BOSTON UNIVERSITY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

PhD Prospectus

BARE-METAL MARKETPLACE AT THE BOTTOM OF THE CLOUD

By

Sahil Tikale

B. Eng., L.D.College of Engineering, Gujarat University, India, 2003

M.S., Nanyang Technological University, Singapore, 2010

Advisor: Prof., Orran Krieger

Bare-metal Marketplace at the Bottom of the Cloud

Abstract

Today's clouds offer huge benefits in terms of on-demand elasticity, economies of scale and its pay-as-you-go model. Yet many organizations continue to host their clusters outside of cloud for security, price or performance reasons. Such organizations form a large section of the economy including financial companies, medical institutions and government agencies. Clusters are typically stood up with sufficient capacity to deal with peak demand; resulting in silos of under-utilized hardware. This situation is common place not only within an individually owned data-center running multiple clusters but also across colocation facilities like the MGHPCC[2] – a 15 megawatt data-center that hosts infrastructure from five different universities.

In the thesis we ask the question, What if we could easily and securely move infrastructure across these silos to match demand? This would obviously increase utilization and reduce the cost. Moreover, as we will see, such a capability could enable an alternative model of cloud; an Open Cloud eXchange (OCX) where multiple organizations, freely cooperate and compete with each other for offering different hardware resources while customers can choose from numerous competing services instead of a single provider.

The objective of this thesis is to build a system that allows mutually non-trusting physically deployed services to efficiently share the physical servers of a data center. The approach proposed here is to build a system composed of a set of services each fulfilling a specific functionality. The scope of this work is limited to design and implementation of only the core set of functionalities critical for sharing bare-metal servers between clusters across different deployment systems and ownership.

These functionalities are: 1. *Bare-metal Allocation and Isolation Service:* to allow different users to stand up clusters from a common pool of hardware. 2. *Diskless Rapid Provisioning Service* that allows deploying the cluster fast enough to be able to respond to rapid fluctuations in demand. 3. *Security Model* that enables cluster owners to control trade-offs between security, price, and performance. 4. *Market based incentive system* that uses an economic model of a marketplace to ensure that resources are allocated to the cluster that needs it most. we have completed (1-3) and describe our architecture and discuss the results. Thereafter open questions regarding the (4) will be discussed followed by proposed timeline for the work pending towards completion of this thesis.

Contents

1 Introduction

1.1 Background

Many different mechanisms are available that simplify deployment of services on physical systems such as OpenStack Ironic, Canonical MaaS, Emulab, GENI, Foreman, xCat, and others [25, 8, 28, 4, 11]. Each of these tools takes control of the hardware it manages, and each provides very different higher-level abstractions. A cluster operator must thus decide between, for example, Ironic or MaaS for software deployment; and the data center operator who wants to use multiple tools is forced to statically partition the data center into silos of hardware. Moreover, it is unlikely that most data centers will be able to transition fully to using a new tool; organizations may have decades of investment in legacy tools, e.g., for deploying HPC clusters, and will be slow to adopt new tools.

Clusters are typically stood up with sufficient capacity to deal with peak demand; resulting in silos of under-utilized hardware. When demand exceeds capacity, a cluster may suffer from degraded quality of service (QoS) or violation of service level agreements (SLAs) while enough capacity of physical servers may be available in a rack right next to it. Those servers cannot be used even if they are sitting idle simply because there is no way to move them between silos of clusters. The problem is sufficiently general whether it is a large enterprise hosting multiple clusters in its own data-center or colocation facilities such as the MGHPCC[2] – a 15 megawatt data-center that hosts infrastructure from five different universities

In this thesis we ask the following questions • Can we design a system such that it is possible to move hardware from one cluster to another on demand? • How can we make setting up a cluster fast enough to be able to respond to rapid fluctuations in demand? • Can we design a single system which is appropriate for a wide variety of scenarios, from multiple clusters of a single company to different tenants in the same colocation facility, to new model of cloud with multiple providers[5]? • Can we design a system that provides cluster owners incentives to offer their hardware resources to other clusters?

