Badhan Chandra Das

Miami, Florida, USA.
bdas004@fiu.edu • **Homepage** • **LinkedIn** • **Google Scholar**

Education

♦ **Doctor of Philosophy** *Aug. 2022 – July 2026 (Expected)*
CGPA: 3.95/4.00
Major: Computer Science.
Knight Foundation School of Computing and Information Science (KFSCIS).
Institution: Florida International University.
Ph.D. Co-major Advisors: **Prof. M. Hadi Amini, Prof. Yanzhao Wu**

♦ **Master of Science** *2018-19*
CGPA: 3.80/4.00
Major: Computer Science and Engineering.
Institution: Jahangirnagar University, Savar, Dhaka, Bangladesh.

♦ **Bachelor of Science** *2014-17*
CGPA: 3.50/4.00
Major: Computer Science and Engineering.
Institution: Jahangirnagar University, Savar, Dhaka, Bangladesh.

Key Accomplishments and Ongoing Projects

✓ Extensively exploring the security vulnerabilities of emergent AI applications in several domains, including healthcare, public safety, and Generative AI.

✓ Published **15+ research papers** in renowned journals and conferences on Trustworthy AI, Federated Learning, Large Language Models, Data Mining, and Social Network Analysis.

✓ Currently working on a **US National Science Foundation (NSF)** project and developing an AI-driven overlapping fingerprint separation technique and its explainability as **sole Research Assistant**.

✓ Made significant contributions to method development and the preparation of final deliverables for multiple **US Department of Homeland Security (DHS)** supported projects as **sole Research Assistant**.

✓ Received multiple awards and recognitions, including FIU's prestigious **Outstanding Paper or Manuscript in STEM, Best Poster Award, Developing Country Researcher Award, and several travel grants.**

✓ Developed and contributed to launch Micro-Credential (foundational short course) at FIU entitled **Artificial Intelligence in Crime Analysis and Detection.**

Experience

Research Experience

✓ **Graduate Research Assistant (solid lab, FIU)** *Jan. 2024 - Present*
- Security challenges of LLMs/VLMs, Federated Learning, and their mitigation.
- AI-based efficient threat detection and mitigation (supported by DHS).
- AI-driven Overlapping fingerprint separation (supported by NSF).

✓ **Research Assistant (DM-research group, Jahangirnagar University)** *Aug. 2018 - Dec. 2020*
- Active online community search. (supported by UGC, Bangladesh).
- Efficient election prediction from social media.

Teaching Experience

✓ **Micro-Credentials, Florida International University.**
Secondery Instructor. *May 2025- Present*
Artificial Intelligence in Crime Analysis and Detection (supported by DHS CINA).

✓ **Florida International University.**
Graduate Teaching Assistant, KFSCIS. *August 2022- Dec -2023*

✓ **Bangladesh University of Business and Technology (BUBT)**
Full-time Lecturer, Department of Computer Science and Engineering. *Dec. 2020 - July 2022*

✓ **University of Development Alternative (UODA)**
Part-time Lecturer, Department of Computer Science and Engineering. *May 2019 - Aug. 2019*

Research Interest

- Trustworthy and Safety of AI
- Security-aware of AI
- Machine Learning and Computer Vision
- Natural Language Processing
- Large Language Models
- Data Mining
- Computational Social Science and Social Network Analysis

Publications

Journal Papers:

1. **Badhan Chandra Das**, M. Hadi Amini, and Yanzhao Wu. "In-depth Analysis of Privacy Threats in Federated Learning for Medical Data." in IEEE Journal of Biomedical and Health Informatics (J-BHI) [Under Review].
2. **Badhan Chandra Das**, Yanzhao Wu, and M. Hadi Amini. "Efficient Gun Detection in Real-World Videos: Challenges and Solutions" in Elsevier Journal of Engineering Applications of Artificial Intelligence. [Under Review]
3. **Badhan Chandra Das**, M. Hadi Amini, and Yanzhao Wu. "Security and Privacy Challenges of Large Language Models: A Survey" in ACM Computing Surveys, 2025. (**IF: 28**).
4. Khandaker Mamun Ahmed, **Badhan Chandra Das**, Yasaman Saadati, M. Hadi Amini, "A Comprehensive Review of Artificial Intelligence and Machine Learning Methods for Modern Healthcare Systems", in Distributed Machine Learning and Computing: Theory and Applications (2024) **[Book Chapter]**.
5. Jubayer Al Mahmud, **Bandhan Chandra Das**, Jungpil Shin, Khan Md Hasib, Rifat Sadik, MF Mridha, "3D Gesture Recognition and Adaptation for Human–Robot Interaction," in IEEE Access, 2022.
6. **Badhan Chandra Das**, Md. Musfique Anwar, Md. Al-Amin Bhuiyan, Iqbal H. Sarker, Salem A. Alyami, and Mohammad Ali Moni. "Attribute Driven Temporal Active Online Community Search", in IEEE Access, 2021.

