SPAINChain: Security, Privacy, and Ambient Intelligence in Negotiation Between IOT and Blockchain

Mohamed A. El-dosuky[1](✉) and Gamal H. Eladl[2]

[1] Computer Sciences Department, Faculty of Computer and Information,
Mansoura University, P.O 35516, Mansoura, Egypt
mouh_sal_010@mans.edu.eg

[2] Information Systems Department, Faculty of Computer and Information,
Mansoura University, P.O 35516, Mansoura, Egypt
gamalhelmy@mans.edu.eg

Abstract. Vulnerability in Internet-of-Things (IoT) necessitates the existence of a safeguard for both security and privacy without sacrificing "smartness" of the environment, or its Ambient Intelligence in scientific terms. Blockchains, underpinning crypto-currency, could be the remedy for this vulnerability. This paper quickly overviews security, privacy, Ambient Intelligence, and the use of Blockchain as a safeguard for IOT, before proposing and evaluating SPAINChain:Security, Privacy, and Ambient Intelligence in Negotiation between IOT and Blockchain. IOT-Blockchain mapping is proven to be feasible. The gamut of blockchain is based on a new concept called solidus. Solidus is basically the sum of blockchain favorability dimensions, adjusted by preference of blockchain type.

Keywords: Security · Privacy · Ambient Intelligence · IOT · Blockchain

1 Introduction

The home sweet home is a smart one indeed. Environment "smartness", or Ambient Intelligence [1] in scientific terms, comes at the cost of vulnerability due to:

- security attacks [2], and
- manipulation of privacy-sensitive data [3].

This vulnerability in Internet-of-Things (IoT) necessitates the existence of a safeguard for both security and privacy without sacrificing "smartness" of the environment [4].

Blockchains, underpinning crypto-currency [5], could be the remedy for this vulnerability.

This paper quickly overviews security, privacy, Ambient Intelligence, and the use of Blockchain as a safeguard for IOT (in Sect. 2), before proposing, evaluating and concluding SPAINChain:Security, Privacy, and Ambient Intelligence in Negotiation between IOT and Blockchain in subsequent sections.

Á. Rocha et al. (Eds.): WorldCIST'19 2019, AISC 930, pp. 415–425, 2019.
https://doi.org/10.1007/978-3-030-16181-1_39

2 Previous Work

This section quickly overviews security, privacy, Ambient Intelligence, and the use of Blockchain as a safeguard for IOT.

2.1 Security

Security is modeled based on CIA model which is an amalgamation of Confidentiality, Integrity, and Availability [6]. The former ensures that solely authorized users have access. Integrity ensures that data is received as sent, without modification, The latter ensures data availability when needed.

Non-bespoke IOT devices usually lack a safeguard for security, that they can be easily hacked [7]. Smart home vulnerability is inevitable, even with the existence of gateways controlling packets exchange to and fro [8] Object security, as implemented in OSCAR architecture [9], is powerful that IoT researchers commence utilizing it as in [10].

Cryptography seems to be a key ingredient in many confidentiality solutions [11]. Recently, a clever Variable Key-length cryptography (VKLC) solution is proposed based on the motto, "A valuable thing needs higher security" [12]. It constructs a dynamic model for the estimated economic value of data, and enforces the appropriate security accordingly. The more"valuable" the data, the bigger the cryptography key length.

Bitcoin, or blockchain v.1, introduces Proof-of-Work (POW) cryptographic puzzles [5]. Not only a blockchain ensures transparency, but also it can be an integrity-assurance ingredient [13].

2.2 Privacy

Access control, usually implemented as an access matrix of privileges [14], is not enough to reaching the holy-grail of privacy [15]. Preserving IOT privacy raises many challenges [16]. Blockchains are at the rescue to provide a decentralized access [17], and credibility verification [18]. A middleware is proposed between sender and receiver to control access [3]. IGOR is recently proposed [19] and augmented to provide a unified IOT access control [20].

2.3 Ambient Intelligence

There is a plethora of smart home projects, leveraging Ambient Intelligence [21]. Implementation usually takes the form of a context-aware middleware as shown in Fig. 1.

The cycle is self-describing. Usually a context is related to energy consumption, and this paper shall stick to that.

