Decision Support Systems and Education
J. Mantas et al. (Eds.)

doi:10.3233/978-1-61499-921-8-170

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

David MENDES[a,1], Irene Pimenta RODRIGUES[a], César FONSECA[a], Manuel José LOPES[b], José Manuel GARCÍA-ALONSO[c], and Javier BERROCAL[c]
[a] *Universidade de Évora, Évora, Portugal*
[b] *Rede Nacional de Cuidados Continuados, Ministério da Saúde, Portugal*
[c] *Universidad de Extremadura, Cáceres, Spain*

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. Personal clinical and demographic information segments to various levels that assures that it can only be rebuilt at the interested and authorized parties and no profiling can be extracted from the blockchain itself. 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. The core of the blockchain model assures non-repudiation possible by any of the involved information producers thus maintaining ledger fidelity of the enclosed historical process information. 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. Healthcare Process, Blockchain, Data privacy, Interoperability, Home Based Care, IoT

1. Introduction

In the realm of clinical information storage and maintenance one of the most hazardous situations that have been developing lately are the ransomware attacks and sensitive information breaches that are frightening the Hospital and National Health Information Services all around the world. Some new forms of data (actually information and knowledge) storage are in need that can circumvent this problem urgently for the adherence to health information processing that is emergent in these times of Artificial Intelligence and Big Data Analytics dawn. Our proposal prevent, by design, all these problems and is not vulnerable to these kind of threats while promoting security in the edge-computing era [1, 2, 3]

[1] Corresponding Author: David Mendes, Departamento de Informática; Universidade de Évora. E-mail: dmendes@uevora.pt.

2. Problem

We define an abstraction that we call ICP (Individual Care Process), a knowledge item that collects comprehensive information about an individual's health and care history. It is necessary for the comprehensive functioning of the ICP, to keep the information coming from many sources, which can change it without central control, but with the consistent need to keep an unchanging record of all state transitions. All the stakeholders may, in accordance with the fulfillment of the necessary authorizations for access to clinical data, consult and change this data. The distributed technology that allows us to guarantee this type of access while maintaining the privacy and confidentiality of the data is Blockchain, in which the different actors maintain the ledger of all the transactions. We can visualize the ICP as the ledger for all events related to the health / care process of a citizen. Blockchain technology ensures that only the owner of the private authentication key can authorize the manipulation of the sensitive data of any ICP.

3. Methods

3.1. Cognitive security impact evaluation

It has become utterly important that data protection be not only concerned with data in isolated terms but with the cognitive power that systems can extract from data when taken aggregated. Individual profiling as well as Group profiling, are currently major privacy concerns, and to avoid them a special attention has to be provided to Cognitive Security [4]. This kind of concern has lead in European Union to the enforcement of General Data Protection Regulation that became effective in all EU countries in May 25 of 2018. In wireless networks like those present in AAL environments special concerns have to be taken has illustrated in [5] and particularly in Smart Environments [6, 7, 8, 9, 10] as already predicted by [11, 12, 13].

3.2. Blockchain data privacy and protection

It is necessary for the operation of the comprehensive ICP (Individual Care Process) to keep the information coming from many sources that can change without central control, but with the need to keep a record of all immutable state transitions. The distributed technology that allows us to ensure this type of access and data confidentiality is the Blockchain [14–18], in which the different actors maintain the ledger of every healthcare transaction [19, 20, 21, 22, 23]. We can visualize the ICP as the ledger of all events related to the process of health/care of a citizen. Access to data, which a particular healthcare provider may have access to is encapsulated in the ICP itself by prior informed consent. For example, be encapsulated in accordance to the legislation (regulation) in force and prepared for the regulations already in place GDPR (General Data Protection Regulation)and eIDAS 910/2014 regarding digital signature and document certification [7, 24, 25]. Specifically it is implemented the DLA that use BFT (Byzantine Fault Tolerance) [15] like Hashgraph and others based on the Hyperledger project of the Linux Foundation [18, 19].With these algorithms, even the IoT gateways, based on smartphones, may act on the ledger while ensuring absolute authenticity and privacy of the ICP [26].

