MAHFUZUL NISSAN

Cybersecurity Engineer | AI/ML Security Researcher

San Antonio, TX (Open to Relocation) | U.S. Work Authorization: **Unrestricted (*No Sponsorship Required)***

minissan@outlook.com | minissan.github.io | github.com/minissan | linkedin.com/in/minissan | Google Scholar

PROFESSIONAL SUMMARY

Cybersecurity Engineer and Researcher with experience securing national critical infrastructure (airports, metro rail) and web application security. Specializes in AI/ML-driven threat detection, reverse engineering, digital forensics, and database security. Built `ANOC`, a generalized NoSQL database carving tool, and `RADAR`, a tamper-resilient framework for detecting unauthorized data operations. Developed ML methods to reverse-engineer SQL queries from process memory and LLM-based insider-threat detection on audit logs. Delivered NSF and Louisiana Board of Regents funded security solutions with engineering-grade validation across real-world systems.

TECHNICAL SKILLS

Security/DFIR: Memory Forensics, Intrusion Detection, Incident Investigation, Log Analysis, Vulnerability Assessment, Artifact Recovery, Penetration Testing
Cybersecurity Tools: Wireshark, Volatility, Burp Suite, Nessus, Nmap, Metasploit, IDA Pro, YARA, Ghidra
Programming & DevOps: Python, C/C++, Java, Bash, Linux, Git, Docker, CI/CD, JSON/BSON
AI & Big Data: PyTorch, TensorFlow, Scikit-learn, Pandas, NumPy, Apache Spark, Hadoop
Databases: SQL: MySQL, PostgreSQL, Oracle, SQLite; NoSQL: MongoDB, Berkeley DB, LMDB, ZODB, etcd, MDBX, Durus, LiteDB, RavenDB, Realm, Nitrite
Web & Mobile: JavaScript, PHP, HTML, CSS, Android

EXPERIENCE

Doctoral Researcher — AI/ML Security Engineering | UNO Cyber Center Jan 2021 – Present
University of New Orleans, Department of Computer Science New Orleans, LA, USA

- **Security Tool Development (ANOC & RADAR):** Engineered ANOC (Generalized NoSQL Carver) and RADAR (Audit Reconciliation) to recover active/deleted/modified records and flag unauthorized operations by correlating recovered artifacts with audit logs, without relying on database APIs; validated across **10 NoSQL databases**, achieving **487 MB/min** processing throughput.
- **AI/ML Memory Forensics:** Developed an ML model that reverse-engineers executed SQL queries directly from process memory with >**90% accuracy**, enabling post-incident analysis even when logging is disabled.
- **Insider Threat Detection:** Developed LLM-based methods to correlate system/application logs with user-action audit events for insider-threat detection, achieving >**95% accuracy** on the CERT dataset
- **Technical Validation:** Published and presented results at security conferences; produced reproducible benchmarks, evidence reports, and visuals.

Instructor of Record | Software Design & Development; Intro. to Computers Jan 2024 – Present
University of New Orleans New Orleans, LA, USA

- Designed and delivered project-based courses emphasizing secure coding, debugging, version control, fundamental computing concepts, and clear technical documentation

Information Security Engineer Mar 2017 – Dec 2020
Nippon Koei Co., Ltd. Dhaka, Bangladesh

- Designed and implemented network architecture and access control policies for national infrastructure projects (airport and metro rail), improving resilience and reducing reported security incidents by 40%
- Introduced the company's first file security framework, reducing unauthorized data exposure by 50% and establishing standards for confidentiality and compliance
- Developed network & security documentation including architecture diagrams, access control policies, and change-control records to support operations, maintainability, and review

Software Engineer Intern Jul 2016 – Dec 2016
Webway E Services Sdn. Bhd. Kuala Lumpur, Malaysia

- Built and deployed client web applications, including the official company site, improving average page load speed by 25% through performance tuning and front-end optimization
- Addressed web security issues and reduced reported bugs by 35% through systematic testing and fixes

Tutor (C/C++ Programming) 2014 – 2016
International Islamic University Malaysia Kuala Lumpur, Malaysia

