Databases
and
Software
Engineering

▲ Hochschule Harz

Towards Secure Dynamic Product Lines in the Cloud

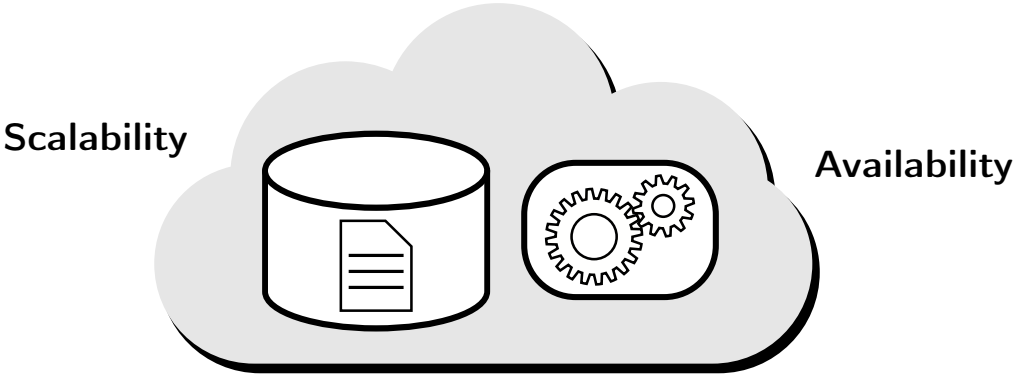
Sebastian Krieter, Jacob Krüger, Nico Weibrodt, Vasily A. Sartakov, Rüdiger Kapitza, Thomas Leich

Harz University of Applied Sciences, University of Magdeburg, TU Braunschweig

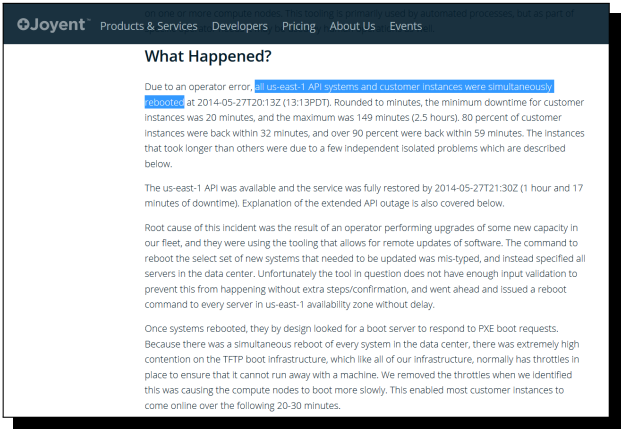
ICSE–NIER 2018

May 29 – June 01 | Gothenburg, Sweden

Motivation



Security Issues in the Cloud



Joyent Products & Services Developers Pricing About Us Events

What Happened?

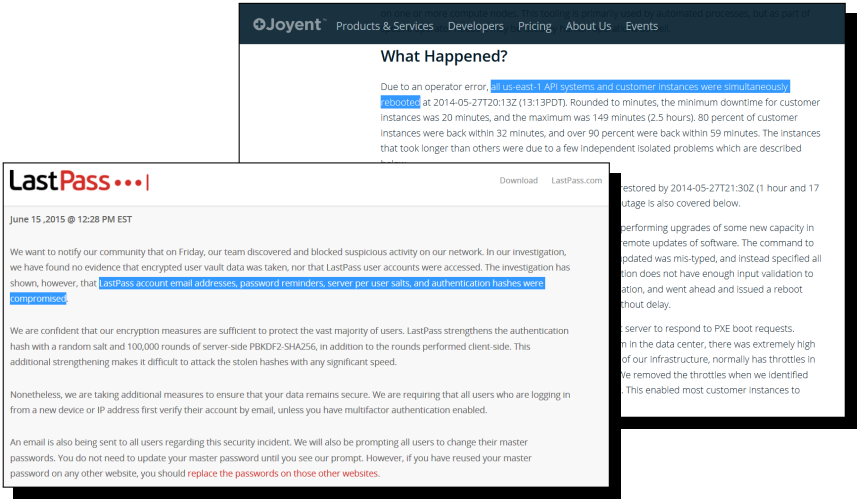
Due to an operator error, all us-east-1 API systems and customer instances were simultaneously rebooted at 2014-05-27T20:13Z (13:13PDT). Rounded to minutes, the minimum downtime for customer instances was 20 minutes, and the maximum was 149 minutes (2.5 hours). 80 percent of customer instances were back within 32 minutes, and over 90 percent were back within 59 minutes. The instances that took longer than others were due to a few independent isolated problems which are described below.

