AISMS: Adaptivity in Intelligent and Secure Mobile Systems

Editorial

Special Track along with ADAPTIVE2022
The Fourteenth International Conference on Adaptive and Self-Adaptive Systems and Applications
April 24 – April 28, 2022 – Barcelona, Spain
https://www.iaria.org/conferences2022/ADAPTIVE22.html

Marc Kurz and Erik Sonnleitner
University of Applied Sciences Upper Austria
Faculty for Informatics, Communications and Media
Department of Mobility & Energy
4232 Hagenberg, Austria
email: {firstname.lastname}@fh-hagenberg.at

***Abstract*— Many modern computer systems not only tend to be used in a more and more mobile context, but also reflect the particular requirement of being *smart* – which, to some extent, can be a confusing verbalism. Smart devices are typically ones which are largely inter-connected (e.g. over the Internet), and provide particular aspects in terms of how environment is perceived and what kind of computational reactions are being issued. This enables adaptivity in terms of the context of the user, by applying generated sensory data in an *intelligent* manner. Privacy and security of personal data is often forgotten but is a crucial factor. Therefore, the special track named "AISMS: Adaptivity in Intelligent and Secure Mobile Systems" tends to provide a combined insight and discussion about those – often considered contentious – aspects.**

***Index Terms*— Artificial Intelligence; Privacy and Security in Mobile Systems; Adaptive Behavior of Mobile Systems; Wearable and Mobile Systems; Context-Awareness and Context-Aware Adaptation**

I. Introduction

With the advent of mobile systems in recent decades, people are ever increasingly connected to smart devices. These devices aim at making our lives more comfortable and assist in different situations – the most prominent examples for such devices might be the mobile phone or also wearable and ubiquitous systems in general.

By applying approaches that can be classified within the topic “artificial intelligence”, these mobile systems strive to provide some kind of “intelligent behavior” adapting to the current user’s contextual state [1]. Additionally, security aspects concerning personal and sensitive data are becoming more and more relevant [2]. These two important factors might be diametrically opposed, since usually “intelligence” needs a lot of data to sense the current context of users, but data might be sensitive in terms of privacy and security concerns. Nevertheless, security in mobile systems needs to be considered as a critical factor.

Therefore, this special track aims at discussing and examining the hybridity of intelligence and security with respect to the (self-) adaptation of mobile systems according to the actual contextual state. The most relevant topics of interest with respect to the aim of the special track that have been targeted include (amongst others): (i) artificial/ambient intelligence, (ii) security aspects for mobile systems, (iii) adaptive behavior of mobile systems, (iv) adaptivity in wearable and mobile systems, (v) context-awareness and context-aware adaptation, and (vi) privacy and security in mobile adaptive systems.

The rest of this editorial is structured as follows: the following section II summarizes the accepted submissions for presentation and publication in the special track. Section III provides a conclusion and gives an outlook to future perspectives and challenges of the topic.

II. Submissions

The first paper entitled "MeUI – Machine Learning Enhanced Adaptive User Interaction" by Kurz and Sonnleitner [3] is a vision/position paper and it discusses the idea of a novel approach/research agenda of interacting with mobile devices. It intends to challenge the classic approach of interacting with mobile devices [4], [5]. Usually, users have to determine how to interact with a device adhering to rules that need to be learned. Following the trend of maximizing user experience and user comfort by radical new technological approaches, the idea is to use ML/AI technologies to reverse the core principal of device utilization by providing a distinct, personalized and dynamically self-adaptive foundation towards modern human computer interaction. The paper formulates a research hypothesis that summarizes the visioned scientific agenda: *ML/AI technologies allow for a significant change in the (mobile) device interaction in terms of usability. The classic approach of one-*

size-fits-all approach can be reversed towards a personalized experienced and a self-learning adaptation of interaction increasing the user experience. Additionally, specific use-cases are discussed that can build a baseline for research prospects:

- UC1: Self-Learning Keyboard Adaptation – the idea with this use-case is that the keyboard is being adapted according to the specific needs of the user.
- UC2: Adaptive Interface Component Recomposition – this use-case discusses the fact that certain interface elements, such as buttons and sliders may not be placed and scaled in the optimal and most efficient way possible for the behavioural characteristics of the utilizing person.
- UC3: Personalized and Context-Aware App Arrangement – the third use-case targets the ordering and grouping of applications on mobile devices.

Additionally, the paper discusses a possible research methodology, risks and challenges, learning and scientific potentials and also summarizes transformative potentials that can be conceivable.

