Birhanu Eshete

Associate Professor

Department of Computer & Information Science
College of Engineering and Computer Science
University of Michigan, Dearborn
☎ *+1 (313) 583 6669*
✉ *birhanu@umich.edu*

Home Page: https//:birhanu-eshete.github.io
Research Lab: https://um-dsp.github.io

Bio

Dr. Birhanu Eshete is an Associate Professor of Computer Science in the College of Engineering and Computer Science (CECS) at the University of Michigan–Dearborn, where he directs the Data-Driven Security & Privacy Laboratory. His research develops methods and systems to identify, characterize, and mitigate security, privacy, safety, transparency, and ethical risks in AI systems with a focus on high-stakes applications such as autonomous vehicles, predictive diagnostics, financial forecasting, and cyber-attack detection.
His work has been published in all leading security, privacy, and AI venues, featured in widely accessible venues such as the Science Magazine, and contributed to national efforts, including the US National Institute of Standards and Technology (NIST) Trustworthy & Responsible AI Resource Center.
Dr. Eshete's research has been recognized with competitive awards and funding, including 2024–2025 Fulbright US Scholar Award from the US Department of State, the 2024–2025 Faculty Excellence in Research Award from the College of Engineering and Computer Science, the 2023 NSF CAREER Award from the US National Science Foundation, the 2018 USENIX Security Symposium Distinguished Paper Award, and he was a finalist for the Best Applied Security Research Award in North America in 2018.
Before joining the University of Michigan, he was a Postdoctoral Researcher in the Systems and Internet Security Lab at the University of Illinois at Chicago. He holds a Ph.D. in Computer Science from the University of Trento, and M.Sc. and B.Sc. degrees in Computer Science from Addis Ababa University.

Research Interests

Studying pitfalls and building countermeasures to make AI systems trustworthy AI in high-stake models with focus on:

- security (adversarial examples, backdoor poisoning, model stealing),
- privacy (membership inference, leakage auditing),
- transparency (interpretability), and
- fairness (bias mitigation) High-stakes domains of focus include:and ethical pitfalls of AI systems and building countermeasures to avoid/manage them in high-stakes domains such as autonomous vehicles (e.g., traffic sign recognition, lane detection, object recognition), predictive diagnostics (e.g., cancer detection), financial forecasting (e.g., fraud detection, credit scoring), and cyber attack detection (e.g., malware/intrusion detection).

Education

2009–2013 **Ph.D., Computer Science**, *University of Trento*, Italy.

Thesis: Effective Analysis, Characterization, and Detection of Malicious Activities on the Web

Supervisor: Adolfo Villafiorita, Ph.D.

Synopsis: Developed techniques and tools for (i) holistic detection of malicious web pages (ii) evolution-aware detection of malicious web pages and (iii) behavioral fingerprinting and detection of exploit kits.

2005–2007 **M.Sc., Computer Science**, *Addis Ababa University*, Ethiopia.

Thesis: *Context Information Refinement for Pervasive Medical Systems*

Supervisor: Dawit Bekele, Ph.D.

Synopsis: Developed a context-awareness framework for pervasive healthcare systems with emphasis on QoS and pervasive healthcare domain requirements.

1999–2004 **B.Sc., Computer Science**, *Addis Ababa University*, Ethiopia.

Professional Experience

09/24–now: **Associate Professor**, *University of Michigan, Dearborn*, U.S.A.
—research, teaching, and service at the intersection of security, privacy, and AI/ML.

09/24–06/25 **Fulbright U.S. Scholar**, *Addis Ababa University*, Ethiopia.
—research and teaching at the intersection of security, privacy, and AI/ML.

09/18–08/24: **Assistant Professor**, *University of Michigan, Dearborn*, U.S.A.
—research, teaching, and service at the intersection of security, privacy, and AI/ML.

02/14–08/18: **Postdoctoral Researcher**, *University of Illinois at Chicago*, U.S.A.
—research on systems security, cybercrime analysis, and advanced cyber-attacks.

04/13–09/13 **Visiting Researcher**, *University of Illinois at Chicago*, U.S.A.
—a novel system for behavioral fingerprinting and detection of exploit kits.

08/09–12/13 **Research Assistant**, *Fondazione Bruno Kessler*, Italy.
—3 novel techniques and tools to analyze and detect web-borne malware.

06/06–12/06 **Main Research Engineer**, *United Nations Economic Commission for Africa*, Ethiopia.
—a prototype mobile medical system to support mobility of physicians in a hospital.

