

## 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)

SAMSUNG



### IT View of Cloud Computing

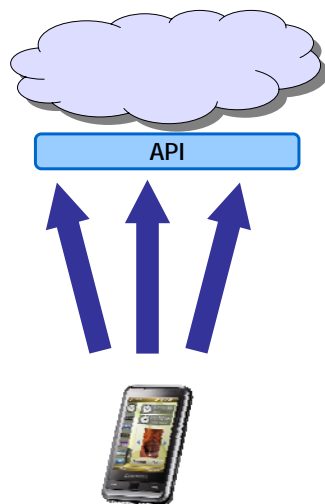
cloud = web service platform

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

- 2 -

## CE + Cloud Computing (2 of 2)

SAMSUNG



### 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

- 3 -

## 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...

- 4 -

## Motivation



### CE Devices



Compute - Fixed  
Storage - Fixed\*  
Power - Limited  
Bandwidth - Limited  
Applications - CONSTRAINED

### The Cloud

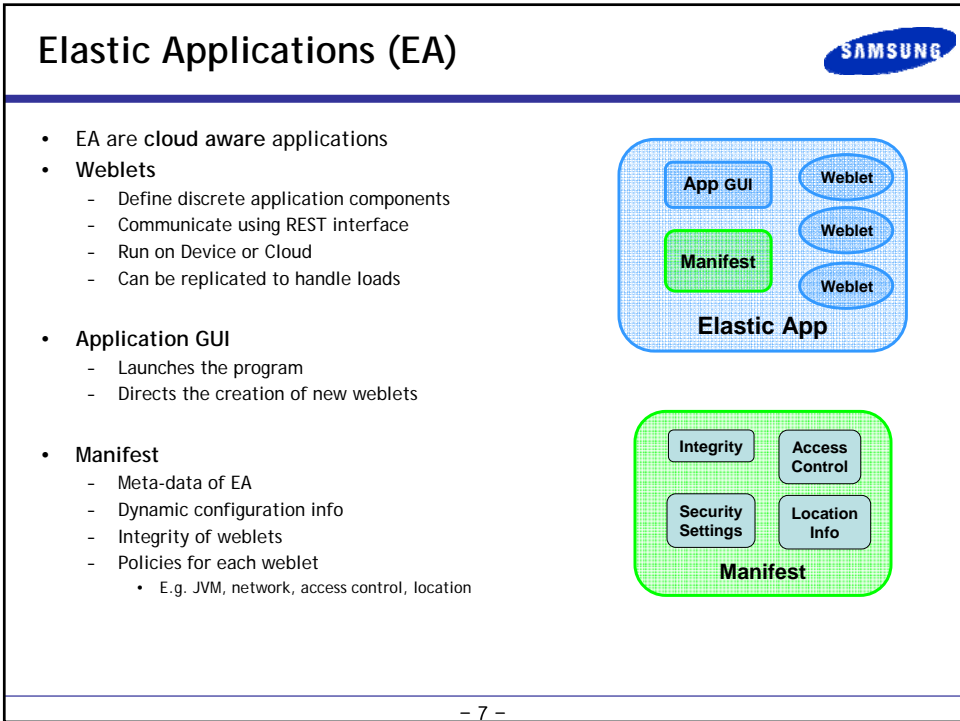
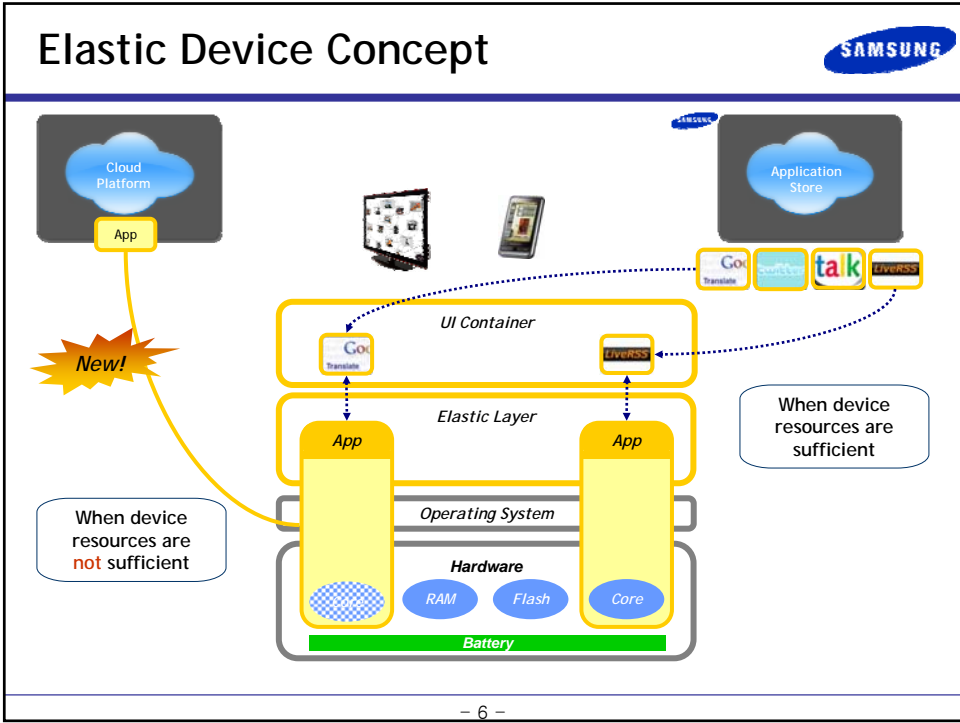


