SecureCloud

Secure Big Data Processing In Untrusted Clouds

RESEARCH NEWSLETTER

SecureCloud Project Overview

Confidentiality, integrity, and availability of applications and their data are of immediate concern to almost all all organizations that use cloud computing. This is particularly true for organizations that must comply with strict confidentiality, availability and integrity policies, including the society's most critical infrastructures, such as finance, utilities, health care and smart grids.

The primary goal of SecureCloud is to ensure the dependability of critical applications that are executed in distributed and potentially untrusted cloud infrastructures. The innovative approach to cloud dependability pursued in the SecureCloud project leverages the emergence of a new and promising technology. Secure commodity CPUs promise to enable a new generation of dependable applications by basing trust in hardware mechanisms offered by the CPUs themselves, as found in Intel's Secure Guard Extensions (SGX). This allows running applications in the cloud in such a way that they are isolated, not only from each other, but also from the underlying operating system and the hypervisor.

It allows users to run their sensitive applications in a public cloud without the need to unconditionally trust the cloud provider.

- SecureCloud leverages on Intel SGX as root of application trust to provide confidentiality and integrity of sensitive data. SGX encrypts the memory contents of protected applications to prevent the operating system or the hypervisor from being able to read or modify application data.
- SecureCloud uses Open-Stack as a common cloud stack infrastructure. Extensions will be added to manage secure virtual resources and to offer a novel, secure and redundant storage service.
- SecureCloud extends standard container-based technologies to allow the execution of Intel SGX secure enclaves inside containers.
- The SecureCloud framework provides highly available and dependable big data applications that are resistant against hardware and operating system failures.
- SecureCloud allows the executions of micro-services in untrusted cloud.

In this Issue

At a Glance

Call: H2020-EUB-2015 (3rd Coordinated Call)

Topic: EUB-1-2015: Cloud Computing, incl. security aspects

Duration: 01. Jan 2016 - 31. Dec 2018 (36 months)

Project cost: € 2,285,377

EU Contribution: € 1,499,627

Contact: https://www.securecloudproject.eu/

European Coordinator:
Prof. Dr. Christof Fetzer
Technische Universität Dresden (DE)
E-mail: Christof.Fetzer@tu-dresden.de

Brazilian Coordinator:
Prof. Dr. Andrey Brito
Federal University of Campina Grande (Brazil)
E-mail: andrey@computacao.ufcg.edu.br

SecureCloud has received funding from the European Union's Horizon 2020 research and innovation programme and was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) and MCTI/RNP 3rd Coordinated Call under grant agreement No 690111.

CONSORTIUM

The SecureCloud consortium is formed by 14 members, coming from 7 different countries (Brazil, Denmark, Germany, Israel, Italy, Switzerland and United Kingdom):

European partners

- Technische Universität Dresden (Germany)
- Imperial College (United Kingdom)
- University of Neuchâtel (Switzerland)
- Chocolate Cloud ApS (Denmark)
- Synclab S.r.l. (Italy)
- Israel Electric Corporation Ltd (Israel)
- CloudSigma AG (Switzerland)

Brazilian partners

- Instituto de Tecnologia para o Desenvolvimento (Brazil)
- Federal University of Campina Grande (Brazil)
- Federal University of Tecnology - Paraná (Brazil)
- Federal University of Itajuba (Brazil)
- Copel Distribuição SA (Brazil)
- CAS Tecnologia S/A (Brazil)
- Intituto Nacional de Metrologia, Qualidade e Tecnologia (Brazil)

Dissemination Activities

Website

The SecureCloud project website www.securecloudproject.eu is fundamental for any dissemination activity. It is one of the main means through which the SecureCloud consortium offers, during the project lifetime and after the end of the project, project information, partner descriptions and results obtained to an external audience. Also a mailing list service was created to provide information about upcoming events (conferences, workshops, etc.). To summarize, primary objectives are:

- To highlight results of the SecureCloud project and disseminate them
- To act as a thrust for cooperation among related projects and initiatives
- To raise awareness of SecureCloud project among the potential users.

As proposed in the project's Description of Action (DOA), the website has connections to the project's profiles in Twitter and Facebook. In this way, interested users may follow project updates even through social media.

