



Md Shahin Alam

Nationality: Bangladeshi **Date of birth:** 26/09/2001

Phone number: (+880) 1959026543

Email address: mshahinalam.cs@gmail.com

LinkedIn: <https://www.linkedin.com/in/uchihashahin>

ACERGION: <https://acergion.github.io>

Home: Surma Vaban, Red Crescent Society, House-1, Road-5, Block-G, Mirpur-1, 1216
Dhaka (Bangladesh)

ABOUT ME

M.Sc. in Cyber Security graduate and proactive Security Analyst with hands-on experience in SOC monitoring, log analysis, and Vulnerability Assessment & Penetration Testing (VAPT). As a competitive security researcher, I lead the CTF team 'ACERGION' (Ranked **1st in Bangladesh** on CTFtime in 2025), demonstrating advanced practical skills in identifying and exploiting complex vulnerabilities. Proficient in SIEM implementation, Linux administration, and leveraging frameworks like MITRE ATT&CK and OWASP Top 10. Equipped with dedicated SOC lab training, I am ready to deliver immediate value in threat hunting and securing enterprise networks.

EDUCATION AND TRAINING

Master of Science in Cyber Security

Asia Pacific University of Technology & Innovation (APU) [03/02/2025 – 09/02/2026]

City: Kuala Lumpur | Country: Malaysia | Website: <https://www.apu.edu.my/>

ELITE Live SOC Module (ESOL) – 50 Lab Hours

Tecforte / Asia Pacific University (APU) [22/02/2025 – 22/06/2025]

City: Kuala Lumpur | Country: Malaysia | Website: <https://www.tecforte.com/>

- Completed 50 hours of intensive, hands-on enterprise SOC operations training.
- Gained practical proficiency in continuous network traffic monitoring, SIEM alert validation, and incident response.

B. Sc. in Computer Science and Engineering

Daffodil International University [01/01/2020 – 01/01/2024]

City: Dhaka | Country: Bangladesh | Website: <https://daffodilvarsity.edu.bd/> | Final grade: CGPA 3.82

Higher Secondary Certificate (HSC)

Rajuk Uttara Model College [01/06/2017 – 01/06/2019]

City: Dhaka | Country: Bangladesh | Website: <http://www.rajukcollege.edu.bd/> | Field(s) of study: Science | Final grade: GPA 5

WORK EXPERIENCE

Simec System Ltd. – Dhaka, Bangladesh

Blockchain Trainer

[01/06/2023 – 01/01/2024]

- Conducted training sessions on blockchain technology for professionals and students.
- Designed course materials, presentations, and hands-on projects.
- Guided learners in applying blockchain concepts to real-world use cases.
- Assessed participants' progress and provided constructive feedback.
- Updated training modules with the latest blockchain advancements.

SKILLS

Capture the Flag (CTF)

Reverse Engineering / Binary Exploitation / Cryptography / Web Exploitation / OSINT

Cyber Security & Frameworks

SOC Operations / VAPT / Incident Response / OWASP Top 10 / MITRE ATT&CK

Programming & OS

Python / Solidity / Java / Javascript / C / Bash / Linux Administration

Network Security

TCP/IP Protocols / Firewalls / IDS/IPS / Network Traffic Analysis

Tools & Forensics

Wireshark / Autopsy / Burp Suite / Wazuh (SIEM) / theHarvester / Log Analysis

PROJECTS

[28/12/2025 – Current]

Kernel-Watch: Real-Time Linux Threat Detection Using eBPF and AI

- Developed a system-level defense framework focusing on real-time memory integrity and protection against unauthorized kernel modifications.
- Implemented AI-driven intrusion detection logic to recognize complex attack vectors and zero-day kernel exploits.
- Achieved low-latency monitoring capabilities, enabling immediate automated mitigation of detected security threats.

[01/02/2026 – Current]

ThreatTriage: Automated SOC Alert & Log Analysis Engine

- Developed a Python-based automation utility to ingest, parse, and analyze enterprise log formats, specifically targeting syslog, HTTP logs, and DB logs for malicious activity.
- Integrated Threat Intelligence APIs (e.g., VirusTotal, AlienVault) to automatically validate SIEM alerts, effectively differentiating false positives from confirmed threats.
- Generated structured incident response reports that map detected anomalies to the MITRE ATT&CK framework, streamlining day-to-day SOC operations.

[15/01/2026 – 15/02/2026]

Auto-VAPT: CI/CD Integrated Vulnerability Assessment Scanner

- Engineered an automated Vulnerability Assessment and Penetration Testing (VAPT) pipeline to systematically identify OWASP Top 10 flaws in web applications.
- Automated the execution of offensive security workflows using Python and Bash, simulating real-world attack vectors to test network defense mechanisms.
- Designed comprehensive mitigation reports detailing identified vulnerabilities, risk levels, and remediation steps tailored for secure financial infrastructure compliance.

HONOURS AND AWARDS

[31/12/2025] CTFtime

1st Place National Rank - CTF 2025 Led team "ACERGION" to achieve the #1 national ranking in Bangladesh and #169 globally on CTFtime for the year 2025, demonstrating elite skills in practical cybersecurity challenges, vulnerability assessment, and offensive security operations.

Link: <https://ctftime.org/team/175853>

[28/12/2025] ASIS CTF

ASIS CTF Finals 2025

Rank: 14/476

Rating Weight: 100

[30/12/2025] Technical University of Munich

hxp 39C3 CTF

Rank: 29/263

Rating Weight: 98.14

[10/11/2025] Infobahn

Infobahn CTF 2025

Rank: 11/803

Rating Weight: 25

I hereby declare that the information provided in this CV is true and accurate to the best of my knowledge. I am eager to contribute my skills and experience to your organization and look forward to the opportunity to discuss my application further.

Md Shahin Alam

Dhaka, 19/02/2026

Md Shahin Alam