Current work done in this thesis so far shows strong evidence that the answer to the first three questions is yes. Our remaining work is focused on answering the last question. The thesis proposes a general architecture that we call the Elastic Secure Infrastructure or (ESI). It is a system composed of a set of micro-services that allows mutually non-trusting physically deployed services to efficiently share the physical servers of a data center. A tenant of the ESI has to trust only a minimal functionality of the tenant that offers the hardware resources. Rest of the services can be deployed by each tenant themselves.

1.2 Broader Impact: An alternative to single provider public clouds

Today's clouds offer huge benefits in terms of on-demand elasticity, economies of scale and its pay-as-you-go model. Yet, organizations that need total control of their hardware; have custom deployment practices; require specific security requirements and do not wish to pay for high prices of storage [7, 17] continue to host their own clusters outside of the public clouds. It includes a large section of the economy including financial companies, medical institutions and government agencies that choose to invest in their own hardware than renting it from public cloud providers.

Furthermore it also limits research and innovation. The bottom-most layer of any single provider public cloud is either a virtualization based black-box with no visibility into the allocation of resources or a bare-metal solution with limited deployment options. Also, tenants have no choice but to trust the cloud provider completely for its security. Only a handful of organizations have the capital for setting up a public cloud. This seriously limits avenues for innovation because the research and academic community does not have access to the internal workings of an at-scale cloud.

We believe that the public cloud can evolve into a marketplace in which many actors can compete and cooperate with each other, and innovation can flourish. We refer to this model as the Open Cloud eXchange model or (OCX) [5]. In addition to breaking silos ESI is a critical requirement to enable OCX as the bottom most stack of a multi-provider cloud – a single platform where stake-holders from both industry and academia together host their hardware and services to each other and to customers on pay-as-you-go basis.

1.3 Scope of thesis:

The scope of this thesis is the design and implementation of the following functionalities. • *Bare-metal Allocation and Isolation Service* that uses network isolation technologies to isolate tenants' bare-metal servers • *Diskless provisioning service* that installs software on servers using network mounted storage. • *A Security Model* that allows different cluster owners to attest the integrity of the physical server before choosing to add it to its cluster. • *Market based incentive system* that uses the economic model of a marketplace to encourage different clusters owners to share their hardware with others.

We have prototype implementation of the *Bare-metal Allocation and Isolation Service*, *Diskless provisioning service* and *The Security Model*. We will discuss each one briefly in the next chapter along with results that demonstrate that it is possible to not only move hardware between silos of clusters with significantly different security requirements but it also possible to deploy it at speeds comparable to hosting a virtualized infrastructure.

1.4 Motivation: Characteristics of different clusters in a Datacenter

To understand the constraints and motivations of different types of services to share infrastructure, we briefly describe four different services:

1. **High Performance Computing (HPC) & High Throughput Computing (HTC) Clusters:** A typical HPC or HTC job is a non-interactive, batch job that is latency insensitive. Users submit jobs to batch systems that may take a long time to execute. These batch systems are designed to maximize the utilization of the system and care about overall computation performed over a long period of time. Such systems will be willing to release compute resources to other clusters to handle their peak demand as long as over the long term they have gained more computational resources from sharing resources using ESI with other clusters.

2. **Clouds:** Applications that are extremely interactive, are robust to performance jitters and network latency and experience high variable demand are well suited to run in a virtualization based cloud. The goal of a cloud is to maximize its profits. Therefore it

needs to be responsive to demand so they don't have to turn away customers, which directly affects their profits. A cloud provider has an incentive to offer its servers to other clusters provided it gets enough resources when the cloud experiences a surge in demand.

3. **Systems Research Testbed:** Scientific groups and researchers involved in low-level OS and systems research require access to raw (sometimes specialized) hardware, ability to setup custom automation for deployment of complex environments and support for reproducible experiments. Thus their constraint is to have access to the same or equivalent type of hardware. When the deadline is close and hardware is limited for experiments researchers will welcome any extra capacity from other clusters as long as they get homogeneous servers and in quantity adequate to perform their experiments. If there is an assurance of getting consistent hardware of preferred configuration they may be flexible towards working at odd hours like nights and weekends.

