--The survey and background are quite complete and provide the required knowledge for the reader.

--2.5 It is not required to use patterns in ref. architectures; in fact most of them do not use them. The first place where I saw them is:

Stricker V, Lauenroth K, Corte P, Gittler F, Panfilis

SD, Pohl K (2010) Creating a reference architecture

for service-based systems - A pattern-based

approach. In: Towards the Future Internet - Emerging

Trends from European Research, pp 149{160, DOI 10.3233/978-1-60750-539-6-149

Then we used them in or security RA.

--You can add something here about the value of RAs. See section 10.1 in my paper:

E.B.Fernandez, Raul Monge, and Keiko Hashizume, “Building a security reference architecture for cloud systems”, *Requirements Engineering*. Doi: 10.1007/s00766-014-0218-7, 2015

Your ref. 99 is incorrect, that was a short early version.

--Section 2.8 We found that describing threat patterns is more precise, because there can be several ways to to produce a misuse and a threat can produce several misuses. See:

A. Uzunov and E.B.Fernandez, “An Extensible Pattern-based Library and Taxonomy of Security Threats for Distributed Systems”- Special Issue on Security in Information Systems of the *Journal of Computer Standards & Interfaces*. 2013. <http://dx.doi.org/10.1016/j.csi.2013.12.008>

--Section 3.1.1 I think that Figure 3.1 is incorrect. I don’t think that threats like CSRF and XSS are examples of social engineering attacks. They are not based on phishing or similar attacks.

--3.1.3 Execution of Javascript code is a special case of XSS or CSRF, it is not a generic attack. The same is true for XSS DOM. You should mention the more general threat.

--Section 3.2.4 Sandboxing is just another name for the pattern “Controlled Execution Domain” in Section 8.4 of my book.

--Section 3.2 Important defenses are Authentication and Secure Channel, both provided by SSL (TLS). All browsers implement SSL, it should be mentioned here.

--Figure 5.1. You confuse use cases with activities. Use cases are complete interactions with the system and for browsers you said that there are only four (p.50). The use case diagram should have only four use cases. What you describe here are activities, not use cases.

--Fig. 5.2. The connections from Browser client to Plugin, Sandbox, and GPU instance should be three separated and named associations. UML does not allow to bundle associations.

--Fig. 5.2. A Sandbox is not a Process. A sandbox describes a set of rights for a process. Aggregation would be correct here.

--Ref. 20. Use E.B.Fernandez to be consistent with my other papers.

--Ref. 99 is an early version of the Requirements Eng. paper. See above.