- Tutored undergraduate students in C/C++

CERTIFICATIONS

- CompTIA Security+ (SY0-701) — Exam Scheduled: January 25, 2026

KEY TECHNICAL PROJECTS

- **Big Data Intrusion Detection:** Built a PySpark-based feature pipeline and trained deep-learning IDS models on CIC-IDS2017 and CIC-DDoS2019; achieved >93% accuracy.
- **Autonomous System Anomaly Detection:** Simulated robotic telemetry in CoppeliaSim and developed autoencoder-based anomaly detection models; achieved >94% accuracy.
- **Vulnerability Assessment:** Performed assessments using Nessus, Nmap, Burp Suite, and Metasploit; delivered prioritized remediation recommendations.
- **Volatile Memory Analysis:** Used Volatility to analyze memory images and extract process/network artifacts for incident investigations.

SELECTED PUBLICATIONS

- Nissan, M.I., Wagner, J., Rasin, A. "ANOC: Automated NoSQL Database Carver." DFRWS USA 2025
- Nissan, M.I., Wagner, J., Aktar, S. "Database Memory Forensics: A Machine Learning Approach to Reverse-Engineer Query Activity." DFRWS EU 2023
- Wagner, J., Nissan, M.I., Rasin, A. "Database Memory Forensics: Identifying Repeatable Cache Patterns for Log Verification." DFRWS USA 2023

EDUCATION

Ph.D., Engineering & Applied Science – Computer Science (GPA: 4.0/4.0) Jan 2021 – Present
All but Dissertation (ABD)
University of New Orleans New Orleans, LA, USA
Focus: Cybersecurity, Machine Learning, Digital Forensics, Database Security

M.Sc., Computer Science (GPA: 4.0/4.0) Jan 2021 – Dec 2022
University of New Orleans New Orleans, LA, USA
Thesis: Analysis of Forensic Artifacts in Database Memory using Support Vector Machine

Graduate Certificate, Machine Learning & Artificial Intelligence (Grade: 4.0/4.0) May 2023
University of New Orleans New Orleans, LA, USA

B.Sc., Computer Science Feb 2013 – Feb 2017
International Islamic University Malaysia Kuala Lumpur, Malaysia
Final Year Project: Exploring Juju & Packaging of Services in Cloud Environment

HONORS & AWARDS

- Phi Kappa Phi Graduate Research Grant: $1,500 (2024)
- Fully Funded Ph.D. Scholarship, University of New Orleans (2021–2026)
- DFRWS EU Conference Scholarship, Bonn, Germany (2023)
- WiCyS Conference Scholarship, Cleveland, OH, USA (2022)
- Louisiana Board of Regents Travel Grant (2022, 2025)
- Phi Kappa Phi Honor Society (top 10% of students, UNO) & UNO Honors Day Recognition (2024)
- Dean's List & Full Tuition Scholarship, International Islamic University Malaysia (2013–2017)

COMPETITIONS

- 3rd Place (of 15 teams): Digital Forensics Rodeo Challenge, DFRWS USA (2024)
- ACM-ICPC Malaysia National Programming Contest, top 3 team from IIUM (2013–2014)

LEADERSHIP & ACTIVITIES

- Technical Program Committee (TPC) member, DFRWS EU (2025, 2026)
- Reviewer: Journals – *Computers & Security*; *FSI: Digital Investigation*; Conference – *ACM CIKM* (2022)
- Organizing Committee & Volunteer Coordinator, DFRWS USA (2024)
- Judge: InnovateUNO (Spring & Fall 2023, Fall 2024); CS Symposium, St. Mary's University (Spring 2025)
- Talks & Posters: DFRWS USA (2024, 2025); DFRWS EU (2023); InnovateUNO (Fall 2021, Spring & Fall 2023)
- Vice President (2022–2023) & Public Relations Officer (2021–2022), Bangladesh Student Association (BSA UNO); secured $9,500 funding; organization awarded *"Outstanding Student Organization of the Year"* (2023)
- Organized International Mother Language Day 2023 (200 attendees) as BSA Vice President
- Volunteer: SUCbAUF Crawfish Boil (2022, 2023); New Student Orientation (Fall 2021), UNO