4. **Government Data Centers:** The defense and federal agencies have resources in multiple data-centers that are kept ready for response in times of national emergency. Because of the rare nature of national emergencies these data-center are grossly under-utilized while incurring constant maintenance cost. Anecdotally, we have heard utilization quoted at small fractions of a percentage. Their preference is to have access to large scale compute resources in times of emergency without having to incur continuous cost of maintaining the infrastructure. According to the RFI[1] released by IARPA their constraint is to be able to scale up rapidly in times of emergency but with security equivalent to an air-gapped private enclave. If the tenants of the co-location data-center agree to let the federal agencies use infrastructure in times of national emergency it would require all participating organizations to provide some security framework and ability to rapidly re-purpose hardware for government use. Such an arrangement will be both time sensitive and security sensitive.

2 System Architecture

2.1 Requirements

A system where different tenants are willing to share resources from their clusters would have to meet the following requirements

1. **Isolation & Bare-metal Multiplexing:** Each organization has developed in-house deployment methods and processes that help them to maximize usage of their resources. For a system that allows borrowing of hardware resources from one owner to another, it must provide a mechanism to provide complete control to the borrower over physical machines that includes all the capabilities they use to debug an installation when there is a failure. Also, the borrowed portion of the cluster should be isolated from the infrastructure used by other users.

2. **Fast provisioning:** Many organizations would be reluctant to offer their resources outside of their cluster if there is no assurance of getting resources when they need

it. Especially for clusters with short term unpredictable demand and time sensitive response (see §1.4.2, pg-2), the ability to have hardware ready for servicing requests rapidly is important. For supporting such clusters it is important to have a mechanism that allows addition/release of servers in a short time interval.

3. **The Security Model:** Different organizations value security differently. A systems researcher (see §1.4.3, pg-3) may not spend as much time and effort to ensure the security of its system as would a security sensitive organization (see §1.4.4, pg-3). Sharing a bare-metal node between clusters with different security requirements can be a major source of concern. To make server exchange possible between group with different standards for security we need a mechanism that allows the borrowing organization to verify whether a server matches the security standard of its cluster.

4. **The Incentive Model:** Building a system that provides fast and secure mechanism for sharing physical servers between organizations does not guarantee that sharing will occur. The use-cases ((see §1.4, pg-3) are an indicative list of organizations which may not trust each other or would be otherwise in competition with each other. We need a mechanism to encourage exchange of resources where no one organization dictates how the resources are allocated. Ideally, we would want a system that allocates resources to the cluster that expresses highest need for it and provides incentives to participating clusters to actively share their under-utilized resources. A marketplace like mechanism that rewards sharing of resources between organizations is an important requirement.

2.2 Design Principles and Architecture

The thesis adopts following design principles towards creating the proposed system. The proposed system will 1. Give control to tenants as much as possible; 2. Will minimize shared services that everyone needs to use which is essential for security purposes and to enable new capabilities. 3. Partition components into micro-services. This will help in software maintenance and support tenants deploying their own services. 4. Exploit marketplace based model that uses incentives to encourage participation rather than a top down decision making system.

We choose to build each component as a microservice so we can have a system that is composed of multiple services, each of which caters to a function; can scale on demand without affecting other components; has its own development life-cycle; and has a well defined API interface for collaborating with other services. Loose coupling and interaction by message passing via defined APIs has the advantage of composing the services in more than one way.

Architecture of a Elastic Secure Infrastructure (ESI)

Figure (2·1-*left*) shows the architecture overview of ESI. Organization-X offers its hardware via the *incentive system* while customers request hardware from the *incentive system*. When a match is found, 1. Customer uses the *Isolation Service* to allocates the server to its cluster. 2. Use the *Attestation Service* to checks the integrity of the server. 3. sets it up

