Md Mahfuj Hossain

AI & CTI Researcher | Prompt Engineer | Independent IT Consultant | Applied AI & LLM

WP. Kuala Lumpur, Federal Territory of Kuala Lumpur, Malaysia

Summary

I work at the intersection of AI and cybersecurity, mainly around making LLM outputs more reliable for threat intelligence workflows. My current research at UTeM (MSc in ICT, Cyber Forensics track) is on a framework called CTI-Shield. It is an 8-agent pipeline that uses local LLMs like Qwen3 and Hermes to collect threat data, extract indicators of compromise, and triage incidents without sending anything to external APIs. The core problem I am trying to solve: LLMs hallucinate, and in a SOC environment, a fabricated CVE or a wrong TTP mapping can cause real damage.

Before the research side, I spent several years doing IT infrastructure work. Active Directory, Windows and Linux servers, Cisco and MikroTik networking, endpoint management. That background is why I gravitate toward the operational side of security rather than just the theoretical.

What I spend most of my time on now: Building and testing RAG pipelines that ground LLM outputs in MITRE ATT&CK data and live OSINT feeds; Prompt engineering for structured security outputs (STIX 2.1 compliance, IOC extraction); SIEM configuration and rule writing in Wazuh and Splunk; Python scripting for security automation and data processing; Multi-agent system design for autonomous threat detection

Research title: "A Lifecycle-Wide Evaluation & Mitigation Framework for Trustworthy AI in Cyber Threat Intelligence"

I am looking for roles in cybersecurity analysis, threat intelligence, SIEM engineering, or applied AI for security. If your team works on any of these problems, I would be glad to talk.

mahfujdev@gmail.com

Contact

01161169434 (Mobile) hossainmahfuj@gmail.com www.linkedin.com/in/mahfujdev (LinkedIn)

Top Skills

TypeScript Cascading Style Sheets (CSS) React.js

Languages

English (Professional Working)

Certifications

Customer Service Foundations; Customer Service: Problem-Solving and Troubleshooting; Cybersecurity Audit and Assessment; Fundamentals for GRC Analysts: From Vendor Risk to Incident Coordination; Data-Driven Decision-Making for Business Professionals; Windows 10 for IT Support: Advanced Troubleshooting

Experience

MediaBrust — Information Technology Analyst

July 2022 - Present (4 years 1 month) United Kingdom

Managed IT infrastructure and security operations for a UK-based digital services firm. Built and maintained Windows Server environments with Active Directory, Group Policy, and DNS. Configured MikroTik and Cisco routers, set up VPNs, and handled firewall rule management across client networks.

Ran Wazuh-based SIEM monitoring for log analysis and threat detection. Wrote Python scripts to automate patch deployment, user provisioning, and system health checks. Handled incident triage when alerts came in, tracked them through resolution, and documented findings for the team.

On the AI side, started building internal tools using LLMs for automated report generation and log summarization. This work directly fed into my current research on applying AI to cyber threat intelligence workflows.

La Finesse — Information Technology Support Specialist

2019 - Present (7 years) Switzerland

Provided remote IT support for a Swiss-based firm handling system administration across Windows and Linux environments. Set up and maintained Active Directory, managed user accounts, and enforced group policy configurations for distributed teams.

Monitored network traffic and responded to security alerts using open-source SIEM tools. Handled VPN configuration, firewall management, and endpoint security across remote workstations. Created technical documentation for IT procedures and security protocols.

Built automation scripts in PowerShell and Bash to streamline repetitive IT tasks, cutting manual work on monthly access reviews and software deployments.

Novi Frozen Food, Kafe and Clothing — Technical Support Assistant

December 2022 - Present (3 years 8 months) Shah Alam

Handled day-to-day IT operations for a multi-location retail business. Deployed and configured POS terminals, network switches, and CCTV security systems across three sites. Set up and maintained local network infrastructure including routers, access points, and NAS storage.

Ran regular vulnerability scans on business systems and applied security patches on a monthly cycle. Managed endpoint protection and access control policies for staff devices. Maintained documentation for IT asset inventory and incident logs.

Gained hands-on experience with firewall configuration, network segmentation for PCI compliance, and basic SIEM log review to identify suspicious traffic patterns.

EXPAT SERVICES (KUALA LUMPUR) SDN BHD — Information Technology Technical Support

July 2025 - December 2025 (6 months) Federal Territory of Kuala Lumpur, Malaysia

Supported 200+ users across a managed services environment, handling L1 and L2 ticket escalations for network, hardware, and software issues. Worked with Active Directory for user provisioning, group policy enforcement, and password resets across a multi-domain setup.

Configured and troubleshot Cisco switches, MikroTik routers, and Ubiquiti access points. Managed endpoint security with Symantec and Windows Defender ATP. Monitored network health using PRTG and responded to alerts for bandwidth anomalies and unauthorized device connections.

Documented all incidents in ServiceNow, tracked resolution metrics, and contributed to the monthly security posture reports for management review.

Applied Materials Limited — Information Technology Support Assistant

January 2018 - July 2022 (4 years 7 months) Dhaka, Bangladesh

Provided hardware and software support in a semiconductor manufacturing environment. Diagnosed and repaired workstations, servers, and peripheral equipment across production and office areas. Managed IT inventory and tracked assets through the company's ticketing system.

Supported Windows and Linux systems, handled user account management in Active Directory, and assisted with network troubleshooting for LAN/WAN connectivity issues. Ran basic security checks on endpoints and escalated suspicious activity to the senior IT team.

csbf — Information Technology Coordinator

October 2019 - 2020 (1 year)

Unified IT infrastructure to ensure the full implementation of network security, enabling not only one to stay ahead of the cyber threats but also providing a more secure environment. Spearhead various data security team members for overall cyber hygiene enhancement with minimum risk associated with data exposure.

Enzenius Consultancy Services Ltd — Information Technology Support Assistant

January 2019 - September 2019 (9 months) Uttara, Dhaka, Bangladesh

Provided technical support to maintain the company's secure systems; enforced network security rules. Contributed to IT infrastructure troubleshooting and to cyber resilience by identifying possible system vulnerabilities.

Eco Travels New Zealand — Technical Support Assistant

January 2019 - September 2019 (9 months) New Zealand

Provided remote technical support by troubleshooting in software and hardware using data integrity measures. Configured and secured digital platforms, following the standard security protocols.

Universe IT Ltd. — Internation Call Center Agent

January 2014 - December 2015 (2 years) Uttara, Dhaka, Bangladesh

Responsibilities

Collected client information through phone calls, interviews, and verification processes.

Assessed client eligibility by comparing gathered data against established requirements.

Established policies by inputting client details and confirming pricing structures.

Provided clear communication to clients by explaining procedures, answering inquiries, and offering relevant information.

Reported equipment issues to ensure smooth operation of communication tools.

Maintained service quality by following established standards and suggesting process improvements.

Kept knowledge up-to-date by reviewing product updates and engaging in training opportunities.

Supported sales and organizational goals by completing related tasks and contributing to overall success.

Education

Universiti Teknikal Malaysia Melaka

Master of Technology - MTech, Cyber/Computer Forensics and Counterterrorism · (December 2025 - January 2027)

Lincoln University College

Bachelor's degree, Information Technology · (November 2022 - March 2025)

Shahzadpur Government College

Associate of Science - AS · (January 2011 - August 2013)