Mohiuddin Ahmed | Portfolio | GitHub | LinkedIn | Google Scholar

Melbourne, FL (Open to Relocation) | sohel.buet.cse.07@gmail.com | +19802670371 | Visa Status: **Permanent Resident**

Education

- **Ph.D.** in Computing and Information Systems | University of North Carolina at Charlotte, NC, USA. [Aug 2016 - Mar 2024]
- **BSc** in Computer Science and Engineering | Bangladesh University of Engineering and Technology, BD. [Jan 2008 - Feb 2013]

Professional Experiences

- **Research Assistant** | University of North Carolina at Charlotte, NC, USA. [Aug 2016 - Apr 2024]
  - ◇ Developed security analytics for distributed threat hunting and automated critical security control enforcement assessment.
- **Team Lead, Software Engineer** | Kona Software Lab Ltd, Dhaka, Bangladesh. [Jan 2016 - June 2016]
  - ◇ Led a team of software developers to build PKI system using *Java, C++, OpenSSL, MySQL, CMake, and Gradle.*
- **Software Engineer** | Kona Software Lab Ltd, Dhaka, Bangladesh. [Mar 2014 - Dec 2015]
  - ◇ Implemented dynamic libraries (.dll, .so, and .dylib) for PKI system and CA toolkits using *C++, OpenSSL, and Java* .
- **Junior Software Engineer** | Nascenia, Dhaka, Bangladesh. [Mar 2013 - Feb 2014]
  - ◇ Developed sports analytic APIs for sports websites using PHP, JavaScript, JQuery, SOAP, REST, JSON, and XML parsing.

Professional Skills

- **Languages and Frameworks:**
  - ◇ **Expert:** Python, Java, C++, C, Shell Scripting, Prolog, Java Spring Boot, JVM, JUnit, Multi-threading, Inter-process communication (IPC), Concurrency, JavaScript, jQuery, SQL, MySQL, Oracle SQL, MongoDB, Elasticsearch, Flask, GraphQL, REST, RabbitMQ, OpenSSL, Cryptography, NumPy, Pandas, Jupyter Notebook, Scikit-learn, Keras, ML, Stanford CoreNLP, NLTK, Prompt Engineering, LangChain, TCP/IP, CVE, CWE, OWASP, MITRE ATT&CK, NIST CSF, CIS CSC.
  - ◇ **Working Knowledge:** R, Lua, PHP, C#, TensorFlow, Terraform, Ansible, Chef InSpec, Apache Kafka, Apache Flink.
- **Tools and Platforms:**
  - ◇ **Expert:** IDAPro, OllyDbg, Wireshark, Docker, Gradle, CMake, Postman, VirtualBox, VMWare, Virtualization, Git, Scrum.
  - ◇ **Working Knowledge:** QEMU, KVM, Kubernetes, AWS VDI, Azure, Weka, Gephi, Maven, Splunk, UML

Professional Projects

- **PKI-Middleware**, A PKI dynamic library developed for Windows, Linux, MAC, and Android platforms which complies with *KISA* and *FIPS* standards. Implemented multi-threading and multiprocessing, smart card profile initialization, asymmetric and symmetric key generation, encrypt and decrypt operation, and X.509 certificate generation, sign, and verify operation. **Tech Stack:** *C++, CMake, OpenSSL, JavaCard OS, Multi-threading, IPC, and Concurrency.* [Apr 2014 - Dec 2015]
- **Custom CSP**, A *Cryptographic Service Provider,* MSDN Compatible library that implements Microsoft's *CryptoAPI (CAPI).* Implemented NFC-based smart card authentication in Windows OS using Custom CSP. **Tech Stack:** *C++, CMake, Windows API, OpenSSL, Multi-threading, IPC, and Concurrency.* [Jan 2016 - June 2016]
- **CMS**, *Cryptographic Message Syntax* is a *PKCS#7* based toolkit developed to support the *CA System* during the certificate Issuance that supports all data types (*Signed, Enveloped, SignedAndEnveloped, data*) of *PKCS#7* and their operations. **Tech Stack:** *Java, Java Spring Boot, JVM, Gradle, MySQL, Multi-threading.* [May 2015 - June 2015]

Dissertation Research and Projects: **Distributed Hierarchical Event Monitoring for Security Analytics**

- **CIS Critical Security Control (CSC) Assessment**, Automated extraction of threat actions, what-to-measure (observables), and development of key measurement indicators (KMI) and metrics to assess and evaluate each CSC safeguard enforcement. **Tech Stack:** *NLP, Python, gpt-3.5-turbo, LangChain, Prompt Engineering, Ansible, Chef InSpec.* [Aug 2018 - Mar 2024]
- **Scalable-Hunter**, Distributed hierarchical event monitoring system for threat hunting. Designed and implemented distributed hierarchical event monitoring system to reduce attack detection time, communication overhead and resource usage. **Tech Stack:** *Python, Java, C++, Gradle, MySQL, GraphQL, RabbitMQ, Elasticsearch, Docker, ETW.* [Aug 2019 - July 2023]
- **TTPHunter**, Automatic and accurate extraction of threat actions from unstructured text of CTI Sources and mapping of threat actions to MITRE ATT&CK techniques. Extracted threat actions and attacker TTPs from CTI reports using NLP and similarity measures- TF-IDF. **Tech Stack:** *Java, Gradle, NLTK, Stanford CoreNLP, TF-IDF, MySQL.* [Jan 2017 - July 2018]

Publications

- **Mohiuddin Ahmed**, Jinpeng Wei, Ehab Al-Shaer. Prompting LLM to Enforce and Validate CIS Critical Security Control. (ACM SACMAT 2024).
- **Mohiuddin Ahmed**, Jinpeng Wei, Ehab Al-Shaer. SCAHunter: Scalable Threat Hunting through Decentralized Hierarchical Monitoring Agent Architecture. (Computing 2023).
- Sharun Akter Khushbu, Nasheen Nur, **Mohiuddin Ahmed**, Nashtarin Nur. A Comparison of Traditional to Advanced Linguistic Models to Analyze Sentiment in Bangla Texts. (EMNLP 2023 workshop BLP).
- **Mohiuddin Ahmed**, Ehab Al-Shaer. Measures and Metrics for the Enforcement of Critical Security Controls: a Case Study of Boundary Defense. (HOTSOS 2019).
- **Mohiuddin Ahmed**, Jinpeng Wei, Yongge Wang and Ehab Al-Shaer. A Poisoning Attack Against Cryptocurrency Mining Pools. (ESORICS CBT 2018).
- Ghaith Husari, Ehab Al-Shaer, **Mohiuddin Ahmed**, Bill Chu, and Xi Niu. TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources. (ACSAC 2017).
- Rawan Al-Shaer, **Mohiuddin Ahmed**, Ehab Al-Shaer. Statistical Learning of APT TTP Chains from MITRE ATT&CK. (RSA Conference, 2018).
- Mohammed Noraden Alsaleh, Jinpeng Wei, Ehab Al-Shaer and **Mohiuddin Ahmed**. gExtractor: Towards Automated Extraction of Malware Deception Parameters. (SSPREW-8, 2018).