Abstract

Wearable xAI: a knowledge-based federated learning framework

Sara Nasiri [1,2,*], Iman Nasiri[1] and Kristof Van Laerhoven[2]

[1] Node 4.0, Martinshardt 19, 57074 Siegen, Germany; iman@node-4.com
[2] Department of Electrical Engineering & Computer Science, University of Siegen, Germany; kvl@eti.uni-siegen.de
* Correspondence: sara.nasiri@uni-siegen.de

Version January 30, 2020 submitted to Proceedings

Abstract: Federated learning is a knowledge transmission and training process that occuring in turn between user models at edge devices and the training model at the central server. Due to privacy policies, concerns and heterogeneous data, this is a widespread requirement in federated learning applications. In this work, we use knowledge-based methods and in particular case-based reasoning (CBR) to develop a wearable explainable artificial intelligence (xAI) framework. CBR is a problem-solving AI approach for knowledge representation and manipulation which considers successful solutions of past conditions that are likely to serve as candidate solutions for a requested problem. It enables federated learning when each user owns not only his/her private data, but also uniquely designed cases. New generated cases can be compared to the knowledge base and the recommendations enable the user to communicate better with the whole system. It improves users' task performance and increases user acceptability while they need explanations to understand why and how AI algorithms arrive at these solutions which is the best decision.

Keywords: articial intelligence; wearable AI; mobile edge computing; case-based reasoning; recommender system

---

1. Introduction

The next generation of wearables and Internet of things (IoT) systems is going to enhance the standard of human life by reassuring high comfort whereas increasing the intelligent use of restricted resources. The current collection of investigations with an innovative approach is concerned about objective measures of evaluating the validity and percision of such wearable devices. Based on the experiments of Shin et al., a productive heading for future research may focus on these significant questions [1]: (i) how users can practically figure out the accuracy and validity of data collected from them without access to scientific tools and methods; (ii) To what extent do certain users care about the accuracy, and how to rebuild trust when they become aware that wearable devices may function inaccurately; and (iii) how users' perception of accuracy may shape their decision to abandon or continue using such devices.

The wearable technology is progressing. It brings multitudinous potential benefits as well privacy concerns of critical information and security risks. Studies and reviews in this field shows the privacy issues related to wearable innovation actualized on all significant computing devices requires intensive thought by the wearable industries and the regulation organizations. Although the rise of wearable technology and innovation brings more benefits to our lives, security assurance and its implication should not be compromised. Clients feel the need to be secured about their data which not to be shared or spilled by any substance or third party. While standard machine learning models give several edges to mobile network operators, notably in terms of making certain consistent quality of experience, the massive knowledge transfer that they need leads to a considerable network footprint and might result in privacy problems. Federated learning (FL) is presented to ensure security by dispersing training data into numerous parties [2]. Each device or entity trains their own model locally and it's that model which they share with the servers in the data center. The server combines the model into a single federated model and it never has direct access to the training data. In this way FL helps to preserve privacy and reduce communication costs [3]. In the other hand, case-based reasoning (CBR) is a methodology of solving problems based on similar experiences. There are five main steps in the CBR recommender system: (i) Case formation identifies the requested problem (profile) and assigning their values based on pre-defind weights stord in case base (CB). It characterizes a CB and ascertain how incoming cases are refined for retrieving. (ii) Case matching and information retrieval to retrieve the incoming case with previous cases from the CB. (iii) Case adaptation to revise the solution of most similar cases for the requested problem. (iv) Case selection recommends the adapted solutions which are the associated recommendation based on the most similar cases. (v) Case evaluation and retain which verifies the adapted solution of new problem (request), which can be stored into the CB for future use [4]. Here experiences are recorded from training models of datasets. In collecting and recording data we considered various parameters (features) which are crucial in performance and acceptability of wearables. The focus of this work is to develop a CBR-FL system as a wearable explainable artificial intelligence (wearable xAI) framework.

2. Wearable xAI

Explainable AI (xAI) is implemented in order to create the choices or activities taken by an AI operator understandable for people who associated with the framework. Explainability or interpretability is the degree to which a human can understand the cause of the final result [5]. Decision making is the main important procedure in the development of "xAI", which assist people to more significantly interact with AI enabled systems and use them effectively. However, according to wearables acceptability problems, we believe that by developing "wearable xAI" systems and infrastructures, users can utilize wearables with better data protection, higher acceptability and improved usability. It is needed that we define wearable xAI which is the explainable process for wearable AI enabled systems to help users in improving their understanding, trust and task performance while they need explanations of why and how algorithms arrive at best solutions. xAI methods are in contrast to the "unchained data" concept in which they use customers' data where even they cannot be aware of that and why AI algorithms used at that point and arrived at a specific decision. We also suggest that wearable xAI which by using its methods and techniques the users can get better understanding of the results and feedbacks generated by wearable applications. They also get more transparency about their data collection and processing. Hence, the wearable producers have to take fundamental actions to secure the users' privacy.