The second paper of the special track, written by Selinger and Dimitrijevic is entitled "Tree-Based Regressors for Predicting Energy Expenditure from Heart Rate in Wearable Devices" [6]. The core idea of this paper is to estimate energy expenditure from heart rate with a higher coefficient of determination using tree-based regressors than commonly used linear models. The authors fitted linear regression models, regression trees, and random forests with data from 892 graded exercise tests on a treadmill with 857 participants and evaluated their performance, as well as memory consumption on a PineTime smartwatch and an Apple Watch. The underlying hypothesis is that it seems promising to investigate whether non-linear regression methods, such as random forests and regression trees which, from a computational point of view, are still feasible for the deployment on wearable devices, allow to more accurately predict energy expenditure rather than linear regression models. In their study the authors used a publicly available database provided by the Exercise Physiology and Human Performance Lab of the University of Malaga [7], [8], [9]. In addition to other measurements, the database contains heart rate, oxygen consumption, carbon dioxide generation, and treadmill speed from 857 amateur and professional athletes (149 females, 708 males) performing 992 graded exercise tests. Results show that their tree-based model does not need to know VO_{2max} but achieves a comparable result as the linear model with VO_{2max} making it especially interesting for amateur athletes. The additional memory on the PineTime smartwach needed to store the tree increased the original firmware size of 390 KiB to 416 KiB. If $VO_{2max}$is available, then a tree with a depth of 11 achieves a coefficient of 0.877, and the total memory size is 418 KiB. The authors close the paper with a statement that because of the characteristics of the dataset (i.e., only treadmill data) it is not possible to validate how the model performs in other contexts, e.g., cycling or nordic walking. Thus, it is planned to extend the database in the future.

The third paper in the special track, "Context-Aware Security Intelligence of Vulnerability Scanners in Cloud-native Environments", written by Ammer et al. [10] presents a system that tries to reduce false positives of scanners in a cloud environment considering contextual information. Relevant information that is being considered is for example the topology of the underlying application or the runtime. Without this information, scanners cannot precisely assess a threat's actual severity, leading to false alarms and a challenge for security experts to prioritize vulnerabilities. Especially with the increasing popularity of microservices deployed in highly dynamic cloud environments, this prioritization task is very difficult. The authors present an approach and a system the tries to bridge this gap by enriching web vulnerability scanner reports with this valuable contextual information to understand security threats better and reduce false positives. The main focus of the paper is DAST (Dynamic Application Security Testing – examine the outside security posture) because they attack an application from the outside and do not have run-time information which the observability platform can provide. The authors present the system *Themis* which is a prototypical implementation of an architecture that combines scanner results and topology information. Additionally, a rule-based filtering approach and a graph-based visualization of found vulnerabilities is included, whereas the helpfulness for security experts has to be further evaluated in production environments.

III. Conclusion & Future Perspectives

The special track "AISMS: Adaptivity in Intelligent and Secure Mobile Systems" provides a significant variety of topics discussing challenges, solutions and possibilities regarding the modern-day concepts of mobile computing from the viewpoint of both, academics and industry with focus on adaptivity in intelligent and secure mobile systems.

Future perspectives regarding the topic include questions concerning the assumption that *intelligence* and *security* in mobile systems are diametrically opposed. Additionally, further "novel" machine learning models (i.e., "deep learning, neural networks", etc.) should be considered when discussing security and adaptivity in mobile systems. Last but not least, comprehensive datasets tackling the AISMS topic would be beneficial. There, question for future challenges in this area arise like how much data would be needed, and how should this data be efficiently annotated?

Acknowledgement

We would like to thank the organizers of ADAPTIVE2022 for accepting AISMS as special track and for their efforts and support during preparation. We are also very thankful to the authors for their very interesting contributions to the special track.

REFERENCES

[1] B. Schilit, N. Adams, R. Want "Context-aware computing applications," 1994 First Workshop on Mobile Computing Systems and Applications, 1994.

[2] N. Kshetri. "Big data's impact on privacy, security and consumer welfare," Telecommunications Policy, 38(11), 1134–1145, 2014.

[3] M. Kurz, E. Sonnleitner, "MeUI – Machine Learning Enhanced Adaptive User Interaction," The Fourteenth International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE 2022), Special Track on Adaptivity in Intelligent and Secure Mobile Systems, Barcelona, Spain, 2022.

[4] A. K. Karlson, B. B. Bederson, and J. Contreras-Vidal, "Understanding single-handed mobile device interaction," Handbook of research on user interface design and evaluation for mobile technology, vol. 1, pp. 86– 101, 2006.

[5] J. Roth, "Patterns of mobile interaction," Personal and Ubiquitous Computing, vol. 6, no. 4, pp. 282–289, 2002.

[6] S. Selinger, L. Dimitrijevic, "Tree-Based Regressors for Predicting Energy Expenditure from Heart Rate in Wearable Devices," The Fourteenth International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE 2022), Special Track on Adaptivity in Intelligent and Secure Mobile Systems, Barcelona, Spain, 2022.

[7] D.Mongin, J.Garcia-Romero, and J.R.Alvero-Cruz, "Treadmill maximal exercise tests from the exercise physiology and human performance lab of the university of malaga (version 1.0.1)," PhysionNet, 2021.

[8] D. Mongin, C. Chabert, D. S. Courvoisier, J. Garcia-Romero, and J. R. Alvero-Cruz, "Heart rate recovery to assess fitness: comparison of different calculation methods in a large cross-sectional study," Research in Sports Medicine, vol. 0, no. 0, pp. 1–14, 2021.

[9] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," Circulation, vol. 101, no. 23, pp. e215–e220, 2000 (June 13).

[10] S. Ammer, J. Krösche, M. Gierlinger, M. Kahlhofer "Context-Aware Security Intelligence of Vulnerability Scanners in Cloud-native Environments," The Fourteenth International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE 2022), Special Track on Adaptivity in Intelligent and Secure Mobile Systems, Barcelona, Spain, 2022.