Anonymized Distributed PHR Using Blockchain for Openness and Non-repudiation Guarantee

International Conference on Theory and Practice of Digital Libraries

TPDL 2018: Digital Libraries for Open Knowledge pp 381-385 | Cite as

- David Mendes (1)
- Irene Rodrigues (1) Email author (ipr@di.uevora.pt)
- César Fonseca (2)
- Manuel Lopes (3)
- José Manuel García-Alonso (4)
- Javier Berrocal (4)

1. LISP, ECT, Universidade de Évora, , Évora, Portugal
2. Departamento de Enfermagem, Universidade de Évora, , Évora, Portugal
3. Rede Nacional de Cuidados Continuados, Ministério da Saúde, , Lisbon, Portugal
4. Universidad de Extremadura, , Cáceres, Spain

Conference paper
First Online: 05 September 2018

Part of the Lecture Notes in Computer Science book series (LNCS, volume 11057)

Abstract

We introduce our solution developed for data privacy, and specifically for cognitive security that can be enforced and guaranteed using blockchain technology in SAAL (Smart Ambient Assisted Living) environments. Using our proposal the access to a patient's clinical process resists tampering and ransomware attacks that have recently plagued the HIS (Hospital Information Systems) in various countries. One important side effect of this data infrastructure is that it can be accessed in open form, for research purposes for instance, since no individual re-identification or group profiling is possible by any means.

Keywords

Blockchain Data privacy Interoperability Open access

This work was supported by 4IE project (0045-4IE-4-P) funded by the Interreg V-A España-Portugal (POCTEP) 2014–2020 program and by LISP, Laboratório de Informática, Sistemas e Paralelismo ref: UID/CEC/4668/2016.

References

1. Ahmed, A., Ahmed, E.: A survey on mobile edge computing. In: 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–8, January 2016
Google Scholar (https://scholar.google.com/scholar?q=Ahmed%2C%20A.%2C%20Ahmed%2C%20E.%3A%20A%20survey%20on%20mobile%20edge%20computing.%20In%3A%2010th%20International%20Conference%20on%20Intelligent%20Systems%20and%20Control%20%28ISCO%29%2C%20pp.%201%E2%80%938%2C%20January%202016)

2. Asano, S., Yashiro, T., Sakamura, K.: Device collaboration framework in IoT-aggregator for realizing smart environment. In: TRON Symposium, December 2016
Google Scholar (https://scholar.google.com/scholar?q=Asano%2C%20S.%2C%20Yashiro%2C%20T.%2C%20Sakamura%2C%20K.%3A%20Device%20collaboration%20framework%20in%20IoT-aggregator%20for%20realizing%20smart%20environment.%20In%3A%20TRON%20Symposium%2C%20December%202016)

3. Castro, M., Liskov, B.: Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst. **20**(4), 398–461 (2002)
CrossRef (https://doi.org/10.1145/571637.571640)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Practical%20byzantine%20fault%20tolerance%20and%20proactive%20recovery&author=M.%20Castro&author=B.%20Liskov&journal=ACM%20Trans.%20Comput.%20Syst.&volume=20&issue=4&pages=398-461&publication_year=2002)

4. Greenstadt, R., Beal, J.: Cognitive security for personal devices. In: Proceedings of the 1st ACM Workshop on Workshop on AISec, AISec 2008, pp. 27–30. ACM, New York (2008)
Google Scholar (https://scholar.google.com/scholar?q=Greenstadt%2C%20R.%2C%20Beal%2C%20J.%3A%20Cognitive%20security%20for%20personal%20devices.%20In%3A%20Proceedings%20of%20the%201st%20ACM%20Workshop%20on%20Workshop%20on%20AISec%2C%20AISec%202008%2C%20pp.%2027%E2%80%9330.%20ACM%2C%20New%20York%20%282008%29)

5. Holler, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Boyle, D.: From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Elsevier Science (2014)
Google Scholar (https://scholar.google.com/scholar?q=Holler%2C%20J.%2C%20Tsiatsis%2C%20V.%2C%20Mulligan%2C%20C.%2C%20Karnouskos%2C%20S.%2C%20Boyle%2C%20D.%3A%20From

%20Machine-to-Machine%20to%20the%20Internet%20of%20Things%3A%20Introduction%20to%20a%20New%20Age%20of%20Intelligence.%20Elsevier%20Science%20%282014%29)

6. Ichikawa, D., Kashiyama, M., Ueno, T.: Tamper-resistant mobile health using blockchain technology. JMIR Mhealth Uhealth **5**(7), e111 (2017)
CrossRef (https://doi.org/10.2196/mhealth.7938)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Tamper-resistant%20mobile%20health%20using%20blockchain%20technology&author=D.%20Ichikawa&author=M.%20Kashiyama&author=T.%20Ueno&journal=JMIR%20Mhealth%20Uhealth&volume=5&issue=7&pages=e111&publication_year=2017)