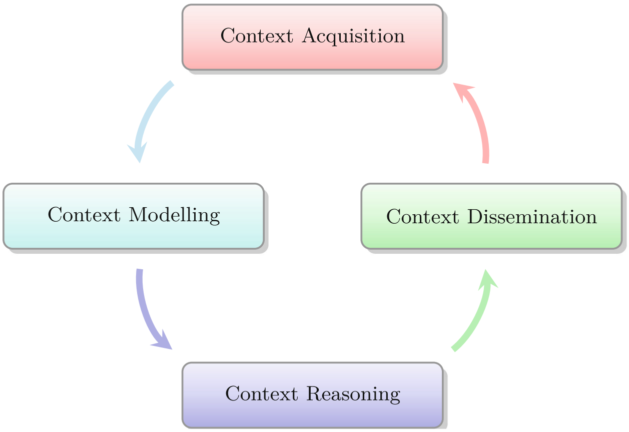

Fig. 1. Middleware context life-cycle [21]

2.4 Blockchain-IOT Integration

For a detailed survey of possible blockchain-IOT integration scenarios, kindly refer to [22]. Integration involves inevitable challenges [23] such as scalability and latency. Blockchain Platforms are meticulously analyzed for IoT [24]. Based on that analysis favorable platforms (Table 1, showing ranking of Security, Scalability, Suitability for smart contract on a scale of 1 to 5) and selection criteria (Fig. 2) are determined.

3 Proposed System

Let us first set the mathematical foundation of IOT-Blockchain Mapping.

Theorem 1 (IOT-Blockchain Mapping)

$$\lambda_B \leftarrow \frac{\delta_B(\varepsilon_T - \lambda_T)}{\varepsilon_T} + \xi_B \tag{1}$$

where λ_B is blockchain feature, usually platform rank, in interval $[\xi_B, \xi_B + \delta_B]$. ξ_B is the minimum and is not necessarily a zero, allowing negative values. $\xi_B + \delta_B$ is the maximum. Hence, δ_B is the range. λ_T is IOT feature, usually energy consumption, in interval $[0, \varepsilon_T]$. Clearly, ε_T is the maximum. □

Proof

$$0 \leq \lambda_T \leq \varepsilon_T \tag{2}$$

$$0 \geq -\lambda_T \geq -\varepsilon_T \tag{3}$$

$$\varepsilon_T \geq \varepsilon_T - \lambda_T \geq 0 \tag{4}$$

$$1 \geq \frac{\varepsilon_T - \lambda_T}{\varepsilon_T} \geq 0 \tag{5}$$

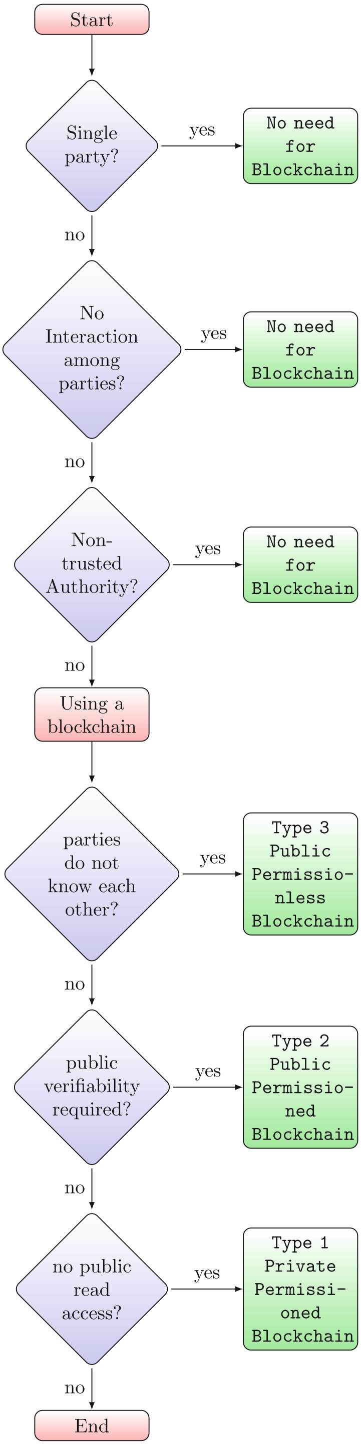
Start
Single party?
yes
No need for Blockchain
no
No Interaction among parties?
yes
No need for Blockchain
no
Non-trusted Authority?
yes
No need for Blockchain
no
Using a blockchain
parties do not know each other?
yes
Type 3 Public Permissionless Blockchain
no
public verifiability required?
yes
Type 2 Public Permissioned Blockchain
no
no public read access?
yes
Type 1 Private Permissioned Blockchain
no
End

