Md Shahidur Rahaman

College Station, TX · mdshahidur_rahaman@tamu.edu · (254) 327-6044 · LinkedIn · GitHub · Google Scholar · Portfolio

Summary

PhD Candidate in Computer Science (GPA 4.0) at Texas A&M University specializing in end-to-end encrypted (E2EE) communication security, authentication ceremonies, and the security of machine learning and LLM systems. Author of 13 peer-reviewed publications (217 citations) spanning E2EE attacks and defenses, AI-driven identity verification, cloud-native security, and multimodal ML. Experienced in designing IRB-approved user studies, building attack and defense prototypes, and running LLM-based evaluation pipelines, backed by four years of industry software engineering in Germany and Bangladesh.

Skills

Programming	Python, Java, C++, JavaScript/TypeScript, SQL (Oracle, MSSQL, MongoDB)
Frameworks	PyTorch, TensorFlow, scikit-learn, Spring Boot, Spring Cloud, ASP.NET Core, Flutter
Security	End-to-End Encryption, Authentication Ceremonies, Device-Linking Protocols, SAS Protocols, OAuth2, TLS, WebAuthn/FIDO2, Threat Modeling, OWASP, Adversarial ML, LLM Security, Prompt Injection
ML/AI	LLM Evaluation and Red-Teaming, Open-Weight LLMs (Llama, Qwen), LLM-as-Judge Pipelines, Adversarial ML, NLP, Model Robustness, Trustworthy AI, CNN, XGBoost, LightGBM
Cloud/DevOps	Docker, Kubernetes, AWS, Jenkins, GitLab CI/CD, Kafka, RabbitMQ
Concepts	Distributed Systems, Microservices, API Design, Cryptographic Protocol Design, Secure System Design, Passkey Architecture, Empirical User Studies

Education

Texas A&M University, *PhD in Computer Science, GPA: 4.0* Jan 2024 – Present
College Station, TX | Advisor: Prof. Nitesh Saxena | Coursework: Network Security, Distributed Systems

Baylor University, *MS in Computer Science, GPA: 3.51* Aug 2021 – Dec 2023
Waco, TX | Coursework: Cybersecurity, Software Engineering, Advanced Algorithms

Military Institute of Science and Technology (MIST), *B.Sc. in Computer Science and Engineering, GPA: 3.54* Jan 2014 – Jan 2018
Dhaka, Bangladesh

Publications

Citations	h-index	i10-index	
217	**6**	**5**	(Google Scholar, All Time)

[1] M. S. Rahaman, N. Saxena. **Stress Testing Social Media Authentication Ceremonies of End-to-End Encrypted Messaging with Ephemeral Fake Accounts**. *International Conference on Information Security (ISC)*, 2026.

[2] A. T. Mahdad, M. S. Rahaman, N. Saxena. **TrackAR: AR/VR Device Fingerprinting and User-Device Pairing Detection via Shared Motion Sensor Data**. *ACM WiSec*, 2026.

[3] D. Amoroso d'Aragona, A. Bakhtin, X. Li, R. Su, . . . , M. S. Rahaman, M. Mäntylä, T. Černý, D. Taibi. **A Dataset of Microservices-Based Open-Source Projects**. *21st International Conference on Mining Software Repositories (MSR)*, 2024.

[4] M. Binte Rashid, M. S. Rahaman, P. Rivas. **Navigating the Multimodal Landscape: A Review on Integration of Text and Image Data in Machine Learning Architectures**. *Machine Learning and Knowledge Extraction*, 6(3):1545–1563, 2024.

[5] M. S. Rahaman, A. Islam, J. Orduz. **Quantune: An Automatic Music Generation Using Quantum Computing**. *Reports on Progress in Physics*, 2024.

[6] S. N. Tisha, M. S. Rahaman, P. Rivas. **A Comparative Evaluation of Image Caption Synthesis Using Deep Neural Network**. *Next Generation Data Science: Southwest Data Science Conference (SDSC), Springer LNCS*, 2024.

[7] M. S. Rahaman, A. Islam, T. Černý, S. Hutton. **Static-Analysis-Based Solutions to Security Challenges in Cloud-Native Systems**. *Sensors*, 23(4):1755, 2023.