06/04–04/05 **Junior Programmer**, *Ethio Telecom*, Ethiopia.
—worked as a developer on a Customer Management System.

Honors and Awards

- **Faculty Excellence in Research Award**: College of Engineering and Computer Science, University of Michigan, Dearborn, 2024-2025.

- **Fulbright U.S. Scholar Award**: U.S. Department of State, 2024-2025.
- **NSF CAREER Award**: U.S. National Science Foundation, 2023.
- **U-M/Ford Alliance Program**: Faculty Summer Sabbatical Awardee, 2019.
- **Distinguished Paper Award**: for the paper "NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications", USENIX Security Symposium, The USENIX Association, Baltimore, MD, USA, Aug. 2018.
- **CSAW'18 US-Canada Finalist**: for the paper "NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications", Applied Research Competition at CSAW, NYU Tandon School of Engineering, 2018.
- **USENIX Travel Grant**: for attending the USENIX Security Symposium, The USENIX Association, Washington D.C., USA, Aug. 2013.
- **Best Paper Award**: for the paper "Context Information Refinement for Pervasive Medical Systems", International Conference on Digital Society (ICDS), 2010.
- **Ph.D. Study Scholarship**: $43, 450 full scholarship for 3 years Ph.D. research in Web Security, Fondazione Bruno Kessler, Trento, Italy, Nov. 2010 - Oct. 2013.
- **Pre-PhD Scholarship**: $15,750 for the project "Tool for Security Testing of Web Applications", Fondazione Bruno Kessler, Trento, Italy, Nov. 2009 - Oct. 2010.

Research Grants (Total: $1,254,103)

- **Sponsor: Bureau of Democracy, Human Rights, and Labor (DRL), United States Department of State**. Project: "DeResistor: Detection Resilient Probing of Censorship Middelboxes", PI: Birhanu Eshete, Amount: $ 300,000, Duration: 09/30/2024 - 12/31/2026.
- **Sponsor: NSF**. Project: "CAREER: Towards Provenance-Driven Understanding of Machine Learning Robustness", Sole PI: Birhanu Eshete, Amount: $ 619, 838, Duration: 05/01/2023 - 04/30/2028.
- **Sponsor: NSF**. Project: "Elements: An Infrastructure for Software Quality and Security Issues Detection and Correction", PI: Marouane Kessentini, Co-PI: Birhanu Eshete, Amount: $599, 999 (Birhanu's Share: $270, 000), Duration: 05/01/2022 - 12/31/2025.
- **Sponsor: Dearborn AI Research Center (DAIR)**. Project: "Towards Robust Machine Learning Models via Moving Target Defense", PI: Birhanu Eshete, Amount: $10, 000, Duration: 09/01/2021 - 07/31/2024.
- **Sponsor: NSF**. Project: "MALDIVES: Developing a Comprehensive Understanding of Malware Delivery Mechanisms", Direct Sponsor: University of Illinois at Chicago, Amount: $54, 263, Duration: 8/16/2019 - 9/30/2020.

Publications

1. **[ACSAC'25]**: Firas Ben Hmida, Abderrahmen Amich, Ata Kaboudi, Birhanu Eshete. *DeepProv: Behavioral Characterization and Repair of Neural Networks via Inference Provenance Graph Analysis*. In Proceedings of the 41st Annual Computer Security Applications Conference (ACSAC), 2025. Acceptance Rate: 18.8%
2. **[ACM CCS'25]**: Philemon Hailemariam, Birhanu Eshete. *PoisonSpot: Precise Spotting*

of Clean-Label Backdoor Poisoning via Fine-Grained Training Provenance Tracking. In Proceedings of the 32nd ACM Conference on Computer and Communications Security (CCS), 2025.

