

# Mst Shapna Akter

✉ jannatul.shapna99@gmail.com

Google Scholar: <https://scholar.google.com/citations?user=PHg000cAAAAJhl=en>



## Employment History

- Current**     **Assistant Professor.** Oakland Univeristy. Auburn Hills, Michigan, USA. Oakland University, Michigan, USA.
1. Teach courses: CIS 4180/5180 Natural Language Processing ( Graduate level course), CSI 3680 Script Programming ( Undergrad level), CSI-8999-Doctoral Dissertation Research, CSI-5970 Independent Study.
  2. Supervise four PhD students in their thesis projects, guiding them to complete projects and prepare for publication; the team submitted two papers to the ICSME 2025 conference.
  3. Write grant proposals. Submitted three grant proposals, including NSF CRII, URC, and NASA MSGC grants.
  4. Serve on committees, including the Senate Budget Review Committee (SBRC) and CSE (UAC).
- 2024**     **Graduate Research Assistant.** University of West Florida, Pensacola, FL, USA.
1. Worked on projects funded by NSF and NIH in the field of machine learning, cyber security, software security, and health care.
  2. Worked on the NIH-funded STTR Phase-2 Project on HIPAA compliance checker for mhealth applications.

## Education

- 2024**     **Ph.D. Candidate in Intelligent Systems and Robotics, University of West Florida, USA.**  
CGPA : 3.89/4.00  
Thesis on "Integrated Machine Learning Framework for Mitigation of Buffer Overflow, Software Supply Chain, and Adversarial Attacks".
- 2021**     **B.Sc. in Computer Science, North South University**  
CGPA: 3.50 *Cum Laude Recipient, top 6% among all students.*  
Thesis on "Forecasting the risk factor of frontier markets: A novel stacking ensemble of neural network approach".

## In-person Presentation

- 2024**     **AI Research Lightning Talks at MICWIC 2024, Michigan, USA**
- i. An Integrated Machine Learning Framework for Software Security.
- Paper presentations at IEEE COMPSAC 2024, Osaka, Japan**
- i. Uncovering the Interpretation of Large Language Models.
  - ii. Quantum Adversarial Attacks: Developing the Quantum FGSM Algorithm.
  - iii. Mitigating Insecure Outputs in Large Language Models (LLMs): A Practical Educational Module.
  - iv. Enhancing HIPAA Compliance in AI-driven mHealth Device Security and Privacy.

## In-person Presentation (continued)



- 2023
- **Paper presentations at IEEE ICCIT 2023, Dhaka, Bangladesh**
    - i. Early Prediction of Cryptocurrency Price Decline: A Deep Learning Approach.
  - **Paper presentations at IEEE SERVICES 2023, Chicago, USA**
    - i. Exploring the Vulnerabilities of Machine Learning and Quantum Machine Learning to Adversarial Attacks Using a Malware Dataset: A Comparative Analysis.
  - **Paper presentations at IEEE Big Data 2023, Turin, Italy**
    - i. Autism Disease Detection Using Transfer Learning Techniques: Performance Comparison Between Central Processing Unit and Graphics Processing Unit Functions for Neural Networks.
    - ii. Feature Engineering-based Detection of Buffer Overflow Vulnerability in Source Code Using Neural Networks.
- 2022
- **Paper presentations at the International Conference on BigData2022, Osaka, Japan**
    - i. Multi-class Skin Cancer Classification Architecture Based on Deep Convolutional Neural Networks.
    - ii. Deep Learning Approach for Classifying Aggressive Comments on Social Media: Machine Translated Data vs Real Life Data.
    - iii. Software Supply Chain Vulnerability Detection in Source Code: Performance Comparison Between Traditional and Quantum Machine Learning Algorithms.
    - iv. Handwritten Word Recognition Using a Deep Learning Approach: A Novel Way of Generating Handwritten Words.
  - **Paper presentation on Cyber-Physical Systems at CNS 2022, Austin, Texas**
    - i. Towards Unsupervised Learning-based Denoising of Cyber-Physical System Data to Mitigate Security Concerns.