7. Iroha. Hyperledger Iroha. Accessed 29 Aug 2017
Google Scholar (https://scholar.google.com/scholar?q=Iroha.%20Hyperledger%20Iroha.%20Accessed%2029%20Aug%202017)

8. Jacobovitz, O.: Blockchain for identity management. Technical report, The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel, December 2016. Technical Report #16-02
Google Scholar (https://scholar.google.com/scholar?q=Jacobovitz%2C%20O.%3A%20Blockchain%20for%20identity%20management.%20Technical%20report%2C%20The%20Lynne%20and%20William%20Frankel%20Center%20for%20Computer%20Science%20Department%20of%20Computer%20Science%2C%20Ben-Gurion%20University%2C%20Beer%20Sheva%2C%20Israel%2C%20December%202016.%20Technical%20Report%20%2316-02)

9. Jain, S., Kajal, A.: Effective analysis of risks and vulnerabilities in internet of things. Int. J. Comput. Corp. Res. **5**(2) (2015)
Google Scholar (https://scholar.google.com/scholar?q=Jain%2C%20S.%2C%20Kajal%2C%20A.%3A%20Effective%20analysis%20of%20risks%20and%20vulnerabilities%20in%20internet%20of%20things.%20Int.%20J.%20Comput.%20Corp.%20Res.%205%282%29%20%282015%29)

10. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L.: Provchain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468–477, May 2017
Google Scholar (https://scholar.google.com/scholar?q=Liang%2C%20X.%2C%20Shetty%2C%20S.%2C%20Tosh%2C%20D.%2C%20Kamhoua%2C%20C.%2C%20Kwiat%2C%20K.%2C%20Njilla%2C%20L.%3A%20Provchain%3A%20a%20blockchain-based%20data%20provenance%20architecture%20in%20cloud%20environment%20with%20enhanced%20privacy%20and%20availability.%20In%3A%202017%2017th%20IEEE%2FACM%20International%20Symposium%20on%20Cluster%2C%20Cloud%20and%20Grid%20Computing%20%28CCGRID%29%2C%20pp.%20468%E2%80%93477%2C%20May%202017

)

11. NASDAQ. Byzantine Fault Tolerance. Accessed 13 Apr 2018
Google Scholar (https://scholar.google.com/scholar?q=NASDAQ.%20Byzantine%20Fault%20Tolerance.%20Accessed%2013%20Apr%202018)

12. Pramanik, M.I., Lau, R.Y., Demirkan, H., Azad, M.A.K.: Smart health: big data enabled health paradigm within smart cities. Expert Syst. Appl. **87**, 370–383 (2017)
CrossRef (https://doi.org/10.1016/j.eswa.2017.06.027)
Google Scholar (http://scholar.google.com/scholar_lookup?title=Smart%20health%3A%20big%20data%20enabled%20health%20paradigm%20within%20smart%20cities&author=MI.%20Pramanik&author=RY.%20Lau&author=H.%20Demirkan&author=MAK.%20Azad&journal=Expert%20Syst.%20Appl.&volume=87&pages=370-383&publication_year=2017)

13. RegEU. Regulation EU No 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC (eIDAS regulation) (2014). European union: 4459
Google Scholar (https://scholar.google.com/scholar?q=RegEU.%20Regulation%20EU%20No%20910%2F2014%20of%20the%20European%20parliament%20and%20of%20the%20council%20of%203%20July%202014%20on%20electronic%20identification%20and%20trust%20services%20for%20electronic%20transactions%20in%20the%20internal%20market%20and%20repealing%20directive%201999%2F93%2FEC%20%28eIDAS%20regulation%29%20%282014%29.%20European%20union%3A%204459)

Copyright information

About this paper

Cite this paper as:

Mendes D., Rodrigues I., Fonseca C., Lopes M., García-Alonso J.M., Berrocal J. (2018) Anonymized Distributed PHR Using Blockchain for Openness and Non-repudiation Guarantee. In: Méndez E., Crestani F., Ribeiro C., David G., Lopes J. (eds) Digital Libraries for Open Knowledge. TPDL 2018. Lecture Notes in Computer Science, vol 11057. Springer, Cham

- First Online 05 September 2018
- DOI https://doi.org/10.1007/978-3-030-00066-0_45
- Publisher Name Springer, Cham
- Print ISBN 978-3-030-00065-3
- Online ISBN 978-3-030-00066-0
- eBook Packages Computer Science

- Reprints and Permissions

Personalised recommendations