# Attack-Defense and Performance Adaptations for Social Virtual Reality Learning Environments

Samaikya Valluripally[a], Vaibhav Akashe[a], David Falana[b], Michael Fisher[c], Prof. Khaza Anuarul Hope[a], Prof. Prasad Calyam[a]
University of Missouri-Columbia[a], Rutgers University[b], Columbia College[c]

## INTRODUCTION

- Social Virtual Reality Learning Environments are 3D spaces designed to educate students remotely via online platforms to enhance learning capabilities.
- Lack of handling performance and security factors can cause a disruption of user's learning experience by inducing cybersickness.
- **Our Contributions: (i)** Develop novel model-driven based adaptation framework, to determine the suitable attack-defense or performance adaptation. **(ii)** Create a full application that allows us to observe the performance and functionality of the systems, architectures, and the developed model behavior.

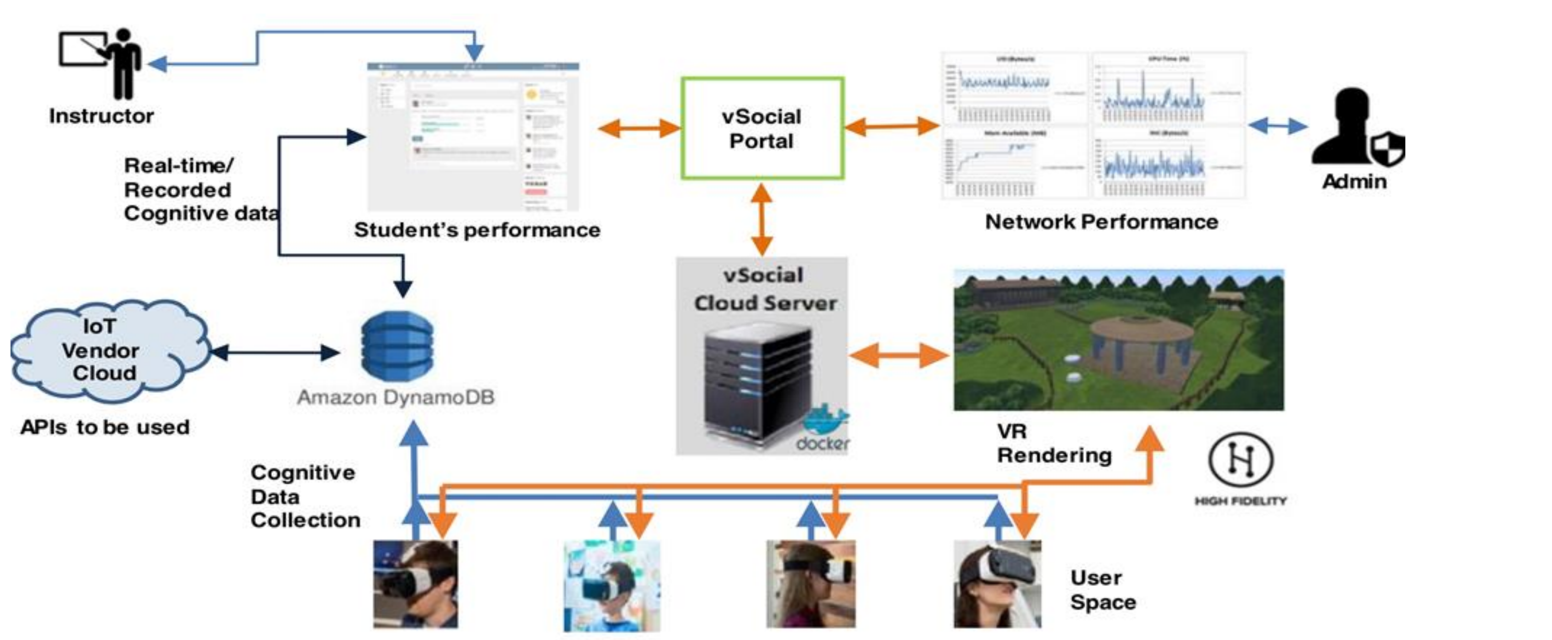



*Figure 1: Overview of vSocial, a Social VRLE for training youth with Autism Spectrum Disorder*