3. **[USENIX SEC'23]**: Abderrahmen Amich, Birhanu Eshete, Vinod Yegneswaran, Nguyen Phong Hoang. *DeResistor: Toward Detection-Resistant Probing for Evasion of Internet Censorship*. In Proceedings of the 32nd USENIX Security Symposium (SEC'23), 2023. Acceptance Rate: 18%
4. **[ACM PETS'23]**: Ismat Jarin, Birhanu Eshete. *MIAShield: Defending Membership Inference Attacks via Preemptive Exclusion of Members*. In Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PETS), 2023. Acceptance Rate: 25%
5. **[ACM HIPS'23]**: Probir Roy, Birhanu Eshete, Pengfei Su. *Designing Secure Performance Metrics for Last Level Cache*. In Proceedings of the 28th International Workshop on High-Level Parallel Programming Models and Supportive Environments, (HIPS), 2023.
6. **[ACM WPES'22]**: Abderrahmen Amich, Birhanu Eshete, Vinod Yegneswaran. *Adversarial Detection of Censorship Measurements*. In Proceedings of the 20th ACM Workshop on Privacy in the Electronic Society (WPES'22), co-located with the 29th ACM Conference on Computer and Communications Security (CCS), 2022. Acceptance Rate: 20.3%
7. **[ACM CODASPY'22]**: Ismat Jarin, Birhanu Eshete. *DP-UTIL: Comprehensive Utility Analysis of Differential Privacy in Machine Learning*. In Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (ACM CODASPY), 2022. Acceptance Rate: 18%
8. **[ACM CODASPY'22]**: Abderrahmen Amich, Birhanu Eshete. *EG-Booster: Explanation-Guided Booster for ML Evasion Attacks*. In Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (ACM CODASPY), 2022. Acceptance Rate: 18%
9. **[ACM ACSAC'21]**: Abderrahmen Amich, Birhanu Eshete. *Morphence: Moving Target Defense Against Adversarial Examples*. In Proceedings of the 37th Annual Computer Security Applications Conference (ACSAC), 2021. Acceptance Rate: 24.5%
10. **[Science'21]**: Birhanu Eshete. *Making Machine Learning Trustworthy*. Science, Vol. 373, Issue. 6556, pp. 743–744, American Association for the Advancement of Science (AAAS), 13 August 2021. Impact Factor: 63.74.
11. **[EAI SecureComm'21]**: Abderrahmen Amich, Birhanu Eshete. *Explanation-Guided Diagnosis of Machine Learning Evasion Attacks*. In Proceedings of the 17th EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2021. Acceptance Rate: 34%
12. **[ACM CODASPY'21]**: Ismat Jarin, Birhanu Eshete. *PRICURE: Privacy-Preserving Collaborative Inference in a Multi-Party Setting*. In Proceedings of the 7th ACM International Workshop on Security and Privacy Analytics (IWSPA'21), co-located with the 11th ACM Conference on Data and Application Security and Privacy (CODASPY), 2021. Acceptance Rate: 29%
13. **[EAI SecureComm'20]**: Abdullah Ali, Birhanu Eshete. *Best-Effort Adversarial Approximation of Black-Box Malware Classifiers*. In Proceedings of the 16th EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2020. Acceptance Rate: 50%

14. **[ACM CCS'19]**: Sadegh M. Milajerdi, Birhanu Eshete, Rigel Gjomemo, V.N. Venkatakrishnan. Poirot: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting. In Proceedings of the 26th ACM Conference on Computer and Communications Security (ACM CCS), 2019. Acceptance Rate: 16%
15. **[IEEE S&P'19]**: Sadegh M. Milajerdi, Rigel Gjomemo, Birhanu Eshete, R. Sekar, V.N. Venkatakrishnan. HOLMES: Real-time APT Detection through Correlation of Suspicious Information Flows. In Proceedings of the 40th IEEE Symposium on Security and Privacy (Oakland), 2019. Acceptance Rate: 12%
16. **[Springer ICISS'18]**: Sadegh M. Milajerdi, Birhanu Eshete, Rigel Gjomemo, V.N. Venkatakrishnan. ProPatrol: Attack Investigation via Extracted High-Level Tasks. In Proceedings of the 14th International Conference on Information Systems Security (ICISS), 2018. Acceptance Rate: 47%
17. **[USENIX SEC'18]**: Abeer Alhuzali, Rigel Gjomemo, Birhanu Eshete, V.N. Venkatakrishnan. NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications. In Proceedings of the USENIX Security Symposium (USENIX SEC), 2018. *** Acceptance Rate: 19.1% *** Distinguished Paper Award Winner! Finalist: CSAW'18 Applied Research Competition North America (US-Canada)***
18. **[USENIX SEC'17]**: Md Nahid Hossain, Sadegh M. Milajerdi, Junao Wang, Birhanu Eshete, Rigel Gjomemo, R. Sekar, Scott Stoller, V.N. Venkatakrishnan. SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data. In Proceedings of the USENIX Security Symposium (USENIX SEC), 2017. Acceptance Rate: 16.3%
19. **[IEEE/IFIP DSN'17]**: Birhanu Eshete, V.N. Venkatakrishnan. DynaMiner: Leveraging Infection Dynamics Analytics for On-the-Wire Malware Detection. In Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017. Acceptance Rate: 24.5%
20. **[ACM CCS'16]**: Abeer Alhuzali, Birhanu Eshete, Rigel Gjomemo, V.N. Venkatakrishnan. Chainsaw: Chained Automated Workflow-based Exploit Generation. In Proceedings of Computer and Communications Security (ACM CCS), 2016. Acceptance Rate: 16.5%
21. **[ISOC NDSS'15]**: Birhanu Eshete, Abeer Alhuzali, Maliheh Monshizadeh, Phillip Porras, V.N. Venkatakrishnan, Vinod Yegneswaran. EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration. In Proceedings of Network and Distributed Systems Security Symposium (ISOC NDSS), 2015. Acceptance Rate: 16.9%
22. **[ACM CODASPY'14]**: Birhanu Eshete, V.N. Venkatakrishnan. WebWinnow: Leveraging Exploit Kit Workflows to Detect Malicious URLs. In Proceedings of Conference on Data and Application Security and Privacy (ACM CODASPY), 2014. Acceptance Rate: 16%
23. **[IEEE COMPSAC'13]**: Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita, Mohammad Zulkernine. EINSPECT: Evolution-Guided Analysis and Detection of Malicious Web Pages. In Proceedings of the International Conference on Computer Software and Applications (IEEE COMPSAC), 2013. Acceptance Rate: 23%
24. **[IEEE SERE'13]**: Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita, Mohammad Zulkernine. ConfEagle: Automated Analysis of Security Configuration Vulnerabilities in Web Applications. In Proceedings of the International Conference on Security and Reliability (IEEE SERE), 2013. Acceptance Rate: 30%