## Publications

### Journal Articles





- 1 Alfredo Cuzzocrea, Carmine Gallo, Mst Shapna Akter, and Hossain Shahriar. "Analysis and Experimental Comparison of State-Of-The-Art Deep-Learning Classification Techniques for Cyberbullying Detection". In: *Procedia Computer Science* 246 (2024), pp. 3800–3809.
- 2 Amrijit Biswas, Iftekhhar Ahmed Uday, KM Rahat, Mst Shapna Akter, and MRC Mahdy. "Forecasting the United State Dollar (USD)/Bangladeshi Taka (BDT) exchange rate with deep learning models: Inclusion of macroeconomic factors influencing the currency exchange rates". In: *Plos one* 18.2 (2023), e0279602.  
DOI: <https://doi.org/10.1371/journal.pone.0279602>.
- 3 Mst Shapna Akter, Hossain Shahriar, Reaz Chowdhury, and MRC Mahdy. "Forecasting the Risk Factor of Frontier Markets: A Novel Stacking Ensemble of Neural Network Approach". In: *Future Internet* 14.9 (2022), p. 252. DOI: <https://doi.org/10.3390/fi14090252>.
- 4 Deponker Sarker Depto, Shazidur Rahman, Md Mekayel Hosen, Mst Shapna Akter, Tamanna Rahman Reme, Aimon Rahman, Hasib Zunair, M Sohel Rahman, and MRC Mahdy. "Automatic Segmentation of Blood Cells from Microscopic Slides: A Comparative Analysis". In: *Tissue and Cell* 73 (2021), p. 101653.  
DOI: <https://doi.org/10.1016/j.tice.2021.101653>.