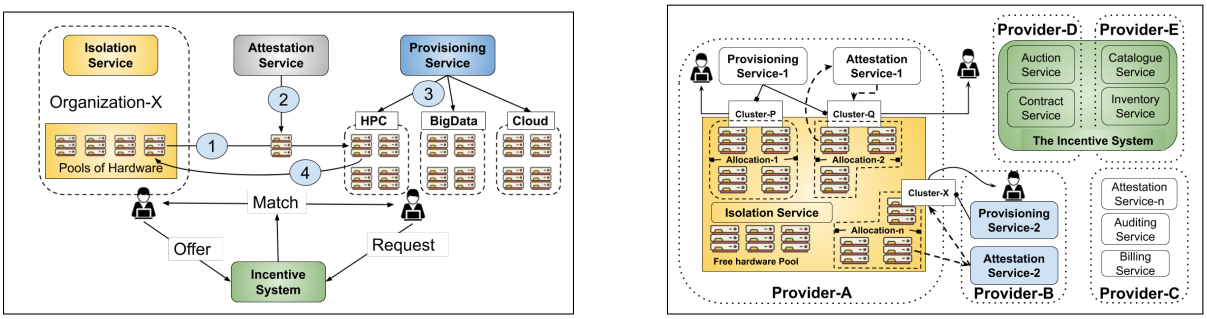

Figure 2·1: (Left) ESI Architecture Overview, (Right) Multiprovider Bare-metal market place: *The Isolation Service* is the only service of the provider (*provider-A*) that tenants have to trust. *Cluster-P* is setup using *Isolation service + Provisioning service-1*. *Cluster-Q* is setup using *Isolation service + Provisioning service-1 + Attestation service-1*. *Cluster-X* is setup using the *Isolation service + Provisioning Service-2 + Attestation Service-2*. Users can also use third party services offered by providers like *Provider-C*. The *incentive system* shows tentative list of services, that may be hosted by different providers, here (*Provider-D,E*)

with system and application software using the *Provisioning Service* 4. When the user no longer needs the server, she uses the *Isolation Service* to return the server.

Following the OCX model, a multi-provider elastic secure infrastructure shall be composed of microservices owned by different tenants as shown in Figure (2·1-*right*). *An Isolation Service* is the only service of the provider (*provider-A*) that tenants have to trust. Tenants can choose to setup their clusters depending on their level of trust on the provider. For example, users that fully trust the provider (*Cluster-P*, used internally by *Provider-A*) may simplify their deployment process by not choosing to use any security or choose to depend on the provider for its security (*Cluster-Q*). Tenants that do not wish to trust the provider can either host their own services (*cluster-X* used by *provider-B*) or use third party services (*attestation service-n* from *Provider-C*). Similarly, the *Incentive system* is proposed to be a combination of services that may be hosted by different providers (*Provider-D,E*).

The focus of this thesis is limited to designing and prototype implementation of an isolation service, a provisioning service, a security model and an incentive model.

1. *An Isolation Service* is a new fundamental layer that allows different physical provisioning systems to share the data center while allowing resources to move back and forth between them. We take an Exokernel-like [19] approach where the lowest layer only isolates/multiplexes the physical resources. It partitions physical hardware and connectivity, while enabling direct access to those resources to the physical provisioning systems that use them.

2. *A Provisioning Service* serves user images that contain the operating system (OS) and applications from remote-mounted boot drives. It relies on a fast and reliable distributed a storage system (CEPH [21], [22] in our implementation) for hosting images of provisioned bare-metal instances.

3. *A Security Model* that enables tenants to control trade-offs between security, price and performance. Security-sensitive tenants can minimize their trust in the provider and achieve similar levels of security and control that they can obtain in their private

data center. At the same time, this framework does not impose overhead on tenants that are security insensitive nor compromises the flexibility or operational efficiency of the provider.

4. *An Incentive Model* proposed here follows a market based economic model where • every tenants earns revenue for offering resources, • change in overall demand and supply is reflected by dynamic changes in the price of the resource, • auctions decide the best placement of resources among competing demands.

This project has involved large number of different people including students, researchers, and developers. I have co-led the design, development and prototype implementation of the isolation service and the security model while worked as a part of the team that designed and implemented the provisioning service. I am leading the efforts towards building the incentive system.

3 Work Completed

3.1 Hardware Isolation Layer (HIL)

Our implementation of the *Bare-metal Allocation and Isolation Service* is called the "Hardware Isolation Layer" or HIL. It decouples the functionality of resource allocation of bare-metal servers from the functionality of installing systems and application software on the servers. It takes the Exokernel-like[10] approach where the lowest layer only isolates/multiplexes the resources and richer functionality is provided by systems that run on top of it. With HIL, we partition physical hardware and connectivity, while enabling direct access to those resources to the physical provisioning systems that use them. HIL uses a driver based model where a standard API maps to different out of band (OBM) modules used for power-cycling physical servers or calls related to network isolation are handled by switch specific drivers.