The SecureCloud website is not foreseen as a collaborative tool. The target audience consists of the following groups:

- Potential industry partners,
- Academia researchers,
- SecureCloud partners.

When the website was created, the informational needs of these groups have been taken into account for what concerns scheduled events, news and relevant background documents.

- To act as a thrust for cooperation among related projects and initiatives
- To raise awareness of SecureCloud project among the potential users.

As proposed in the project's Description of Action (DOA), the website has connections to the project's profiles in Twitter and Facebook. In this way, interested users may follow project updates even through social media.

https://www.securecloudproject.eu/

Twitter Profile

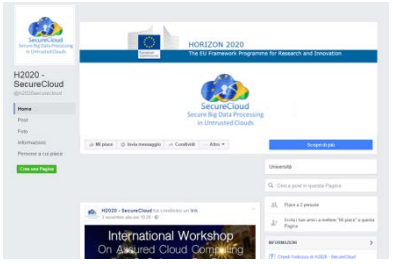
The Twitter SecureCloud Project Page is available at the following address:

https://twitter.com/H2020SecCloud

Facebook Page

The SecureCloud Facebook Page is available at the following address:

https://www.facebook.com/h2020securecloud/



SecureCloud has received funding from the European Union's Horizon 2020 research and innovation programme and was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) and MCTI/RNP 3rd Coordinated Call under grant agreement No 690111.

Project Workshops

First Workshop on System Software for Trusted Execution (SysTEX 2016)

SecureCloud, in collaboration with SERECA project, organized the 1st Workshop on System Software for Trusted Execution (SysTEX 2016).

The program committee was chaired of:

- **Pascal Felber**, University of Neuchâtel, CH
- **Christof Fetzer**, TU Dresden, DE
- Rüdiger Kapitza, TU Braunschweig, DE
- **Peter Pietzuch**, Imperial College, UK

The aim of the conference was the design, implementation, deployment, and evaluation of distributed system platforms and architectures for computing, storage, and communication environments. The SysTEX workshop was focused on system software and middleware that set up new hardware for trusted execution. Besides Intel Software Guard Extensions (SGX) and ARM TrustZone, additional hardware features that enable the implementation of trustworthy systems have been proposed during this conference.

International Workshop on Assured Cloud Computing and QoS Aware Big Data

The International Workshop on Assured Cloud Computing and QoS aware Big Data, in conjunction with the 17th IEEE /ACM CCGRID, in Madrid, Spain, May 14-17, 2017 will be supported by the EU-Bra-BIGSEA project consortium.

The workshop was organized by:

- Ignacio Blanquer, Universitat Politnica de Valncia, ES
- Rakesh Bobba, Oregon State University, US
- **Andrey Brito**, Federal University of Campina Grande, BR
- Roy Campbell, University of Illinois at Urbana-Champaign, US
- Roberto Cascella, Trust-IT Services, UK
- **Christof Fetzer**, TU Dresden, DE
- Zbigniew Kalbarczyk, University of Illinois at Urbana-Champaign, US
- Charles Kamhoua, Air Force Research Laboratory, US.

EUBra-BIGSEA project aims at developing a set of cloud services empowering Big Data analytics to ease the development of massive data processing applications. It proposes to develop models, predictive and reactive cloud infrastructure QoS techniques, efficient and scalable Big Data operators and a privacy and quality analysis framework, exposed to several programming environments. Also aims at covering general requirements of multiple application areas.

CCGrid 2017, 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, aims at bringing together developers of bioinformatics and biomedical applications and researchers in the field of distributed IT systems. The goals of the workshop are to exchange and discuss existing solutions and latest developments in both fields.

The workshop further intends to collaboratively explore new approaches to successfully apply distributed IT-systems in translational research, clinical intervention, and decision-making. The workshop will be a forum of dialogue centered upon the development and advancement of an effort to design, implement, and evaluate dependable cloud architectures that can provide assurances with respect to security, reliability, and timeliness of computations (or services). Research on cloud services,

ICT-skilled data scientists and application developers can find complementary solutions and partnerships to evaluate and integrate additional solutions.

Clustering Activities

The SecureCloud consortium collaborated with other projects and groups increasing SecureCloud visibility and potential impact.