### Conference Proceedings

- 1 Mst Shapna Akter, Md Abdul Barek, Md Mostafizur Rahman, Abm Kamrul Islam Riad, Md Abdur Rahman, Md Raihan Mia, Hossain Shahriar, William Chu, and Sheikh Iqbal Ahamed. "HIPAA Technical Compliance Evaluation of Laravel-based mHealth Apps". In: *2024 IEEE International Conference on Digital Health (ICDH)*. IEEE. 2024. Pp. 58–67.
- 2 Mst Shapna Akter, Md Abdur Rahman, Md Mostafizur Rahman, Juanjose Rodriguez-Cardenas, Hossain Shahriar, Fan Wu, and Muhammad Rahman. "Authentic Learning Approach for Data Poisoning Vulnerability in LLMs". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 1504–1505.
- 3 Mst Shapna Akter, Hossain Shahriar, and Alfredo Cuzzocrea. "Towards analysis and interpretation of large language models for arithmetic reasoning". In: *2024 11th IEEE Swiss Conference on Data Science (SDS)*. IEEE. 2024. Pp. 267–270.
- 4 Mst Shapna Akter, Hossain Shahriar, Alfredo Cuzzocrea, and Fan Wu. "Quantum Adversarial Attacks: Developing Quantum FGSM Algorithm". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 1073–1079.
- 5 Mst Shapna Akter, Hossain Shahriar, Alfredo Cuzzocrea, and Fan Wu. "Uncovering the interpretation of large language models". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 1057–1066.
- 6 MD Abdul Barek, Md Mostafizur Rahman, Shapna Akter, ABM Kamrul Islam Riad, Md Abdur Rahman, Hossain Shahriar, Akond Rahman, and Fan Wu. "Mitigating Insecure Outputs in Large Language Models (LLMs): A Practical Educational Module". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 2424–2429.
- 7 Momotaz Begum, Mehedi Hasan Shuvo, Md Golam Mostofa, Abm Kamrul Islam Riad, Md Arabin Islam Talukder, Mst Shapna Akter, and Hossain Shahriar. "M-DBSCAN: Modified DBSCAN Clustering Algorithm for Detecting and Controlling Outliers". In: *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*. 2024. Pp. 1034–1035.
- 8 Md. Shazzad Hossain Shaon, Md. Fahim Sultan, Tasmin Karim, Md. Shoaib Hossain Alshan, Alfredo Cuzzocrea, and Mst Shapna Akter. "NeuroBooster: A Robust Classifier for the Discovery of Neuropeptide Sequences based on Meta-learning Approach". In: *2024 IEEE International Conference on Big Data (BigData)*. 2024. Pp. 6132–6141.  DOI: 10.1109/BigData62323.2024.10825409.
- 9 Md. Shazzad Hossain Shaon, Md. Fahim Sultan, Tasmin Karim, Alfredo Cuzzocrea, and Mst Shapna Akter. "An Advanced Liver Disease Detection Tool with a Stacking-Ensemble-based Machine Learning Approach". In: *2024 IEEE International Conference on Big Data (BigData)*. 2024. Pp. 6123–6131.  DOI: 10.1109/BigData62323.2024.10825884.
- 10 Emran Kaanan, Tasmin Karim, Md. Shazzad Hossain Shaon, Md. Fahim Sultan, Mst Shapna Akter, and Alfredo Cuzzocrea. "LLM-Based Approach for Buffer Overflow Detection in Source Code". In: *Proceedings of the 2024 27th International Conference on Computer and Information Technology (ICCIT)*. 2024. To appear.
- 11 Chase Lamkin, Mst Shapna Akter, Hossain Shahriar, and Guillermo Francia. "Architecture Design and Implementation of a Security Threat Data Sharing Platform". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 1502–1503.
- 12 Md Abdur Rahman, Mst Shapna Akter, Emily Miller, Bogdan Timofti, Hossain Shahriar, Mohammad Masum, and Fan Wu. "Fine-tuned Variational Quantum Classifiers for Cyber Attacks Detection based on Parameterized Quantum Circuits and Optimizers". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 1067–1072.
- 13 Md Mostafizur Rahman, MD Abdul Barek, Mst Shapna Akter, Abm Kamrul Islam Riad, Md Abdur Rahman, Hossain Shahriar, Akond Rahman, and Fan Wu. "Authentic Learning on DevOps Security with