2.1. Problem Statement

There are only a few existing studies that address usability and acceptability challenges in wearable devices, which their performance parameter is assessed based on distinctive estimations of readiness to utilize, simplicity, reliability, wearable time, and the level of satisfaction [6]. Figure 1 illustrates the results of a survey of German Consumer Associations as part of the Market Watch Digital World project. Data protection diagram shows the results of examinations (percentage) that carried out on 12 wearable devices and the selected matching fitness applications [7]. Data Unchained diagram shows the results of a representative telephone survey of 1055 participants above 14 years old who used the Internet in the last three months [7]. The last diagram tells us about customers' trust according to their willingness to share their data which could be even sold. Percentage responds of how profiting from the direct sale of data impacts the customer trust [8].

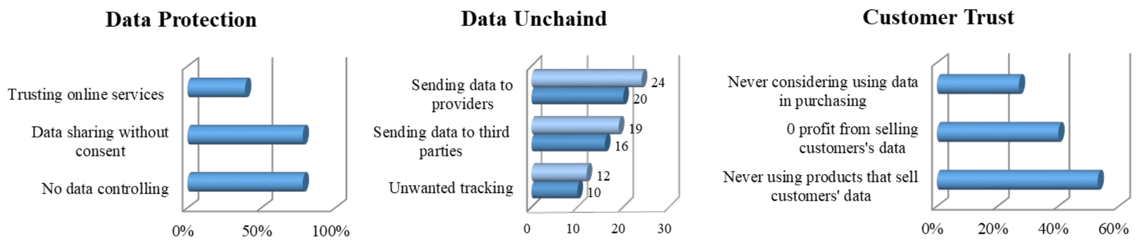

Figure 1. Data protection and Data unchained, data adopted from [7]; and Customer trust, which is a consumer pulsing survey in the US, UK, China and Brazil, adopted from [8].

2.2. Knowledge-based Federated Learning

In case online feedback is required, a novel interaction channel for embedded devices must be created. However a few procedures are able to be reached the verification of those components which is regularly very low. Investigations incorporate subsequently non-intrusive communication channels for quick real-time feedback. Due to the huge information and data from the validation steps extraordinary center needs to be laid on ease of use, interaction plan and context-aware interface. Data, information and knowledge management for wearable devices also have to be bargain with human admissibility and privacy issues. Subsequently, AI strategies and machine learning calculations have ended up a fundamental portion on wearables because they permit to form different sorts of analysis from the sensor data and information [9].

By utilizing dynamic training models (see Fig. 2), FL succeed in dealing with those challenges by training a centralized model on decentralized data [10]. It allows knowledge engineers to build a model while keeping the data at its source.

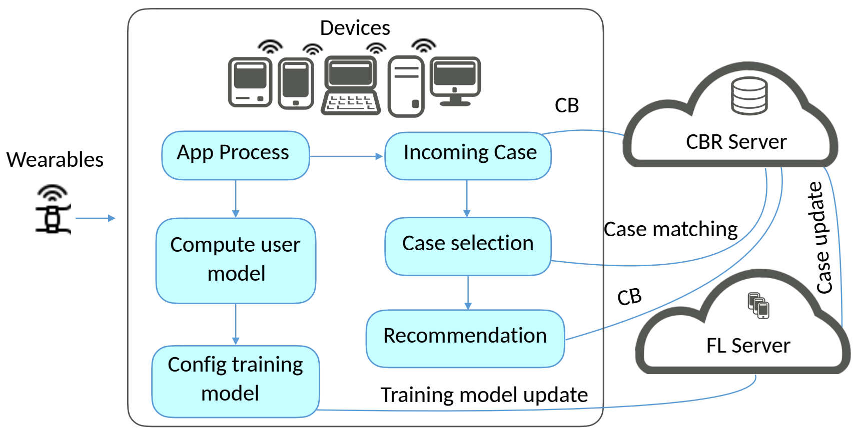

Figure 2. An overview of CBR-FL as a werable xAI framework.

