A Simplified Cloud

Cloud Controller (CLC)

Cluster Controller (CC)

Node Controller (NC)

VM VM VM

Node Controller (NC)

VM VM VM

Node Controller (NC)

VM VM VM

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
A Simplified Cloud

Monitor the Cloud

- To provide system-wide visibility
- CloudWatch (AWS/Eucalyptus)
A Simplified Cloud

Monitor the Cloud

- To provide system-wide visibility
- CloudWatch (AWS/Eucalyptus)
A Simplified Cloud

Monitor the Cloud

- To provide system-wide visibility
- CloudWatch (AWS/Eucalyptus)

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
A Simplified Cloud

Monitor the Cloud

- To provide system-wide visibility
- CloudWatch (AWS/Eucalyptus)
A Simplified Cloud

**Questions**

1. Monitor more efficiently?
2. Utilize the statistics for security purpose?
ATOM Architecture

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
ATOM Architecture
ATOM Architecture

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
ATOM Architecture
ATOM Architecture
ATOM Architecture
ATOM Architecture

**Motivation**

**Design**

**Evaluation**

**Discussion**

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
ATOM Architecture

ATOMIC: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
ATOM Architecture

Motivation

Design

Evaluation

Discussion

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
What if a small error $\Delta$ is allowed?

$\text{Sequence: } \{0, 6, 0, 6, 0, 6, \ldots \}$; $\Delta = 4$

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Tracking Component

What if a small error $\Delta$ is allowed?

- Sequence: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Tracking Component

What if a small error $\Delta$ is allowed?

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Tracking Component

Node Controller \rightarrow \{CPUUtilization, NetworkIn, DiskReadBytes, \ldots\} \rightarrow Cloud Controller

What if a small error $\Delta$ is allowed?

- Sequence: \{0, 6, 0, 6, 0, 6, \ldots\}; $\Delta = 4$
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}; \; \Delta = 4$
- **A naive way:**
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- A naive way:
What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}; \quad \Delta = 4$
- **A naive way:**

\[
\begin{array}{c}
\text{Data Value} \\
6 \\
4 \\
2 \\
0 \\
\end{array}
\]

\[
\begin{array}{c}
\text{Time} \\
0 \\
\end{array}
\]
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence:** \( \{0, 6, 0, 6, 0, 6, \ldots\}; \; \Delta = 4 \)
- **A naive way:**

![Graph showing data value over time]
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}; \quad \Delta = 4$
- **A naive way:**

![Graph showing a data value over time](image)
Tracking Component

Node Controller \{CPUUtilization, NetworkIn, DiskReadBytes, \ldots\} \rightarrow Cloud Controller

What if a small error $\Delta$ is allowed?

- **Sequence:** \{0, 6, 0, 6, 0, 6, \ldots\}; $\Delta = 4$

- **A naive way:**

![Graph showing data value changes over time](image)
Tracking Component

What if a small error $\Delta$ is allowed?
- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- A naive way:

![Graph showing data value over time with error tolerance]
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- **A naive way:**
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- **A naive way:**

```
Data Value

0  2  4  6

Time
```
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}$; $\Delta = 4$
- A naive way:

![Graph showing data values over time](image)

**ATOM**: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- **A naive way**:

* Values sent: $\{0, 6, 0, 6, 0, 6, \ldots\}$
Tracking Component

What if a small error $\Delta$ is allowed?

- Sequence: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$

- A naive way:

* Values sent: $\{0, 6, 0, 6, 0, 6, \ldots\}$
* Optimal offline algorithm could only send one value: 3
**Tracking Component**

What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- **A naive way:**

```
* Values sent: $\{0, 6, 0, 6, 0, 6, \ldots\}$
* Optimal offline algorithm could only send one value: 3
* Competitive ratio: Unbounded
```
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- **The optimal one dimension online tracking algorithm:**

![Graph showing data values over time](image)
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- **The optimal one dimension online tracking algorithm**:
Tracking Component

What if a small error $\Delta$ is allowed?