- Labware: Git Hooks To Facilitate Automated Security Static Analysis". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 2418–2423.
- 14 ABM Kamrul Islam Riad, Md Abdul Barek, Md Mostafizur Rahman, Mst Shapna Akter, Tahia Islam, Md Abdur Rahman, Md Raihan Mia, Hossain Shahriar, Fan Wu, and Sheikh Iqbal Ahamed. "Enhancing HIPAA Compliance in AI-driven mHealth Devices Security and Privacy". In: *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2024. Pp. 2430–2435.
  - 15 Shahriyar Zaman Ridoy, Md. Shazzad Hossain Shaon, Alfredo Cuzzocrea, and Mst Shapna Akter. "En-Stack: An Ensemble Stacking Framework of Large Language Models for Enhanced Vulnerability Detection in Source Code". In: *2024 IEEE International Conference on Big Data (BigData)*. 2024. Pp. 6356–6364.  DOI: 10.1109/BigData62323.2024.10825609.
  - 16 Mst Shapna Akter, Nova Ahmed, and Hossain Shahriar. "Understanding Rural Women's Experience in STEM and Non-STEM Field in Bangladesh". In: *Proceedings of the 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), 26-30 June, Turin, Italy*. 2023. Pp. 1–10.  DOI: 10.1109/COMPSAC57700.2023.00159.
  - 17 Mst Shapna Akter, Juanjose Rodriguez Cardenas, Hossain Shahriar, Alfredo Cuzzocrea, and Fan Wu. "Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions". In: *Proceedings of the 2023 IEEE International Conference on Big Data (BigData), Dec 15-18, Sorrento, Italy*. IEEE. 2023. Pp. 1–10.
  - 18 Mst Shapna Akter, Hossain Shahriar, Sheikh Iqbal Ahamed, Kishor Datta Gupta, Muhammad Rahman, Atef Mohamed, Mohammad Rahman, Akond Rahman, and Fan Wu. "Case Study-Based Approach of Quantum Machine Learning in Cybersecurity: Quantum Support Vector Machine for Malware Classification and Protection". In: *Proceedings of the 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), 26-30 June, Turin, Italy*. 2023. Pp. 1–10.  DOI: 10.1109/COMPSAC57700.2023.00161.
  - 19 Mst Shapna Akter, Hossain Shahriar, and Zakirul Alam Bhuiya. "Automated Vulnerability Detection in Source Code Using Quantum Natural Language Processing". In: *Proceeding of the 3rd International Conference on Ubiquitous Security 2023 (UbiSec-2023), November 1–3, Exeter, UK*. Singapore, 2023. Pp. 1–10.  DOI: [https://doi.org/10.1007/978-981-99-0272-9\\_6](https://doi.org/10.1007/978-981-99-0272-9_6).
  - 20 Mst Shapna Akter, Hossain Shahriar, Juan Rodriguez Cardenas, Sheikh Iqbal Ahamed, and Alfredo Cuzzocrea. "Feature Engineering-Based Detection of Buffer Overflow Vulnerability in Source Code Using Neural Networks". In: *Proceedings of the 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), 26-30 June, Turin, Italy*. 2023. Pp. 1–10.  DOI: 10.1109/COMPSAC57700.2023.00106.
  - 21 Mst Shapna Akter, Hossain Shahriar, Juan Rodriguez Cardenas, Sheikh Iqbal Ahamed, and Alfredo Cuzzocrea. "Feature Engineering-Based Detection of Buffer Overflow Vulnerability in Source Code Using Neural Networks". In: *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. 2023. Pp. 765–776.
  - 22 Mst Shapna Akter, Hossain Shahriar, Juanjose Rodriguez Cardenas, Md Mostafizur Rahman, Akond Rahman, and Fan Wu. "Teaching DevOps Security Education with Hands-on Labware: Automated Detection of Security Weakness in Python". In: *Proceedings of the ISCAP Conference ISSN, Nov 1 - 4, Albuquerque, New Mexico*. 2023. Vol. 2473. Pp. 1–10.
  - 23 Mst Shapna Akter, Hossain Shahriar, and Alfredo Cuzzocrea. "Autism Disease Detection Using Transfer Learning Techniques: Performance Comparison Between Central Processing Unit vs Graphics Processing Unit Functions for Neural Networks". In: *Proceedings of the 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), 26-30 June, Turin, Italy*. 2023. Pp. 1–10.  DOI: 10.1109/COMPSAC57700.2023.00164.
  - 24 Mst Shapna Akter, Hossain Shahriar, Alfredo Cuzzocrea, Fan Wu, and Juanjose Rodriguez Cardenas. "A Trustable LSTM-Autoencoder Network for Cyberbullying Detection on Social Media Using Synthetic

Data". In: *Proceedings of the 2023 IEEE International Conference on Big Data (BigData), Dec 15-18, Sorrento, Italy*. IEEE. 2023. Pp. 1–10.

