Securing Elastic Applications for Cloud Computing

Many to One Virtualization

Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, and Sangoh Jeong

Samsung Information Systems America
Pennsylvania State University

Outline

- Cloud Computing for CE devices
- Elastic Application concept and examples
- Security problems and approaches
CE + Cloud Computing (1 of 2)

IT View of Cloud Computing

cloud = web service platform

- Cloud is a platform for service delivery
- Push from services into devices

CE + Cloud Computing (2 of 2)

Proposed CE View of Cloud Computing

cloud = data/core center + API

- Cloud is a platform for new applications that run across the cloud and device ("elastic applications")
- Expand the device into the cloud
Ongoing Approaches for Mobile + Cloud

- CloneCloud (HotCloud’09)
  - Clone of phone image at cloud
- Dynamic Composable Computing (HotMobile’08)
  - Dynamic composition of functions with mobile devices and surrogates.
- Cloudlet (PVC’09)
  - Offloading VM to proximate infrastructure
  - 60-90s on VM synthesis
- HW-supported VM migration (Atom) (MobiCase’09)
  - Focus on mobility of app
- ...

- Elastic Device/Application
  - On application level
  - Dynamic execution configuration
  - More flexible and easy for parallel...

Motivation

CE Devices
- Compute - Fixed
- Storage - Fixed
- Power - Limited
- Bandwidth - Limited
- Applications - CONSTRAINED

The Cloud
- Compute - ELASTIC
- Storage - ELASTIC
- Applications - UNCONSTRAINED

The goal of the Elastic Device project is to enable development of cross device/cloud applications. The advantages are:
- Remove device constraints, create new classes of powerful applications
- Help realize a new business model for device applications
- Provide developers a transition path to multi/many core
Elastic Device Concept

When device resources are sufficient

When device resources are not sufficient

Elastic Applications (EA)

- EA are cloud aware applications
- Weblets
  - Define discrete application components
  - Communicate using REST interface
  - Run on Device or Cloud
  - Can be replicated to handle loads

- Application GUI
  - Launches the program
  - Directs the creation of new weblets

- Manifest
  - Meta-data of EA
  - Dynamic configuration info
  - Integrity of weblets
  - Policies for each weblet
    - E.g. JVM, network, access control, location
Elastic Devices (ED)

- **ED support EAs**
  - Enable seamless migration of weblets
  - Manage resources to optimize costs
  - Interface with cloud providers

- **Elastic Manager**
  - spawns weblets on demand
  - Migrates weblets to / from cloud
  - Senses resource availability

- **Cloud Fabric Interface**
  - Exposes cloud services to devices
  - Controls weblets on behalf of EM
    - Start / Stop / Create / Destroy
  - Can provide PaaS or IaaS model

Benefits

- **Many-to-one virtualization**
  - Seamlessly expands and shrinks of platform capability

- **Dynamic user experience**
  - User control of expending/shrinking based on factors such as battery consuming, monetary cost, latency/throughput, etc.

- **Device flexibility**
  - CE device computation and storage capabilities need not be designed to satisfy the most demanding applications.

- **Dependability**
  - Migrating applications to cloud when device is low in battery/weak signal

- **Future proof**
  - Move app from cloud to device, extend app lifetime, reduce development cost
Challenges

- Application model (data model, concurrency, lang features, ...)
- Performance (QoS, caching, scheduling, ...)
- Dynamic configuration (costs, migration, replication, ...)
- Security (new threats, data privacy, access control, ...)

Reference Architecture

- Elastic application package including UI and weblets
- Cloud nodes running on Amazon EC2 instances
- Web service-based CFI
- Application installation on both cloud and device sides
Elasticity Patterns and Applications

- Elastic image processing
- Elastic augmented reality
- Elastic augmented video

Elastic Image Processing

Samsung Q1 Samsung Omnia

App on Device
(Analysis & Filtering of images)

ElasticIP App

on device: image processing
on cloud: image processing
### Elastic Augmented Video

**Samsung Q1**

- **ElasticAV Application** (identify, track & replace target images)
- **Splitter**
- **Matcher 1**
- **Matcher 2**
- **Matcher n**
- **Tracker**

