Dear Hiring Manager,

With my Ph.D. in Software and Information Systems, and several years of FinTech industry experience, I have honed my Cyber Threat Hunting, Malware Analysis, Machine Learning and Software development skills. I am a Graduate Assistant at the University of North Carolina at Charlotte, developing a distributed security analytics system for distributed threat hunting. My research has been funded by DOE and ONR. My work aims to deliver monitoring intrusiveness, reduce communication overhead among agents, and enable local decision-making while maintaining attacks and attack techniques detection accuracy high and in time. Another goal of my research is to develop measures and metrics for the assessment of Center for Internet Security’s (CIS) critical security control enforcement.

As a Teaching Assistant, I teach, design, and prepare 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, where I developed 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. For the development of those libraries, I used 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 web development, scripting and database management with Shell Scripting, PHP, JavaScript, and relational (MySQL, Oracle Database, Microsoft SQL Server) and non-relational (ElasticSearch, MongoDB) databases. I am proficient in using visualization tools such as UML, Weka, and Gephi and version control tools such as Git. During my research work, I used extensively virtualization tools like VirtualBox, VMWare, Kubernetes, and Docker, and 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 threat hunting. I have worked extensively with Cryptography, OpenSSL, MITRE ATT&CK framework, ElasticSearch, RabbitMQ, IDAPro, Wireshark, Sysmon, OllyDbg, and Splunk.

During my tenure as a Software engineer and Ph.D. student, I was involved and led Several research and projects. I am currently working on AUTO-Hunter, a distributed hierarchical event monitoring System for attack diagnosis through active Investigation of attacker activities. I designed and implemented this system to reduce attack detection time, communication overhead, and resource usage. I also developed low-level log collecting agents for the Windows system (ETW, event logs, Syslog, NetFlow) and detectors to map low-level traces to the MITRE ATT&CK technique and evidential reasoning framework. I have also worked on the Critical Security Control (CSC) Assessment project, which involved automated extraction of threat action, observables (what-to-measure), and development of key measurement indicators (KMI) and metrics for the KMI of each CSC. Additionally, I worked on TTPDrill, which was an automatic and accurate extraction of threat actions from unstructured text of CTI sources and mapping of threat actions to MITRE ATT&CK techniques. For the development and evaluation of the above-mentioned projects, I used Python, Java, C++, SQL, ElasticSearch, RabbitMQ, Docker, IDAPro, OllyDbg and ML libraries. Finally, I developed PKI-Middleware, a PKCS#11 cryptographic dynamic library for smart card operations that complies with KISA and FIPS standards.

I am excited to bring my skills and experience to your team. I appreciate your consideration.

Sincerely,

Mohiuddin Ahmed