Advances in Informatics, Management and Technology in Healthcare
J. Mantas et al. (Eds.)

doi:10.3233/SHTI220725

Evaluating a Smart Healthcare System Design Through Participatory Approach

Thais WEBBER [a], Juliana BOWLES[a,1], Argyris CONSTANTINIDES[b], Marios BELK[b], and Emma MORLEY[a]
[a] *School of Computer Science, University of St Andrews, UK*
[b] *University of Cyprus, Cyprus & Cognitive UX LTD, Cyprus*

Abstract. Advances in computer communication technology have enabled the rapid growth of e-health services for delivering healthcare, such as facilitating online consent and data sharing between patients and health professionals. Developing a patient-centric healthcare system is challenging because by necessity, it should be secure, reliable, and resilient to cyber threats, whilst remaining user-friendly. Key to any development aiming for a refined proof-of-concept (PoC) system is the pursuit of comprehensive public system testing and evaluation. This paper focuses on the methodology and results obtained from the participatory approach adopted by the EU H2020 project Serums to evaluate and demonstrate the effectiveness of a smart healthcare system based on emergent technologies like blockchain, data lake, and multi-factor authentication. We discuss the challenges faced by remote PoC system evaluations with end-users as a consequence of the Covid-19 pandemic.

Keywords. Healthcare provision, system design, participatory evaluation

1. Introduction

Sharing of medical records with health professionals across different treatment centres is an essential part of medical care. This facilitates that numerous factors relating to a patient's health are accounted for, then higher quality treatment can be offered [1,3]. However, several challenges arise on cyber security and users' privacy when setting up data sharing systems, especially in the healthcare domain [3]. It is essential the data controller is fully aware of the access policies for what will be shared, when it will be shared and with whom. Importantly, the patient must also decide and understand who is able to access their medical information in the system and what they have permission to do with it [2]. Secondly, and of paramount importance, data sharing must be secure [3]; an individual accessing the record needs to have a legitimate reason to do so and to have a legitimate, medical relationship with the patient.

Advancements in security technology have enabled rapid growth of e-health services, such as obtaining online consent and exchanging data between patients and healthcare professionals in real time and on-demand. User authentication is a key security task within modern systems [4] together with access control strategies [2], privacy-

[1] Corresponding author, Dr Juliana K. F. Bowles, School of Computer Science, University of St Andrews, St Andrews, KY16 9 SX, UK; Email: jkfb@st-andres.ac.uk. This research is funded by the EU H2020 project SERUMS (grant 826278). We thank all project partners for contributions on the overall system development and PoC system design and evaluation.

preserving, data encryption, and several other approaches [3,5] to guarantee patients trust in secure data sharing transactions. In addition, the capability to deliver a full audit trail is also essential to identify any patterns of use that suggest data is being illegally accessed, with a system ability to identify unauthorised data sharing [1,3].

The EU Serums project[2] [3] is developing a Proof of Concept (PoC) system promoting a patient-centric web-based data sharing platform in Europe. It includes a personalised user authentication scheme, a data lake for efficient data management, blockchain for data access control and audit trail [1,4], among other technologies [3]. Essential to the Serums project outcome is a rigorous public system evaluation. Due to the Covid-19 pandemic, Serums uses an online participatory approach to evaluate the integrated system [3], i.e., to ascertain public perception of usability, security and trust in the system. This paper describes the applied methodology to demonstrate the system effectiveness using public feedback, discussing some challenges faced in a series of PoC evaluations with patients and professionals.

2. Overview on the Serums system design

Figure 1 shows users (patients, healthcare professionals, admin personnel, etc.) and the interactions of core components in the system. In order to retrieve medical data, regardless of format, language and origin in Europe, Serums integrates a Smart Patient Health Record (SPHR) to represent the varying formats of patient data across different sources, i.e., a central information database for patients' medical history registered with healthcare providers. It allows secure data manipulation capability in a Data Lake composed of different data vaults [1].

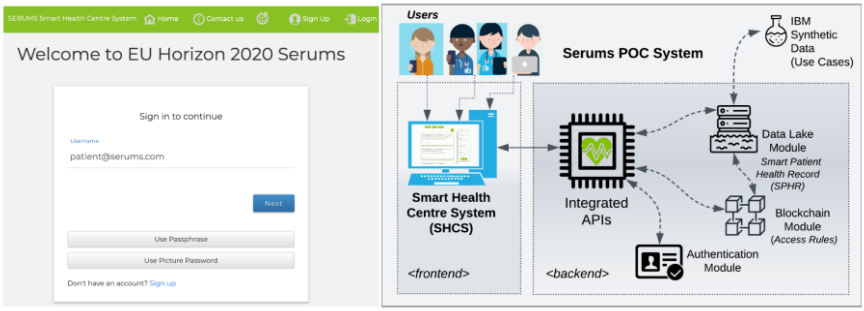

Figure 1. Serums PoC System overview on users and components.

The system is underpinned by the primary requirement for the patient to be in full control of who has access to their data, whilst still complying with relevant legislation such as GDPR [3]. A private and permissioned Blockchain manages the user access control storing fine-grained access rules, defined primarily by patients in a user-friendly interface [1,2]. The authorisation scheme, with underlying formal logic representation [2], runs checks every time data requests are issued to the Data Lake from users authenticated in the system. Consequently, all interactions by any individual are stored within the chain for auditing and identification of any potentially inappropriate or illegal attempt to access patient information [1].

