Introduction. Canadians are increasingly reliant on cloud-based services to drive key aspects of everyday life with each passing year. Analysts expect that Canada's cloud market cap will reach $13 billion by 2023 [9], and 92% of our businesses are currently using cloud infrastructure in some form. However, as we entrust more of our digital lives to the cloud, so too do we implicitly place our trust in aetherial distributed platforms, often running unknown software in unknown environments. In a perfect world, this trust would be well-founded; however, the distributed and multi-tenant nature of the cloud can create security problems in practice, which in turn negatively impact the safety, privacy, and prosperity of Canadian stakeholders.

While we may expect the entities which control cloud platforms to provide some level of security guarantees, the logistics of managing distributed, multi-tenant computing clusters running untrusted, Internet-connected software precludes any form of security certainty in practice. In particular, malware, zero-day vulnerabilities, misconfiguration of cloud security policy, and software misbehaviour all represent severe threats to the security and stability of our cloud deployments [8].

To facilitate confidence in the security of our cloud deployments and improve the security and privacy of Canadian stakeholders, I hypothesize that we must design new cloud security mechanisms that are robust in the presence of attacker innovation. Classically, security has been a game of cat-and-mouse; attackers find new holes in existing system configurations and exploit them to achieve malicious purposes, while defenders focus on remediating these holes as they crop up. Thus, rather than defenders simply *reacting* to attacker innovation, a truly robust security mechanism instead *adapts* to attacker innovation as it occurs. Anomaly detection [2, 7] has historically proved a valuable technique for addressing such concerns, proactively guarding against unknown threats by establishing and enforcing criteria for normal system behaviour.

To date, anomaly detection has seen little deployment in cloud environments, with vendors preferring to fix security problems as they occur rather than directly addressing the root of the problem [10]. I theorize that the underlying cause for this phenomenon is primarily rooted in existing technological barriers. Traditionally, operating systems have not been designed to accommodate the powerful observability capabilities required to build an effective anomaly detection system. However, a new Linux kernel technology, eBPF [11], enables researchers to revisit prior assumptions about system observability and security. In particular, eBPF enables programmers to safely and effectively extend the kernel at runtime, gaining powerful insight into system behaviour. These properties perfectly align with the requirements of a cloud-based anomaly detection system.

Proposed Research Objectives. My past work has focused on how eBPF can solve operating system security problems in individual hosts. ebpH [3] is an anomaly detection system that uses eBPF programs to analyze system call patterns in userspace applications. BPFBox [4, 6] and BPFContain [4, 5] are policy enforcement mechanisms that use eBPF programs to enforce a simple confinement policy on user processes and containers respectively. While effective in their own right, each of these mechanisms is insufficient for a full cloud security solution, as they all lack a semantic model of the higher-level APIs (Application Programming Interfaces) that bind cloud services together.

My proposed research plan is to create a *distributed anomaly detection system* for the Kubernetes container orchestration framework. Kubernetes currently holds a dominant market share in cloud services and is positioned to maintain its status as a driving force in cloud infrastructure going forward. However, Kubernetes deployments must be carefully configured to avoid security issues, and this configuration is not necessarily a trivial process [10]. Anomaly detection can benefit Kubernetes by providing an extra layer of protection against unknown attack patterns and reducing the impact of spurious program behaviours. Using eBPF, we can attach various monitoring programs to various parts of the Kubernetes stack, instrumenting security-critical behaviour at the userspace, Kubernetes API, system call, and networking levels.

Designing such an anomaly detection system will involve careful considerations about combining various event sources to arrive at policy decisions. To that end, I plan to conduct a rigorous analysis of the Kubernetes stack, informed by ad-hoc eBPF programs to gain visibility into how components interact with each other. These findings can then inform the design of a generic event filter and feedback mechanism, which takes an event stream as input and produces policy decisions as output. Leveraging the Kubernetes control plane, event streams from separate physical nodes can be combined into a singular model of cluster behaviour, providing further insight into how security-sensitive events impact the overall cluster. My ultimate goal is to provide a modular framework for developing downstream policy enforcement programs that enforce policy decisions at various layers of the Kubernetes stack. This architecture would encourage the participation of the broader research community in developing open security extensions for the cloud.

To evaluate the research prototype, we have plans to deploy it in our security lab and measure its ability to detect and defeat a variety of attacks and its performance impact on the lab infrastructure. This testing will involve a combination of security and performance benchmarks as well as ad-hoc data generated by day-to-day traffic — malicious and otherwise.

Diversity Considerations. Cloud security impacts the lives of all Canadians, regardless of any underlying differences in age, sex, race, gender, or any other label. Moreover, minority populations may be disproportionately impacted by attacks that target our social safety net. Attackers targeting government infrastructure is not a new phenomenon. Recent events have illustrated the profound societal implications of ill-defended critical infrastructure, particularly in light of the extraordinary circumstances surrounding the COVID-19 pandemic [1, 12].

To ensure that this research equally improves the lives of all Canadians, incorporating diversity considerations into its design is of paramount importance. To that end, I plan to carefully study the potential impacts this work can have on securing Canada's social safety net and protecting our vulnerable populations from malicious activity. This investigation will involve focused case studies surrounding how new security solutions can protect critical infrastructure from an innovative adversary with significant computational resources (e.g. an adversary acting on behalf of a foreign nation-state).

Security research — particularly systems security research — has traditionally suffered from accessibility issues. These concerns primarily arise from the significant technical background required to design and develop such mechanisms. With this work, I hope to democratize system security and design accessible cloud security mechanisms that promote future innovation, regardless of systemic barriers to entry. In addition, developing a systems security mechanism with accessibility in mind can encourage underrepresented groups to actively participate in the security community in ways previously impossible.

Finally and perhaps most importantly, I will be making all software, experiments, data, and publications from this study available free and open-source in perpetuity. Making this work freely and publicly available will ensure that all Canadians can freely benefit from this work in perpetuity, regardless of any financial, prejudicial, or other systemic constraints.

Conclusion. Coming out of this research, we will have gained insight into how cloud security can be improved by introducing adaptive security mechanisms that are robust in the presence of attacker innovation. By focusing on accessibility and encouraging others to actively participate in systems security research, this work can help to address systemic barriers that might otherwise preclude underrepresented populations from being included in the security community. This work will impact the lives of all Canadians by directly improving the security and privacy of our families, small businesses, and government institutions.