The DPSP Cluster

The first call of H2020 LEIT WP2014-2015 gave birth to a significant number of grants addressing research and innovation on diverse solutions for ensuring data protection, security and privacy in the cloud.

The DPSP Cluster[1] was born with the aim to seek synergies between these projects and to join efforts towards greater impact. The topics addressed in the Cluster give continuity to research and innovation in the context of other EU-funded projects of the FP7 and CIP Programmes, and therefore these were invited to join the Cluster too.

SecureCloud is providing a contribution to the DPSP cluster and, at the same time, is receiving something back. SecureCloud added new topics to the research areas covered by the project (i.e. the unexplored trusted execution with SGX), and new innovative ideas (i.e. the possibility to secure sensitive data against malicious cloud provider). Furthermore, the use cases implemented in SecureCloud are of interest for the DPSP cluster since they provide additional requirements which are really important, since these come from critical infrastructures. Finally SecureCloud,

[1] https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

SecureCloud has received funding from the European Union's Horizon 2020 research and innovation programme and was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) and MCTI/RNP 3rd Coordinated Call under grant agreement No 690111.

thanks to the DPSP Cluster, is improving the strategy of exploitation of project results.

SERECA

Cloud security is of immediate concern to organisations that must comply with strict confidentiality and integrity policies. More broadly, security has emerged as a commercial imperative for cloud computing across a wide range of markets. The lack of adequate security guarantees is becoming the primary barrier to the broad adoption of cloud computing.

The Secure Enclaves for REactive Cloud Applications (SERECA) project[2] aims to remove technical impediments to secure cloud computing, and thereby encourage greater uptake of cost-effective and innovative cloud solutions in Europe. It proposes to develop secure enclaves, a new technique that exploits secure commodity CPU hardware for cloud deployments, empowering applications to ensure their own security without relying on public cloud operators. Secure enclaves additionally support regulatory-compliant data localisation by allowing applications to securely span multiple cloud data centres.

SecureCloud and SERECA are both exploring the same core technology: Intel SGX. This is an innovative and extremely recent security hardening mechanism. Therefore, the exchange of knowledge regarding SGX between the two project is highly fruitful. In fact, there are a number of aspects of SGX, which still need to be more explored. The establishment of synergies between SERECA and SecureCloud can be productive for both projects helping them to quickly solve issues and define better approaches on SGX.

KONFIDO

KONFIDO[3] (Secure and Trusted Paradigm for Interoperable eHealth Services) advances the state of the art of eHealth technology with respect to four key dimensions of digital security, namely: data preservation, data access and modification, data exchange, and interoperability and compliance.

The federation-based approach makes cross-border interoperation of eHealth services provided by individual countries possible, while allowing each participating entity (private and public actors, as well as empowered citizens), to enforce specific policies for protection and control of personal and health related data. Data is collected, processed, and exchanged at multiple architectural levels, and over a number of devices (including mobile ones) and communication protocols with differing security guarantees.

KONFIDO develops solutions that will prevent unauthorised access, loss of data, and cyber-attacks. These include mechanisms that will protect data from intrusions by the cloud provider itself. The approach will be implemented in a technological framework that relies on six technology pillars: security extensions provided by main CPU vendors, security solutions based on photonic technologies, homomorphic encryption mechanisms, customised STORK-compliant eID support, and customised extensions of selected SIEM solutions, disruptive logging and auditing mechanisms.

KONFIDO and SecureCloud projects have different technological aspects in common like the security extensions provided by main CPU vendors. Collaboration between them will provide benefits for both parts.

Scientific Publications

During the first project year the following papers were produced:

Journal Publications

"Building Critical Applications Using Micro-Services"

C. Fetzer

IEEE Security & Privacy, vol. 14, no. 6, pp. 86-89, Nov.-Dec. 2016. doi: 10.1109/MSP.2016.129

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7782696&isnumber=7782693

Conference Papers

"Security and Privacy Preserving Data Aggregation in Cloud Computing"

Leandro José Ventura Silva, Rodolfo Marinho, José Luis Vivas, Andrey Brito

SAC 2017 – ACM Symposium on Applied Computing, April 03-07, 2017, Marrakesh Morocco

"SecureCloud: Secure Big Data Processing in Un-trusted Clouds"