Fig. 2. Blockchain platform selection [24]

Table 1. Blockchain platform favorability [24]

Blockchain	(Security, scalability, smart contract)
Bitcoin (Type 3)	(3, 1, 1)
Ethereum (Type 3)	(3, 3, 4)
Hyperledger (Type 2)	(4, 4, 4)
Ripple (Type 2)	(4, 4, 4)
Multichain (Type 1)	(4, 4, 1)
Eris (Type 1)	(4, 3, 4)

$$0 \leq \frac{\varepsilon_T - \lambda_T}{\varepsilon_T} \leq 1 \tag{6}$$

$$0 \leq \frac{\delta_B(\varepsilon_T - \lambda_T)}{\varepsilon_T} \leq \delta_B \tag{7}$$

$$\xi_B \leq \frac{\delta_B(\varepsilon_T - \lambda_T)}{\varepsilon_T} + \xi_B \leq \xi_B + \delta_B \tag{8}$$

Note that the middle expression:

$$\frac{\delta_B(\varepsilon_T - \lambda_T)}{\varepsilon_T} + \xi_B \tag{9}$$

is a blockchain feature in interval $[\xi_B, \xi_B + \delta_B]$. Denoting it λ_B,

$$\lambda_B \leftarrow \frac{\delta_B(\varepsilon_T - \lambda_T)}{\varepsilon_T} + \xi_B \tag{10}$$

□

Based on this mapping theorem, it is possible to seek the optimal blockchain-IOT pairing as in Fig. 3, in which device T (seeking context C) is paired with blockchain B (with configuration suitable for the same context C). Hence, shifting from access matrix to a dichotomy of B matrix and T matrix. The former determines the context for each blockchain (Table 1 and Fig. 2 help in constructing such a matrix), and the latter determines the context for each IOT device (It could be dynamically constructed, utilizing cycle shown in Fig. 1). Context elicitation and blockchain matching are depicted in Fig. 4. Now the time is ripe

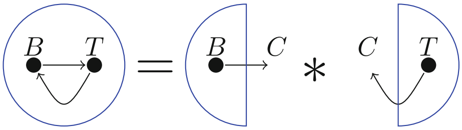

Fig. 3. Blockchain-IOT pairing

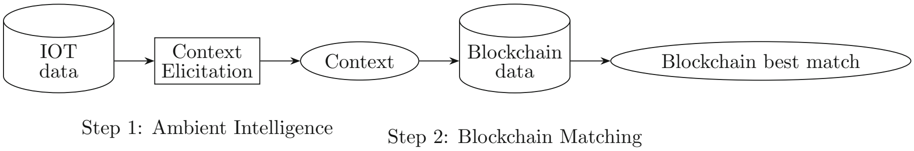

Fig. 4. Context elicitation and blockchain matching

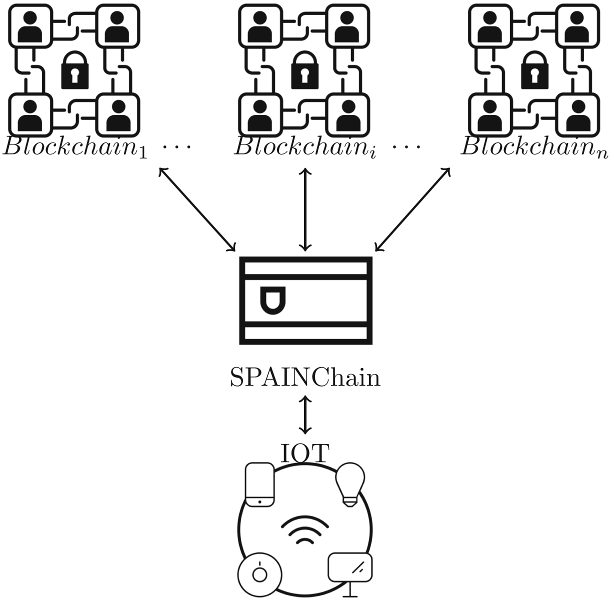

Fig. 5. Conceptual model of SPAINChain

to propose SPAINChain conceptual model (Fig. 5), implemented as a set of layers (Fig. 6). SPAINChain elects the best blockchain to safeguard a specific IOT device in a certain context.