25. **[ACM WWW'13]**: Birhanu Eshete. Effective Analysis, Characterization, and Detection of Malicious Web Pages. In Proceedings of the International Conference on World Wide Web (ACM WWW) Companion, 2013. Acceptance Rate: 14%
26. **[ACM DEV'25]**: Aaron Ciaghi, Birhanu Eshete, Pietro Molini, Adolfo Villafiorita. SAMo: experimenting a social accountability web platform. In Proceedings of the ACM Symposium on Computing for Development (ACM DEV), 2013. Acceptance Rate: 33%
27. **[EAI SecureComm'12]**: Birhanu Eshete, Adolfo Villafiorita, Komminist Weldemariam. BINSPECT: Holistic Analysis and Detection of Malicious Web Pages. In Proceedings of the International Conference on Security and Privacy in Communication Networks (EAI SecureComm), 2012. Acceptance Rate: 28.8%
28. **[IEEE AFRICOMM'12]**: Aaron Ciaghi, Birhanu Eshete, Pietro Molini, Adolfo Villafiorita. Social Accountability for Mozambique: an Experience Report from the Moamba District. In Proceedings of the International IEEE EAI Conference on e-Infrastructure and e-Services for Developing Countries (IEEE AFRICOMM), 2012.
29. **[IEEE ARES'11]**: Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita. Early Detection of Security Misconfiguration Vulnerabilities in Web Applications. In Proceedings of the International Conference on Availability, Reliability and Security (IEEE ARES), 2011. Acceptance Rate: 25%
30. **[IEEE SysSec'11]**: Birhanu Eshete, Adolfo Villafiorita, Komminist Weldemariam. Malicious Website Detection: Effectiveness and Efficiency Issues. In Proceedings of the System Security Workshop (IEEE SysSec), 2011.
31. **[IEEE ICDS'11]**: Valentino Sartori, Birhanu Eshete, Adolfo Villafiorita. Measuring the Impact of Different Metrics on Software Quality: A Case Study in the Open Source Domain. In Proceedings of the International Conference on Digital Society (IEEE ICDS), 2011.
32. **[IEEE CRiSIS'10]**: Biniyam Asfaw, Dawit Bekele, Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita. Host-based Anomaly Detection for Pervasive Medical Systems. In Proceedings of the International Conference on Risks and Security of Internet and Systems (IEEE CRiSIS), 2010. Acceptance Rate: 44%
33. **[IEEE ICDS'10]**: Birhanu Eshete, Dawit Bekele, Komminist Weldemariam, Adolfo Villafiorita. Context Information Refinement for Pervasive Medical Systems. In Proceedings of the International Conference on Digital Society (IEEE ICDS), 2010. ***Best Paper Award Winner!***
34. **[IEEE ICDS'10]**: Birhanu Eshete, Komminist Weldemariam, Adolfo Villafiorita, Andrea Mattioli. ICT for Good: Opportunities, Challenges and the Way Forward. In Proceedings of the International Conference on Digital Society (IEEE ICDS), 2010.

