Abstract: A Secure Cloud-based Platform to Host Healthcare Applications

G. Pierantoni, T.Kiss, G.Terstyanszky, H.V.Dang
Centre for Parallel Computing, University of Westminster,
London UK
{pierang, t.kiss g.z.terstyanszky,
H.Dang}@westminster.ac.uk

Y.Y.Kassaye Yitbarek, J.G. Bellika ,Norwegian Centre for
E-health Research, University Hospital of North Norway
kassaye.yitbarek.yigzaw@ehealthresearch.no

S.Olabarriaga, M.Tuler de Oliveira
Amsterdam Medical Centers, KEBB
University of Amsterdam, The Netherlands
{s.d.olabarriaga, m.tuler}@amc.nl

D. Krefting
Center for Biomedical Image and Information Processing
University of Applied Sciences Berlin
dagmar.krefting@htw-berlin.de

T.PENZEL, Charite Universitätsmedizin Berlin
thomas.penzel@charite.de

ABSTRACT

Digital technologies, such as Big Data analytics, artificial intelligence, cloud and high-performance computing are presenting new opportunities to transform healthcare systems, increase connectivity of hospitals and other providers, and therefore potentially and significantly improve patient care. However, such networked computing infrastructures also raise significant cybersecurity risks, especially in the healthcare domain, where protecting sensitive personal information is of paramount importance.

Project ASCLEPIOS[1] aims at strengthening the trust of users in cloud-based healthcare services by utilizing trusted execution environment and several modern cryptographic approaches such as attribute based encryption, searchable encryption, functional encryption to build a cloud-based e-health framework that protects users' privacy, prevents both internal and external attacks, verifies the integrity of medical devices before application, and runs privacy-preserving data analytics on encrypted data. The project investigates modern encryption techniques and their combination in order to provide increased security of e-health applications that are then presented towards end-users utilizing a cloud-based platform. Although some topics such as security and privacy are already investigated through block-chain related technologies, it has been decided that the selected approaches would be more suitable for these particular challenges. In order to prototype its security services, ASCLEPIOS develops and deploys three large-scale healthcare demonstrators, provided by three leading hospitals from Europe. These demonstrators are rooted in the practice-based problems and applications provided by the project's healthcare partners. The Amsterdam University Centers, University of Amsterdam, plans to improve stroke hyper-acute care through secure information sharing on a cloud computing platform to improve patient management. Additionally, they are also building prediction models to enable earlier discharge of patients from hospitals with lower risk factors. Charité Berlin plans to improve inpatient and outpatient sleep medication by remotely controlling the quality of the collected data and transferring it on-line for further analysis. Finally, the Norwegian Centre for e-health Research, University Hospital of North Norway is developing a system for privacy-preserving monitoring and benchmarking of antibiotics prescription of general practitioners. The common characteristics of these three scenarios are the increased demand for high levels of security in data transfer, storage and privacy preserving analytics on cloud infrastructures. In order deploy, operate and further develop these applications to increase their security with the ASCLEPIOS framework, a cloud computing testbed is being setup. The testbed uses state-of-the-art technologies for cloud application deployment and run-time orchestration in order to ensure the optimized deployment and execution of the demonstrator applications. As the data sources do not require the local execution (albeit in one case data may remain on the data source) of processing, there is no need for fog or edge computing, but the testbed is based on private OpenStack cloud computing infrastructures and utilizes the MiCADO[2] framework which is compatible with different containers such as Docker and Kubernetes. The project started only recently, and currently it is in the early stages of systems design and specification. This presentation will provide a short introduction to the ASCLEPIOS project and its demonstrators and will present early results of the currently ongoing requirements specification and platform design processes.

Keywords—HealthCare, Privacy, Security, Cloud applications.

REFERENCES

[1]   "ASCLEPIOS," [Online]. Available: https://www.asclepios-project.eu/. [Accessed: 22-Mar-2019].

[2]   T. Kiss, et al., "MiCADO - Microservices-based Cloud Application-level Dynamic Orchestrator", Future Generation Computer Systems, Vol 95, pp 937 – 946, May 2019. DOI: https://doi.org/10.1016/j.future.2017.09.050