OPEN ACCESS

2nd International Electronic Conference on Sensors and Applications 15–30 November 2015

www.mdpi.com/journal/sensors

Conference Proceedings Paper – Sensors and Applications

Privacy in Affective Computing based on Mobile Sensing Systems

Elsa Macías[1,*], Alvaro Suárez[1], Raquel Lacuesta[2] and Jaime Lloret[3]

[1] Departamento de Ingeniería Telemática, Universidad de Las Palmas de Gran Canaria. Edificio de Electrónica y Telecomunicación, 35017. Las Palmas de Gran Canaria, Spain;
E-Mail: elsa.macias@.ulpgc.es; alvaro.suarez@.ulpgc.es

[2] Universidad de Zaragoza, Pedro Cerbuna, 12, 50018, Zaragoza, Spain;
E-Mail: raquelinvestigacion1@gmail.com

[3] Universidad Politécnica de Valencia, Camino Vera s/n, 46022, Valencia, Spain;
E-Mail: jlloret@dcom.upv.es

* Author to whom correspondence should be addressed; E-Mail: elsa.macias@.ulpgc.es;
Tel.: +34 928 45 80 54; Fax: +34 928 45 13 80.

Published: 11 November 2015

Abstract: The term *affective computing* was coined twenty years ago to refer to computers human-like capabilities to detect and recognize user's emotions. Mobile sensing systems can be used to sense the emotional state of one or more users and let a third-party can use this information to produce changes in the user's emotional state, or analyze hundreds of thousands of pictures, gestures, speeches and so on of people and train recognition systems for affective computing applications. For example teachers or e-learning systems as third-party systems can react appropriately maintaining motivation for their students according their emotional states using augmented reality techniques or changing the multimedia resources used in the lectures. Despite the direct benefits of knowing the emotional states, people in general is opposed to a system captures their emotions with smart phones equipped with built-in or external sensors such as image sensor to capture images and record videos, or a pressure sensor to detect the force or rhythm of a finger or stylus pen strokes within the display area. For that reason, currently privacy is one of the important barrier that limits the social acceptance of mobile sensing systems to do affective computing. In this paper we focus on mobile sensing systems to do affective computing preserving the user's privacy to motivate the users to be sensed.

Keywords: Affective Computing; Mobile Sensing; Privacy

1. Introduction

Affective computing is computing that relates to, arises from, or deliberately influences emotion or other affective phenomena [1]. Affective computing let emotions be recognized using facial expressions, speech, gesture, posture and physiological signals (arousal, breathing and heart rates, blood pressure, skin resistance and some facial electromyography activities). Affective computing systems are expected to have positive impacts on many domains. For example on learning with online courses since different from traditional classrooms, teachers cannot guess the students are paying attention or mind wandering [2]. To supply this lack of information such as facial cues, Information and Communications Technology (ICT) can be enriched with enhanced devices and software that detect the emotions of students [3].

Today's mobile phones are equipped with sophisticated and numerous *sensors*, such as GPS and high-quality microphone and cameras, *advanced computing hardware* (e.g. multicore CPUs and gigabytes of memory) and a range of *communication interfaces*, such as WiFi, Bluetooth, 4G/LTE, and a near-field communication (NFC) [4]. These sensing capabilities added to the growing computing hardware and communication interfaces are extending the way mobiles devices can sense our emotions and processing them distributed between the mobile device and the cloud, opening an inquiry on the mobile apps programming to do affective computing for the full scope of the domain applications (educational, mental health, psychology...).

Leaks of personal data in mobile sensing systems are a social barrier and a general concern in research community. That is the reason why solutions that guarantee privacy are welcome to promote the wide adoption of these systems [5-8].

This paper is concerned about reviewing some techniques to preserve the user's privacy in mobile sensing affective computing. In section 2 we review some current works that make mobile sensing to do affective computing that are concerned about privacy but they do not provide a current solution to this problem. Section 3 presents some techniques and proposals to provide a privacy solution that can be applied in affective computing. The system proposal and analytical verification is presented in Section 4. Finally, some conclusions are derived in Section 5.

2. Mobile sensing in affective computing

In the introduction we mention some of the signals and expressions usually are sensed to do the affective computing. In our previous work [5] the reader can review papers closely related to the sensing of those variables using current smartphones.

Recently, some authors propose collect a big amount of personal data to create a multi-dimensional emotional data collection process [8-9]. In [8] the authors also propose the usage of the mobile cloud computing to enhance the capability of mobile devices in order to do the resource intensive affective computing a reality. These authors conclude that privacy and security issues of user data in the multi-dimensional emotional data collection process must be researched in the ongoing work. Authors in [9] propose the usage of sensors from thousands of mobile phones to do a multi-modal emotion recognition system. As data are collected from many users, they will present a prototype that uses a cloud-based big data architecture to create this emotion recognition system.