Explainable knowldeg-based system is developing by utilizing CBR for the explanation about algorithms which is used for data analysis and methods for making recommendation. It works based on the result of retrieved user request from case bases which is created from basic models and datasets. Figure 2 presents how this case-based FL framework works; First, a smart device with the connection of a wearable device downloads a generic machine learning model. After personalizing and improving the on-device model, it computes a summary about the changes. Thousands of summaries are anonymously combined when the devices are plugged in. This provides a global improvement to the model that makes it work better for everybody. Hence, users can have a smarter device, and their data stays in their hands. Parallel to this procedure, the CBR system as an explainable process for wearable AI help users first, in improving their understanding from the model analysis and trust to the system. In addition, CBR system can generate appropriate recommendations for users based on the results of the comparison similarity between the incoming case (user profile) and the proper data of previuos stored cases. Which is enable them to improve users' task performance while they need explanations to understand why and how AI algorithms arrive at their solutions. The algorithm of our proposed CBR-FL framework is illustrated in Table 1.

Table 1. CBR-FL Algorithm.

Algorithm 1. The CBR-FL framework enabling case-based reasoning and federated learning for secure and understandable data analysis model.

Data: Given: User dataset; training model; n, number of users.
  Given: IC, incoming case of new test; CB, case base; m, number of cases to be retrieved; k, number of most similar cases.
Result: Global model
  R_{ap}: Predicted action plan; R_{up}: Analysis of user profile; R_{dm}: Explanation of decision-making algorithm;
  RC : Recommended case with maximum similarity degree.
begin
Computation: All n users locally compute training parameters and send trained ML parameters to the server.
Aggregation: It is performed across all parameters from n users without learning local information.
Model and configuration: The aggregated parameters are sent to selected devices from n clients.
Update: All users update their respective models and server aggregates updates into the global model.
$c \in CB$
$IC =$ new created case based on the CB template and user profile
$k = 0$
  for $(i = 1, i \leq m, i++)$ **then**
    if $\text{sim}(IC, c_i) > 70\%$
      $k = k++$
      $s = \text{solution}((ic, c_k) \quad \forall c \in CB)$
      $R^k_{\text{ap}} = \text{predict } (IC, s)$
      $R^k_{\text{up}} = \text{predict } (IC, s)$
      $R^k_{\text{dm}} = \text{predict } (IC, s)$
      $RC^k = \text{recommend } (IC, c_k)$
    return $R^k_{\text{ap}}, R^k_{\text{up}}, R^k_{\text{dm}}, RC^k$
    else
      $RC = \text{recommend } (IC, c_i) \quad \forall \text{ max } (\text{sim}(IC, c_i))$
    return RC
    end
  end
end

3. Conclusion

As a result, although some works looked into the plausibility of actualizing on-device machine learning models and changing existing algorithms to fit into the asset obliged gadgets, CBR-FL allows for smarter models, higher acceptability, lower latency, less power consumption and with the higher level of usability, all while ensuring privacy. Explainable AI enabled wearables which we called it wearable xAI, is not designed to track the information, but moreover characterizes what the client must do and how they ought to perform and to progress their exercises among other bits of knowledge. For instance, AI based personal trainers or caregivers can help in a smarter way by providing real-time tracking of exercises to make informed choices as an empowering device in fitness industry or to assist patients and caregivers in remote caring and diagnostics.

References

1. G. Shin et al., Wearable activity trackers, accuracy, adoption, acceptance and health impact: A systematic literature review, J. Biomed. Inform., vol. 93, pp. 103-153, 2019.

2. A. Ghosh, J. Hong, D. Yin, and K. Ramchandran, Robust Federated Learning in a Heterogeneous Environment, arXiv Preprint, arXiv:1906.06629, 2019.
3. Li, T., Sahu, A. K., Talwalkar, A., and Smith, V., Federated learning: Challenges, methods, and future directions, arXiv:1908.07873, 2019.
4. S. Nasiri, J. Zenkert, M. Fathi, Improving CBR adaptation for recommendation of associated references in a knowledge-based learning assistant system, Journal of Neurocomputing, 250, pp. 5–17, 2017.
5. T. Miller, "Explanation in artificial intelligence: Insights from the social sciences", arXiv Preprint, arXiv:1706.07269, 2017.
6. B. Klaassen, B. J. van Beijnum, and H. J. Hermens, 'Usability in telemedicine systems—A literature survey', Int. J. Med. Inform. 93, pp. 57–69, 2016.
7. "Wearables, fitness apps, and data protection" survey(08-09/2016), mindline media GmbH and survey (07-08/2016), datenschutz nord GmbH, Verbraucherzentrale NRW e.V. Mintropstr. 27, 40215 Düsseldorf.
8. 2020 Global Marketing Trends - Deloitte, 2019.
9. S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, A Survey of Wearable Devices and Challenges, IEEE Communications Surveys & Tutorials, Vol. 19, no. 4 , pp. 2573 - 2620, 2017.
10. A. Ghosh, J. Hong, D. Yin, and K. Ramchandran, Robust Federated Learning in a Heterogeneous Environment, arXiv Preprint, arXiv:1906.06629, 2019.