based signcryption scheme with efficient revocation for smart grid downlink communication," in *In Proceedings of the IEEE International Conference on Internet of Things 2019* **iThings**, (Atlanta, USA), July 2019.

[C28] M. Baza, **M. Nabil**, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicle," in *Proceedings of the International IEEE Wireless Communications and Networking Conference* **WCNC**, (Marrakech, Morocco), April 2019.

[C29] M. Baza, **M. Nabil**, M. Ismail, M. Mahmoud, E. Serpedin, and M. A. Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," in *The 2019 IEEE International Conference on Blockchain* **Blockchain-2019**, (Atlanta, USA), July 2019. Submitted.

[C30] **M. Nabil**, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe, and E. Serpedin, "Deep recurrent electricity theft detection in AMI networks with random tuning of hyper-parameters," in *Proceedings of the International Conference on Pattern Recognition 2018* **ICPR**, (Beijing, China), August 2018.

[C31] **M. Nabil**, A. Alsharif, A. Sherif, M. Mahmoud, and M. Younis, "Efficient multi-keyword ranked search over encrypted data for multi-data-owner settings," in *IEEE International Conference on Communications* **ICC**, (Kansas City, USA), May 2018.

[C32] A. Alsharif, **M. Nabil**, M. Mahmoud, and M. Abdallah, "Privacy-preserving collection of power consumption data for enhanced AMI networks," in *the 25th International Conference on Telecommunications* **ICT**, (Saint-Malo, France), June 2018.

[C33] **M. Nabil**, A. Atyia, and M. Aly, "Cufe at task 4: A gated recurrent model for sentiment classification," in *In Proceedings of the 10th International Workshop on Semantic Evaluation* **SemEval**, (San Diego, US), June 2016.

[C34] **M. Nabil**, A. Atyia, and M. Aly, "ASTD: arabic sentiment tweets dataset," in *Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing*, **EMNLP**, (Lisbon, Portugal), August 2015.

[C35] **M. Nabil**, A. Atyia, and M. Aly, "New approaches for extracting arabic key phrases," in *International Conference on Intelligent Text Processing and Computational Linguistics* **CICLing**, (Cairo, Egypt), June 2015.

[C36] M. Nawar, **M. Nabil**, and M. B. Fayek, "Improved tokenization and pos tagging for arabic text," in *Egyptian Society Conference on Language Engineering* **ESOLEC**, (Cairo, Egypt), June 2012.

Awards and Recognation

2023 **575k NSF Excellence in Research Award** for my proposal entitled "Excellence in Research: Towards Secure Unmanned Aerial Vehicles-based Systems"

2023 **Association of College and University Educators (ACUE)** Effective College Teaching Credential.

2023 **Summer Visiting Faculty at the Fermi National Accelerator Laboratory (FNAL)** through Department of Energy's (DOE) Visiting Faculty Program

2022 **Defense Advanced Research Projects Agency (DARPA) Forward Riser** [Link]

2020 **5k USD SEED Seed Grant** from the Centers of Excellence Seed Grant Program (Center of Excellence in Cybersecurity Research, Education, and Outreach at NCAT

2017-2019 **Carnegie Classification Scholarship** Fully funded three years PhD scholarship at Tennessee Tech.

2012 **Intel Excellent software optimization skills**, awarded by the Intel in for being ranked 27th over more than 750 participants in Acceler8 your code contest 2012.

2012 **Graudate Assistantship**, Cairo University, 2012.

2012 **2nd position**, in Egyptian Engineering day graduation projects competition over more than 90 participants for "Bel-Arabi" project. "Bel-Arabi" is a C++ machine leaning and information retrieval framework for Arabic texts. It can be used in many natural language processing applications such as machine translation, text to speech, search engines, text mining etc.

2011 **Intel Excellent software optimization skills**, awarded by the Intel for being ranked 12th over more than 500 participants in Acceler8 your code contest 2011 (Won Notebook).

Teaching - Developed Courses

I am a certified instructor through the Association of College and University Educators (ACUE) Effective College Instruction Credential.

