# Mohiuddin Ahmed | Portfolio | GitHub | LinkedIn | Google Scholar

Melbourne, Florida, USA | sohel.buet.cse.07@gmail.com | +1 980-267-0371

## Education

- **Doctor of Philosophy (Ph.D.)** in Software and Information Systems. [August 2016 - August 2023]
  - ◇ University of North Carolina at Charlotte, NC, USA. *GPA: 3.93.*
- **Bachelor of Science** in Computer Science and Engineering. [January 2008 - February 2013]
  - ◇ Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh.

## Professional Skills

- **Languages and Frameworks:**
  - ◇ **Expert:** Python, Java, C++, C, Prolog, Shell Scripting, Java Spring, JavaScript, SQL, MySQL, Oracle SQL, Elasticsearch, RabbitMQ, OpenSSL, Cryptography, CoreNLP, AllenNLP, NLTK, Scikit-learn, Keras, Machine Learning, LangChain, TCP/IP, OSI Model, MITRE ATT&CK Framework, CIS Critical Security Control, Cyber Threat Hunting.
  - ◇ **Working Knowledge:** R, PHP, Laravel, C#, TensorFlow, Terraform, Ansible, Chef InSpec.
- **Tools and Platforms:**
  - ◇ **Expert:** IDAPro, OllyDbg, Docker, Gradle, CMake, VirtualBox, VMWare, Git, Scrum/Agile, Windows, Linux, Mac.
  - ◇ **Working Knowledge:** Kubernetes, AWS, Azure, Weka, Gephi, Maven, Splunk, UML, Android.

## Professional Experiences

- **Graduate Assistant**, University of North Carolina at Charlotte, NC, USA. [August 2016 - May 2023]
  - ◇ Developed distributed hierarchical event monitoring system to detect attacks based on attack technique description (static and behavioral features) provided by the MITRE ATT&CK framework, and taught graduate courses on cybersecurity.
- **Team Lead, Security Lab**, Kona Software Lab Ltd, Dhaka, Bangladesh. [January 2016 - June 2016]
- **Software Engineer, Security Lab**, Kona Software Lab Ltd, Dhaka, Bangladesh. [March 2014 - December 2015]
  - ◇ Implemented dynamic libraries (.dll, .so, and .dylib) and different corresponding PKI system and CA toolkits using *Java and C++* that comply with *PKCS#11, FIPS, KISA, and PKCS#7.*
- **Junior Software Engineer**, Nascenia, Dhaka, Bangladesh. [March 2013 - February 2014]
  - ◇ Integrated different sports analytic API's in sports websites using PHP and MODX CMS.

## Professional Projects

- **PKI-Middleware**, A *PKCS#11* dynamic library developed for Windows, Linux, MAC and Android platform which complies *KISA* and *FIPS* standards. Implemented multi-threading and multiprocessing, smart card profile initialization, asymmetric (RSA, ECA) and symmetric (DES3, AES, MAC, SEED) key operation (encrypt and decrypt, sign and verify, and key generation). *Development Language/Tools: C++, OpenSSL, JavaCard OS.* [May 2014 - December 2015]
- **Custom CSP**, A *Cryptographic Service Provider,* MSDN Compatible library that implements the Microsoft's *CryptoAPI (CAPI).* Implemented NFC-based smart card authentication in Windows OS using Custom CSP.
  *Development Language: C++, Windows API, OpenSSL.* [January 2016 - April 2016]
- **CMS**, *Cryptographic Message Syntax* is a *PKCS#7* based toolkit developed to support *CA System* during certificate Issuance that supports all data types (*Signed, Enveloped, SignedAndEnveloped, data*) of *PKCS#7* and their operations.
  *Development Language: Java.* [May 2015 - June 2015]
- **PKI-Middleware Wrapper** is a Java wrapper to use *PKCS#11* middleware library in java application. It reduces maintenance complexity of *JNI* so that application developer dont' have to write core C code to handle function calls of *PKCS#11* libraries. *Development Language: Java, JNI.* [January 2015 - March 2015]

## Dissertation Research Projects

- **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. Developed low-level log collecting agents for Windows system (ETW, event logs).
  *Development Language/Tools: Python, Java, RabbitMQ, ElasticSearch, Docker.* [August 2019 - till date]
- **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. *Development Language/Tools: NLP, Python, gpt-3.5-turbo, LangChain.* [August 2018 - till date]
- **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 from CTI reports using NLP and mapped the extracted threat actions to MITRE ATT&CK techniques and tactics using document similarity measures TF-IDF.
  *Development Language/Tools: Java, CoreNLP, TF-IDF.* [January 2017 - July 2018]

## Publications

- **Mohiuddin Ahmed**, Jinpeng Wei, Ehab Al-Shaer. SCAHunter: Scalable Threat Hunting through Decentralized Hierarchical Monitoring Agent Architecture. (Computing 2023).
- **Mohiuddin Ahmed**, Jinpeng Wei, Yongge Wang and Ehab Al-Shaer. (2018). A Poisoning Attack Against Cryptocurrency Mining Pools. (CBT 2018).
- **Mohiuddin Ahmed**, Ehab Al-Shaer. (2019). Measures and metrics for the enforcement of critical security controls: a case study of boundary defense. (HOTSOS 2019).
- Ghaith Husari, Ehab Al-Shaer, **Mohiuddin Ahmed**, Bill Chu, and Xi Niu. (2017). TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources. (ACSAC 2017).
- Rawan Al-Shaer, **Mohiuddin Ahmed**, Ehab Al-Shaer. (2018). Statistical Learning of APT TTP Chains from MITRE ATT&CK. (RSA Conference, 2018).
- Mohammed Noraden Alsaleh, Jinpeng Wei, Ehab Al-Shaer and **Mohiuddin Ahmed**. (2018). gExtractor: Towards Automated Extraction of Malware Deception Parameters. (SSPREW-8, 2018).