4. Blockchain

Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. Transactions can be verified and recorded through the consensus of all parties involved. The blockchain is permissioned and offers enhanced privacy. Through the use of IDs and permissions, users can specify which transaction details they want other participants to be permitted to view. Because participants in a transaction have access to the same records, they can validate transactions and verify identities or ownership without the need for third-party intermediaries. Electronic medical records are currently maintained in data centers (in a cloud-like environment), and access is limited to hospital and care provider networks. Most healthcare data is held in some type of centralized location: an EHR system, a data warehouse, or a repository run by a health information exchange. Each system may have been developed independently and might generate and store the data in its own particular format, leading to the data siloes and interoperability woes that frustrate providers, patients, researchers, and facilitators. Centralization of such information also makes it vulnerable to security breach and can be expensive [14]. The blockchain approach might just be the overhaul that healthcare is looking for. No single entity is in charge of holding the data, yet all participants are responsible for ensuring data integrity and security. Because participants in a blockchain in healthcare are more likely to be altruistic and operate under real identities than are users of a highly anonymous the benefits of avoiding PoW may outweigh the risks associated with node voting like the solution to byzantine faults [27].

4.1. Distributed Ledger Algorithms

It is important to use Distributed Ledger Algorithms (DLA) algorithms that only require small computational power and maintain an adequate level of justice in the transaction order. We use these algorithms, specifically, DLAs implementing "Byzantine Fault Tolerance" [15] such as Hashgraph and others based on the Linux Foundation's Hyperledger project [18, 19]. With these algorithms, the implemented Smartphone-based SAAL (Smart Ambient Assisted Living) IoT gateways can act on the ledger while guaranteeing the authenticity and absolute privacy of the ICP, even in IoT [26].

4.2. Byzantine Fault Tolerance

Byzantine Fault Tolerant systems are designed to tolerate a number f of Byzantine faulty nodes in a network. To ensure that a transaction is accepted as valid, $2f+1$ valid signatures from distinct peers are needed. In non-failure cases, a client submits a transaction to a leader peer. That peer verifies the transaction and signs it. It then broadcasts to the remaining $2f+1$ validating peers. The other peers do their own signature. The broadcast is sequentially made until the last needed peer receives the required number of valid signatures, including its own. All the signatures are validated and that transaction is then considered valid. Having met the consensus state, a final broadcast to all peers is done so that they can add the transaction, with all the signatures, to the ledger. The process is repeated until reaching $2f+1$ valid signatures [16].

4.3. Information hiding through API

Encapsulating in the ICP as an object that contains the named authorizations for its manipulation. Authorizations allow the object itself to be viewed/changed by who (human or device) authenticates, according to eIDAS 910/2014 [24, 25]. An authenticated user can reconstruct the identity, but always in an ephemeral and non-transmissible environment to prevent personal re-identification according to the GDPR, HIPPA and the Umbrella Protocol [28]. To enable the development, using Deep Learning (DL) techniques, of the models that activate the less differentiated caregiver. Allow the application of DL algorithms to reason about the ICP in order to suggest rules for automatic activation of care providers (human or devices).

5. Solution

According to the several considerations introduced above, we developed our solution using a raw blockchain implementation [14] with the Hyperledger Fabric DLA [5] in order to attain computable reasoning over a highly secure and authentic home based ambient assisted living environment. Some other related proposals have been emerging recently as of late 2017 like [17].

6. Conclusions

While completely tamper proof, we indicate the Blockchain technology algorithms which usage can lead to a fair, democratic maintenance of the ledger while being low computational power consumers. This characteristic enables the usability by low computing power device like those present in the AAL environments. The level of safety perceived by monitored patients in these domiciled or institutionalized environments is very high while their health information is guaranteed to be at no risk.

Acknowledgement

This work was supported by 4IE project (0045-4IE-4-P) funded by the Interreg V-A España-Portugal (POCTEP) 2014-2020 program.

References

[1] A. Ahmed, E. Ahmed, A survey on mobile edge computing, *10th International Conference on Intelligent Systems and Control-ISCO* (2016), 1–8. doi:10.1109/ISCO.2016.7727082.

[2] M.T. Beck, M. Werner, S. Feld, T. Schimper, *Mobile Edge Computing: A Taxonomy*, Citeseer, 2014, Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.670.9418.

[3] R.S. Ransing, M. Rajput, Smart home for elderly care, based on Wireless Sensor Network, *International Conference on Nascent Technologies in the Engineering Field - ICNTE* (2015).

[4] W. Kinsner, Towards cognitive security systems, *IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing* (2012), 539–539. doi:10.1109/ICCI-CC.2012.6311207.

