# Personal statement

**Motivation** Cloud computing has become the backbone of modern society, relied on by hospitals, financial institutions, and AI companies to process and store highly sensitive information. Yet, its limitations continue to be exposed by cyberattacks. In 2023, 725 data breaches that exposed nearly 170 million records were reported by the U.S. healthcare sector alone. By 2024, the number of exposed records rose to almost 280 million (HHS Breach Portal). Further, all industries are seeing increasing attack scales: the 2024 Verizon Data Breach Investigations Report (DBIR) documented 10,626 confirmed breaches, while the 2025 report recorded 12,195 – the highest in the report's history. Worse, *each* data breaches cost up to USD 4.4 million on average, estimated by a 2025 report by IBM. These costly and frequent data breaches erode trust in cloud providers and underscore the urgent need for more resilient cloud systems.

To address these risks, Trusted Execution Environments (TEEs) are introduced by technology vendors like Intel and AMD. These technologies isolate in-use data from bad actors by arming cloud processors with mechanisms to encrypt in-use data and prevent unauthorized data access. TEE technologies form the foundation of Confidential Computing, a paradigm shift toward trustworthy private data processing in the cloud. Unfortunately, as explained shortly after, confidential computing is not without its challenges.

First, increasingly complex cloud workloads with diverse stakeholders introduce a new problem: *conflicts of interest*. This issue is demonstrated most vividly by machine learning in the cloud, where multiple stakeholders exist (Table 1). The problem arises when each stakeholder has a security interest that is at odds with those of other stakeholders. For example, machine learning workload owners are required by regulations like General Data Protection Regulation (GDPR) to handle data transparently and responsibly. Unfortunately, to prove this, they must reveal the proprietary logic to the data owner. Addressing conflicts of interest is a running challenge with confidential cloud computing, hindering its wider adoption.

Table 1: Representative stakeholders in cloud machine learning

| Stakeholder | Asset | Security interest |
|---|---|---|
| Data owner | Personal Data | Data is used transparently and responsibly |
| Workload owner | Machine learning algorithm | Hide proprietary logic |
| Cloud provider | Compute power | Robust resource accounting |

Second, a critical and persistent vulnerability exists in TEE implementations: *side channels*. They are indirect signals – such as the time a sensitive operation takes – through which an attacker can infer private information. Side-channels are acknowledged as a formidable threat to trustworthy confidential computing (Amazon AWS, Microsoft Azure, IBM Cloud, and Alibaba Cloud). Efforts to completely remove side channels often run into roadblocks. Some side-channel sources are buried deep in the processor's internal circuitry (their *micro-architecture*), requiring massive hardware redesigns. Others come from everyday cloud operations, such as system memory management, and removing them would impair flexibility.

**Research Proposal** There has been research that addresses the above challenges. These solutions leverage a compiler to enforce security policies on confidential programs; the compiler inserts code into programs that ensures stakeholders' security requirements or removes side-channel information leaks. These solutions require developers to rewrite or recompile the software, which makes them difficult to adopt, especially for closed-source software. Additionally, due to the expensive compiler-inserted code, many solutions can slow applications by hundreds or even thousands of times. Worse, to remedy the performance hit, some solutions make security-to-performance trade-offs that are often ad hoc and lack a sound theoretical basis.

Taking a departure from existing research, this proposal explores how *Operating Systems (OSes)* could be repurposed to tackle confidential computing challenges. Newer iterations of confidential computing can now protect the entire virtual machine, incorporating the OS into the protection. The OS, as the mediator between software and hardware, is the ideal layer point to implement security policies without relying on a compiler.

**TODO: Detailed research plan** Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

**Fit with UBC** UBC is an ideal base for this work under the following pillars. First, the proposed project is strongly interdisciplinary; it requires elements from *theoretical security analysis* and *system design* to succeed. This makes the UBC Department of Computer Science, where world-renowned expertise in both security and systems converges, an ideal institution.

I propose to carry out this research under the supervision of Prof. Aastha Mehta, a faculty member from UBC Security & Privacy Group. TODO: Aastha's fit

At the same time, UBC's Systopia Group, chaired by Margo Seltzer, offers leading expertise in operating systems. TODO: Aastha's fit

I also look forward to contributing to UBC's teaching mission. I have plans for guest lectures in CPSC 436A (Operating Systems Design and Implementation), and CPSC 538M (Systems Security).

The project will be conducted mainly within UBC's campus. All core work can be conducted locally using open-source platforms such as Linux and QEMU, while additional hardware requirements can be achieved remotely. Occasional short-term travel will be necessary for collaboration and to present results at leading conferences such as ACM CCS, IEEE S&P, USENIX Security, and NDSS. In this regard, the location of UBC, being close to the States where those conferences are commonly hosted, significantly cuts down travel costs.

