Mohiuddin Ahmed | Portfolio | GitHub | LinkedIn | Google Scholar

Melbourne, FL | sohel.buet.cse.07@gmail.com | +1 (980) 267-0371

Education

- **Doctor of Philosophy** in Computing and Information Systems [Aug 2016 - May 2024]
  University of North Carolina at Charlotte, NC, USA.
  Dissertation Title: "Distributed hierarchical event monitoring for security analytics"
  Advisor: Dr. Jinpeng Wei.
- **Bacelor of Science** in Computer Science and Engineering [Jan 2008 - Feb 2013]
  Bangladesh University of Engineering and Technology, Dhaka, Bangladesh.

Research Interests

Teaching Interests

Dissertation Research and Projects:

Dissertation Title: Distributed Hierarchical Event Monitoring for Security Analytics

- **CIS Critical Security Control 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]

Teaching and Mentoring Experiences

- **Teaching Assistant, Principles of Info Security and Privacy** [Spring 2018, Fall 2018, Spring 2019, Spring 2021, Fall 2021, Spring 2022, Fall 2022]
  Software and Information System Department, University of North Carolina at Charlotte, NC, USA
  - ◇ Conducted lectures in both online and offline settings multiple times during the semester on topics of my expertise.
  - ◇ Prepared multiple hands-on demos on malware analysis and attack simulation (SQL Injection, Cross-site Scripting) to demonstrate to the students.
  - ◇ Prepared and graded different exam questions, quizzes, and assignments.
  - ◇ Conducted TA sessions every week during the semester to help understand students' complicated course topics, answering students' queries and clearing different course policies.
- **Teaching Assistant, Enterprise and Infrastructure Protection** [Spring 2023]
  Software and Information System Department, University of North Carolina at Charlotte, NC, USA
  - ◇ Conducted lectures in both online and offline settings multiple times during the semester on topics of my expertise (First-order logic, Second-order logic, and Prolog).
  - ◇ Prepared multiple hands-on demos on event monitoring and analysis using tools like Splunk and VM and network programming using WebSocket for client-server communication to demonstrate to the students.
  - ◇ Prepared and graded different exam questions, quizzes, and assignments.
  - ◇ Conducted TA sessions every week during the semester to help understand students' complicated course topics, answering students' queries and clearing different course policies.
- **Teaching Assistant, Secure Programming and Penetration Testing** [Fall 2020]
  Software and Information System Department, University of North Carolina at Charlotte, NC, USA

- ◇ Prepared and graded different exam questions, quizzes, and assignments.
- ◇ Conducted TA sessions every week during the semester to help understand students' complicated course topics, answering students' queries and clearing different course policies.

- **Teaching Assistant, Intro to Info Security and Privacy** [Fall 2016, Fall 2017, Fall 2019]
  Software and Information System Department, University of North Carolina at Charlotte, NC, USA
  - ◇ Conducted lectures in both online and offline settings multiple times during the semester on topics of my expertise (network intrusion and attacks on OS and Infrastructure).
  - ◇ Prepared multiple hands-on demos on network traffic analysis using Wireshark.
  - ◇ Prepared and graded different exam questions, quizzes, and assignments.
  - ◇ Conducted TA sessions every week during the semester to help understand students' complicated course topics, answering students' queries and clearing different course policies.
- **Teaching Assistant, Knowledge Discovery in Database** [Spring 2020]
  Software and Information System Department, University of North Carolina at Charlotte, NC, USA
  - ◇ Conducted lectures in both online and offline settings multiple times during the semester on topics of my expertise (Document similarity measuring techniques such as Cosine similarity and TF-IDF).
  - ◇ Prepared and graded different exam questions, quizzes, and assignments.
  - ◇ Conducted TA sessions every week during the semester to help understand students' complicated course topics, answering students' queries and clearing different course policies.
- **Lead Teaching Assistant, Intro to Operating System and Networking** [Spring 2017]
  Software and Information System Department, University of North Carolina at Charlotte, NC, USA
  - ◇ Managed, coordinated, and distributed tasks to a team of six TAs who are responsible for grading and mentoring undergraduate students of the course.
  - ◇ Prepared and graded different exam questions, quizzes, and assignments.
  - ◇ Conducted TA sessions every week during the semester to help understand students' complicated course topics, answering students' queries and clearing different course policies.
- **Lead Teaching Assistant, Software Engineering** [Spring 2017]
  Software and Information System Department, University of North Carolina at Charlotte, NC, USA
  - ◇ Managed, co-ordinated and distributed tasks to a team of six TAs who are responsible for grading and mentoring undergraduate students of the course.
  - ◇ Prepared and graded different exam questions, quizzes, and assignments.
- **Mentor, CyberDNA Lab** [Jan 2021 - Dec 2022]
  University of North Carolina at Charlotte, NC, USA
  - ◇ Mentored two junior Ph.D. students on developing research ideas, implementing a proof of concept system, and writing research papers.

