Dear Hiring Manager,

I am excited to apply for the Security Engineer position. With my background in Software and Information systems, extensive experience in the software development industry, and academic research, I believe that I possess the skill set and passion to make valuable contributions to your team. My research endeavors have been centered around developing a distributed security analytics for distributed threat hunting and automated extraction of measures and metrics for the assessment of the Center for Internet Security's (CIS) critical security control (CSC) enforcement. My work focuses on developing automated measures and metrics generation approach for security controls, and delivering monitoring intrusiveness, reducing communication overhead among agents, and enabling local decision-making while maintaining high accuracy and timely detection of attacks and attack techniques.

As a Teaching Assistant, I taught and designed graduate courses in Principles of Information Security and Privacy, Network Infrastructure Security, and Data Mining. Before joining UNC Charlotte as a Ph.D. student, I worked as a Software Engineer and Team Lead at Kona Software Lab Ltd., Dhaka, Bangladesh, developing middleware libraries for PKI and CA systems. I also led a team of three software developers to design and develop NFC-based smart card authentication for wearable OS. I developed those libraries using C++, Java, JNI, OpenSSL, and JavaCard OS.

I am an expert in programming languages like Python, Java, C++, C, and Prolog. Additionally, I have expertise in relational (MySQL, Oracle Database, Microsoft SQL Server), non-relational (ElasticSearch, MongoDB), and graph (neo4j) databases. I am proficient in using visualization tools such as UML, Weka, and Gephi and version control tools such as Git. During my research, I extensively used virtualization tools like VirtualBox, VMWare, and Docker. I am familiar with AWS, Azure, and Scrum/Agile development. I am well-versed in TCP/IP networking, OSI models, Cryptography, and CI/CD. I gained experience in machine learning libraries such as CoreNLP, AllenNLP, NLTK, Scikit-learn, Keras, LangChain, and TensorFlow while evaluating my research on distributed security analytics and doing coursework. I have worked extensively with Cryptography, OpenSSL, MITRE ATT&CK framework, RabbitMQ, IDAPro, Wireshark, Sysmon, OllyDbg, and Splunk.

While a Software Engineer at Kona Software Lab Ltd in Bangladesh, I was a lead developer on the PKI middleware development team. The project aims to develop a PKI middleware (.dll, .so, and .dylib) library that complies with PKCS#11 standards and successfully earned the KISA and FIPS certification. This middleware library is used in applications that communicate with the Kona smart card. In this library, I implemented multi-threading and multiprocessing, smart card profile initialization, asymmetric (RSA, ECA) and symmetric (DES3, AES, MAC, SEED) key operations (encrypt and decrypt, sign and verify, and key generation). I used C++, OpenSSL, JavaCard OS, and Java for the development. Later, this product was used in the Certificate issuance product of the same company. I also led a team of three developers and built another Custom CSP project to implement smart authentication in Windows OS through chip-based smart cards and wearable OS. This project used the PKI middleware library I developed previously for key operations. This library is now actively used in KONA I certificate issuance and smart card applications in South Korea.

During my tenure as a Research Assistant at UNC Charlotte, I was a member of the project TTPdrill. The goal of this project is to convert threat reports into actionable knowledge. To convert CTI reports to actionable knowledge, we have to map threat actions to adversary TTPs such as those provided by MITRE ATT&CK Framework. To generate the mapping, we used TF-IDF similarity measures. However, before performing similarity measures among CTI reports and adversary TTPs, one has to extract relevant informants from the CTI reports. In this extraction part, I was actively involved in defining the information (threat actor, threat action, threat object, how- tools used by the adversary, and why- the adversary's intent) to extract from the CTI reports. I used Java, CoreNLP and AllenNLP. Following the extracted TTPs from CTI reports, I started two separate projects later about techniques to attack mining pools and detect such attacks by analyzing System Call logs collected through Symbolic Execution of System Calls and developing distributed hierarchical monitoring agent architecture for automated threat hunting. In the monitoring architecture development, I solved the problem of optimal hierarchy generation using approximation algorithms based on monitoring task similarity and end-host locations. Later, I published our work on this topic in ACSACS 2017, SSPREW-8 2018, ESORICS CBT 2018, and Computing 2023.

While a Research Assistant at UNC Charlotte, I was a core research member in developing specifications to assess CIS CSC enforcement. This project aims to determine what to measure (observables), how to measure (tools required), and metrics to evaluate the enforcement of CSCs. I used prompt engineering (Zero-shot prompting, Few-shot prompting, Chain-of-Thought, Tree-of-Though) with LLM (ChatGPT, LLaMA) to extract that information from the CIS CSC guidelines. Later, The CIS reviewed and published our proposed approach as guidelines for the industry to assess CSCs. I also published my works at HOTSOS 2018 and ACM SACMAT 2024 as a novel way to develop automated measures and metrics for CIS CSC assessment.

I am a *Permanent Resident (Green Card Holder) of the USA and willing to relocate within the USA.*

As a dedicated researcher with experience in software development, my technical skills, research experience, and passion for problem-solving align well with the vision and requirements of the team. I am eager to contribute my expertise and collaborate with your team to drive innovation and create impactful solutions. Thank you for considering my application.

Sincerely,
Mohiuddin Ahmed