We anticipate in [5] that privacy is an important aspect to preserve the personal data that are sensed. Recently, also the authors in [6] with author W. Picard who is a well-recognized researcher on affective computing shows how the accelerometer currently embedded in smartphones can be used to monitor cardiovascular health under limited conditions *offering the possibility for intrusion of privacy*. We can affirm again that up to date there is a general concern in research community about the privacy before mobile sensing system be widely adopted with guarantees. Protecting privacy is far from trivial. Privacy concerns must be properly addressed in order to increase participation and trustworthiness. Next section faces this issue.

3. Privacy in affective computing

Historically, some techniques have been used to tackle abuses in privacy: i) *cryptographic* techniques to increase the difficulty to access to unauthorized data [10-11]; ii) *obfuscation* techniques [12] to minimize information content (sensitive information is neither published nor derived, avoiding the access to the information even with aggregation and inference attacks [13]); iii) and the use of *reputation* techniques [14] to evaluate the behavior of the systems. Some drawbacks of these techniques could be aspects such as requiring complex mechanisms for key sharing, reducing the value of the published information or the trustworthiness of some systems.

One of the main areas of privacy research is the identification of identifiers when surfing the web or accessing to social networks. Some research has been made in order to achieve privacy when working with sensory data, however there is little research on areas related with affective computing, for example when working with facial recognition or using wearable sensors to catch personal information. Authors in [15] analyze some privacy risks exposing that there are some user's privacy awareness in reference with the implications that sharing personal data in social networks or mobile devices (location, video, photos…) can entail. Nevertheless, little is known by users about the inferred and acquired knowledge about their activities, context and behaviors that we can obtain from sensors measurements on affective computing. In order to protect individual's identity we can use some anonymity, perturbation, suppression or generalization techniques [16-19].

In [20], the authors propose a lightweight algorithm to classify facial expressions. In order to maintain privacy they use randomization techniques. Some surveys have been done about privacy protection in pervasive systems. In [21], authors consider representative classes of pervasive applications, and identify the requirements they impose in terms of privacy and trade-off with service quality. Then, they review the most prominent privacy preservation approaches.

In [22], the authors try to preserve user's privacy when working with participatory sensing. They come up with a proposal not based on the use of tessellation techniques as the common technique for location privacy, but on microaggregation ones. They propose use the positive insights of both techniques when proposing his Variable size Maximum Distance to Average Vector (Hybrid-VMDAV) algorithm. They also study k-anonymity limitations and propose an l-diverse method to improve this algorithm. They show some advantages of that proposal after carrying out the simulation tests. An extra layer of security is implemented by applying Gaussian noise scan to user locations. In [23] the authors propose a mechanism based on incentives to protect user privacy. Their participatory sensing architecture open up security in spite of the presence of strong adversaries.

In [24] the authors review a number of solutions presented in the bibliography to establish "face recognition" privacy in public spaces or social networking sites. Some solutions proposed are based on the use of strong cryptography, using different mechanisms and times to carry out the matching and identification phases. Other proposals let to maintain most facial pictures aspects avoiding identification using de-identifying algorithms. Authors in [25] try to preserve sensitive data before transmitting it. They transform these data using arithmetic and database operations in order to modify the original data. The data obtained do not let the service provider to get hold of any conclusion from it. When the customer receives the pseudo-result, they carry out a retransformation to access to the result. In [26] they proposed a system, which provides data ownership privacy using token generation for each user, each session and data security using RSA. Their approach to enhanced data security work by separating private data content from metadata concerning its origin and semantics. An unknown identification system based on public-key cryptography provides billing of anonymous customers without connecting their private data to their authentications.

4. System proposal and analytical verification

Our proposal uses trust chains to access the sensible data of the mobile devices. There are levels of trust, which range from 0 to 1 in a scale of 0.1. A trust chain is obtained by multiplying the level of trust of the involved in the path. Thus, when there is a non-trustable node, this path cannot be selected because the trust chain is equal to zero. Paths to send data between nodes are selected based on the trust chain value. The higher the value, the most appropriate is the path. The algorithm followed by our proposed system is shown in Figure 1. Moreover, the data is sent cyphered. In figure 2, we show how impacts the trust level of both Node 1 and Node 2 selecting the path when there are only two nodes. We can see that even when node 1 has very high trust (Trust=1), if node 2 has very low trust, this path has low trust chain value, so it will not be selected.