SPAINChain is decomposed of $4 + 1$ layers. The lowest layer, L_0, is the basic blockchain scanner. The top layer, L_4, is for interaction with entities outside SPAINChain. It integrates IGOR ([19] for authentication and access control, striving for privacy), an updated ontology of IOT devices, an updated ontology of available Blockchains, Data Importer, and Data Exporter. L_3 is for user convenience. It integrates an updated Users' list, Context Aquisitioner, Preprocessor, and Visualizer. The layer beneath, L_2, is for maintaining ambient intelligence. It integrates an updated ontology of Contexts, Context Modeler, and Context Disseminator. L_1 integrates the core Negotiator, Context Reasoner, OSCAR ([9] for security), and VKLC ([12], determining sufficient degree of security based on context).

4 Case Study and Evaluation

Assume an arbitrary smart home shown in Fig. 7. The gamuts of blockchains and devices are shown in Figs. 8, 9 respectively.

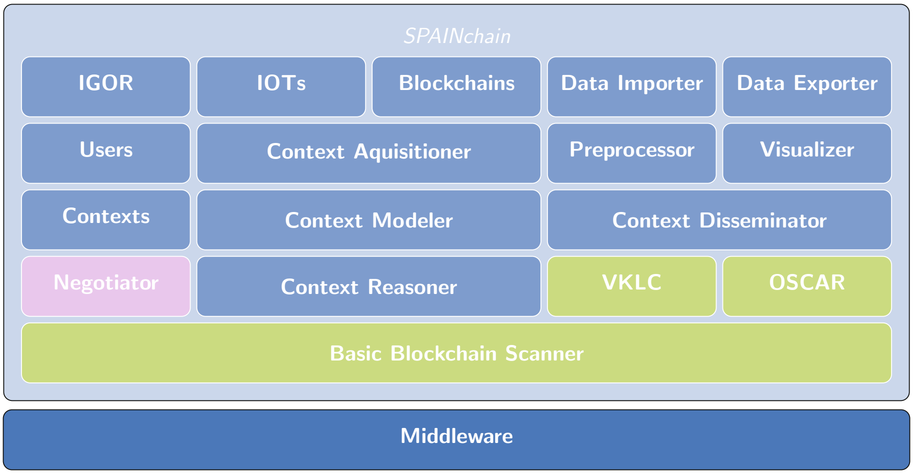

Fig. 6. SPAINChain layers

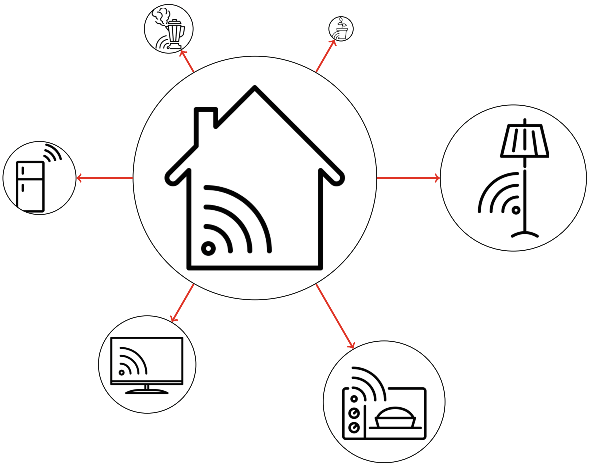