Conference Papers:

1. **Badhan Chandra Das**, M. Hadi Amini, and Yanzhao Wu. "System Prompt Extraction Attacks and Defenses in Large Language Models." arXiv preprint arXiv:2505.23817 (2025) [Under Review].
2. **Badhan Chandra Das**, Tasnim Jawad, Md Jueal Mia, M. Hadi Amini, and Yanzhao Wu. "Jailbreaking Large Vision Language Models in IEEE Intelligent Transportation Systems." in International Conference on Machine Learning and Applications (ICMLA-2025) [Accepted].
3. **Badhan Chandra Das**, M. Hadi Amini, and Yanzhao Wu. "Privacy Risks Analysis and Mitigation in Federated Learning for Medical Images" in IEEE International Conference on Bioinformatics and Biomedicine (BIBM-2023), Acceptance Rate: 19.7%.
4. Md. Mahbubur Rahman, **Badhan Chandra Das**, Al Amin Biswas, and Md. Musfique Anwar. "Predicting Participants' Performance in Programming Contests using Deep Learning Techniques." International Conference on Hybrid Intelligent Systems (HIS-2022).
5. Rafsun Jani, Md. Shariful Islam Shanto, **Badhan Chandra Das**, and Khan Md. Hasib. "Machine learning-based Social Media News Popularity Prediction." International Conference on Hybrid Intelligent Systems (HIS-2022).
6. Md. Jubier Ali, **Badhan Chandra Das**, Suman Saha, Al Amin Biswas and Partha Chakraborty. "A Comparative Study of Machine Learning Algorithms to Detect Cardiovascular Disease with Feature Selection Method", International Conference on Machine Intelligence and Data Science Application (MIDAS-2021).
7. **Badhan Chandra Das**, Md Musfique Anwar, Iqbal H. Sarker. "Reducing Social Media Users' Biases to Predict the Outcome of Australian Federal Election 2019", 7^{th} IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE-2020).
8. **Badhan Chandra Das**, Md. Musfique Anwar, "Attribute Driven Temporal Local Active Online Community Detection", 12^{th} IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM 2020), Acceptance Rate: 19.2%.
9. **Badhan Chandra Das**, Md. Musfique Anwar, Md. Al-Amin Bhuiyan. "Query Oriented Temporal Active Community Search", 9^{th} International Conference on Complex Networks and their Applications-2020.
10. **Badhan Chandra Das**, Md Shoaib Ahmed and Md Musfique Anwar, "Query-Oriented Active Community Search", Proceedings of International Joint Conference on Computational Intelligence.
11. **Badhan Chandra Das**, Md. Shoaib Ahmed and Md Musfique Anwar. "Location-based Temporal Sentiment Analysis to Predict Election Outcome.". IEEE International Symposium on Technology and Society (ISTAS-2020).

12. Md. Shoaib Ahmed, **Badhan Chandra Das** and Md Musfique Anwar. "Attribute-Driven Active Local Community Detection", International Conference on Innovation in Engineering and Technology (ICIET-2018).
13. **Badhan Chandra Das**, Md. Shoaib Ahmed and Md Musfique Anwar. "Attribute-Driven Active Community Search". 5^{th} International Conference on Networking, Systems and Security (NSysS 2018).

Teaching

✓ **Artificial Intelligence in Crime Analysis and Detection [FIU Microcedential]**
- Sencondary Instructor (Summer-2025)
- Designing lecture materials, organizing resources, and assessment rubrics.

✓ **Graduate Teaching Assistant, KFSCIS, FIU**
- Introduction to Artificial Intelligence (Spring 2025).
- Introduction to Deep Learning [Mentored K-12 teachers under NSF RET] (Summer 2023)
- Operating System (Spring 2023 and Fall 2023)

✓ **Guest Lectures, FIU**
- Foundation of Machine Learning, Break Through Tech (Summer-2025)
- Introduction to Artificial Intelligence (Fall-2025, Spring-2025, and Fall-2023)
- Advanced Topics in Machine Learning (Fall-2024)