[8] M. S. Rahaman, S. N. Tisha, E. Song, T. Černý. **Access Control Design Practice and Solutions in Cloud-Native Architecture: A Systematic Mapping Study**. *Sensors*, 23(7):3413, 2023.

[9] M. Rahman, M. S. Rahaman, M. S. H. Chy. **Bless: An Interactive Application to Show Gratitude**

towards Doctors. *IEEE 11th International Conference on Serious Games and Applications for Health (ICHI)*, 2023.

[10] M. Rahman, M. S. H. Chy, A. Rahman, S. Ahmed, T. Sharmin, M. S. Rahaman. **Exploring Chromatin Interaction Between Two Human Cell Types and Different Normalization Techniques for HI-C Data**. *27th International Computer Science and Engineering Conference (ICSEC)*, 2023.

[11] M. Ishak, M. S. Rahaman, T. Mahmud. **FarmEasy: An Intelligent Platform to Empower Crops Prediction and Crops Marketing**. *13th International Conference on Information and Communication Technology and System (ICCIT)*, 2021.

[12] M. S. Rahaman, N. R. Oyshee, S. A. Pratik, K. A. Al Mamun. **Developing an mHealth Application to Empower Community Health Service for Married Couple: Challenges and Opportunities**. *4th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT)*, 2018.

[13] M. S. Rahaman, N. R. Oyshee, S. A. Pratic, K. A. Al Mamun. **Development of an Intelligent Platform to Digitize Marriage, Empower Married Couple for Life and Family Wellbeing Towards Digital Bangladesh**. *21st International Conference of Computer and Information Technology (ICCIT)*, 2018.

Papers Under Review

[1] M. S. Rahaman, N. Saxena. **Inaccessibility-Triggered Security Vulnerabilities in QR Code-Based Device Linking and Browser Syncing**.

[2] M. S. Rahaman, A. T. Mahdad, N. Saxena. **When Seeing Deceives: Compromising Multi-Device Linking in End-to-End Encrypted Messaging**.

[3] M. S. Rahaman, N. Saxena. **Impersonating Zoom's E2EE-Protected Static Media and Textual Communications via Voice Scrambling: Design and User Study**.

Academic Experience

Graduate Research Assistant, *Texas A&M University, College Station, TX* Jan 2024 – Present

- Stress-tested social-media-based authentication ceremonies in E2EE messaging, showing that ephemeral fake accounts can compromise identity verification; work accepted at ISC 2026.
- Leading an ongoing study of AI-mediated conversational leakage: whether an LLM summarization assistant, shown only one participant's view of a group chat, can infer messages it was never given. Built a targeted-query attack pipeline (Llama-3.1-8B attacker, Qwen2.5-7B judge) evaluated on Supreme Court oral-argument transcripts and Reddit ChangeMyView threads.
- Designed and conducted empirical user studies on E2EE device-linking attacks, achieving over 90% attacker success rate across 30 participants under live attack conditions.
- Built and evaluated Passkey-Anchored Linking (PAL), a FIDO2/WebAuthn-based defense replacing replayable QR codes with hardware-backed passkeys, a keyed and sealed BLE proximity channel, and mutual authentication.
- Developed Voice-Zeus, a ceremony-level impersonation attack on Zoom E2EE via voice reordering (MCD = 0 by construction), confirmed in an IRB-approved 300-trial user study with 76.9% attack success rate.
- Implemented two malware variants targeting browser syncing accessibility failures, confirming evasion of eight major antivirus products on Windows 10 and 11.
- Designed SIVAI, a hybrid agentic AI system (XGBoost + GPT-4) achieving 0.9958 AUC and 95.6% accuracy across 2,576 real-world accounts.
- Built EPAS, a secure LLM execution framework with network isolation, memory integrity validation, and policy enforcement against inference-layer attacks.

Graduate Research Assistant, *Baylor University, Waco, TX* Jan 2023 – Dec 2023

- Trained and fine-tuned LLaMA on 50,000 network packet traces for automated anomaly detection, improving accuracy by 18% over baseline.
- Optimized preprocessing pipelines, reducing data handling time from 3.5 hours to 1.2 hours (65% faster).
- Directed a cybersecurity education project for 110+ students, improving secure coding performance by 25%.

Graduate Teaching Assistant, *Baylor University, Waco, TX* Aug 2021 – Dec 2022

- Managed 12 software engineering lab projects (72 students) as Scrum Master, applying Agile methodologies.
- Mentored students in lab sessions, providing technical support and encouraging growth in software engineering.