- Sequence: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- The optimal one dimension online tracking algorithm:

![Diagram showing Node Controller connected to Cloud Controller with data points (0, 6) and a line indicating data value over time.](image)
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}$; $\Delta = 4$
- The optimal one dimension online tracking algorithm:
What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}$; $\Delta = 4$
- **The optimal one dimension online tracking algorithm**: 

![Diagram](image-url)
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence:** $\{0, 6, 0, 6, 0, 6, \ldots\}$; $\Delta = 4$
- The optimal one dimension online tracking algorithm:

![Diagram of tracking component]
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- The optimal one dimension online tracking algorithm:
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \Delta = 4$
- The optimal one dimension online tracking algorithm:

```
Values sent: \{0, 3\}
Competitive ratio: \log \Delta
```
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\} \; ; \; \Delta = 4$
- **The optimal one dimension online tracking algorithm**:

* Values sent: $\{0, 3\}$
Tracking Component

What if a small error $\Delta$ is allowed?

- **Sequence**: $\{0, 6, 0, 6, 0, 6, \ldots\}; \quad \Delta = 4$
- **The optimal one dimension online tracking algorithm**:
  - Values sent: $\{0, 3\}$
  - Competitive ratio: $\log \Delta$

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Tracking Component
ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Monitoring Component

Data matrix reported from each node (with up to \( \Delta \) tracking error):

\[
\begin{bmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0 d} \\
& \vdots & \ddots & \ddots & \vdots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{\text{now}0} & V_{\text{now}1} & V_{\text{now}2} & \cdots & V_{\text{now}d}
\end{bmatrix}
\]

Anomaly detection using this matrix.

Use Principal Component Analysis (PCA).

Sliding window.
## Monitoring Component

Data matrix reported from each node (with up to $\Delta$ tracking error):

\[
\begin{pmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \ddots & \ddots & \cdots & \vdots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(now)0} & V_{(now)1} & V_{(now)2} & \cdots & V_{(now)d}
\end{pmatrix}
\]

$n$ time instances

$d$ metrics
Monitoring Component

Data matrix reported from each node (with up to $\Delta$ tracking error):

\[
\begin{pmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(\text{now})0} & V_{(\text{now})1} & V_{(\text{now})2} & \cdots & V_{(\text{now})d}
\end{pmatrix}
\]

$d$ metrics \hspace{1cm} $n$ time instances

- Anomaly detection using this matrix;
Monitoring Component

Data matrix reported from each node (with up to $\Delta$ tracking error):

$$
\begin{bmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(\text{now})0} & V_{(\text{now})1} & V_{(\text{now})2} & \cdots & V_{(\text{now})d}
\end{bmatrix}
$$

$n$ time instances

$d$ metrics

- Anomaly detection using this matrix;
- Use Principal Component Analysis (PCA);
Motivation Design Evaluation Discussion

Monitoring Component

Data matrix reported from each node (with up to $\Delta$ tracking error):

$$
\begin{pmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \ddots & & & \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(now)0} & V_{(now)1} & V_{(now)2} & \cdots & V_{(now)d}
\end{pmatrix}
$$

$d$ metrics \(\longleftarrow\) \(n\) time instances

- Anomaly detection using this matrix;
- Use Principal Component Analysis (PCA);
- Sliding window.
Monitoring Component - Anomaly Detection
Monitoring Component - Anomaly Detection

PCA:
Monitoring Component - Anomaly Detection

PCA:
Monitoring Component - Anomaly Detection

PCA:
Monitoring Component - Anomaly Detection

PCA:
Monitoring Component - Anomaly Detection

PCA:

- Threshold
- $\alpha$ is computed according to a given false alarm rate $\alpha$.
- Tracking component introduces error $\Delta$ to data matrix.
- Given $\mu$, dynamically adjust $\Delta$ according to PCA results, to ensure false alarm rate $\in (\alpha - \mu, \alpha + \mu)$. 

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Monitoring Component - Anomaly Detection

PCA:

Threshold $Q_\alpha$ is computed according to a given false alarm rate $\alpha$. 

Projection Length > Threshold

+ Tracking component introduces error $\Delta$ to data matrix.
+ Given $\mu$, dynamically adjust $\Delta$ according to PCA results, to ensure false alarm rate $\in (\alpha - \mu, \alpha + \mu)$. 
Monitoring Component - Anomaly Detection

**PCA:**

- Threshold \( Q_\alpha \) is computed according to a given false alarm rate \( \alpha \).
- Tracking component introduces error \( \Delta \) to data matrix.
Monitoring Component - Anomaly Detection

PCA:

+ Threshold $Q_\alpha$ is computed according to a given false alarm rate $\alpha$.
+ Tracking component introduces error $\Delta$ to data matrix.
+ Given $\mu$, dynamically adjust $\Delta$ according to PCA results, to ensure false alarm rate $\in (\alpha - \mu, \alpha + \mu)$
Monitoring Component - Metrics Identification
Monitoring Component - Metrics Identification