Patents

- **2023**: System and Method Associated with Expedient Detection and Reconstruction of Cyber Events in a Compact Scenario Representation Using Provenance Tags and Customizable Policy. Inventors: Ramasubramanian Sekar, Junao Wang, Md Nahid Hossain, Sadegh M. Milajerdi, **Birhanu Eshete**, Rigel Gjomemo, V. N. Venkatakrishnan, Scott Stoller. Patent number: 11601442. Type: Grant. Filed: August 19, 2019. Date of Patent: March 7, 2023.

Teaching

Graduate

1. **Fall 2025**: Data Security and Privacy (CIS 545)
2. **Fall 2025**: Foundations of Information Security (CIS 540)
3. **Winter 2025**: Trustworthy Artificial Intelligence, Addis Ababa University.
4. **Winter 2024**: Trustworthy Artificial Intelligence (CIS 582)
5. **Winter 2024**: Compiler Design (CIS 574)
6. **Fall 2023**: Data Security and Privacy (CIS 545)
7. **Fall 2023**: Foundations of Information Security (CIS 540)
8. **Winter 2023**: Advanced Computer & Network Security (CIS 584)
9. **Winter 2023**:Compiler Design (CIS 574)
10. **Fall 2022**: Data Security and Privacy (CIS 545)
11. **Fall 2022**: Foundations of Information Security (CIS 540)
12. **Winter 2022**:Compiler Design (CIS 574)
13. **Fall 2021**: Data Security and Privacy (CIS 545)
14. **Fall 2021**: Foundations of Information Security (CIS 540)
15. **Winter 2021**: Compiler Design (CIS 574)
16. **Fall 2020**: Data Security and Privacy (CIS 545)
17. **Fall 2020**: Foundations of Information Security (CIS 540)
18. **Winter 2020**: Compiler Design (CIS 574)
19. **Fall 2019**: Data Security and Privacy (CIS 545)
20. **Winter 2019**: Compiler Design (CIS 574)
21. **Fall 2018**: Data Security and Privacy (CIS 545)

Undergraduate

1. **Winter 2024**: Trustworthy Artificial Intelligence (CIS 482)
2. **Winter 2024**: Compiler Design (CIS 474)
3. **Winter 2023**: Compiler Design (CIS 474)
4. **Winter 2022**: Design Seminar I (CIS 4951)
5. **Winter 2022**: Design Seminar II (CIS 4952)
6. **Winter 2022**: Compiler Design (CIS 474)
7. **Fall 2021**: Data Security and Privacy (CIS 4851)
8. **Winter 2021**: Compiler Design (CIS 474)
9. **Winter 2021**: Digital Forensics II (CIS 467)
10. **Fall 2020**: Data Security and Privacy (CIS 4851)
11. **Winter 2020**: Compiler Design (CIS 474)
12. **Fall 2019**: Data Security and Privacy (CIS 4851)
13. **Winter 2019**: Compiler Design (CIS 474)
14. **Fall 2018**: Data Security and Privacy (CIS 4851)

Student Advising

Doctoral Dissertations

1. **2023 - 2028 (expected)**: Firas Ben Hmida, University of Michigan-Dearborn.
2. **2023 - 2028 (expected)** : Philemon Hailemariam, University of Michigan-Dearborn.
3. **2019 - 2024**: Abderrahmen Amich, University of Michigan-Dearborn.
4. **2019 - 2022**: Ismat Jarin, University of Michigan-Dearborn.

Master's Theses

1. **2024**: By Poornaditya Mishra. "AI-Augmented Vulnerability Detection and Patching", University of Michigan-Dearborn.
2. **2024**: By Elie Rizk. "Towards a Holistic Framework for Machine Learning Trustworthiness", University of Michigan-Dearborn.
3. **2023**: By Christine Carlton. "AI Risk Management Framework for Autonomous Vehicles", University of Michigan-Dearborn.
4. **2023**: By Jon-Nicklaus Jackson. "Exploring Training Provenance for Clues of Data Poisoning in Machine Learning", University of Michigan-Dearborn.
5. **2022**: By Olajide David. "CYTAG: Multi-Source Behavioral Aggregation of Natural Language Cyber Threat Intelligence", University of Michigan-Dearborn.
6. **2019**: By Abdullah Ali. "Adversarial Approximation of a Black-Box Malware Detector", University of Michigan-Dearborn.
7. **2015**: By Stefano Arseni. "Hyper-Sift: Multi-Family Analysis and Detection of Exploit Kits", University of Illinois at Chicago.