## ANOMALY DATA COLLECTION

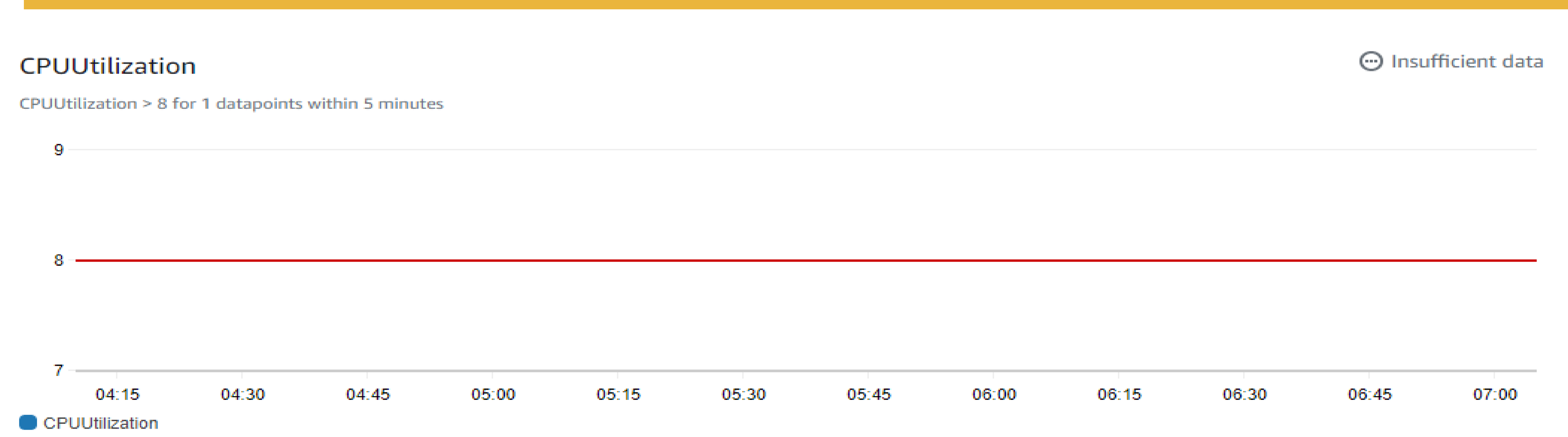
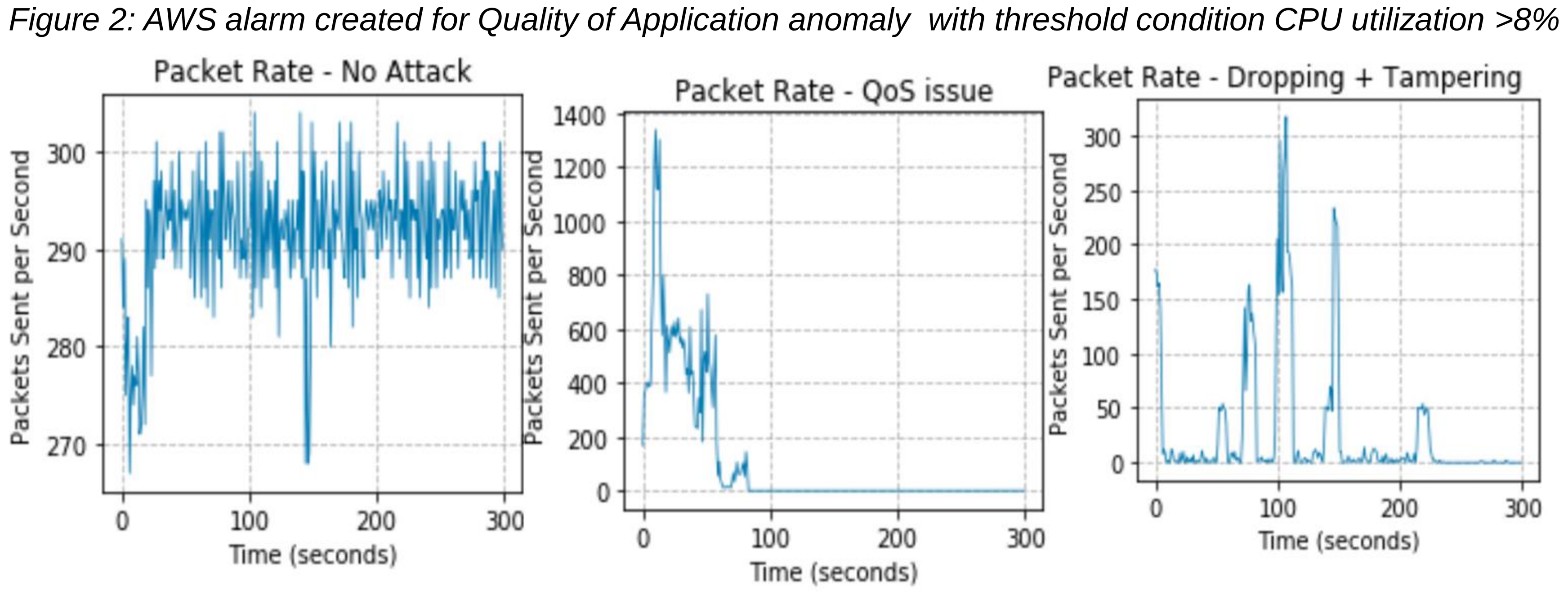



*Figure 2: AWS alarm created for Quality of Application anomaly with threshold condition CPU utilization >8%*




We collected the relevant SPS/3Q anomaly data, once the alarms created in AWS triggers for the vSocial application.