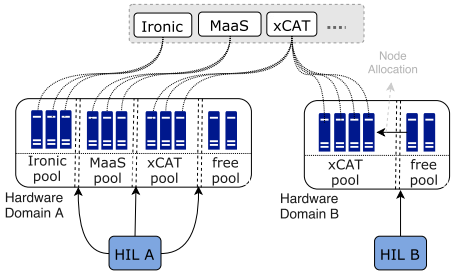

Figure 3·1: HIL provides strong network-based isolation between flexibly-allocated pools of hardware resources, enabling normally incompatible provisioning engines (e.g. Ironic, MaaS, xCAT) to manage nodes in a data center.

This approach makes HIL adaptable to any new OBM module or network control switch. It also allows existing provisioning systems, including Ironic, MaaS, and Foreman, to be adapted with little or no change. Figure 3·1 provides a diagrammatic overview of how HIL can enable provisioning systems to build clusters using servers from different pools of hardware. The fundamental operations HIL provides are *1)* allocation of physical nodes, *2)* allocation of networks, and *3)* connecting these nodes and networks. In normal use a user would interact with HIL to allocate nodes into a pool, create a management network between the nodes, and then connect this network to a provisioning tool such as Ironic or MaaS. As demand grows, the user can allocate additional nodes from the free pool; when demand shrinks, they may be released for other use. Developed with less than 3,000 lines of code in the core functionality, this is a minimalist and the only service that has to be

trusted by the organizations borrowing bare-metal nodes from owning clusters.

3.2 Bare-metal Provisioning Service (BMI)

Our implementation of *Provisioning Service* is called Bare-metal Provisioning Service or BMI. It makes use of remote-mounted boot-drives to host user images containing the operating system and applications. It exploits advancements in disaggregated storage and networking technologies to offer performance comparable to local-disk-based systems. The rapid provisioning and snapshotting capabilities offer elasticity and support for fast transition among different frameworks for datacenter administrators.

3.3 Bolted - The Security Model

To enable a multi-provider bare-metal exchange between providers with varying security practices Bolted is an implementation of the *security framework* that enables tenants to control trade-offs between security, price, and performance. Security-sensitive[1] tenants can minimize their trust in the provider and achieve similar levels of security and control that they can obtain in their own private data centers. At the same time, Bolted neither imposes overhead on tenants that are security insensitive nor compromises the flexibility or operational efficiency of the provider.

We categorize the threats that the tenant faces into the following phases: *Prior to occupancy:* Malicious (or buggy) firmware can threaten the integrity of a server, as well as that of other servers it is able to contact. A tenant servers firmware may be infected prior to the tenant using it, either by the previous tenant(e.g., by exploiting firmware bugs) or by the cloud provider insider (e.g., by unauthorized firmware modification). *During occupancy:* Although many side-channel attacks are avoided by disallowing concurrent tenants on the same server, if the servers network traffic is not sufficiently isolated, the provider or other concurrent tenants of the cloud may be able to launch attacks against it or eavesdrop on its communication with other servers in the enclave. Moreover,if network attached storage is used (as in our implementation) all communication that is not sufficiently secured between server and storage may be vulnerable. Finally, there is a threat to the tenant from denial of service attacks. *After occupancy:* Once the tenant releases a server, the confidentiality of a tenant may be compromised by any of its state (e.g, storage or memory) being visible to subsequent software running on the server

The security model proposes attestation service (measuring all firmware and software and ensuring that it matches known good values) that can be implemented by the tenant rather than just validation(ensuring that software/firmware is signed by a trusted party).This is critical for firmware which may contain bugs [16, 15, 27, 6, 22, 12] that can disrupt tenant security. Attestation provides a time-of-use proof that the provider has kept the firmware up to date. More generally, the whole process of incorporating a server into an enclave can be attested to the tenant. Further, we propose using deterministically built firmware, so that the tenant can not only inspect it for correct implementation but

[1] "Security-sensitive" organizations are defined as entities that are both willing to pay a significant price (dollars and/or performance) for security and that have the expertise, desire, or requirement to trust their own security arrangements over those of a cloud provider.

then easily check that this is the firmware that is actually executing on the machine assigned to the tenant. For tenant-deployed functionality, small firmware with open source implementations are valuable to enable user-specific customization.

3.4 Results

Here we present some results demonstrating the effectiveness of each service in moving resources between mutually non-trusting bare-metal clusters with different security requirements.