Selected Projects

AI Leakage Study	Ongoing study of privacy leakage from AI assistants in E2EE group chats: a targeted-query attack (open-weight LLM attacker with an LLM judge) measures what an assistant can infer about non-consenting participants' messages; addresses a gap explicitly left open in prior E2EE-and-AI policy work.
SocFakeID	Stress test of social-media-based authentication ceremonies in E2EE messaging using ephemeral fake accounts (ISC 2026).
FORTRESS	Multi-boundary trust framework for E2EE messaging (DARPA Direct to Phase II proposal) covering Human-Application, Application-Device/Network, and Application-Service attack surfaces.
PAL	Passkey-Anchored Linking: FIDO2/WebAuthn device enrollment replacing QR bearer tokens with hardware-backed passkeys and BLE proximity gating.
Voice-Zeus	Ceremony-level impersonation attack on Zoom E2EE via voice reordering; MCD = 0, undetectable by synthesis-based classifiers. [Demo]
CFA	Ceremony-First Admission: secure group messaging protocol binding human identity verification to cryptographic group admission.
SASLinker	E2EE device-linking prototype with SAS-based Short Authentication String verification. [GitHub]
SIVAI	Hybrid agentic AI system (XGBoost + GPT-4) for social identity verification, achieving 0.9958 AUC.
Cloudalyze	Static/dynamic analysis pipeline for cloud-native security research. [GitHub]

Industry Experience

Software Engineer, *BASIS Europe GmbH, Germany* Dec 2020 – Jul 2021

- Implemented OAuth2/SAML authentication for enterprise car-management system, meeting EU compliance and cutting onboarding friction.
- Automated onboarding pipelines, reducing manual work by 53% and enabling scale to thousands of clients.
- Deployed containerized microservices (Docker/Kubernetes) to improve scalability and reduce production downtime.
- Integrated end-to-end encrypted APIs across cross-functional teams, strengthening enterprise data protection.

Senior Officer (Software), *Dutch Bangla Bank, Bangladesh* Mar 2019 – Nov 2020

- Developed a debit card API serving 3M+ customers, reducing latency by 20%.
- Led migration from SOAP to REST APIs, modernizing infrastructure and lowering maintenance costs.
- Enhanced fraud detection modules by integrating real-time monitoring and logging pipelines.
- Conducted performance benchmarking and optimization of transaction systems supporting millions of concurrent requests.

Software Engineer, *Southtech Ltd., Bangladesh* Mar 2018 – Feb 2019

- Designed ASP.NET Core systems for Ascend Finance, serving 100K+ users with strong scalability demands.
- Refactored scheduling algorithms, achieving 65% efficiency gains and reducing manual interventions.
- Implemented role-based access control (RBAC) and secure APIs aligned with OWASP security guidelines.

Student Supervision & Mentoring

[7] Patrick Boyle [B.Sc. Undergraduate Capstone Research] Fall, 2023
Baylor University, Waco, TX, USA

[6] Francis Boyle [B.Sc. Undergraduate Capstone Research] Fall, 2023
Baylor University, Waco, TX, USA

[5] Tahasin Mahmud [B.Sc. Undergraduate Student, Independent Research] Spring, 2021
Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

[4] Md Ishak [B.Sc. Undergraduate Student, Independent Research] Spring, 2021
Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

[3] Shafiqul Alam Shawon [B.Sc. in CSE Final Year Thesis] Spring – Fall, 2018
Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

[2] Syed Abdullah [B.Sc. in CSE Final Year Thesis] Spring – Fall, 2018
Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

[1] Shoab-ur-Rashid Mollah [B.Sc. in CSE Final Year Thesis] Spring – Fall, 2018
Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

Leadership & Awards

Dean's List, Military Institute of Science and Technology (MIST)	2017
Dean's List, Military Institute of Science and Technology (MIST)	2016
General Secretary, Bangladesh Student Association (70+ members), Baylor University	2022
General Secretary, Cricket Club (120+ members), Baylor University	2023

Research Interests

End-to-End Encryption | Authentication Protocols | ML/LLM Security | AI and Privacy in Secure Messaging | Device-Linking Security | Accessibility & Security | AR/VR Privacy | Cryptographic Protocol Design | Secure Systems