## CONTROL LOOP ADAPTIVE FRAMEWORK

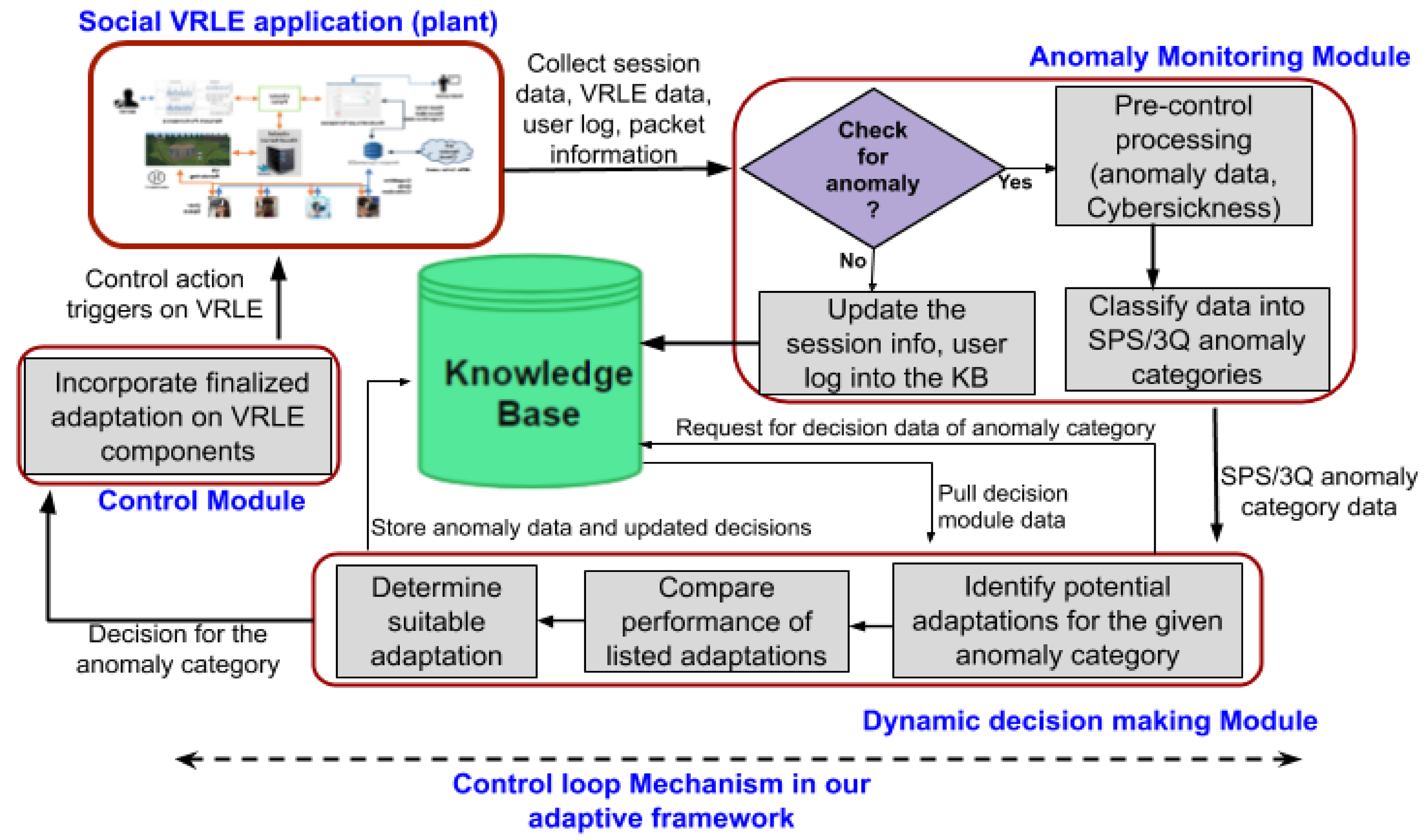



*Figure 3: Adaptative Framework*

Using our proposed control loop adaptive framework, we implement the real-time adaptations to mitigate cybersickness in social VRLEs.

**Step-1:** VRLE data (user data, session info is collected to determine any anomalies using our anomaly monitoring tool

**Step-2**: If any anomaly is detected, our framework proceeds to categorize the anomaly into a performance or security issues.