The us-east-1 API was available and the service was fully restored by 2014-05-27T21:30Z (1 hour and 17 minutes of downtime). Explanation of the extended API outage is also covered below.

Root cause of this incident was the result of an operator performing upgrades of some new capacity in our fleet, and they were using the tooling that allows for remote updates of software. The command to reboot the select set of new systems that needed to be updated was mis-typed, and instead specified all servers in the data center. Unfortunately the tool in question does not have enough input validation to prevent this from happening without extra steps/confirmation, and went ahead and issued a reboot command to every server in us-east-1 availability zone without delay.

Once systems rebooted, they by design looked for a boot server to respond to PXE boot requests. Because there was a simultaneous reboot of every system in the data center, there was extremely high contention on the TFTP boot infrastructure, which like all of our infrastructure, normally has throttles in place to ensure that it cannot run away with a machine. We removed the throttles when we identified this was causing the compute nodes to boot more slowly. This enabled most customer instances to come online over the following 20-30 minutes.

Security Issues in the Cloud



Joyent Products & Services Developers Pricing About Us Events

What Happened?

Due to an operator error, all us-east-1 API systems and customer instances were simultaneously rebooted at 2014-05-27T20:13Z (13:13PDT). Rounded to minutes, the minimum downtime for customer instances was 20 minutes, and the maximum was 149 minutes (2.5 hours). 80 percent of customer instances were back within 32 minutes, and over 90 percent were back within 59 minutes. The instances that took longer than others were due to a few independent isolated problems which are described

restored by 2014-05-27T21:30Z (1 hour and 17
utage is also covered below.

performing upgrades of some new capacity in
remote updates of software. The command to
pdated was mis-typed, and instead specified all
tion does not have enough input validation to
ation, and went ahead and issued a reboot
thout delay.

server to respond to PXE boot requests.
n in the data center, there was extremely high
of our infrastructure, normally has throttles in
We removed the throttles when we identified
. This enabled most customer instances to

LastPass ••• | Download LastPass.com

June 15 ,2015 @ 12:28 PM EST

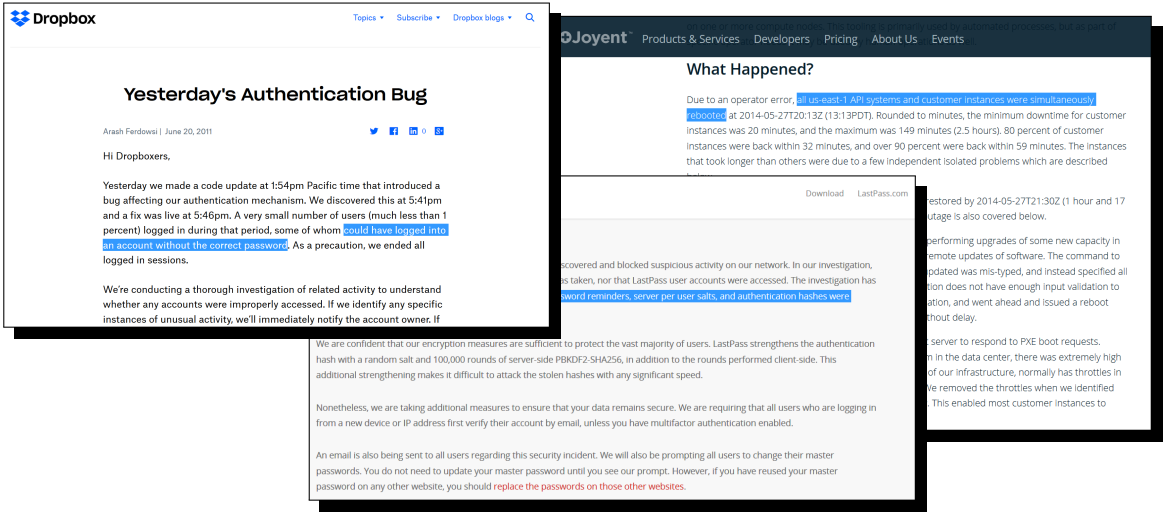
We want to notify our community that on Friday, our team discovered and blocked suspicious activity on our network. In our investigation, we have found no evidence that encrypted user vault data was taken, nor that LastPass user accounts were accessed. The investigation has shown, however, that LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised.