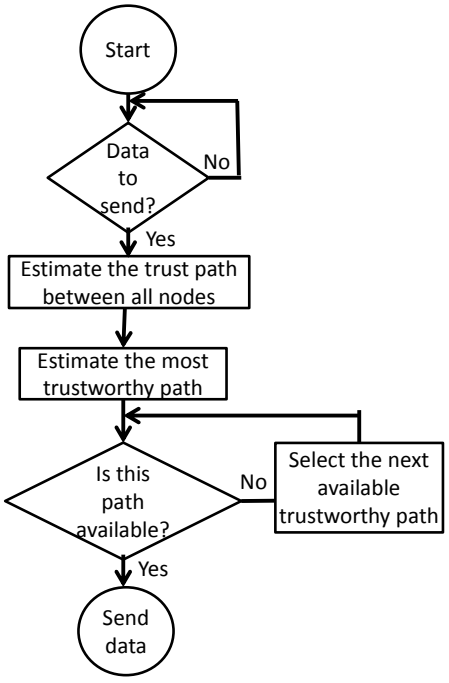

Figure 1. System Algorithm.

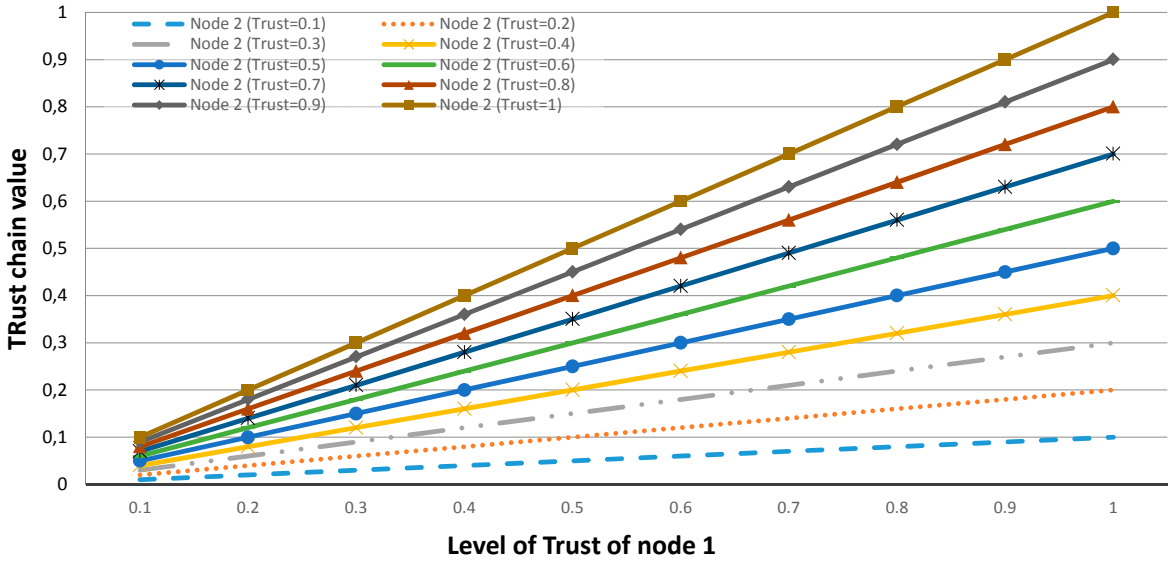

Figure 2. Trust chain value for selecting the path between 2 nodes

5. Conclusion

As the content is each time more "sensitive" we need to be more cautious about the generation of implicit and explicit content, the use of these data and the design of modeling tools that protect users' rights. We must define the limiting access of participants (restrictions, preservation and deletions), the content owned, times and control to make unintended use technically unfeasible. Privacy can be considered as a measure relative to the information exposure of a participant. Certain data should be anonymized and other available to the participants. We also must protect the privacy of the user also in presence of interference and context information or against aggregation of heterogeneous data.

Despite the fact there are techniques and solutions to provide privacy, mobile applications to do mobile sensing with privacy are welcomed. We are in the phase of designing a mobile application that preserves the user's privacy to do affective computing.

Author Contributions

All authors contributed to the research related to mobile sensing and privacy in affective computing and the preparation of this manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Picard, R.W.; *Affective Computing*, MIT Press, Cambridge, 1997.
2. Pham, P.; Wang, J. AttentiveLearner: Improving Mobile MOOC Learning via Implicit Heart Rate Tracking. *Artificial Intelligence in Education*; Springer, 2015; pp. 367-376.
3. Akbiyik, C. Can Affective Computing Lead to More Effective Use of ICT in Education? *Revista de Educacion,* **2010**, *352*.