✓ **Full-time Lecturer, Bangladesh University of Business and Technology (BUBT)**
- Data Mining Theory and Application (Spring-2021, Summer-2021, Fall-2021, Spring-2022, and Summer-2022)
- Machine Learning (Summer-2021 and Fall-2022)
- Database Systems (Fall-2021)
- Pattern Recognition (Summer-2022)
- Project Management and Professional Ethics (Summer-2021)
- Object-Oriented Programming with Java (Spring-2021 and Summer-2022)
- Advanced Software Development and Project (Spring-2021, Fall-2021, and Spring-2022)

✓ **Part-time Lecturer, University of Development Alternative**
- Web Development and Internet Technology. (Summer-2019)
- Numerical Analysis (Summer-2019)

Technical and Programming Skills

- **Programming Language:** Python, C, C++, Java, C#, R.
- **LLM Expertise:** Efficient Prompting, Deploying, and Fine-Tuning LLMs, Efficient Use of Huggingface Models and Datasets.
- **Machine Learning and Data Science:** PyTorch, Tensorflow, Keras, Scikit-learn, Networkx, Pandas, Numpy, Matplotlib, and Seaborn.
- **Technical Writing and Presentation:** Overleaf, Microsoft Office.
- **Training, Courses and Certificates:**
  - Red Teaming LLM Applications, *Deeplearning.AI*
  - Cybersecurity Awareness Training, *Florida International University*
  - LLMs-Nexus: Bridging Technical Innovation and Ethical Horizons, *Southern Illinois University Carbondale*
  - Applied Data Science Specialization from *coursera.org* offered by *University of Michigan, Ann Arbor.*

Awards, Grants, and Scholarships

1. University Graduate School Excellence Award *April. 2025*

FIU's Prestigious Award for Outstanding Paper or Manuscript in STEM.

2. Best Poster Award *April. 2025*

In the scholarly forum of FIU's Graduate Student Appreciation Week [3rd place].

3. Student Travel Grant *Nov. 2023*

NSF travel grant from International Conference on Bioinformatics and Biomedicine (BIBM-2023)

4. Conference Travel Grant *Aug. 2025, Nov. 2023*

From Graduate and Professional Student Committee (GPSC) at Florida International University.

3. **Student Travel Award** *2022-23*

From Bangladesh Sweden Trust Fund

6. **Developing Country Researcher Award** *Dec. 2020*

At 7^{th} IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE-2020), Gold Coast, Australia.

7. **Scholarship on Conference Registration** *Dec. 2020*

At IEEE CSDE/i-COSTE 2020 on the basis of research merit. Gold Coast, Australia.

8. **Special Research Grant from University Grants Commissions of Bangladesh (UGC)** *2019-20*

Project Title: Attribute Driven Active Local Community Detection.

Peer-Review Activities

- **Journals:**
  - IEEE Transactions on Information Forensics and Security (TIFS).
  - IEEE Transactions on Big Data (TBD).
  - ACM Transactions on Privacy and Security (TOPS).
  - Applied Artificial Intelligence (AAI), Taylor and Francis.
  - IEEE Transactions on Machine Learning in Communications and Networking (TMLCN).
  - Springer Journal of Supercomputing.
  - IEEE Access.
- **Conferences:**
  - International Conference on World Wide Web (WWW)
  - International Joint Conference on Artificial Intelligence (IJCAI)
  - International Conference on Learning Representations (ICLR)
  - IEEE International Conference on Distributed Computing Systems (ICDCS)
  - IEEE Asia-Pacific Conference on Computer Science and Data Engineering (IEEE CSDE),
  - International Conference on Machine Learning and Applications (ICMLA)
  - International Conference on Intelligent Computing and Systems at the Edge (ICEDGE)

Mentorship and Collaboration

- Mentored graduate students at FIU for research projects on VLM security and published a conference paper in International Conference on Machine Learning and Applications (ICMLA-2025) - Spring and Summer 2025.
- Mentored undergraduate students at BUBT, Bangladesh, and published a conference paper at Hybrid Intelligent Systems (HIS-2022)- Summer 2022.
- Collaborated on research with undergrad students and faculty at BUBT, and published a conference paper at International Conference on Machine Intelligence and Data Science Application (MIDAS-2021)- Summer 2021.

Selected Media Coverages

- Featured on KFSCIS social media for winning UGS excellence award for outstanding manuscript on the paper published in ACM Computing Survey (CSUR) - Spring 2025
- UGS-FIU social media spotlighting on the excellence award for outstanding manuscript and best poster award on FIU's Graduate Student Appreciation Week - Spring 2025

Leadership and Voluntary Activities

- Worked at Jahangirnagar University computer club (JU computer club) as General Secretary from August 2017 to August 2019.
- Organized and hosted several events and workshops introducing CS freshers to different research and industry technologies under the JU computer club.

Memberships.

- ACM Student Member.
- AAAI Student Member.