We are confident that our encryption measures are sufficient to protect the vast majority of users. LastPass strengthens the authentication hash with a random salt and 100,000 rounds of server-side PBKDF2-SHA256, in addition to the rounds performed client-side. This additional strengthening makes it difficult to attack the stolen hashes with any significant speed.

Nonetheless, we are taking additional measures to ensure that your data remains secure. We are requiring that all users who are logging in from a new device or IP address first verify their account by email, unless you have multifactor authentication enabled.

An email is also being sent to all users regarding this security incident. We will also be prompting all users to change their master passwords. You do not need to update your master password until you see our prompt. However, if you have reused your master password on any other website, you should replace the passwords on those other websites.

Security Issues in the Cloud



Dropbox

Topics ▾ Subscribe ▾ Dropbox blogs ▾

Yesterday's Authentication Bug

Arash Ferdowsi | June 20, 2011

Hi Dropboxers,

Yesterday we made a code update at 1:54pm Pacific time that introduced a bug affecting our authentication mechanism. We discovered this at 5:41pm and a fix was live at 5:46pm. A very small number of users (much less than 1 percent) logged in during that period, some of whom could have logged into an account without the correct password. As a precaution, we ended all logged in sessions.

We're conducting a thorough investigation of related activity to understand whether any accounts were improperly accessed. If we identify any specific instances of unusual activity, we'll immediately notify the account owner. If

Joyent Products & Services Developers Pricing About Us Events

What Happened?

Due to an operator error, all us-east-1 API systems and customer instances were simultaneously rebooted at 2014-05-27T20:13Z (13:13PDT). Rounded to minutes, the minimum downtime for customer instances was 20 minutes, and the maximum was 149 minutes (2.5 hours). 80 percent of customer instances were back within 32 minutes, and over 90 percent were back within 59 minutes. The instances that took longer than others were due to a few independent isolated problems which are described

estored by 2014-05-27T21:30Z (1 hour and 17 utage is also covered below.

performing upgrades of some new capacity in emote updates of software. The command to pdated was mis-typed, and instead specified all tion does not have enough input validation to ation, and went ahead and issued a reboot thout delay.

server to respond to PXE boot requests. n in the data center, there was extremely high of our infrastructure, normally has throttles in We removed the throttles when we identified . This enabled most customer instances to