**Research vision.** My vision is to enhance the security of cloud software against adversaries through practical and rigorous approaches. This vision focuses on two main areas: software compartmentalization, which involves dividing programs into isolated components to contain potential compromises, and securing confidential computing against side-channel attacks. To fulfill this, I have proposed solutions that have been recognized by the research community. My work on program compartmentalization with hardware mechanisms, CAPACITY, earned the **Distinguished Paper Award at the ACM CCS 2023** and the Korean government's **BK21 Research Scholarship in 2024**. More recently, INCOGNITOS, my solution toward practically addressing side-channel attacks in the cloud, was featured at the **IEEE Symposium on Security and Privacy 2025**, a premier conference in computer security.

At UBC, I plan to expand the vision toward developing new methodologies to address these challenges and emerging problems in cloud computing. Under the guidance of my postdoctoral supervisor, **Aastha Mehta**, I will develop operating system-supported solutions to enhance cloud security. I also plan to collaborate across the Computer Science department: with **Hugo Lefeuvre** on designing robust networking software, and with **Margo Seltzer**, **Thomas Pasquier**, and **Alexandra Fedorova** on applying systems provenance and application-ware memory management to software compartmentalization and side-channel mitigation. To this end, UBC's interdisciplinary research culture is crucial for advancing my research.

**Leadership and community engagement.** I strongly believe that a good researcher is an outreaching one. As Richard Hamming observed in his lecture, the scientists who leave doors open (and welcome interruptions) often make the most impactful contributions. Basing research in a geographically isolated location, I am motivated to be proactive: I independently sought out and participated in international projects with researchers from UBC's Systopia lab and CISPA, Germany. At the same time, I contributed to the broader field through service on artifact evaluation and poster committees at major conferences. My service earned me the **Noteworthy Reviewer Recognition** at Usenix Security 2025. I also engaged in open-source work, participating in security discussions and implementing new features for the Unikraft unikernel. Through open-source, I also created tools for others, such as my bibliography manager, bibli-ls. These outreach efforts expanded my horizons, exposed me to like-minded researchers, and built long-lasting connections that extended beyond research.

The collaborative, respectful, and inclusive culture being built at UBC deeply resonates with me. In this environment, I am eager to continue my outreach trajectory. Specifically, I plan to actively engage with campus communities by participating in discussions at reading groups and sharing my perspective in research seminars. Building on a practice that helped me, I also intend to start a writing study group, where students can refine their technical communication skills and support each other in the writing process.

**Teaching.** To me, the most effective learning is enabled by interactivity. As a teaching assistant for *Computer Security* and *System Programming* at SKKU, I developed and maintained ctf.skku.edu, a platform where students engaged in Capture-the-Flag (CTF) challenges. The system, modeled after real-world cybersecurity competitions, required students to solve security problems and earn points. This game-like, interactive approach not only sparked the curiosity of many students but also motivated several to join my lab. I found that the effort invested in teaching is never wasted; it connects me with the next generation of researchers while deepening my own understanding of complex concepts.

I am eager to contribute to UBC's teaching mission. I plan to bring my CTF-organizing experiences to UBC's MapleBacon CTF team and to courses like CPSC 538M: Systems Security – on which I have already served as a guest lecturer. Furthermore, I aspire to make challenging topics such as operating systems engaging for students. To achieve this, I will design interactive teaching materials based on my experiences developing video games and visualizing security algorithms. With the same skill set, I also plan to assist students in creating visualizations for their research to enhance its impact and reach.

# 1 Appendix: Guide

Address the following:

- Describe your research experience and relevant work experiences
- Describe your personal qualities through other activities such as athletic/artistic achievements, leadership activities, community engagements, volunteerism, etc.
- Describe your career aspirations
- Include details concerning what teaching, if any, you will be doing and how it is related to your work

# 2 Appendix: Evaluation criteria

The search is for candidates whose work is beyond “excellent” and whose research is convincingly ground-breaking.

Excellence in scholarly work and independent research - 60%

- quality of contributions to research to date
- scholarships and awards held
- duration of graduate studies, taking into account the nature of the program and relevant personal circumstances
- determination and ability to complete projects within an appropriate period of time
- critical thinking, judgment, and initiative
- resilience and flexibility in adjusting research plans, particularly in response to COVID-19 impacts

Quality of proposed research project - 30%

- originality in developing a research agenda
- merit, potential significance, clarity, and feasibility of the proposed project
- relevance of applicant’s work experience and academic training to the field of proposed research
- suitability and quality of research environment (proposed supervisor, facilities, support of academic unit) Personal qualities of the applicant - 10%

Personal qualities of the applicant - 10%

- character: integrity, collegiality, and respect for others
- communication skills
- Preference will be given to applicants who have not already held a postdoctoral award or fellowship.
- leadership abilities as demonstrated by employment, athletic/artistic achievements, community engagement, volunteering, etc.