SecureCloud Consortium

DATE 2017, EU Project Special Session: from Secure Clouds to reliable and variable HPC

"GenPack: A Generational Scheduler for Cloud Data Centers"

A. Havet, V. Schiavoni, P. Felber, M. Colmant, R. Rouvoy, C. Fetzer

IEEE International Conference on Cloud Engineering (IC2E 2017), April 4-7, 2017, Vancouver, Canada

"FFQ: A Fast Single-Producer/Multiple-Consumer Concurrent FIFO Queue"

S. Arnautov, P. Felber, C. Fetzer and B. Trach

EuroSys 2017 – The Euro-pIPDPS 2017 – 31st IEEE International Parallel & Distributed Processing Symposium, May 29 June 2, 2017 Orlando, Florida USA

[2] http://www.serecaproject.eu/

[3] http://konfido-project.eu

SecureCloud has received funding from the European Union's Horizon 2020 research and innovation programme and was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) and MCTI/RNP 3rd Coordinated Call under grant agreement No 690111.

"SGXBounds: Memory Safety for Shielded Execution"

D. Kuvaiskii, O. Oleksenko, S. Arnautov, B. Trach, P. Bhatotia, P. Felber, C. Fetzer

EuroSys 2017 – The European Conference on Computer Systems, April 23-26, 2017, Belgrade Serbia

"Cloudifying Critical Applications: a Use Case from the Power Grid Domain"

F. Campanile, L. Coppolino, S. D'Antonio, L. Lev, G. Mazzeo, L. Romano, L. Sgaglione, F. Tessitore

PDP 2017, 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing St. Petersburg, Russia, March 6-8, 2017

"Secure Content-Based Routing Using Intel Software Guard Extensions"

R. Pires, M. Pasin, P. Felber, C. Fetzer

Middleware '16 Proceedings of the 17th International Middleware Conference

http://dl.acm.org/citation.cfm?doid=2988336.2988346

"SecureKeeper: Confidential ZooKeeper using Intel SGX"

S. Brenner, C. Wulf, D. Goltzsche, N. Weichbrodt, M. Lorenz, C. Fetzer, P. Pietzuch, R. Kapitza

Middleware '16 Proceedings of the 17th International Middleware Conference

http://dl.acm.org/citation.cfm?id=2988350

"SCONE: Secure Linux Containers with Intel SGX"

S. Arnautov, B. Trach, F. Gregor, T. Knauth, A. Martin, C. Priebe, D. Muthukumaran, D. O'Keeffe, M. Stillwell, D. Goltzsche, D. Eyers, R. Kapitza, P. Pietzuch, C. Fetzer

12th USENIX Symposium on Operating Systems Design and Implementation

https://zenodo.org/record/163059

Open Access Paper

"Teechan: Payment Channels Using Trusted Execution Environments"

J. Lind, I. Eyal, P. Pietzuch, and E. G. Sirer.

https://arxiv.org/pdf/1612.07766v1

Project Meetings

Kick-Off Meeting in Champery, January 2016

During the first project year the SecureCloud consortium met three times. During these meetings the project status was evaluated and subgroups meetings on specific topics were held. Through these sessions other projects for potential collaborations were selected.

Kick-Off Meeting, January 2016 in Champery, Switzerland

The SecureCloud Kick-Off Meeting (KOM) took place in Champery (CH) January 26-28, 2016.

The objective of the kick off meeting was to make all members aware of the project objectives, assumptions, constraints, deliverables, challenges, methodologies, procedures, plans, working environment. All project partners have understood the project objectives well. This helped them to start the project more efficiently.

Plenary Meeting, May 2016 in Dresden, Germany

The first SecureCloud Plenary Meeting took place in Dresden (DE) on May 25, 2016.

Plenary Meeting, October 2016 in Procida, Italy

The second Plenary Meeting was held on October 4-6, 2016 at the La Tonnara Hotel in Procida, Italy. During this meeting each technological provider has highlighted the achieved results in the development of the components that will be used for the implementation of the SecureCloud platform.

Plenary Meeting in Procida, October 2016

SecureCloud has received funding from the European Union's Horizon 2020 research and innovation programme and was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) and MCTI/RNP 3rd Coordinated Call under grant agreement No 690111.