Download LastPass.com

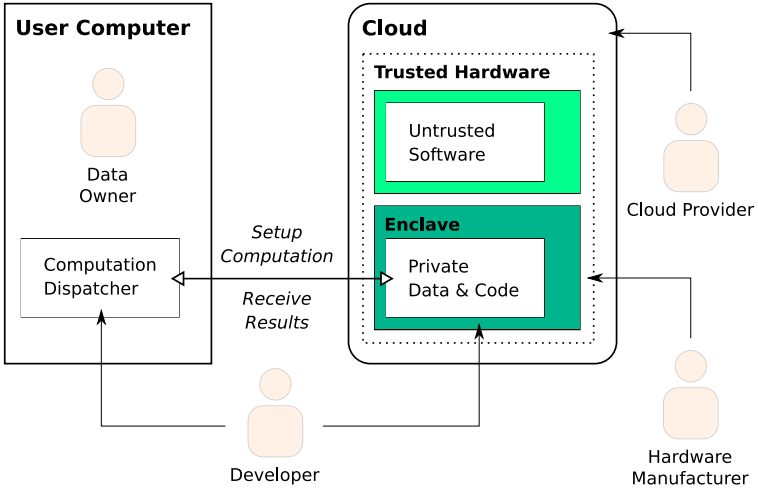
scovered and blocked suspicious activity on our network. In our investigation, as taken, nor that LastPass user accounts were accessed. The investigation has sword reminders, server per user salts, and authentication hashes were

We are confident that our encryption measures are sufficient to protect the vast majority of users. LastPass strengthens the authentication hash with a random salt and 100,000 rounds of server-side PBKDF2-SHA256, in addition to the rounds performed client-side. This additional strengthening makes it difficult to attack the stolen hashes with any significant speed.

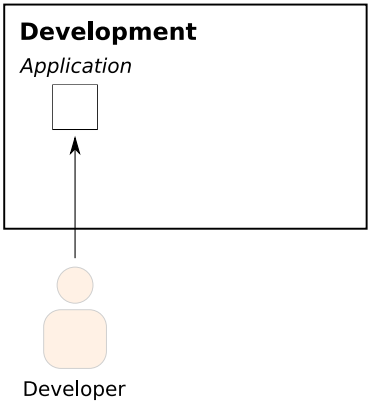
Nonetheless, we are taking additional measures to ensure that your data remains secure. We are requiring that all users who are logging in from a new device or IP address first verify their account by email, unless you have multifactor authentication enabled.

An email is also being sent to all users regarding this security incident. We will also be prompting all users to change their master passwords. You do not need to update your master password until you see our prompt. However, if you have reused your master password on any other website, you should replace the passwords on those other websites.