- 25 Mst Shapna Akter, Hossain Shahriar, Iysa Iqbal, MD Hossain, M.A. Karim, Victor Clincy, and Razvan Voicu. "Exploring the Vulnerabilities of Machine Learning and Quantum Machine Learning to Adversarial Attacks Using a Malware Dataset: A Comparative Analysis". In: *Proceedings of the 2023 IEEE International Conference on Software Services Engineering (SSE), June 2-8, Chicago, USA*. 2023. Pp. 1–10.  DOI: 10.1109/SSE60056.2023.00037.
- 26 Mst Shapna Akter, Hossain Shahriar, Dan Lo, Nazmus Sakib, Kai Qian, Michael Whitman, and Fan Wu. "Authentic Learning Approach for Artificial Intelligence Systems Security and Privacy". In: *Proceedings of the 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), 26-30 June, Turin, Italy*. 2023. Pp. 1–10.  DOI: 10.1109/COMPSAC57700.2023.00151.
- 27 Mst Shapna Akter, Hossain Shahriar, Md Abdur Rahman, Muhammad Rahman, and Alfredo Cuzzocrea. "Early Prediction of Cryptocurrency Price Decline: A Deep Learning Approach". In: *Proceedings of the 2023 26th International Conference on Computer and Information Technology (ICCIT), December 13-15, Cox's Bazar, Bangladesh*. IEEE. 2023. Pp. 1–6.
- 28 Mst Shapna Akter, Nafisa Anjum, Mohammad Masum, Hossain Shahriar, Nazmus Sakib, Akond Rahman, Fan Wu, and Alfredo Cuzzocrea. "Software Supply Chain Vulnerabilities Detection in Source Code: Performance Comparison between Traditional and Quantum Machine Learning Algorithms". In: *Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), December 17-20, Osaka, Japan*. 2022. Pp. 1–10.  DOI: 10.1109/BigData55660.2022.10020813.
- 29 Mst Shapna Akter and Hossain Shahriar. "Towards Unsupervised Learning based Denoising of Cyber Physical System Data to Mitigate Security Concerns". In: *Proceedings of the 2022 IEEE Conference on Communications and Network Security (CNS), 3-5 October, Austin, TX, USA*. 2022. Pp. 1–6.  DOI: 10.1109/CNS56114.2022.10044378.
- 30 Mst Shapna Akter, Hossain Shahriar, Nova Ahmed, and Alfredo Cuzzocrea. "Deep Learning Approach for Classifying the Aggressive Comments on Social Media: Machine Translated Data Vs Real Life Data". In: *Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), December 17-20, Osaka, Japan*. 2022. Pp. 1–10.  DOI: 10.1109/BigData55660.2022.10020249.
- 31 Mst Shapna Akter, Hossain Shahriar, Alfredo Cuzzocrea, Nova Ahmed, and Carson Leung. "Handwritten Word Recognition using Deep Learning Approach: A Novel Way of Generating Handwritten Words". In: *Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), December 17-20, Osaka, Japan*. 2022. Pp. 1–10.  DOI: 10.1109/BigData55660.2022.10021025.
- 32 Mst Shapna Akter, Hossain Shahriar, Sweta Sneha, and Alfredo Cuzzocrea. "Multi-class Skin Cancer Classification Architecture Based on Deep Convolutional Neural Network". In: *Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), December 17-20, Osaka, Japan*. 2022. Pp. 1–10.  DOI: 10.1109/BigData55660.2022.10020302.
- 33 Kumar Priyansh, Ritu Dimri, Fahim Islam Anik, Mst Shapna Akter, Nazmus Sakib, Hossain Shahriar, and Zakirul Alam Bhuiyan. "DuRBIN: A Comprehensive Approach to Analysis and Detection of Emerging Threats due to Network Intrusion". In: *Proceedings of the 2022 IEEE International Conference on Dependable, Autonomic and Secure Computing, September 12-15, Calabria, Italy*. IEEE. 2022. Pp. 1–8.  DOI: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927856.
- 34 Kazi Rumman Reswan Turjo, Partho Anthony D'Costa, Surjo Bhowmick, Asadullah Galib, Sami Raian, Mst Shapna Akte, Nova Ahmed, and MRC Mahdy. "Design of Low-Cost Smart Safety Vest for the Prevention of Physical Abuse and Sexual Harassment". In: *Proceedings of the 2021 24th International Conference on Computer and Information Technology (ICCIT), December 18-20, Dhaka, Bangladesh*. IEEE. 2021. Pp. 1–6.  DOI: <https://doi.org/10.1371/journal.pone.0279602>.