[5] R. Greenstadt, J. Beal, Cognitive Security for Personal Devices, *Proceedings of the 1st ACM Workshop on Workshop on AISec, New York, NY, USA*, 2008. doi:10.1145/1456377.1456383 : 27–30.

[6] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos and D. Boyle, *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*, Academic Press, 2014.

[7] *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)*, European Union, 2014, 44–59.

[8] S. Asano, T. Yashiro, K. Sakamura, Device collaboration framework in IoT-aggregator for realizing smart environment, *TRON Symposium (TRONSHOW)* (2016). 1–9. doi:10.1109/TRONSHOW.2016.7842886.

[9] M. Alirezaie, J. Renoux, U. Köckemann, A. Kristoffersson, L. Karlsson, E. Blomqvist, N. Tsiftes, T. Voigt, A. Loutfi, An Ontology-based Context-aware System for Smart Homes: E-care@home, *Sensors* **17** (7) (2017),doi:10.3390/s17071586.

[10] M.I. Pramanik, R.Y.K. Lau, H. Demirkan, M.A.K. Azad, Smart Health: Big Data Enabled Health Paradigm within Smart Cities, *Expert Syst Appl.* Elsevier, 2017. Available: http://www.sciencedirect.com/science/article/pii/S095741741730444X.

[11] T.C. Clancy, N. Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, doi:10.1109/CROWNCOM.2008.4562534:1–8.

[12] A. Attar, H. Tang, A.V. Vasilakos, F.R. Yu, V.C.M. Leung, A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions. *Proc. IEEE* (2012), doi:10.1109/JPROC.2012.2208211: 3172–3186.

[13] A.G. Fragkiadakis, E.Z. Tragos, A survey on security threats and detection techniques in cognitive radio networks, *IEEE Communications Surveys & Tutorials* (2013).

[14] M. Gupta, *Blockchain for Dummies*, John Wiley & Sons, Inc Burchfield CA, 1995.

[15] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos, D. Boyle, *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Academic Press, 2014.

[16] *hyperledger/iroha*, In: GitHub [Internet], [cited 29 Aug 2017], available: https://github.com/hyperledger/iroha.

[17] D. Ichikawa, M. Kashiyama, T. Ueno, Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR mHealth and uHealth* **5** (2017), doi:10.2196/mhealth.7938.

[18] O. Jacobovitz, *Blockchain for Identity Management*, 2016. Available: https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf.

[19] C. Cachi, Architecture of the Hyperledger blockchain fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers* (2016), available: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

[20] M. Mainelli, M. Smith, Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology), *The Journal of Financial Perspectives* **3** (3) (2015), 38-58.

[21] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* (2016), doi:10.1109/ACCESS.2016.2566339: 2292–2303.

[22] H, Kakavand, N. Kost De Sevres, B. Chilton, *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*, 2017. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251.

[23] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. *International Symposium on Cluster, Cloud and Grid Computing, IEEE/ACM*, 2017.

[24] F. Jordan, H. Pujol, D. Ruana, Achieving the eIDAS Vision Through the Mobile, Social and Cloud Triad. *ISSE 2014 Securing Electronic Business Processe*s, Springer Vieweg, Wiesbaden, 2014. doi:10.1007/978-3-658-06708-3_6: 81–93.

[25] F. Morgner, P. Bastian, M. Fischlin, Securing Transactions with the eIDAS Protocols, *Information Security Theory and Practice*, Springer, 2016. doi:10.1007/978-3-319-45931-8_1: 3–18.

[26] S. Jain, A. Kajal, Effective Analysis Of Risks And Vulnerabilities In Internet Of Things, *International Journal of Computing and Corporate Research,* 2015. Available: http://www.ijccr.com/March2015/4.pdf.

[27] NASDAQ, *Distributed. Byzantine Fault Tolerance: The Key for Blockchains.* In: NASDAQ.com [Internet], NASDAQ, 29 Jun 2017 [cited 29 Aug 2017], available: http://www.nasdaq.com/article/byzantine-fault-tolerance-the-key-for-blockchains-cm810058.

[28] A. Ouaddah, H. Mousannif, A. Abou Elkalam, A. Ait Ouahman, Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks: The International Journal of Computer and telecommunications Networking* **112** (2017), 237-262, doi:10.1016/j.comnet.2016.11.007: 237–262