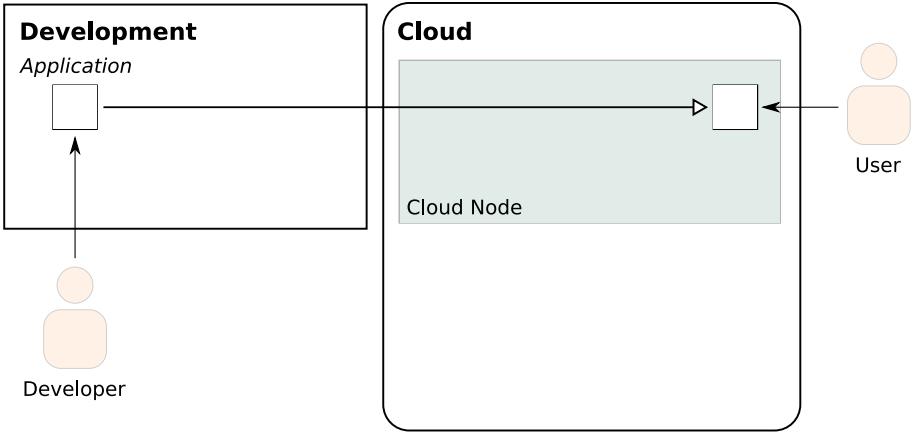
Intel Software Guard Extensions



Envisioned Approach

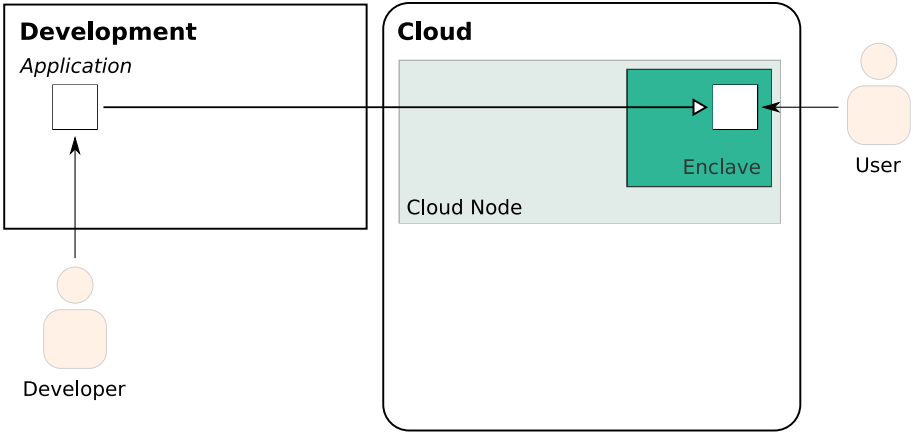


Envisioned Approach



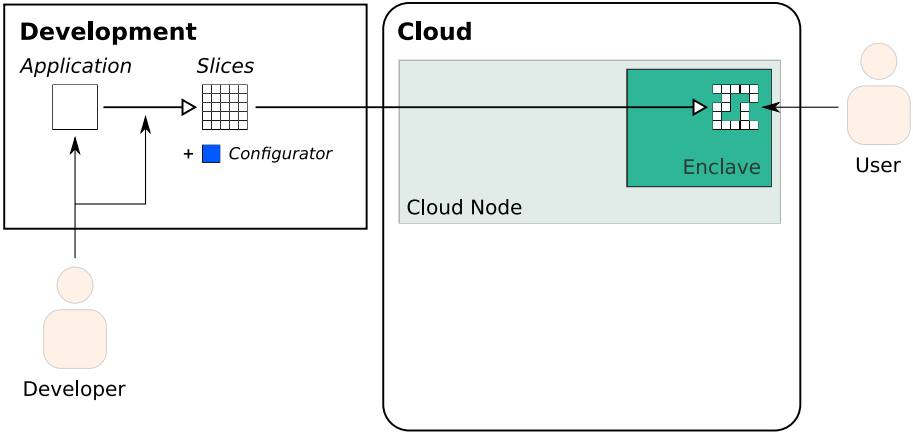
Envisioned Approach

P_1: Protecting the entire code base from unauthorized access



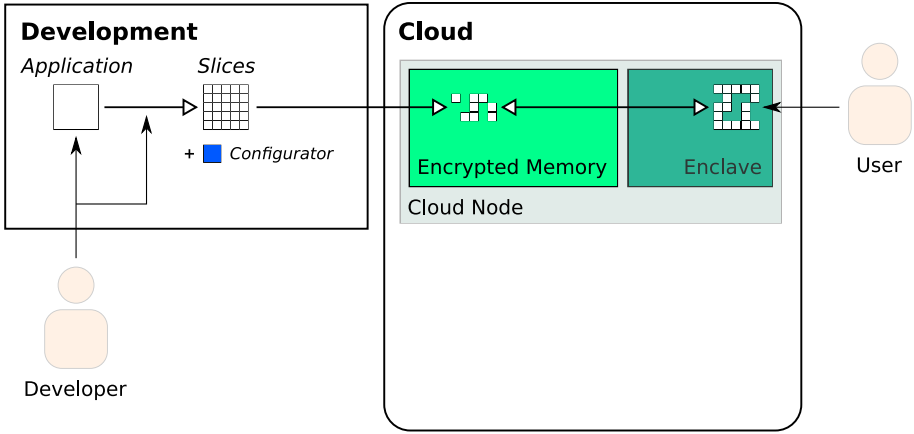
Envisioned Approach

P_2: Running sliced applications within the enclave



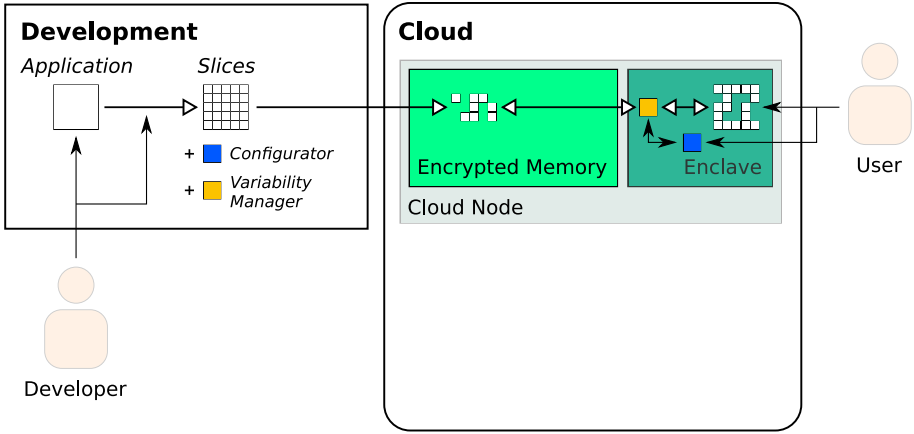
Envisioned Approach

P_3: Enabling dynamic loading of variable application parts



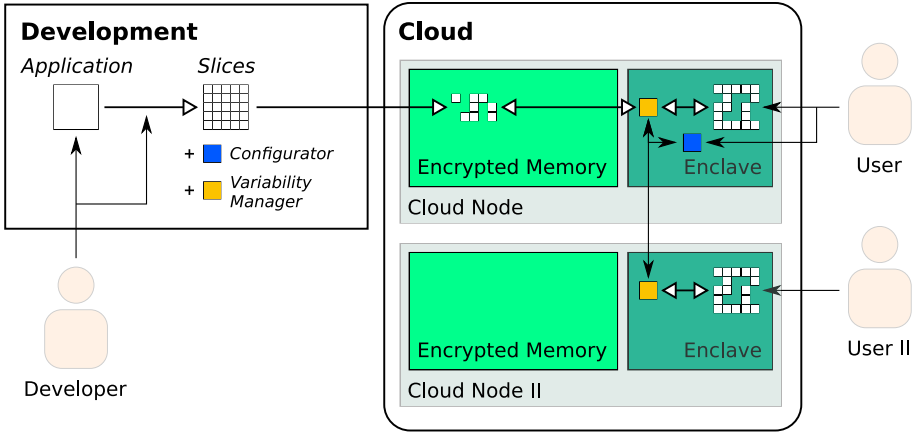
Envisioned Approach

P_4: Supporting self-adaptive reconfiguring of applications