Hardware Isolation Layer

Figure 3·2 shows the performance of synchronous HIL API operations as we scale the number of concurrent clients from 1 to 16, while making requests in a tight loop.

As expected, operations that primarily make use of the DB, like allocating or deallocating a project, node or network, complete in less than a tenth of second even with 16 concurrent clients. Freeing a node takes about 5x the time of the other allocation-related operations and degrades more rapidly with increased concurrency because of a call out to ipmitool to ensure that any consoles connected to the node are released before it is deallocated.

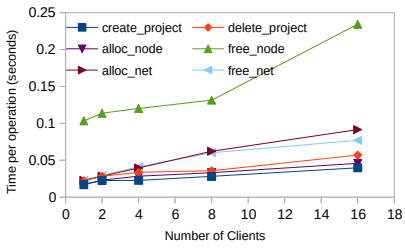

Figure 3·2: Scalability of HIL synchronous operations

Bolted - The Security Model

To understand the elasticity Bolted supports, we first examine its performance for provisioning servers under different assumptions of security. Figure 3·3 compares the time to

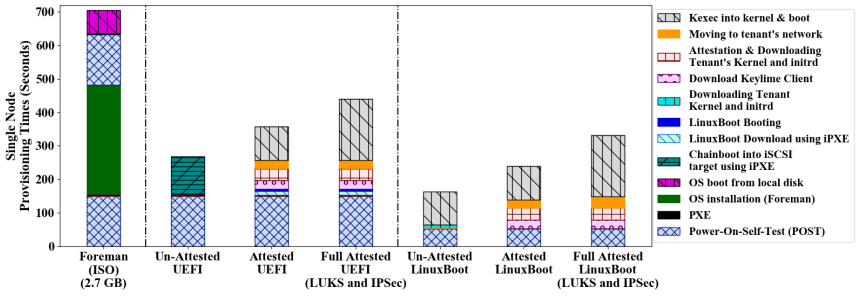

Figure 3·3: Provisioning time of one server.

provision a server with Foreman [11] to Bolted with both UEFI and LinuxBoot firmware under 3 scenarios: *no attestation* which would be used by clients that are insensitive to security, *attestation* where the tenant trusts the provider, but uses (provider deployed) attestation to ensure that previous tenants have not compromised the server, and *Full attestation*, where a security-sensitive tenant that does not trust the provider uses LUKS to encrypt the disk and IPsec to encrypt the path between the client and iSCSI server.

There are a number of important high-level results from this figure. First for tenants that trust the provider, Bolted using LinuxBoot burned in the ROM is able to provision a server in under 3 minutes in the unattested case and under 4 minutes in the attested case; numbers that are very competitive with virtualized clouds. Second, attestation adds only a modest cost to provision a server and is likely a reasonable step for all systems. Third, even for tenants that do not trust the provider, (i.e. LUKS & IPsec) on servers with UEFI, Bolted at ∼7 minutes is still 1.6x faster than Foreman provisioning; note that Foreman implements no security procedures and is likely faster than existing cloud provisioning systems that use techniques like re-flashing firmware to protect tenants from firmware attacks.

4 Pending work

This section discusses the open questions needed to be addressed for the completion of the thesis.

4.1 Incentive System

Building a system that provides fast and secure mechanism for sharing physical servers between organizations does not guarantee that sharing will occur. A centralized system would be more efficient[9, 26, 23, 14, 3, 18] and may be adequate for sharing resources across clusters owned by a single organization but may not be suitable for a co-location facility or a multi-provider cloud. With providers/tenants, each with their own optimization objective, joining and leaving the system regularly, it would be difficult for a centralized system to adapt to continuously changing requirements. Also, providers would not be willing to relinquish control of their resources to a third party.

As a result, we designed a system with following goals. • Allows organizations to have complete control on how they wish to share their resources, if they choose to share. • Provides incentives that encourages providers to proactively share their resources with others. • Uses fair and transparent mechanisms for matching resources to jobs that expresses the highest need for it. • Offers a revenue mechanism for the providers to realize the OCX model.