NC&AT-ECEN 678 **Introduction to Neural Networks** The course introduce Deep Learning, Neural Networks, and their applications. With companion PyTorch exercises and research papers, students can practice the concepts learned.
Semesters: S22, **Graduate Course at NC&AT** [Developed Course materials]

NC&AT-ECEN 885 **Machine Learning in Cybersecurity** The course address cutting-edge technologies for privacy-preserving AI and how to use AI to improve the security of a system and how to use ML to launch attacks and countermeasures.
Semesters: F19, S20, **Graduate Course at NC&AT** [Developed Course materials]

NC&AT-ECEN 474-674 **Genetic Algorithms**, Genetic algorithms are receiving greater attention in machine learning applications where they can help expert systems acquire new knowledge. In this course, the theory and application of genetic algorithms are studied.
Semesters: S21, **Graduate Course at NC&AT** [Developed Course materials]

NC&AT-ECEN 377 **Engineering Applications of AI**, In this course, the students dive in various AI algorithms and their practical applications.
Semesters: F22,F23, **Undergraduate Course at NC&AT** [Developed Course materials]

NC&AT-ECEN 478 **Senior Design Project**, The course deals with design implementation, system block testing, interfacing, and prototype testing. Teamwork, technical writing, communications, and project management are stressed throughout the semester.
Semesters: F21 **Under Graduate Course at NC&AT** [Developed Course materials]

NC&AT-ECEN 227 **Discrete System Modeling**, This course introduces discrete mathematical structures and finite-state machines. Students will learn how to use logical and mathematical formalisms to formulate and solve problems in computer engineering. Topics include propositional logic, proof techniques, recurrence relations, sets, combinatorics, relations, functions, graphs, trees, and finite-state machines.
Semesters: F19, S20, F20, S21, F21 **Under Graduate Course at NC&AT** [Developed Course materials]

Service to the Research Community

- Program committee member for IEEE BSC 2021-2022-2023: IEEE International Workshop on Blockchain and Smart Contracts. Organizing and review the submitted papers.
- Program committee member for IEEE CPS-Sec 2021-2021-2022-2023: International Workshop on Cyber-Physical Systems Security Protocols. Organizing and review the submitted papers.
- Program committee member for IEEE COMPSAC 2020: IEEE Computer Society Signature Conference on Computers, Software and Applications. Organizing and review the submitted papers.
- Program committee member for IEEE STPSA 2020: The 15th IEEE International Workshop on Security, Trust Privacy for Software Applications. Organizing and review the submitted papers.
- Program committee member for IEEE CPS-Sec 2020: The 5th IEEE International Workshop on Cyber-Physical Systems Security 2020. Organizing and review the submitted papers.
- Program committee member for IEEE Blockchain-2020: The 3rd IEEE International Conference on Blockchain. Organizing and review the submitted papers.
- Program committee member for IEEE Blockchain-2020: The 3rd IEEE International Conference on Blockchain. Organizing and review the submitted papers.

Service to Profession

- Reviewer, IEEE Transactions on Smart Grid, IEEE Transactions on Affective Computing, IEEE Internet of Things journal (IoT), IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Information Forensics and Security, IEEE Access, IEEE Computer Magazine, Nature Energy, Sensors, Algorithms, Peer-to-Peer Networking and Applications journal, Arabian Journal for Science and

Engineering (Springer), Applied Sciences. Samples of thank you letters are attached.

- IEEE Active Member.
- Guest Editor, for a special Issue of the journal Machine Learning and Knowledge Extraction on the subject of "Machine Learning for Cyber Security".
- Guest Editor for Springer special edition Artificial Intelligence in Mobile Ad Hoc Networks for Urban Traffic Environments.
- Editor Frontiers in Energy Research (2023-Present).

Graduate Students Advised at N.C. A&T

- **Moses Ndebugre** - **Degree:** PhD - **Expected Graduation:** Fall 2027 - **Thesis Title:** TBD
- **Issac Adom** - **Degree:** PhD - **Expected Graduation:** Fall 2026 - **Thesis Title:** On Explainable AI for Autonomous Vehicles Systems
- **Rachu Acharya** - **Degree:** MSc - **Expected Graduation:** Fall 2025 - **Thesis Title:** Communication Efficient and Privacy Preserving Federated Learning Framework
- **Mohammed Mynuddin** - **Degree:** Ph.D. - **Expected Graduation:** Fall 2025 - **Thesis Title** Trojan and Adversarial Attack on Unmanned Aerial Vehicles Navigation Systems
- **Sultan Khan** - **Degree:** MSc - **Graduated** - **Thesis Title:** Addressing Trojan and Targeted Universal Adversarial Attacks on Smart Grids: A Time Series Analysis Approach
- **Funminiyi Olagunju** - **Degree:** MSc - **Graduated** Spring 2024 - **Thesis Title:** Adversarial Attacks Against Federated Learning Algorithms
- **Richmond Agyapong** - **Degree:** MSc - **Graduated** - **Thesis Title:** Efficient Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles Using Deep Learning
- **Habeeb A Shittu** - **Degree:** MSc - **Graduated** - **Thesis Title** Blockchain based smart supply chain management with ABE access control
- **Mohammad Iqbal Hossain** - **Degree:** MSc - **Graduated** - **Thesis Title:** Privacy-Preserving Traffic Forecasting Using Deep Learning
- **Mikol Forney** - **Degree:** PhD-Co-Advised - **Graduated** - **Thesis Title:** A Framework for Outlier Detection in Pivotal Time Series Data Utilizing Parallel Processing