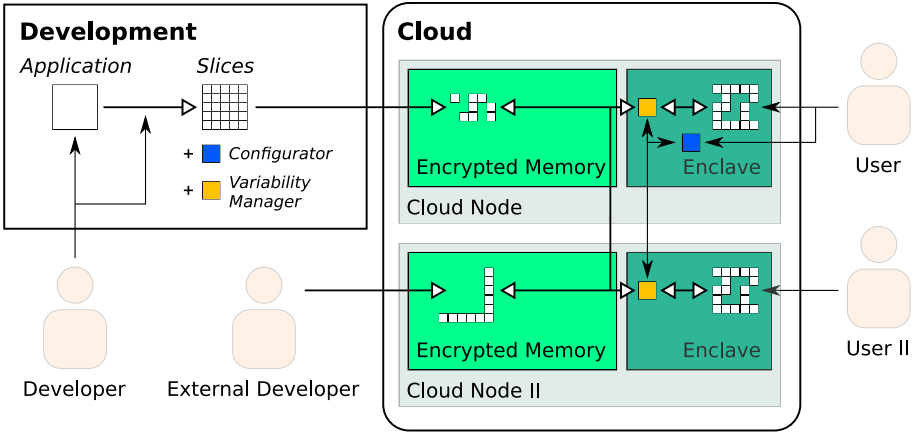
Envisioned Approach

P_5: Utilizing the scalability and availability of cloud computing



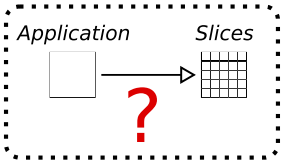
Envisioned Approach

P_6: Including and securing third-party services



Variability in the Enclave

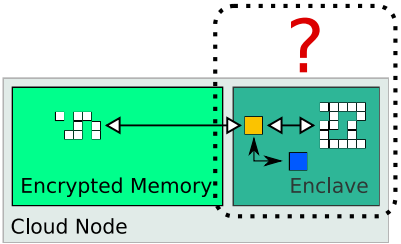
How can we identify meaningful features within an unsliced application?



Self-Adaption at Runtime

What are meaningful heuristics for self-adaptation?

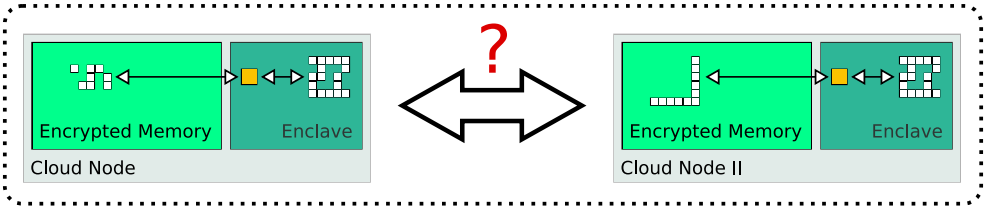
Especially, at which point should features be removed from the enclave?



Utilizing the Cloud