Master's Projects

1. **2023**: By Hassaan Ali "Large-Scale Correlation Analysis of Public Information of Notable Individuals with Security Questions on Websites", University of Michigan-Dearborn.
2. **2023**: By Ata Kaboudi. "Code Property Graph-Based Security Vulnerability Analysis", University of Michigan-Dearborn.
3. **2022**: By Hassan Ali. "Empirical Characterization of Benign and Adversarial Predictions of a Neural Network", University of Michigan-Dearborn.
4. **2021**: By Majed Chamseddine. "Automated Characterization of Decision Provenance in Neural Networks", University of Michigan-Dearborn.
5. **2015**: By Sai Kommini. "Architectural Isolation of Plugins in Web Applications", University of Illinois at Chicago.

Undergraduate Independent Studies

1. 2022: By Chevy Pawlik. Project Title: "Correlation and Temporal Analysis of Malware Infection Traffic and APT Reports"
2. 2022: By Ata Kaboudi. Project Title: "Morphence-2.0: Evasion-Resilient Moving Target Defense Powered by Out-of-Distribution Detection"
3. 2021: By Zeineb Moalla. Project Title: "Building a Behavior-Based Malware Detector and

Evaluating its Adversarial Robustness"

Dissertation Committees

Doctoral

1. **Candidate**: Yonas Kibret. **Dissertation Title**: PRIVACY PRESERVED ONLINE DDOS ATTACK DETECTION FRAMEWORKS FOR IOT SYSTEMS. **Advisor(s)**: Dr.Surafel Lemma, Dr. Henock Mulugeta. Addis Ababa University. October 2025.
2. **Candidate**: Mifta Ahmed Umer. **Dissertation Title**: Provenance Blockchain with Predictive Auditing Framework for Mitigating Cloud Manufacturing Risks in Industry 4.0. **Advisor(s)**: Prof. Luis Borges Gouveia, Dr. Elefelious Getachew. Addis Ababa University. June 2025.
3. **Candidate**: Worku Gachena Negera. **Dissertation Title**: Lightweight Deep Learning Model for Botnet Attack Detection in SDN Orchestrated IoT. **Advisor(s)**: Prof. Dr. Freidhelm Schowenker, Dr. Henock Mulugeta Melaku, Dr. Taye Girma Debelee. Addis Ababa University. July 2024.
4. **Candidate**: Robert Kaster. **Dissertation Title**: Automotive Software Attestation: Self, Remote, and Peer - Building Trust in Autonomous Driving Safety Systems. **Advisor**: Dr. Di Ma. University of Michigan-Dearborn. 2024.
5. **Candidate**: Linxi Zhang. **Dissertation Title**: Intrusion Detection Systems to Secure In-Vehicle Networks. **Advisor**: Dr. Di Ma. University of Michigan-Dearborn. 2024.
6. **Candidate**: Weixing Zhou. **Dissertation Title**: Correlation Algorithm Method Based Vehicle CAN Network Identification Mapping. **Advisor**: Dr. Di Ma. University of Michigan-Dearborn.

Master's

1. **Candidate**: Zachary T. Puhl. **Thesis Title**: Voucher-Based Addressing & Sessions: A Simple, Flexible, Privacy-Preserving Recipe for Mitigating IPv6 Neighbor Discovery Redirection Attacks. **Advisor**: Dr. Jinhua Guo. 2024.
2. **Candidate**: Ali Zein. **Thesis Title**: Profile-Guided Optimization of Cold Starts in Serverless Applications with ColdSpy. **Advisor**: Dr. Probir Roy. 2024.
3. **Candidate**: Magdalena Spinu. **Thesis Title**: A Comprehensive Review of Machine Learning Methods in Stock Market. **Advisor**: Dr. Jin Lu. 2022.
4. **Candidate**: Francesco E. Mangano. **Thesis Title**: Modernization of Manufacturing with Cybersecurity at the Forefront. **Advisor**: Dr. Di Ma. 2018.

Professional Service

Organization Committee Member

- **43rd IEEE Symposium on Security & Privacy**: Diversity, Equity, and Inclusion Co-Chair. 2022.
- **Dearborn AI Symposium**: Poster and Demo Track Co-Chair: University of Michigan, Dearborn, Nov 05 – Nov 06, 2020.
- **Dearborn Cybersecurity Day**: University of Michigan, Dearborn, April 01, 2019.