Undergraduate Students Advised at N.C. A&T

- **Jaquan Blanks** - **Degree:** Undergrad NCAT - **Year:** F24 - **Project:** Autonomous Driving System using Deep Learning
- **Mekhi Parker** - **Degree:** Undergrad NCAT - **Year:** F22 - **Project:** Smart supply chain management
- **Israel Barnes** - **Degree:** Undergrad NCAT - **Year:** F22 - **Project:** Smart supply chain management
- **Connor Bishop** - **Degree:** REU Undergrad FIT - **Year:** F22 - **Project:** Smart supply chain management
- **Emil Lobachev** - **Degree:** REU Undergrad FIT - **Year:** F21 - **Project:** Smart supply chain management
- **Demetrius Pruitt** - **Degree:** REU Undergrad FIT - **Year:** F21 - **Project:** Smart supply chain management
- **Talha Jahnagir** - **Degree:** Undergrad NCAT - **Year:** F22 - **Project:** Autonomous Driving System using ML
- **David Andraos** - **Degree:** Undergrad NCAT - **Year:** F22 - **Project:** Autonomous Driving System using ML
- **Lamoye Augustus** - **Degree:** Undergrad NCAT - **Year:** F21 - **Project:** Autonomous Driving System using ML
- **Bryce Kearney** - **Degree:** Undergrad NCAT - **Year:** F21 - **Project:** Engineering Applications of AI

Students Dissertation Committee at N.C. A&T

- **Nima Namvar** - **Degree:** PhD - **Title:** Resource Allocation and Network Management in 5G Cellular Networks - **Graduation:** 2020 - **Adviser:** Dr. Abdollah Homaifar
- **Abbigail Waddell** - **Degree:** MSc - **Title:** The Use of Artificial Intelligence Algorithms to Improve the Safety of Unmanned Aerial Vehicles - **Graduation:** 2021 - **Adviser:** Dr. John Kelly