4. Pejovic, V.; Musolesi, M. Anticipatory Mobile Computing: A Survey of the State of the Art and Research Challenges. *ACM Comput. Surv.* **2015**, *47, 3*. 29 pages.
5. Macias, E.; Suarez, A.; Lloret, J., Mobile Sensing Systems. *Sensors* **2013**, *13*, 17292-17321.
6. Hernandez, J.; McDuff, D.; Picard, R. BioPhone: Physiology Monitoring from Peripheral Smartphone Motions. Int. Conf. of the IEEE Engineering in Medicine and Biology Society (EMBC), Milan, Italy, August 2015.
7. Rana, R.; Hume, M.; Reilly, J.; Jurdak, R.; Soar, J., Opportunistic and Context-aware Affect Sensing on Smartphones: The Concept, Challenges and Opportunities. Available on online: http://arxiv.org/ftp/arxiv/papers/1502/1502.02796.pdf (accessed on 12th October 2015).
8. Chen, M.; Zhang, Y.; Li, Y.; Mao, S.; Leung, V.C.M. EMC: Emotion-aware mobile cloud computing in 5G. *IEEE Network.* **2015**, *29, 2*, 32 - 38.
9. Baimbetov, Y.; Khalil, I.; Steinbauer, M.; Anderst-Kotsis, G. Using Big Data for Emotionally Intelligent Mobile Services through Multi-Modal Emotion Recognition. *Inclusive Smart Cities and e-Health*; Springer International Publishing, 2015; pp. 127-138.
10. Hajny, Jan, et al. "Performance evaluation of primitives for privacy-enhancing cryptography on current smart-cards and smart-phones." Data Privacy Management and Autonomous Spontaneous Security. Springer Berlin Heidelberg, 2014. 17-33.
11. Barni, Mauro, Giulia Droandi, and Riccardo Lazzeretti. "Privacy Protection in Biometric-Based Recognition Systems: A marriage between cryptography and signal processing." Signal Processing Magazine, IEEE 32.5 (2015): 66-76.
12. Chen, Terence, et al. "On the effectiveness of obfuscation techniques in online social networks." Privacy Enhancing Technologies. Springer International Publishing, 2014.
13. Bhamidipati, Sandilya, et al. "PriView: Personalized Media Consumption Meets Privacy against Inference Attacks." IEEE Software, 32.4 (2015): 53-59.
14. Wang, Xinlei, et al. "Enabling reputation and trust in privacy-preserving mobile sensing." IEEE Transactions on Mobile Computing, 13.12 (2014): 2777-2790.
15. Raij, Andrew, et al. "Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment." SIGCHI Conf. on Human Factors in Computing Systems. ACM, 2011.
16. Sweatt, Brian M. A Privacy-Preserving Personal Sensor Data Ecosystem. Diss. Massachusetts Institute of Technology, 2014.
17. Sweeney, Latanya. "Achieving k-anonymity privacy protection using generalization and suppression." Int. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10.05 (2002): 571-588.
18. Hay, Michael, et al. "Resisting structural re-identification in anonymized social networks." Proceedings of the VLDB Endowment 1.1 (2008): 102-114.
19. Yin, L., et al. "Re-Identification Risk versus Data Utility for Aggregated Mobility Research Using Mobile Phone Location Data." PloS one 10.10 (2014): e0140589-e0140589.
20. Rajarajan, M., and R. Yogachandran. "Efficient Privacy-Preserving Facial Expression Classification." IEEE Transactions on Dependable and Secure Computing (2015).
21. Bettini, Claudio, and Daniele Riboni. "Privacy protection in pervasive systems: State of the art and technical challenges." Pervasive and Mobile Computing 17 (2015): 159-174.

22. Huang, Kuan Lun, Salil S. Kanhere, and Wen Hu. "Preserving privacy in participatory sensing systems." Computer Communications 33.11 (2010): 1266-1280.
23. Gisdakis, Stylianos, Thanassis Giannetsos, and Panos Papadimitratos. "SPPEAR: security & privacy-preserving architecture for participatory-sensing applications." Proceedings of the 2014 ACM Conference on Security and privacy in wireless & mobile networks. ACM, 2014.
24. Cammozzo, Alberto. "Face Recognition and Privacy enhancing techniques." The Social Impact of Social Computing: 101-109.
25. Boyens, Claus, and Oliver Günther. "Using Online Services in Untrusted Environments: A Privacy Preserving Architecture." ECIS 2003 Proceedings (2003): 9.
26. Kharat, Pramila, and Amar Buchade. "Survey on Privacy Preserving and Data Security Techniques." International Journal of Science and Research (IJSR), Volume 4 Issue 7, July 2015, Pp. 1912-1916.