We propose an incentive based systemof sharing resources that follows a market-based economic model. Every resource is priced using a standard currency. Price of a resource (say a bare-metal server) indicates its overall demand across all clusters at a given point of time. A price rise of a resource indicates that either its availability has reduced or more jobs are demanding that specific resource. It is an incentive for organizations to offer more of those resources. Similarly, price drop is an indication of resource abundance or reduction in demand. Organizations may take advantage of the price drop to fulfill more jobs. Essentially, with such a system everyone is better off sharing their resources than not. And in the event a cluster is not able to find suitable shared resources its utilization is only as bad as when it was a statically partitioned silo. Also, dynamic change in prices allows different organizations to offer their resources and express their demands without revealing any more information than is needed.

4.2 Open Questions

1. Is it feasible to have a bare-metal marketplace ? **Proposed Approach:** Show using prototype implementation what are the real world issues towards realizing such a system.

2. Is the model general enough that clusters with different optimization objective can benefit from participating in the marketplace ? **Proposed Approach:** Using simulations, show that clusters with different optimization objectives benefit from sharing their servers in the marketplace.

3. Compared to static partitioning how much more jobs can a cluster service by participating in a marketplace? **Proposed Approach:** Using trace simulation, show how much more overall work can be accomplished when participants are willing to share servers in the market.

Proposed Methodology

To answer the above question we propose building a prototype implementation and a simulator of the marketplace. Prototype implementation will allow us to study the complexity of building such a system. Simulator will use traces from different clusters (Cloud, BigData, HPC) to study its properties at a larger scale.

4.3 Proposed Timeline

- Allocation and Isolation Service: Done. Published in *SoCC 2016[13]*
- Provisioning Service: Done. Published in *Hot Cloud 2016[24], IC2E 2018[19]*
- Security Framework: Done Published in *USENIX Hot Cloud 2018[21] & ATC 2019[20]*
- The Incentive Model: (Aiming to submit it at OSDI 2020)
  - Prototype and preliminary results : Spring Semester 2020
- Thesis writing: Summer 2020
- Thesis Defense: Fall Semester 2020

Bibliography

[1] Creating a Classified Processing Enclave in the Public Cloud |IARPA, 2017. https://www.iarpa.gov/index.php/working-with-iarpa/requests-for-information/creating-a-classified-processing-enclave-in-the-public-cloud.

[2] The Massachusetts Green High Performance Computing Center, 2019. https://www.mghpcc.org/.

[3] Anderson, D. P. Boinc: A system for public-resource computing and storage. In *proceedings of the 5th IEEE/ACM International Workshop on Grid Computing* (2004), IEEE Computer Society, pp. 4–10.

[4] Berman, M., Chase, J. S., Landweber, L., et al. Geni: A federated testbed for innovative network experiments. *Computer Networks 61*, 0 (2014), 5 – 23. Special issue on Future Internet Testbeds.

[5] Bestavros, A., and Krieger, O. Toward an open cloud marketplace: Vision and first steps. *IEEE Internet Computing 18*, 1 (Jan 2014), 72–77.

[6] Bulygin, Y., Loucaides, J., Furtak, A., Bazhaniuk, O., and Matrosov, A. Summary of attacks against BIOS and secure boot. *Defcon-22* (2014).

[7] Butler, B. Which is cheaper: Public or private clouds?, Oct. 2016. https://www.networkworld.com/article/3131942/which-is-cheaper-public-or-private-clouds.html.

[8] Canonical. Metal as a Service. https://maas.ubuntu.com/.

[9] Duplyakin, D., Johnson, D., and Ricci, R. The part-time cloud: Enabling balanced elasticity between diverse computing environments. In *Proceedings of the 8th Workshop on Scientific Cloud Computing* (New York, NY, USA, 2017), ScienceCloud '17, ACM, pp. 1–8.

[10] Engler, D. R., Kaashoek, M. F., and Otoole, J. Exokernel: an operating system architecture for application-level resource management. In *ACM SIGOPS Operating Systems Review* (New York, NY, USA, 1995), SOSP '95, pp. 251–266.

[11] Foreman. Foreman provisioning and configuration system. http://theforeman.org.

[12] Heasman, J. Rootkit threats. *Network Security 2006*, 1 (2006), 18–19.

[13] Hennessey, J., Tikale, S., Turk, A., Kaynar, E. U., Hill, C., Desnoyers, P., and Krieger, O. Hil: Designing an exokernel for the data center. In *Proceedings of the Seventh ACM Symposium on Cloud Computing* (New York, NY, USA, 2016), SoCC '16, ACM, pp. 155–168. http://doi.acm.org/10.1145/2987550.2987588.