Program Committee Member

- **The Web Conference**: The ACM Web Conference, 2026. * **Senior PC Member**
- **ACM PETS**: Privacy Enhancing Technologies Symposium, 2026.
- **ACM CODASPY**: ACM Conference on Data and Application Security and Privacy, 2025.
- **The Web Conference**: The ACM Web Conference, 2025.
- **USENIX SEC**: The USENIX Security Symposium, 2024.
- **The Web Conference**: The ACM Web Conference, 2024.
- **ACM CODASPY**: ACM Conference on Data and Application Security and Privacy, 2024.
- **USENIX SEC**: The USENIX Security Symposium, 2023.
- **IEEE EuroS&P**: IEEE European Symposium on Security and Privacy, 2023.
- **ACM CODASPY**: ACM Conference on Data and Application Security and Privacy, 2023.
- **USENIX SEC**: The USENIX Security Symposium, 2022.
- **USENIX SEC**: The USENIX Security Symposium, 2020.
- **SecureComm**: Security and Privacy in Communication Networks, 2020.
- **SecureComm**: Security and Privacy in Communication Networks, 2019.
- **SecureComm**: Security and Privacy in Communication Networks, 2018.
- **SecureComm**: Security and Privacy in Communication Networks, 2017.
- **MAICS**: Modern Artificial Intelligence and Cognitive Science Conference, 2017.
- **SecureComm**: Security and Privacy in Communication Networks, 2016.
- **MAICS**: Modern Artificial Intelligence and Cognitive Science Conference, 2016.

Invited Journal Reviewer

- **TIFS**: IEEE Transactions on Information Forensics & Security, 2024.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2023.
- **IJIS**: International Journal of Information Security, 2022.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2021.
- **IJIS**: International Journal of Information Security, 2020.
- **ITS**: IEEE Intelligent Transportation Systems Magazine, 2019.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2018.
- **TIFS**: IEEE Transactions on Information Forensics & Security, 2018.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2017.
- **IJIS**: International Journal of Information Security, 2016.
- **NEPL**: Neural Processing Letters, 2015.
- **TDSC**: IEEE Transactions on Dependable and Secure Computing, 2015.
- **ESEJ**: e-Informatica Software Engineering Journal, 2015.
- **JSS**: Journal of Systems and Software, 2013.

K-12 Outreach

- Advisory Board Member: Cybersecurity Program, Taylor High School, MI. 2022 - present.

Invited Talks & Presentations

1. **Repairing Deep Learning Models by Watching How they Behave**, Monthly Cybersecurity Webinar, Ethiopian Cybersecurity Association (ECySA), September 2025.

2. **Scholarly Research in the Age of Generative AI**, Distinguished Diamond Jubilee Seminar, College of Natural and Computational Sciences, Addis Ababa University, Addis Ababa, June 2025.
3. **Triangular Dynamics of AI & Cybersecurity: Defense Arsenal, Attack Surface, and Weaponization**, Third International Conference on Collaboration in Cybersecurity and Digital Transformation, Addis Ababa, June 2025.
4. **Generative AI at the Crossroads of Language, Culture, and Identity: Promises, Perils, and the Pursuit of Digital Trust**, Annual Conference on Language, Culture and Technology in Development, Addis Ababa University, June 2025.
5. **Generative AI in Education: Risks and Pitfalls to Keep an Eye On**, 3rd International Research Conference Artificial Intelligence (AI) in Education: Opportunities and challenges for the Global South, Addis Ababa, February 2025.
6. **Defending Machine Learning Against Adversarial Inputs and Privacy Leaks**, Addis Ababa Science and Technology University, February 2025.
7. **Enhancing Machine Learning Resilience to Adversarial Manipulations via Moving Target Strategies**, Addis Ababa Institute of Technology, Addis Ababa University, December 2024.
8. **Navigating the AI-Powered Threat Landscape**, Information Network Security Administration (INSA), Addis Ababa, Ethiopia, December 2024.
9. **Navigating the AI-Powered Threat Landscape: Cyber Incidents and Beyond**, United States Embassy, Addis Ababa, Ethiopia, October 2024.
10. **State of the Model: Promising Progress and Remaining Challenges Towards Trustworthy Machine Learning**, Blacks in Cybersecurity (BIC) Village @ DEF CON 30, Las Vegas, NV, August, 2022. Video.
11. **State of the Model: Making Machine Learning Models Resilient Against Evasion and Inference Attacks**, SRI International, Menlo Park, CA, March 2022.
12. **Best-Effort Adversarial Approximation of Black-Box Malware Classifiers**, EAI SecureComm'20, Washington, DC, October, 2020. Video.
13. **Adventures with Cybercrime Toolkits: Insights for Pragmatic Defense**, USENIX ENIGMA Conference, San Francisco, CA, USA, January, 2020. Video.
14. **Real-time Detection of Advanced Persistent Threats using Correlation of Information Flows**, Computer and Information Science Research Seminar, College of Engineering and Computer Science, University of Michigan, Dearborn, MI, USA, October, 2018.
15. **Intrusion Detection: Theoretical Foundations and Practical Flavors,** Graduate Seminar, Addis Ababa Institute of Technology (AAiT), Addis Ababa, Ethiopia, July, 2018.
16. **Learning from Offline Infection Episodes for On-the-Wire Malware Detection,** 7th Greater Chicago Area Systems Research Workshop (GCASR), Chicago, IL, USA, April, 2018.
17. **A Multi-faceted Strategy to Fight Cybercrime,** University at Albany, Albany, NY, USA, March, 2018.
18. **A Multi-faceted Strategy to Fight Cybercrime,** Duke University, Durham, NC, USA, March, 2018.
19. **A Multi-faceted Strategy to Fight Cybercrime,** University of Michigan, Dearborn, MI,