How can we efficiently store and transfer the internal configuration of running DSPL among different nodes?

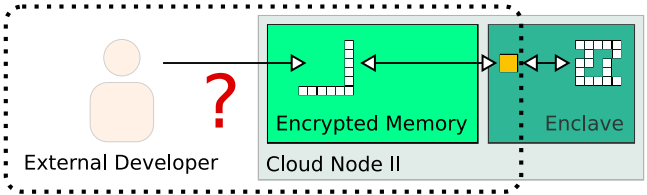
How can we efficiently apply distributed computation in different DSPLs among different nodes?



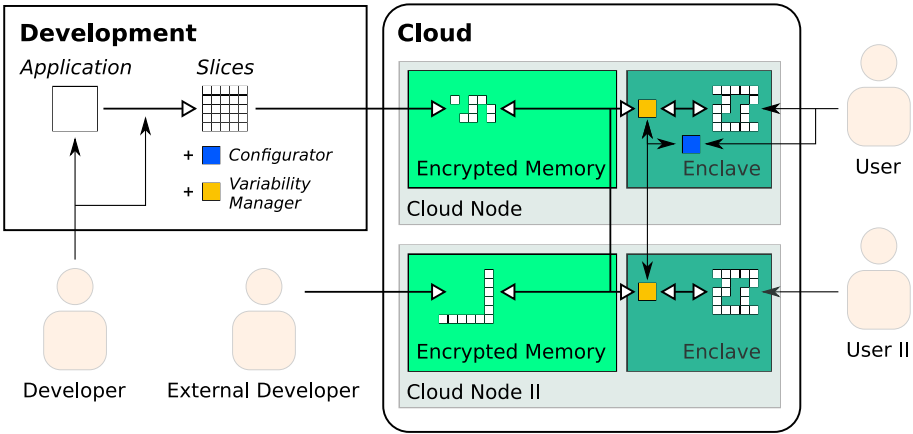
Integrating Cloud Services

How can we efficiently include third-party services into our DSPL?

How can we efficiently check the integrity of services and their parts?



Conclusion


Development
Application
Slices
+ Configurator
+ Variability Manager
Developer
External Developer
Cloud
Encrypted Memory
Enclave
Cloud Node
Encrypted Memory
Enclave
Cloud Node II
User
User II