Goal: Pinpoint the abnormal dimensions of suspicious data points to assist Orchestration component.
Monitoring Component - Metrics Identification

Goal: Pinpoint the abnormal dimensions of suspicious data points to assist Orchestration component.

\[
\begin{pmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(now)0} & V_{(now)1} & V_{(now)2} & \cdots & V_{(now)d}
\end{pmatrix}
\]
Monitoring Component - Metrics Identification

Goal: Pinpoint the abnormal dimensions of suspicious data points to assist Orchestration component.

\[
\begin{pmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(now)0} & V_{(now)1} & V_{(now)2} & \cdots & V_{(now)d}
\end{pmatrix}
\]
Goal: Pinpoint the abnormal dimensions of suspicious data points to assist Orchestration component.

\[
\begin{pmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(now)0} & V_{(now)1} & V_{(now)2} & \cdots & V_{(now)d}
\end{pmatrix}
\]

Main idea: Compare each dimension of the abnormal data points and normal ones.
Goal: Pinpoint the abnormal dimensions of suspicious data points to assist Orchestration component.

\[
\begin{pmatrix}
V_{00} & V_{01} & V_{02} & \cdots & V_{0d} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
V_{(n-2)0} & V_{(n-2)1} & V_{(n-2)2} & \cdots & V_{(n-2)d} \\
V_{(n-1)0} & V_{(n-1)1} & V_{(n-1)2} & \cdots & V_{(n-1)d} \\
V_{(now)0} & V_{(now)1} & V_{(now)2} & \cdots & V_{(now)d}
\end{pmatrix}
\]

Main idea: Compare each dimension of the abnormal data points and normal ones.
Monitoring Component
Orchestration Component

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Orchestration Component
Orchestration Component

Virtual Machine Introspection (VMI)

- Introspect VM memory using existing VMI tools;
Motivation Design Evaluation Discussion

Orchestration Component

Virtual Machine Introspection (VMI)

- Introspect VM memory using existing VMI tools;

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Orchestration Component

Virtual Machine Introspection (VMI)

- Introspect VM memory using existing VMI tools;

[Diagram showing memory space with a relevant memory space highlighted]
Orchestration Component

Virtual Machine Introspection (VMI)

- Introspect VM memory using existing VMI tools;
- Raise alarm;
- Optionally, kill process.
Orchestration Component

Virtual Machine Introspection (VMI)

- Introspect VM memory using existing VMI tools;
- Raise alarm;
- Optionally, kill process.
Evaluation

+ Implemented on the Eucalyptus Cloud platform;
Evaluation

- Implemented on the Eucalyptus Cloud platform;

- Modified Node Controller and Cloud Controller source code.
Recall the two questions:

1. Monitor more efficiently?
   - Tracking Component
2. Utilize the statistics for security purpose?
   - Monitoring and Orchestration Component
Evaluation

Recall the two questions:

1. Monitor more efficiently?
Recall the two questions:

1. Monitor more efficiently?

2. Utilize the statistics for security purpose?
Recall the two questions:

1. Monitor more efficiently?
   - Tracking Component

2. Utilize the statistics for security purpose?
Recall the two questions:

1. Monitor more efficiently?
   - Tracking Component

2. Utilize the statistics for security purpose?
   - Monitoring and Orchestration Component
Recall the two questions:

1. Monitor more efficiently?
   - Tracking Component

2. Utilize the statistics for security purpose?
   - Monitoring and Orchestration Component

Metrics monitored for each VM:

- The default 7 metrics monitored by Eucalyptus CloudWatch.
Evaluation - Tracking

A comparison on number of values sent by NC for each metric.

- VM workload: TPC-C benchmark on MySQL database;
- \( \Delta \): The average for each metric when VM is \textit{idle}.
Evaluation - Tracking

A comparison on number of values sent by NC for each metric.

- VM workload: TPC-C benchmark on MySQL database;
- $\Delta$: The average for each metric when VM is idle.
Evaluation - Monitoring

Experiment setting:

- 3 VMs being monitored: VM 1 idle, VM 2 and 3 run Apache web server;
- VM 2 and 3 are compromised as DDoS bots later.
Evaluation - Monitoring

Experiment setting:

- 3 VMs being monitored: VM 1 idle, VM 2 and 3 run Apache web server;
- VM 2 and 3 are compromised as DDoS bots later.
Evaluation - Monitoring

Experiment setting:

- 3 VMs being monitored: VM 1 idle, VM 2 and 3 run Apache web server;
- VM 2 and 3 are compromised as DDoS bots later.