Compute - ELASTIC  
Storage - ELASTIC  
Applications - UNCONSTRAINED

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*

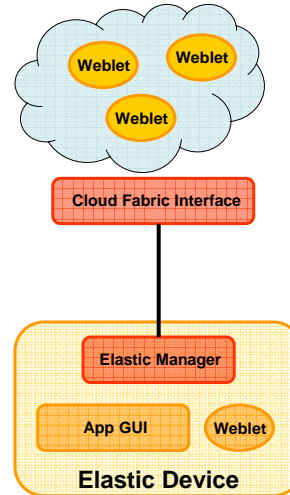
- 5 -



## Elastic Devices (ED)

SAMSUNG

- 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



- 8 -

## Benefits

SAMSUNG

- 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

- 9 -

# Challenges

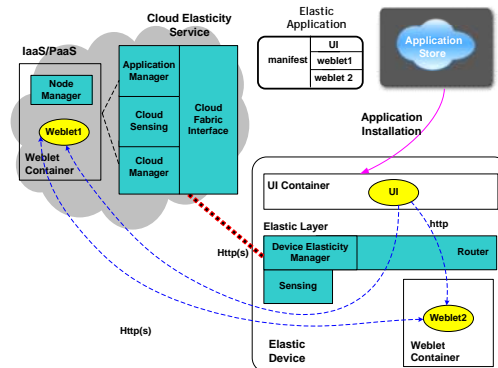


- Application model (data model, concurrency, lang features, ...)
- Performance (QoS, caching, scheduling, ...)
- Dynamic configuration (costs, migration, replication, ...)
- Security (new threats, data privacy, access control, ...)

# 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

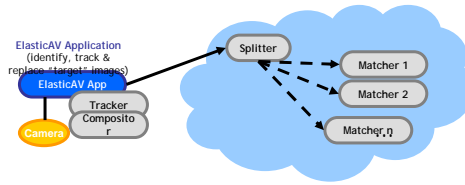
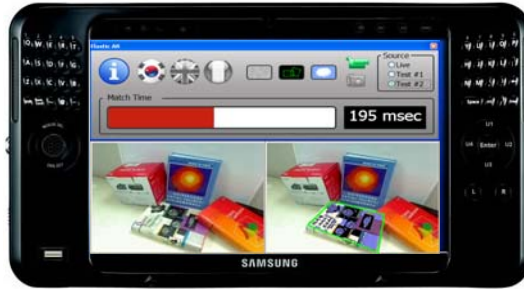
# Elastic Image Processing



# Elastic Augmented Video



Samsung Q1



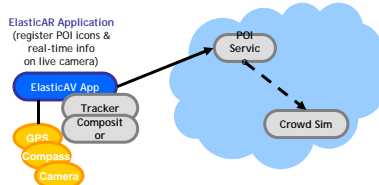
planar object recognition and replacement

**on device:** feature point extraction from video, tracking, compositing  
**on cloud:** matching live features against library of target images