- **Niloofar Bahadori** - **Degree:** PhD - **Title:** Device-to-Device Communication in 5G Wireless Networks - **Graduation:** 2021 - **Adviser:** Dr. John Kelly and Dr. Abdollah Homaifar
- **Shabnam Nazmi** - **Degree:** PhD - **Title:** A rule-based evolutionary approach to multi-label classification - **Graduation:** 2021 - **Adviser:** Dr. Abdollah Homaifar
- **Mrinmoy Sarkar** - **Degree:** PhD - **Title:** Testing and Evaluation of Operational Performance of Autonomous Multi-agent UAV Systems with inbuilt Safety Feature - **Graduation:** Spring 2022 - **Adviser:** Dr. Abdollah Homaifar
- **Biniam Gebru** - **Degree:** PhD - **Title:** Evaluation of trust in human-machine teams - **Graduation:** Spring 2022 - **Adviser:** Dr. Abdollah Homaifar
- **Brinta Chowdhury** - **Degree:** PhD - **Title:** Metamaterial Device Design for Terahertz Applications - **Graduation:** Summer 2022 - **Adviser:** Dr. Abdullah Eroglu
- **Mikol Forney** - **Degree:** PhD - **Title:** A Framework for Outlier Detection in Pivotal Time Series Data Utilizing Parallel Processing - **Graduation:** Spring 2022 - **Adviser:** Dr. Abdollah Homaifar and Dr. Mahmoud Mahmoud
- **Jelani Ownes** - **Degree:** MSc - **Title:** CLCS: A Convolutional Learning classifier system for the surrogate model in higher-dimensional space - **Graduation:** Summer 2022 - **Adviser:** Dr. Abdollah Homaifar
- **Abenezer Girma** - **Degree:** PhD - **Title:** Attention Augmented Deep Neural Network Design for Vehicular Time Series and Computer Vision Applications - **Graduation:** Summer 2022 - **Adviser:** Dr. Abdollah Homaifar
- **Nana Kankam Gyimah** - **Degree:** PhD - **Title:** A Novel Data-driven Approach for Surface Defect Detection and Localization - **Graduation:** Fall 2022 - **Adviser:** Dr. Abdollah Homaifar
- **Thisara Walpita** - **Degree:** PhD - **Title:** AI-based Dual-Core Architecture for RF Power Amplifier Control and Frequency Synthesis with Power Calibration - **Graduation:** Fall 2022 - **Adviser:** Dr. Abdullah Eroglu
- **Kristofer Bailey** - **Degree:** MSc - **Title:** Crowd Sourcing of Training Data for Machine Learning Models for a Video Game Controller - **Graduation:** Fall 2022 - **Adviser:** Dr. Corey Graves
- **Biniam Gebru** - **Degree:** PhD - **Title:** Evaluation of Trust in Autonomous Systems: human trust sensing and trustworthy autonomous driving - **Graduation:** Spring 2023 - **Adviser:** Dr. Abdollah Homaifar
- **Michael Chestnut** - **Degree:** PhD - **Title:** Using a Smart Hyperspace for Implicit and Explicit Logging of Human Data (S.H.I.E.L.H.D.) for Ubiquitous and Secure Fatigue Tracking - **Graduation:** Summer 2023 - **Adviser:** Dr. Corey Graves
- **Yohannes Bekele** - **Degree:** PhD - **Title:** Reliability and Performance of Secured Single Board Computer-Based Autonomous Systems: A Study on Hardware Fault Occurrence - **Graduation:** Summer 2023 - **Adviser:** Dr. Daniel Limbrick
- **Mushahid I. Rasul** - **Degree:** MSc - **Title:** Autonomous Landing of Unmanned Aerial Vehicles on Mobile Landing Platforms - **Graduation:** Summer 2023 - **Adviser:** Dr. Abdollah Homaifar
- **Mansi H. Bhavsar** - **Degree:** PhD - **Title:** A Dynamic Architecture for an Anomaly Detection System for IoT Devices - **Graduation:** Summer 2023 - **Advisers:** Dr. John Kelly and Dr. Koshik Roy
- **Lydia A Zeleke** - **Degree:** PhD - **Title:** A Unified Approach for Enhancing Detect-And-Avoid System Trustworthiness to Facilitate Seamless UAS Airspace Integration - **Graduation:** Spring 2025 - **Adviser:** Dr. Abdollah Homaifar
- **Yahi Negasa** - **Degree:** PhD - **Title:** Risk-Aware Integrated Decision-making and Motion Planning for Separation Assurance of UAM Aircraft - **Graduation:** Summer I 2025- **Adviser:** Dr. Ali Karimoddini

Other Services at N.C. A&T

- Served as University Representative in the NVIDIA AI Summit 2024. In this role, I engaged in the symposium, which took place on Oct 7th and 9th at the Washington D.C. During the event, various projects were discussed for potential collaboration.
- Served as a committee member for a new bachelor's program in Artificial Intelligence (2024). My responsibilities included preparing the proposal, curriculum guidelines, attending the meetings, and providing feedback to the committee.
- Served as a hiring committee member for the Project Manager position at the Center of Excellence in Education and Outreach at North Carolina A&T State University (2024). Responsibilities included reviewing applications,

conducting interviews, and providing recommendations to ensure the selection of a highly qualified candidate aligned with the center's goals and objectives.

- Served as Graduate College Representative for some graduate students. As the representative of the Graduate College faculty, I participated in the doctoral dissertation committee, exercising the same rights and responsibilities as any other committee member.
- Served as a committee member in the Computer Engineering Curriculum Committee, collaborating with fellow members to enhance the curriculum with a primary focus on bolstering freshman retention. Substantial modifications to the major curriculum were suggested in 2021 and subsequently sanctioned by the college.
- Coordinator of the ECE senior design project. As the coordinator, I facilitated a dynamic learning environment that encouraged students to integrate their knowledge, skills, and creativity to address real-world challenges. This involved liaising with industry partners, mentors, and fellow educators to ensure the project's alignment with industry standards and best practices.
- Served as a Senior Design Project Advisor for the project titled "Autonomous Driving System using Machine Learning."
- Served as a hiring committee member for the ECE department lab manager position in 2021. Responsibilities included reviewing applications, participating in interviews, evaluating candidates, and providing recommendations to ensure the selection of a qualified individual to support the department's laboratory needs.
- Served as University Representative in the 2023 Space Force USSF University Consortium Symposium. I engaged in the symposium, which took place on August 9th and 10th at the University of Colorado Boulder campus. During the event, various projects were discussed for potential collaboration.
- Served as Hiring committee member for ECE Student Specialist 2023. The committee succeeded in filling the position with a candidate meeting the required qualifications. My role involved reviewing candidate CVs, attending interviews, evaluating candidates, and providing feedback to the committee.
- Panelist for N.C. A& T cross-culture diversity event 2022. The event aimed to foster a deeper understanding of the challenges experienced by individuals from various cultural backgrounds, promoting inclusivity and unity within the university.
- Served as Judge for the College of Engineering Annual Graduate Poster Presentation Competition 2020, 2021, 2022. I reviewed the posters and provided feedback to the students. In addition, helped in the selection of the best posters.
- President at North Carolina A& T Society of Hispanic Professional Engineers organization (SHPE) 2019-2021. My role is to help the Hispanic community reach its full potential and make a positive influence on the world through increasing STEM knowledge, access, support, and development.
- Adviser and Co-Founder for Crypto Club student organization. I provide guidance and support to students interested in exploring the world of cryptocurrencies and blockchain technology 2022-2023.
- Alternate Senator of the ECE department. This role involved active participation in the university's senate meetings, where there are substantive discussions about matters that transcended departmental boundaries and had an impact at the university level. In these meetings, fellow senators from various departments collaborate to deliberate on policies, initiatives, and decisions that influenced the broader university community.