[2] EU H2020 project SERUMS website: https://www.serums-h2020.org/

The Authentication module, coined FlexPass [4], composes the first layer of cyber security. It offers a flexible, user-adaptable and personalised approach that combines graphical and textual passwords, and a multi-factor authentication (mFA) via a mobile application. This module is central for regulating Data Lake and Blockchain permission to run requests issued by authenticated users. Serums also uses the IBM synthetic data fabrication platform to replicate realistic medical data for system testing/validation [3].

3. Serums PoC evaluation guidelines and methodology

Participatory approaches for PoC system evaluation essentially require stakeholder's (i.e., healthcare professionals, IT staff, patients) to *assess the validity of requirements and guide the definition of technical needs to meet end-user expectations* [3]. We highlight the main idea behind the methodology as follows: teams in three countries used a collaborative strategy to recruit participants (end-users) via social media. Participants were selected as healthcare users residing at (or close) to a healthcare environment. We faced a few challenges in the recruitment/scheduling of online sessions, including extra effort in preparation and execution, factors that likely had a negative effect on our sample size and diversity. Interactive 45-minute sessions (online due to Covid-19 restrictions) enabled teams to collect qualitative/quantitative data, e.g., using explanatory videos, textual materials, semi-structured interviews, and system exploration tasks. A final questionnaire (with 75 questions including some free-text) based on state-of-the-art research and guidelines on usability, user experience, security and trust (e.g., System Usability Scale (SUS), AttrakDiff, Technology Acceptance models) [6], introduced questions on the perceived usability, usefulness, security, and trust in the system design.

Examples of questions on perceived usability are "Overall, how difficult or easy do you find the password creation task?" and "Overall, how difficult or easy do you find the *login task?*". Users rated all the statements through a 5-point Likert Scale (e.g., 1: Not at all - 5: Absolutely). For the perceived usefulness [7], questions included "*Using Serums would make it possible to share and get insight in the patient's medical data*", "*Using Serums would make finding and sharing the medical information more efficient*". On perceived security, based on usable security research [5], we included questions on whether users 'believe the authentication system is secure', whether they 'believe their password is strong' as well as questions that relate to their trust towards the system, like its 'ability to protect their data privacy', their 'trust to keep their data safe'. With regards to patients' trust towards the overall system design, example questions include: "*How comfortable or uncomfortable would you be with this system managing your medical data?*" and "*How capable or incapable do you consider this system in handling medical data securely?*".

4. Serums PoC evaluation results

The second evaluation (44 participants) showed an increase of perceived usability (PoC1: 3.85 vs. PoC2: 4.11), security (PoC1: 3.88 vs. PoC2: 4.2) and trust towards the authentication technology (PoC1: 3.98 vs. PoC2: 4.1). The increase reflects the positive impact of the refined system based on previous end-user feedback, e.g., PoC1 suggested the graphical password needed improvement as users commented on the gesture input functionality. Hence, PoC2 system included the mFA mobile application. The overall

authentication system usability (74.77%) scores well based on the guidelines of SUS [6], which suggests that a score above 68% entails adequate usability practices.

Security-related scores remained stable on both PoC results mainly because we applied the same authentication tasks. It is worth noticing that other technologies integrated into the backend are not visible to the users in the frontend, which poses difficulties for users to assess their benefits. One such example is how internally the system brings together distributed and heterogeneous data into a unique format in the data lake. Finally, users rated the authentication system, and the majority of users *extremely* (26/44) or *very much* (14/44) appreciated the flexible approach, with 4 users either *moderately* (1/44) or *slightly* (3/44) liked the idea. Users with higher computer literacy skills may have skewed the results, though the evaluation of their trust reflects the extent to which we disseminate clear information on the Serums features and technologies.

5. Conclusions

The public system evaluation outcomes ascertained during the PoC have produced valuable feedback on the perceived usability and security of the platform. As a result, the Serums PoC design has been refined and evaluated by end-users. The European use cases have guided the elicitation of Serums functional and non-functional requirements, and contributed to test the overall system design to potentially meet user expectations.

References

[1] Bowles JK, Mendoza-Santana J, Vermeulen AF, Webber T, Blackledge E. Integrating healthcare data for enhanced citizen-centred care and analytics. InIntegrated Citizen Centered Digital Health and Social Care 2020 (pp. 17-21). IOS Press.

[2] Banton M, Bowles J, Silvina A, Webber T: Conflict-free access rules for sharing smart patient health records. In: Proc. of the 5th Conf. RuleML+RR 2021. LNCS, 12851, p. 1–15. Springer, Cham.

[3] Janjic V, Bowles JK, Vermeulen AF, Silvina A, Belk M, Fidas C, Pitsillides A, Kumar M, Rossbory M, Vinov M, Given-Wilson T. The serums tool-chain: ensuring security and privacy of medical data in smart patient-centric healthcare systems. In2019 IEEE International Conference on Big Data (Big Data) 2019 Dec 9 (pp. 2726-2735). IEEE.

[4] Constantinides A, Belk M, Fidas C, Pitsillides A. Design and Development of a Patient-centric User Authentication System. InAdjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization 2020 Jul 14. p. 201-203.

[5] Díaz-Oreiro I, López G, Quesada L, Guerrero LA. Standardized questionnaires for user experience evaluation: A systematic literature review. Multidisciplinary Digital Publishing Institute Proceedings. 2019;31(1):14.

[6] Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly. 1989 Sep 1:319-40.

[7] Reese K, Smith T, Dutson J, Armknecht J, Cameron J, Seamons K. A Usability Study of Five {Two-Factor} Authentication Methods. InFifteenth Symposium on Usable Privacy and Security (SOUPS 2019) 2019. p. 357-370.