[14] Hindman, B., Konwinski, A., Zaharia, M., Ghodsi, A., Joseph, A. D., Katz, R. H., Shenker, S., and Stoica, I. Mesos: A platform for fine-grained resource sharing in the data center. In *NSDI* (2011), vol. 11, pp. 22–22.

[15] Hudson, T., Kovah, X., and Kallenberg, C. ThunderStrike 2: Sith Strike. *Black Hat USA Briefings* (2015).

[16] Hudson, T., and Rudolph, L. Thunderstrike: EFI firmware bootkits for Apple Macbooks. In *Proceedings of the 8th ACM International Systems and Storage Conference* (2015), ACM, p. 15.

[17] Kirkwood, G., and Suarez, A. Cloud Wars! Public vs Private Cloud Economics, 2017. `https://www.openstack.org/summit/boston-2017/summit-schedule/events/17910/cloud-wars-public-vs-private-cloud-economics`.

[18] Lai, K., Huberman, B. A., and Fine, L. Tycoon: A distributed market-based resource allocation system. *arXiv preprint cs/0404013* (2004).

[19] Mohan, A., Turk, A., Gudimetla, R. S., Tikale, S., Hennesey, J., Kaynar, U., Cooperman, G., Desnoyers, P., and Krieger, O. M2: Malleable Metal as a Service. In *2018 IEEE International Conference on Cloud Engineering (IC2E)* (Apr. 2018), pp. 61–71. `https://arxiv.org/pdf/1801.00540.pdf`.

[20] Mosayyebzadeh, A., Mohan, A., Tikale, S., Abdi, M., Schear, N., Hudson, T., Munson, C., Rudolph, L., Cooperman, G., Desnoyers, P., and Krieger, O. Supporting security sensitive tenants in a bare-metal cloud. In *2019 USENIX Annual Technical Conference (USENIX ATC 19)* (Renton, WA, July 2019), USENIX Association, pp. 587–602.

[21] Mosayyebzadeh, A., Ravago, G., Mohan, A., Raza, A., Tikale, S., Schear, N., Hudson, T., Hennessey, J., Ansari, N., Hogan, K., Munson, C., Rudolph, L., Cooperman, G., Desnoyers, P., and Krieger, O. A secure cloud with minimal provider trust. In *10th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 18)* (Boston, MA, 2018), USENIX Association. `https://www.usenix.org/conference/hotcloud18/presentation/mosayyebzadeh`.

[22] Rutkowska, J. Intel x86 considered harmful, 2015. `https://blog.invisiblethings.org/papers/2015/x86_harmful.pdf`.

[23] Schwarzkopf, M., Konwinski, A., Abd-El-Malek, M., and Wilkes, J. Omega: flexible, scalable schedulers for large compute clusters. In *SIGOPS European Conference on Computer Systems (EuroSys)* (Prague, Czech Republic, 2013), pp. 351–364.

[24] Turk, A., Gudimetla, R. S., Kaynar, E. U., Hennessey, J., Tikale, S., Desnoyers, P., and Krieger, O. An experiment on bare-metal bigdata provisioning. In *8th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 16)* (Denver, CO, 2016), USENIX Association. `https://www.usenix.org/conference/hotcloud16/workshop-program/presentation/turk`.

[25] Van der Veen, D., et al. Openstack ironic wiki. `https://wiki.openstack.org/wiki/Ironic`.

[26] Verma, A., Pedrosa, L., Korupolu, M., Oppenheimer, D., Tune, E., and Wilkes, J. Large-scale cluster management at google with borg. In *Proceedings of the Tenth European Conference on Computer Systems* (New York, NY, USA, 2015), EuroSys '15, ACM, pp. 18:1–18:17.

[27] Wagner, H., Zach, D.-I. M., and Lintenhofer, D.-I. F. M. A.-P. BIOS-rootkit LightEater.

[28] White, B., Lepreau, J., Stoller, L., Ricci, R., et al. An Integrated Experimental Environment for Distributed Systems and Networks. *SIGOPS Oper. Syst. Rev. 36*, SI (Dec. 2002), 255–270.