Fig. 7. Arbitrary smart home

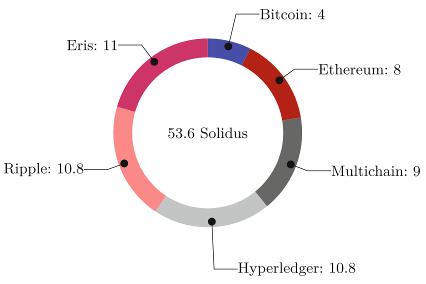

Fig. 8. Blockchain gamut

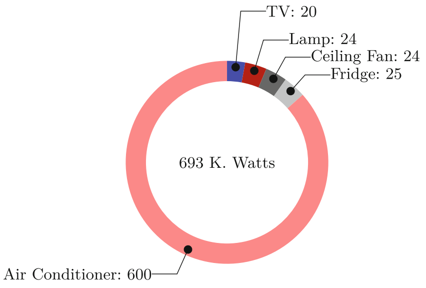

Fig. 9. Device gamut

The gamut of devices is based on monthly energy consumption, as estimated by Electric Regulatory Agency in Egypt [25].

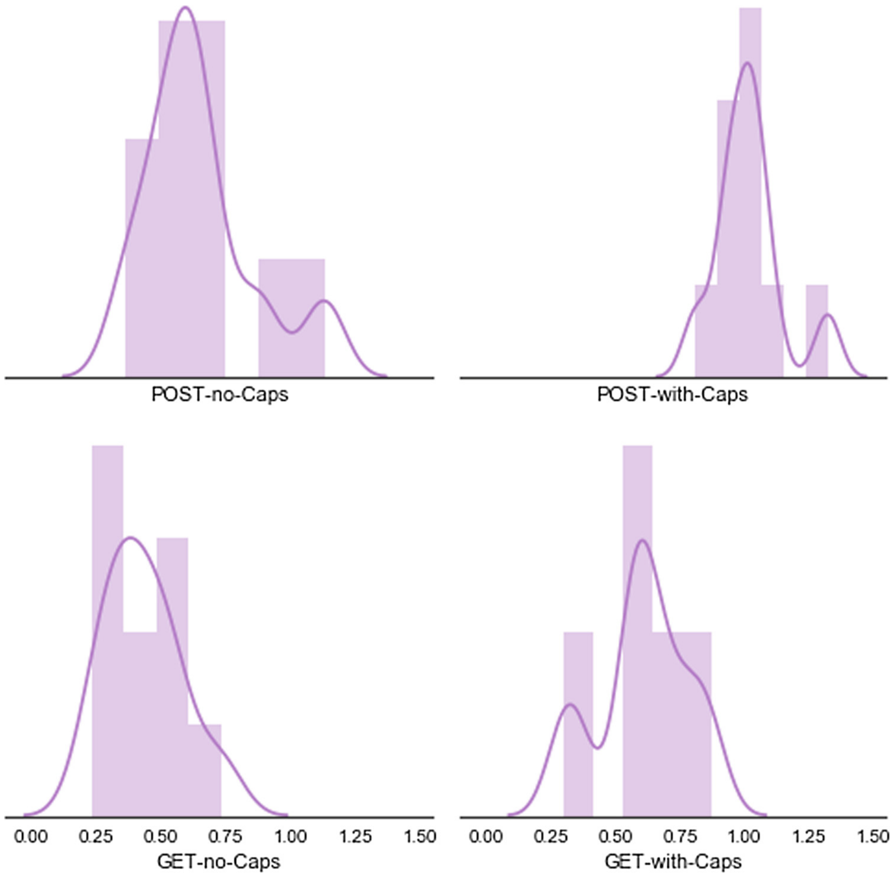

Fig. 10. Mean time overheads

The gamut of blockchain is based on a new concept called solidus. Solidus is basically the sum of favorability dimensions shown in Table 1, adjusted by preference of blockchain type, as follows.

$$Solidus(B) = (1 - \gamma * (B_{Type} - 1)) * \sum_{dim \in FavDims} B^{dim} \tag{11}$$

where γ is a degradation factor, set to 0.1. For Eris with $B_{Type} = 1$ and favorability (4, 3, 4), Solidus(Eris) = 11.

Distribution of mean time overheads either with or without capabilities are shown in Fig. 10. Overheads are bearable. The key merit here is the dynamic determination of sufficient degree of IOT privacy and security based on context. This allows for a dynamic overhead compared to fixed blockchain-based overhead solutions such as [26].