**Step-3:** Using this categorized data, the framework invokes the decision module to determine the suitable adaptation for the detected SPS/3Q anomaly event.

**Step-4:** The dynamic decision-making algorithm updates the determined adaptation and their respective anomaly into the knowledge base.

**Step-5:** Now, the resultant adaptation is incorporated on the VRLE components and further checked if the anomaly still exists.

## EVALUATION RESULTS

**Anomalies Detected**

| Type | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| SPS | 557.369417 | 128.206.20.46 | 128.206.20.43 | UDP | 92 | 58222 > 62054 Len=50 |
| SPS | 421.962237 | 128.206.20.43 | 128.206.20.46 | UDP | 89 | 40102 > 58222 Len=47 |
| SPS | 553.712925 | 128.206.20.46 | 128.206.20.43 | UDP | 90 | 58222 > 62054 Len=48 |
| SPS | 113.666930 | 128.206.20.46 | 128.206.20.43 | UDP | 78 | 58222 > 62054 Len=36 |
| SPS | 421.248308 | 128.206.20.43 | 128.206.20.46 | UDP | 83 | 62058 > 58222 Len=41 |
| QoA | 82.558665 | 3.20.240.238 | 192.168.10.68 | UDP | 128 | 48001 > 52766 Len=86 |
| SPS | 223.134959 | 128.206.20.46 | 128.206.20.43 | UDP | 90 | 58222 > 62054 Len=48 |
| SPS | 556.242194 | 128.206.20.46 | 128.206.20.43 | UDP | 92 | 58222 > 62054 Len=50 |

*Figure 4: Anomaly Monitoring tool showing the Detected Anomalies related to SPS/3Q events*

| Current Solution | Good Solution 12.8 / Bad Solution | | |
|---|---|---|---|
| **Solution** | **Cost($)** | **Runtime (ms)** | **Resource Cost(mb)** |
| AWS GuardDuty | 1.0 | 513.0 | 128 |

**Active module: SPS**

[AWS GuardDuty, Higher Resources, Higher Network Bandwidth, Enhanced Networking, Upgrading Instance Type]

SPS, 115.244831, 128.206.20.46, 128.206.20.43, UDP, 92, 58222 > 62054 Len=50

*Figure 6: Decision Module determine AWS Guard Duty as the suitable solution to implement for an SPS issue*

| Anomaly Category: | Specific Anomaly Issue: | Adaptation Name: | AWS Service Used: | Threshold Metrics: | Response Time: |
|---|---|---|---|---|---|
| QoA | High CPU Utilization | Upgrading Instance Type (A1) | AWS Lambda | (Before) CPU Utilization 9%<br>(After) CPU Utilization 4% | 553.066 ms |
| | | Higher Resources (A2) | AWS Autoscaling | (Before) CPU Utilization 9%<br>(After) CPU Utilization 4% | 300 s |
| QoS | Low Network Bandwidth | Enabling Enhanced Networking (A3) | AWS Lambda | (Before) Average Network Packets Out >= 7280<br>(After) Average Network Packets Out = 7280 | 900.067 ms |
| | | Higher Network Bandwidth (A4) | AWS Autoscaling | (Before) Average Network Packets Out >= 7280<br>(After) Average Network Packets Out <7280 | 300 s |
| SPS | Unauthorized Access | Malicious Monitoring Tool (A5) | AWS GuardDuty | Best Practices Suggested By AWS Services | 513 ms |

*Figure 5: Performance of the determined adaptations for the detected anomalies using our framework in terms of response time and threshold Metrics*

**Key Findings:**

- We determine the cybersickness occurrence can be quantified using certain QoS (packet loss), QoA (visualization delay) metrics from our simulation experiments in vSocial.
- We perform trade-off analysis of our framework for the decision making of the adaptation in terms of different threshold metrics, system response time, resource usage and cost metric.
- With these results, we also show a before after scenario, where we determine that addressing most vulnerable anomaly (Low bandwidth) can aid in mitigating the cybersickness occurrence with the given response time.
- From our QoA adaptation, the CPU Utilization went from 9% to 4% after the adaption occurred, and for the QoS adaptation we observe the Average Packets Per Second is stabilized to meet the threshold value.

## CONCLUSION

- Proposed a novel control loop adaptive framework to address the performance and security issues that induces cybersickness in a social VRLE application.
- We perform real-time adaptations on the identified issues and mitigate them to reduce the cybersickness level of the users.

In the future, we plan to expand our framework to make active decision making for zero-day anomaly events.

## ACKNOWLEDGEMENTS

Our work was funded by National Science Foundation Awards: CNS-1647213 and CNS-1659134. Any opinions, findings, and conclusions or recommendations expressed in this publications are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.