USA, Feb, 2018.

20. **DynaMiner: Leveraging Offline Infection Analytics for On-the-Wire Malware Detection,** IEEE/IFIP DSN'17, Denver, CO, USA, June, 2017.
21. **EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration,** GCASR'15, Chicago, IL, USA, April, 2015.
22. **EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration,** NDSS'15, San Diego, CA, USA, February 2015.
23. **WebWinnow: Leveraging Exploit Kit Workflows to Detect Malicious URLs,** CODASPY'14, San Antonio, TX, USA, March 2014.
24. **Effective Analysis, Characterization, and Detection of Malicious Activities on the Web,** Computer Science Department, University of Illinois at Chicago, Chicago, IL, USA, April 2013.
25. **Effective Analysis, Characterization, and Detection of Malicious Web Pages,** WWW'13, Rio De Janeiro, Brazil, May 2013.
26. **Leveraging Exploit Kit Workflow to Detect Malicious URLs,** Computer Science Department, University of Illinois at Chicago, Chicago, IL, USA, August 2013.
27. **BINSPECT: Holistic Analysis and Detection of Malicious Web Pages,** SecureComm'12, Padua, Italy, September 2012.
28. **Early Detection of Security Misconfiguration Vulnerabilities in Web Applications,** Vienna, Austria, August 2011.
29. **Malicious Website Detection: Effectiveness and Efficiency Issues,** SysSec'11, Amsterdam, Netherlands, July 2011.
30. **Host-Based Anomaly Detection in Pervasive Medical Systems,** CRISIS'10, Montreal, Canada, October 2010.

Media Coverage

1. **Oct 2025: Communications of the ACM:**: You Deserve Some Cybersecurity Today: Lax security put the records of 64 million McDonald's job applicants at risk: Article.
2. **Aug 2025: Epsiloon (French Science Magazine)**: AI Vulnerability: Article in French.
3. **July 2024: UM-Dearborn Reporter**: Reckoning with AI's Trust Issues: Article.
4. **June 2023: UM-Dearborn Reporter**: Is AI really a threat to human civilization? Article.
5. **April 2023: UM-Dearborn Reporter**: Cybersecurity researcher Birhanu Eshete scores prestigious NSF CAREER award: Article.
6. **August 2022: New Frontiers: Emerging Science and Technology Podcast**: Machine Learning for Environment with Bad Actors: Audio.
7. **November 2021: UM-Dearborn Reporter**: Should we view cyberattacks as acts of war? Article.
8. **November 2021: UM-Dearborn Reporter**: Helping scientists become better coders: Article.
9. **August 2021: Science Magazine Podcast**: Attacks on Machine Learning: Audio.
10. **June 2021: WXYZ Detroit**: How to strengthen your cybersecurity while working at home: Video.
11. **June 2021: UM-Dearborn Reporter**: Can we make artificial intelligence more ethical?

Article.

12. **July 2020: UM-Dearborn Reporter**: UM-Dearborn's 'Blue Bytes' group is helping students build-up their arsenal of cybersecurity skills: Article.
13. **November 2019: UM-Dearborn Reporter**: A dispatch from the cybersecurity 'arms race': Article.