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** [Jan 2016 - June 2016]
  Kona Software Lab Ltd, Dhaka, Bangladesh.
  - ◇ Led a team of software developers to build PKI system using *Java, C++, OpenSSL, MySQL, CMake, and Gradle.*
  - ◇ Implemented NFC-based smart card authentication in Windows OS using Custom CSP (MSDN compatible library that implements Microsoft's *CryptoAPI (CAPI)*).
  - ◇ Developed *PKCS#7* based toolkit to support the *CA System* during the certificate Issuance that supports all data types (*Signed, Enveloped, SignedAndEnveloped, data*) of *PKCS#7* and their operations.
- **Software Engineer** [Mar 2014 - Dec 2015]
  Kona Software Lab Ltd, Dhaka, Bangladesh.
  - ◇ Implemented dynamic libraries (.dll, .so, and .dylib) for PKI system and CA toolkits using *C++, OpenSSL, and Java* .
  - ◇ 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.
  - ◇ Developed a Java wrapper to load *PKCS#11* middleware library in Java application, which reduces

the maintenance complexity of *JNI* so that application developers don't have to write core C code to handle function calls of *PKCS#11* libraries.

- **Junior Software Engineer** [Mar 2013 - Feb 2014]
  Nascenia, Dhaka, Bangladesh.
  ◇ Developed sports analytic APIs for sports websites using PHP, JavaScript, JQuery, SOAP, REST, JSON, and XML parsing.

Publications

- **Mohiuddin Ahmed**, Jinpeng Wei, and Ehab Al-Shaer. Prompting LLM to Enforce and Validate CIS Critical Security Control. (ACM SACMAT 2024).
- **Mohiuddin Ahmed**, Jinpeng Wei, and Ehab Al-Shaer. SCAHunter: Scalable Threat Hunting through Decentralized Hierarchical Monitoring Agent Architecture. (Computing 2023).
- Sharun Akter Khushbu, Nasheen Nur, **Mohiuddin Ahmed**, and Nashtarin Nur. A Comparison of Traditional to Advanced Linguistic Models to Analyze Sentiment in Bangla Texts. (EMNLP 2023 workshop BLP).
- **Mohiuddin Ahmed**, and 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**, and 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).

Presentations

- **Conference Presentations**
  ◇ **Mohiuddin Ahmed** and Others. Prompting LLM to Enforce and Validate CIS Critical Security Control. San Antonio, TX, USA. (ACM SACMAT 2024).
  ◇ **Mohiuddin Ahmed** and Others. SCAHunter: Scalable Threat Hunting through Decentralized Hierarchical Monitoring Agent Architecture. London, UK. (Computing 2023).
- **Poster Presentations**
  ◇ **Mohiuddin Ahmed** and Others. Measures and Metrics for the Enforcement of Critical Security Controls: a Case Study of Boundary Defense. Nashville, TN, USA. (HOTSOS 2019).
  ◇ **Mohiuddin Ahmed**. Distributed Hierarchical Event Monitoring for Security Analytics. Charlotte, NC, USA. (UNC Charlotte Graduate School Research Symposium 2022).

Honors and Awards

- **Graduate School Summer Fellowship** [Summer 2023]
  ◇ Awarded to develop my Ph.D. dissertation during summer 2023.
- **Proposal Development Summer Fellowship** [Summer 2021]
  ◇ Awarded to develop my Ph.D. dissertation proposal during the summer of 2021.
- **Higher Secondary School Board Scholarship in Talent Pool** [Year 2008]
  ◇ Awarded to top students among all who graduated from higher secondary school in 2007.
- **Secondary School Board Scholarship in Talent Pool** [Year 2006]
  ◇ Awarded to top students among all who graduated from secondary school in 2005.
- **Secondary School (Class Eight) Board Scholarship in Talent Pool** [Year 2004]
  ◇ Awarded to top students among all who graduated from class eight in 2003.
- **Primary School Board Scholarship in Talent Pool** [Year 2001]
  ◇ Awarded to top students among all who graduated from primary school in 2000.

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.
  - ◇ **Working Knowledge:** R, Go, Lua, Tcl, PHP, C#, TensorFlow, Terraform, Ansible, Chef InSpec.
- **Tools and Platforms:**
  - ◇ **Expert:** Apache Kafka, Apache Flink, Docker, Gradle, CMake, Postman, VirtualBox, VMWare, Git, Scrum.
  - ◇ **Working Knowledge:** QEMU, KVM, Kubernetes, AWS VDI, Azure, Maven, Splunk, UML.
- **Security and Networking :** Malware Analysis, IDAPro, OllyDbg, Wireshark, Process monitor, OpenSSL, Cryptography, TCP/IP, OSI Model, CVE, CWE, OWASP, MITRE ATT&CK, NIST CSF, CIS CSC.
- **ML Techniques and Libraries:** Prompt Engineering, LangChain, NumPy, Pandas, Jupyter Notebook, Scikit-learn, Keras, Deep Learning, Stanford CoreNLP, NLTK.

References

Research Advisor
Jinpeng Wei
Associate Professor
UNC Charlotte, NC, USA
jwei8@uncc.edu | website

Co-Advisor
Ehab Al-Shaer
Distinguished Career Professor
Carnegie Mellon University, Pittsburgh, PA
ehabalshaer@cmu.edu | website