### Metrics Identification Result

<table>
<thead>
<tr>
<th>Dim (j)</th>
<th>vm1-d1</th>
<th>vm1-d2</th>
<th>vm1-d3</th>
<th>vm1-d4</th>
<th>vm1-d5</th>
<th>vm1-d6</th>
<th>vm1-d7</th>
<th>vm2-d1</th>
<th>vm2-d2</th>
<th>vm2-d3</th>
<th>vm2-d4</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd(j)</td>
<td>23.70</td>
<td>-0.98</td>
<td>-0.98</td>
<td>-0.55</td>
<td>-0.57</td>
<td>4.27</td>
<td>3.76</td>
<td>9.14</td>
<td>64.18</td>
<td>65.05</td>
<td>3.50</td>
</tr>
<tr>
<td>stddev(j)</td>
<td>0.78</td>
<td>0.42</td>
<td>0.58</td>
<td>0.00</td>
<td>0.67</td>
<td>0.00</td>
<td>0.71</td>
<td>3.17</td>
<td>8.01</td>
<td>8.30</td>
<td>0.00</td>
</tr>
<tr>
<td>meandiff(j)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dim (j)</th>
<th>vm2-d5</th>
<th>vm2-d6</th>
<th>vm2-d7</th>
<th>vm3-d1</th>
<th>vm3-d2</th>
<th>vm3-d3</th>
<th>vm3-d4</th>
<th>vm3-d5</th>
<th>vm3-d6</th>
<th>vm3-d7</th>
</tr>
</thead>
<tbody>
<tr>
<td>rd(j)</td>
<td>-0.51</td>
<td>-0.82</td>
<td>4.23</td>
<td>9.04</td>
<td>60.56</td>
<td>61.16</td>
<td>1.45</td>
<td>-0.56</td>
<td>1.89</td>
<td>-0.51</td>
</tr>
<tr>
<td>stddev(j)</td>
<td>0.31</td>
<td>0.00</td>
<td>0.35</td>
<td>7.23</td>
<td>6.06</td>
<td>6.98</td>
<td>0.17</td>
<td>3.39</td>
<td>0.12</td>
<td>3.65</td>
</tr>
<tr>
<td>meandiff(j)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ATOM: Automated Tracking, Orchestration and Monitoring of Resource Usage in Infrastructure as a Service Systems
Evaluation - Orchestration

- Received a VMI request with information:
  - A possible network problem;
  - Similar patterns for VM 2 and 3.
Evaluation - Orchestration

- Received a VMI request with information:
  - A possible network problem;
  - Similar patterns for VM 2 and 3.

- Node Controller call existing VMI tools to introspect:
  - VM 2: Volatility found suspicious DDoS process;
  - VM 3: Same with VM 2?
  - Raise alarm to user;
  - Kill the processes automatically using StackDB if confirmed.
Discussion - Overhead

Overhead introduced:
▶ On NC:
O (1) to apply tracking algorithm and call VMI tools;
▶ On CLC: Depending on the PCA algorithm used, polynomial to sliding window size and number of dimensions monitored.

Overhead saved:
▶ Significant amount of network traffic sending from NC to CC to CLC;
▶ Significant amount of memory space to be introspected by VMI.
Discussion - Overhead

Overhead introduced:

- On NC: $O(1)$ to apply tracking algorithm and call VMI tools;
- On CLC: Depending on the PCA algorithm used, polynomial to sliding window size and number of dimensions monitored.
Discussion - Overhead

Overhead introduced:

- On NC: $O(1)$ to apply tracking algorithm and call VMI tools;
- On CLC: Depending on the PCA algorithm used, polynomial to sliding window size and number of dimensions monitored.

Overhead saved:

- Significant amount of network traffic sending from NC to CC to CLC;
- Significant amount of memory space to be introspected by VMI.
Discussion - Possible Extension

- Monitor more metrics;
- Extend VMI tools to find more complicated attacks.
Discussion - Possible Extension

- Monitor more metrics;
- Extend VMI tools to find more complicated attacks.
Thank you.
Thank you.

Questions?