5 Conclusion and Future Work

IOT-Blockchain mapping is proven to be feasible. Based on this mapping theorem, it is possible to seek the optimal blockchain-IOT pairing, in which device T (seeking context C) is paired with blockchain B (with configuration suitable for the same context C). Hence, shifting from access matrix to a dichotomy of B matrix and T matrix. The former determines the context for each blockchain, and the latter determines the context for each IOT device. The gamut of devices is based on monthly energy consumption, while the gamut of blockchain is based on a new concept called solidus. Solidus is basically the sum of favorability dimensions, adjusted by preference of blockchain type.

Then came SPAINChain, decomposed of $4+1$ layers. The lowest layer,L_0, is the basic blockchain scanner. The top layer, L_4, is for interaction with entities outside SPAINChain. It integrates IGOR [19], devices, Blockchains, Data Importer, and Data Exporter. L_3 is for user convenience. The layer beneath,L_2, is for maintaining ambient intelligence. L_1 integrates the core Negotiator, Context Reasoner, OSCAR [9], and VKLC [12].

SPAINChain attempts to determine sufficient degree of IOT privacy and security based on context, by allowing an automatic negotiation between IOT and blockchains.

Future direction shall consider producing SPAINChain based on the proof-of-concept provided in this paper.

References

1. Ramos, C., Augusto, J.C., Shapiro, D.: Ambient intelligence-the next step for artificial intelligence. IEEE Intell. Syst. **23**(2), 15–18 (2008)
2. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in internet of things. Comput. Netw. **76**, 146–164 (2015)

3. Chakravorty, A., Wlodarczyk, T., Rong, C.: Privacy preserving data analytics for smart homes. In: IEEE 2013 Security and Privacy Workshops (SPW), pp. 23–27. IEEE (2013)
4. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
5. King, S.: Primecoin: cryptocurrency with prime number proof-of-work, 7 July 2013
6. Komninos, N., Philippou, E., Pitsillides, A.: Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun. Surv. Tutor. **16**(4), 1933–1954 (2014)
7. Notra, S., Siddiqi, M., Gharakheili, H.H., Sivaraman, V., Boreli, R.: An experimental study of security and privacy risks with emerging household appliances. In: 2014 IEEE Conference on Communications and Network Security (CNS), pp. 79–84. IEEE (2014)
8. Sivaraman, V., Chan, D., Earl, D., Boreli, R.: Smart-phones attacking smart-homes. In: Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 195–200. ACM (2016)
9. Vučini ć, M., et al.: OSCAR: object security architecture for the Internet of Things. Ad Hoc Netw. **32**, 3–16 (2015)
10. Alphand, O., et al.: IoTChain: a blockchain security architecture for the Internet of Things. In: 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6. IEEE (2018)
11. Delfs, H., Knebl, H.: Introduction to Cryptography, vol. 2. Springer, Heidelberg (2002)
12. Khorsheed, N.K., et al.: Management of data security based on data cost evaluation. J. Comput. Theor. Nanosci. **14**(10), 4964–4969 (2017)
13. Weizhi, M.E.N.G., et al.: When intrusion detection meets blockchain technology: a review. IEEE Access **6**, 10179–10188 (2018)
14. Sandhu, R.S., Samarati, P.: Access control, principle and practice. IEEE Commun. Mag. **32**(9), 40–48 (1994)
15. Colombo, P., Ferrari, E.: Privacy aware access control for Big Data, a research roadmap. Big Data Res. **2**(4), 145–154 (2015)
16. Ziegeldorf, J.H., Morchon, O.G., Wehrle, K.: Privacy in the Internet of Things, threats and challenges. Secur. Commun. Netw. **7**(12), 2728–2742 (2014)
17. Ali, M.S., Dolui, K., Antonelli, F.: IoT data privacy via blockchains and IPFS. In: Proceedings of the Seventh International Conference on the Internet of Things, p. 14. ACM (2017)
18. Qu, C., et al.: Blockchain based credibility verification method for IoT entities. Secur. Commun. Netw. (2018)
19. Pemberton, S.: An architecture for unified access to the internet of things. In: XML London 2017 Conference Proceedings, vol. 1, pp. 38–42 (2017)
20. Shieng, P.S.W., Jansen, J., Pemberton, S.: Fine-grained access control framework for igor, a unified access solution to the internet of things. Procedia Comput. Sci. **134**, 385–392 (2018)
21. Che-Bin, F., