Md. Al-Amin Khandaker

Email: khandaker@s.okayama-u.ac.jp
Portfolio: https://al-amin.tech/
Mobile: +81-80-9791-8581
Github: https://github.com/eNipu/

Career Summary and Objective

6+ years experience in working with diverse software development teams and almost 5 years of experience with research and development. Have contributed to adopting emerging technologies for quality product building and delivery. As a team players always keep a growth mindset to contribute to the growth of the team and grow individually as a by-product of the team's growth. My proactive adaptability to new technologies helps me to learn quickly and pursue new challenges in different roles that I've not yet worked.

Education

- **Okayama University** — Okayama, Japan
  Ph.D. in Public Key Cryptography, GPA: 4.0/4.0 — *Oct 2015 - March 2019*
  ***Advisor**:Professor Yasuyuki Nogami*
  ***Ph.D. thesis**: A Study of Efficient Pairing Computation Algorithm Using KSS Curves*

Skills Summary

- **Languages**: Python, C++, Java, Rust, SQL
- **Frameworks**: Scikit, NLTK, TensorFlow, Keras, FastAPI, Flask, PyTest
- **Dev Tools**: Kubernetes, Docker, Git
- **Build Tools**: Poetry, Skaffold, Bazel, CMake, GitHub Actions, GitLab CI
- **Platforms**: Linux, Mac OS X, Raspberry Pi, Azure, AWS, GCP
- **Soft Skills**: Leadership, Project Management, Writing, Public Speaking

Experience

- **Research Engineer, R&D** — Full-time
  EAGLYS Inc. Tokyo, Japan — *Nov 2020 - present*
  - **Design**: Experiment and design the company's flagship product on secure-computing with the relevant cryptographic technologies and protocols.
  - **Implementation**: Contributed to gain over 30% performance boost after implementing performance critical part of the product in Rust. Also improved some IO parts using gRPC.
  - **Test and Delivery**: Solved the product build issues and build speed using Bazel for reproducible builds and GitLab CI for test automation. Experimenting with Skaffold, K8s, Terraform, and Azure ecosystem for creating reusable deployment pipeline.

- **Systems Development Engineer** — Full-time
  Cardservice Inc. Tokyo, Japan — *Apr 2019 - Oct 2020*
  - **Development**: Implemented several POS and QR-code payment applications for embedded systems using C++, Java.
  - **Design**: Worked closely with different teams for designing and implementing unattended payment systems for POS terminals used for car parking, vending machines, and train stations.

- **Associate Software Engineer** — Full-time
  Metatude Asia Ltd., under Viadesk BV, The Netherlands — *May 2012 - Sep 2015*
  - **Development Viadesk**: Implemented native iOS app from early stage to production for a social Intranet service using Objective-C.
  - **Project Coursepath:** : Developed prototype of an online E-learning platform for private organizations.

Projects

- *DataArmor GateDB*: A database proxy application that enables users to perform SQL queries on encrypted data without storing the key to the database server. The major contributions are
  - Implemented Homomorphic-encryption(HE) to perform 'SQL aggregate functions' as a user-defined function in PostgreSQL server in C++.
  - Improved the IO and encryption/decryption speed by 17 times by efficient implementation of HE algorithms and multi-processing in Rust and Python.
  - Implemented Lifted-ElGamal as Somewhat-Homomorphic-Encryption (using BLS-12 elliptic curve pairing) for Homomorphic-addition of cipher-text.
  - Improved the bulk data transmission using gRPC between the multiple proxies.
  - Improved the end-to-end CI/CD pipeline with Bazel, Skaffold, GitLab CI and Kubernetes.
  - Implemented efficient logging using Grafana and FluentD.
- *User Identity Management System*: To give efficient and secure access for different services, developing an identity and access management (IAM) system (Work in progress)
  - Implementing fine-grained access control system using Attribute-Based Encryption(ABE) as service.

- Using Python, OAuth2, REST, FastAPI, PostgreSQL, Bazel, Kubernetes to build the prototype.

- *Secure morphological analyzer for Japanese text*: This project aims to solve the issue of a secure input pipeline for privacy-sensitive text as encrypted text to Machine Learning models.(Completed POC)
  - Designed the core architecture security architecture of the system and implemented several services of this project.
  - Used tech stacks are Python, GitLab CI, OAuth2, gRPC, FastAPI, MySQL, and Docker.

- *DataArmorGate AI*: This project allows to get inference from pre-trained(plain text) ML models using encrypted data.
  - Improved the inference performance by 20% by implementing performance-critical modules from Python to C++.
  - Implemented Homomorphic-Encryption Library bindings for Python using *pybind11.*

Selected Publications

- **Book Chapter: Progress in Cryptology**: "Efficient Optimal Ate Pairing at 128-Bit Security Level". Dec. 2017, pp. 186–205. DOI: 10.1007/978-3-319-71667-1_10.
- **Journal: IEICE Transactions on Discrete Mathematics**: **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "An Improvement of Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve". pp. 1838-1845. DOI: 10.1587/transfun.E100.A.1838

Honors and Awards

- Dean's *"Best scientific research award"* within Faculty of Engineering. 2019
- Japan Govt. MEXT scholarship for doctor's course. 2015
- Bangladesh Govt. merit scholarships. (From 6 grade to Bachelor final semester.)

Volunteer Experience

- **Teaching Assistant at enPit-Security by MEXT** Okayama, Japan
  Implemented and demonstrated the side-channel-attack on RSA for Arduino-UNO for the participants. *2017*

Language Proficiency

- English: Fluent in business communication, TOEIC: 890
- Japanese: Proficient in daily conversation, JLPT N4
- Bengali: Native speaker