Technical Skills

Programming Languages	Python, C++, Java, JavaScript, TypeScript, Go, Rust, SQL, Bash/Shell scripting
Cloud & DevOps	AWS, Azure, Google Cloud Platform, Docker, Kubernetes, CI/CD pipelines, Terraform
Data Science & AI	TensorFlow, PyTorch, Scikit-learn, Pandas, NumPy, Jupyter, Deep Learning
Databases	PostgreSQL, MongoDB, Redis, Elasticsearch, Apache Cassandra
Tools & Frameworks	Git, GitHub Actions, Jenkins, Jira, Confluence, VS Code, PyCharm, Jupyter Lab

Professional References (Order by Relevance)

1. Abdollah Homaifar

Occupation: Professor
Address: Department of Electrical & Computer Engineering, North Carolina A&T, Greensboro, NC, 27411.
Office: McNair Hall 537
Phone: +1 (336) 285-3709
Email: homaifar@ncat.edu
Homepage: https://www.ncat.edu/employee-bio.php?directoryID=430387136
Relation: Ph.D. supervisor.

2. Mohamed Mahmoud

Occupation: Professor
Address: Department of Electrical & Computer Engineering, Tennessee Technological University, Cookeville, TN, 38505.
Phone: +1 (931) 372-3677
Fax: +1 (931) 372-3436
Email: mmahmoud@tntech.edu
Homepage: http://www.cae.tntech.edu/~mmahmoud
Relation: Ph.D. supervisor.

3. Ahmad Patooghy

Occupation: Associate Professor
Address: Department of Computer Systems Technology, North Carolina A&T, Greensboro, NC, 27411.
Phone: +1 336-285-3141
Cell: +1 617-909-7108
Email: apatooghy@ncat.edu
Homepage: https://www.intcyberlab.org/home
Relation: Research Collaborator.

4. Ahmad Alsharif

Occupation: Assistant Professor
Address: Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487.
Cell: +1 (931) 252-9230
Email: ahmad.alsharif@ua.edu
Homepage: https://eng.ua.edu/eng-directory/dr-ahmad-alsharif/
Relation: Research Collaborator.

5. Hossein Sarrafzadeh, PhD

Occupation: University Distinguished Professor
Address: Department of Electrical & Computer Engineering, North Carolina A&T, Greensboro, NC, 27411.
Office: +1 (336) 285-4261
Cell: +1 (716) 790-0771
Email: hasarrafzadeh@ncat.edu
Homepage: https://ncat.edu/research/centers/creo/leadership/index.php
Relation: Research Collaborator.

6. Mohammad Ashiqur Rahman

Occupation: Associate Professor
Address: Department of Electrical & Computer Engineering, Florida International University, Miami, FL, 33174.
Phone: +1 (305) 348-3724
Cell: +1 (704) 241-9165
Email: marahman@fiu.edu
Homepage: https://rahman.eng.fiu.edu
Relation: Research Collaborator.

7. Mohamed Younis

Occupation: Professor
Address: Department of Computer Science & Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD 21250.
Phone: +1 (410) 455-3968
Fax: +1 (410) 455-3969
Email: younis@cs.umbc.edu
Homepage: http://www.csee.umbc.edu/~younis
Relation: Research Collaborator

8. Kemal Akkaya

Occupation: Professor
Address: Department of Electrical & Computer Engineering, Florida International University, Miami, FL, 33174.
Phone: +1 (305) 348-3017
Fax: +1 (305) 348-3807
Email: kakkaya@fiu.edu
Homepage: http://web.eng.fiu.edu/kakkaya
Relation: Research Collaborator