Exploring Operating System Mechanisms for Practical and Resilient Confidential Computing

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.