**ElasticAV Application** (identify, track & replace target images)

**Camera**

**Compositor**

**Planar object recognition and replacement**

**On device:** feature point extraction from video, tracking, compositing

**On cloud:** matching live features against library of target images

---

### Elastic Augmented Reality

**Samsung Galaxy**

- **ElasticAR Application** (register POI icons & real-time info on live camera)
- **Tracker**
- **Compositor**
- **GPS**
- **Crowd Sim**

**On device:** using compass and GPS to align POI markers with live video from camera

**On cloud:** POI service and crowd simulator (gives # people in proximity to POI's)
Security Threats

- **Threats from Applications**
  - Untrusted applications can damage the weblets, weblet containers, the elastic manager, and their behaviors
    - Compromise the code and data integrity of installed elastic applications
    - Change or disable the elastic manager’s functionality
    - Launch weblets on cloud platforms without user authorization/awareness

- **Threats in the Cloud**
  - Malicious change to cloud VM, including VM itself and any configurations.
  - Malicious change to weblet code and data on cloud side
  - Malicious change to network and cost settings: e.g., use expensive network connections
  - Hidden malicious activities that consume cloud resources

- **Threats on the Network**
  - Man-in-the-Middle (MITM) attack:
    - Passive eavesdropping all the traffic in the middle
    - Active replay attack
    - Session hijack.
  - Dynamic Denial-of-Service (DDoS) attack to both ED and cloud
  - Generate random traffic to weblets such consume user bill

Elastic Application Security Requirements

- **Trust**
  - Applications must trust both the cloud and device.

- **Weblets**
  - Communication with weblets must be secure. Only application should be able to issue requests to its weblets.
  - Privacy of weblet data. Maintaining isolation.

- **Migration**
  - What happens to access rights when an weblet is migrated.
  - How are sessions maintained when a weblet is migrated.

- **Monitoring / Aggregation**
  - Want to monitor and collect device and cloud data. Privacy considerations.
  - Using cloud to detect malicious behavior.
5 Security Aspects

I: Building secure communication between weblets:
- Secure session management
- Communication upon authentication
- Secure weblet migration

II: Resource Usage Monitoring, Logging, and Auditing:
- Monitoring resource usage on both ED and cloud
- Detect and confine any malicious behavior

III: Building trusted elastic device:
- Secure downloading and installation
- Secure weblet runtime environment
- Trusted behavior in cloud VM, e.g., no hidden resource consuming

IV: Building trusted cloud VM:
- Authentication and launching weblets
- Secure weblet migration

V: Authorization to access external services:
- Fine-grained permission control
- Secure revocation
- Privacy control

Secure Session and Authentication

- Issues and Challenges:
  - Secure session and authentication with heterogeneous clouds
    - Cloud weblets may need access other cloud/services on behalf of user, so need permission
  - Weblet migration: seamless accessing resource after migration
    - Weblet migrates between ED and cloud
    - Session migration is need to provide seamless runtime performance
  - Least of privilege:
    - Not sharing user account credential in cloud weblets - otherwise malicious weblets can get all user info
    - Give less trust to cloud weblets
    - So far, user does not trust cloud environment too much
  - Permission delegation:
    - A cloud weblet only can access authorized resources specified by the user or application developer
  - Must be efficient
  - Must have minimum application developer awareness:
    - We are building an infrastructure for application developers
  - Must have minimum user interference:
    - E.g., user only needs to login to external web services
Authentication & Session Management

Security Objectives

- **Session Identity**
  - To identify a session between weblets in different locations
  - Identify instances of the same elastic app (EA)

- **Prevent network attacks**
  - Replay attack
  - Session hijack

- **Accountability**
  - Monitor usage and cost of elastic applications

Secure Migration

Security Objectives

- **Integrity**
  - Maintain session secrets and tokens during migration
  - Resume secure communication between weblets

- **Transparency**
  - Transparent to cloud-level migration
  (When a cloud node weblet container is migrated from one physical machine to another.)
Ongoing and Future Work

- Fine-grained authorization for cloud-based weblets
  - Delegate subset of permissions to cloud weblets: less trust for cloud components
  - For least-privilege, information flow control, etc.

- Secure elasticity layer
  - Resistant to compromise

- Verifying distributed application integrity with less trust on service provider
  - Results depend on all weblets’ integrity
  - Data and control flow integrity verification

- Establishing trust in public cloud systems
  - Trusted Computing
  - Integrity Measurement / Verification

Q & A