# Elastic Augmented Reality



Samsung Galaxy



**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

- 16 -

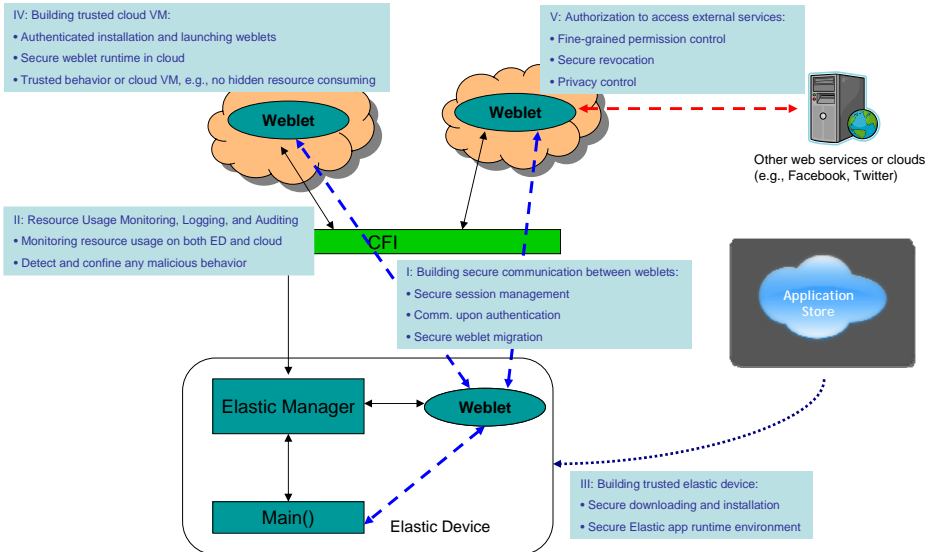
# Elastic Application Security Requirements



- 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.

- 17 -

## 5 Security Aspects



- 18 -

## Secure Session and Authentication



- Issues and Challenges:
  - Secure session and authentication with heterogeneous clouds
    - Cloud weblots may need access other cloud/ws on behalf of user, so need permission
  - Weblot migration: seamless accessing resource after migration
    - weblot migrates between ED and clouds
    - Session migration is need to provide seamless runtime performance
  - Least of privilege:
    - not sharing user account credential in cloud weblots - otherwise malicious weblots can get all user info
    - Give less trust to cloud weblots
    - So far, user does not trust cloud environment too much
  - Permission delegation:
    - a cloud weblot 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

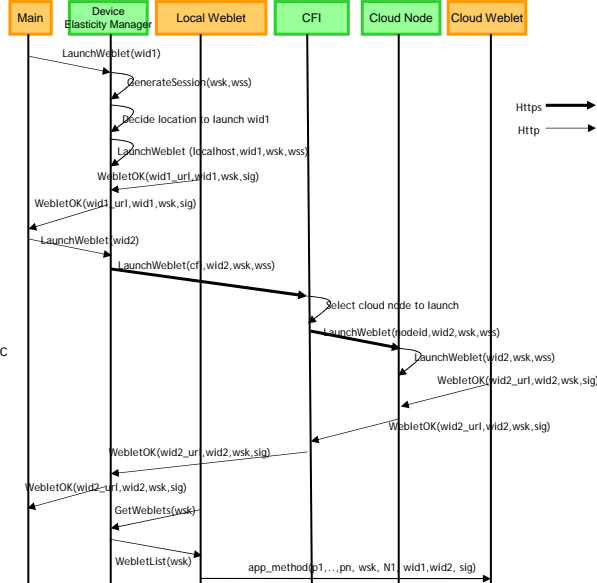
- 19 -

# 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



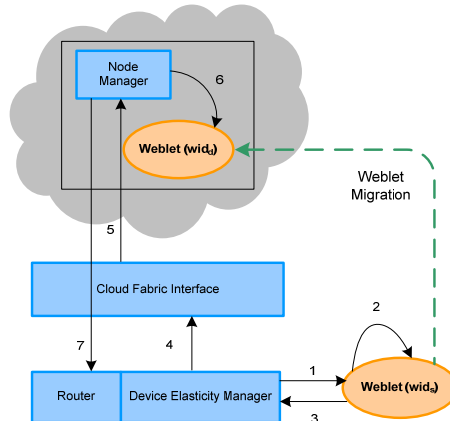
- 20 -

# 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.)



1. DEM -> Weblet : migrate(wid<sub>l</sub>, wsk)
2. Weblet: enter\_migrate(); save\_state(state<sub>s</sub>)
3. Weblet -> DEM: state<sub>s</sub>, wid<sub>l</sub>
4. DEM -> CFI: migrate\_req(wid<sub>l</sub>, wsk, state<sub>s</sub>)
5. CFI -> NM: migrate\_req(wid<sub>l</sub>, wsk, state<sub>s</sub>)
6. NM: LaunchWeblet(localhost, wid<sub>l</sub>, wsk, state<sub>s</sub>)
7. NM -> Router: update\_table(url\_wid<sub>l</sub>, wid<sub>l</sub>, wsk)

- 21 -

## 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

- 22 -

## Q & A



- 23 -