## Projects





- 2023  **Computer Vision Projects.**
- Developed microscopic segmented large scale data, submitted one conference to MICCAI 2025.
  - Computer vision project on hand gesture-based slide moving.
- 2022  **AI in Cybersecurity and Cybersecurity for AI.**
- Delivered webinar lecture in three modules.
  - Developed hands on module on adversarial attacks on AI-based systems.
  - Delivered lectures and hands-on demos in online webinars and faculty workshops.
-  **Health Insurance Portability and Accountability Act (HIPAA) checking for mobile health applications (Android and iOS)**
- Managed a team of 12 student researchers, including weekly team meetings and tracking progress on deliverables.
  - Collected data on HIPAA compliance violations for Laravel and Django-based health applications.
  - Conducted LLM-based query analysis and vulnerability checks using a customized pretrained model to automate and improve the accuracy of static analysis techniques.
  - Project main website (limited access available for user testing), with links to the LLM model code, dataset, etc.: <https://hipachecker.health/>.
-  **NSF Machine Learning in Cybersecurity Project (funded by the Secure and Trustworthy Computing program).**
- Developed hands-on modules on (i) Captcha bypassing, (ii) Intrusion detection, (iii) Malware classification, (iv) Website Phishing.
  - Delivered webinar lectures during Fall 2022, Spring 2023, Fall 2023, and Spring 2024; Participants were college / university professors and graduate / undergraduate students.
  - Updated hands-on modules and managed the project website (<https://sites.google.com/view/ml4cs/home?authuser=o>).
- QML in Cybersecurity**
- Developed quantum machine learning algorithms for software security.
  - Developed a Google site for hands-on modules.

## Skills

Languages  Python, R, Java, Android, Laravel, Ruby on Rails, PHP, C, C++, My-SQL, MSSQL, L<sup>A</sup>T<sub>E</sub>X, ...

## Miscellaneous Experience

### Awards and Achievements

- 2023  **Outstanding PhD Student - Research Award at KSU**
-  **Earned Dean's 4.0 Club recognition at KSU**
- 2022  **NSF Travel Grant (\$2000)**, to present an accepted paper at the ACM SIGAPP SAC 2024 conference.
-  **NSF Travel Grant (\$1200)**, to present an accepted paper at the IEEE Conference on Communications and Network Security, September 2022.

## Miscellaneous Experience (continued)

---

- **Graduate College Travel Grant (\$2000)**, to present an accepted paper at the IEEE Big Data 2022 conference.
- **First place in Computing Showcase at Kennesaw State University C-DAY 2022**, received \$600.



## Services

---

- 2025     ■ Guest Editor for the following Special Issues:
- "Applications of Natural Language Processing (NLP) in Software Security and Vulnerability Management" in the journal \*The International Journal of AI and Knowledge Engineering (IJAIKE)\*.
  - "Artificial Intelligence in Cybersecurity: Practices, Challenges, and Innovations" in the journal \*Electronics\* (Impact Factor: 2.6, CiteScore: 5.3).
- 2024     ■ Reviewer for the following journals:
- Expert Systems with Applications
  - MDPI Entropy
  - MDPI Sensors
  - CMES — Computer Modeling in Engineering & Sciences
  - Electronics
- Reviewer for the following conferences:
- IEEE COMPSAC 2024
  - IEEE SERVICES 2024
  - IEEE Big Data 2024

## Services (continued)

---

- 2023      Session Chair at IEEE Services 2023 (ICDH).  
Reviewer for the following conferences:
- IEEE COMPSAC 2023
  - IEEE SERVICES 2023
  - EMNLP 2023
  - IEEE Big Data 2023
  - ACM SAC 2024
- Reviewer for the following journals:
- IEEE Access
  - Security and Communication Networks (Hindawi)
  - Connection Science
  - IEEE Transactions on Network and Service Management
  - Expert Systems with Applications (Elsevier)
- 2022      Reviewer for SIGCSE TS 2023.  
Session Chair of Machine Learning at IEEE Big Data 2022.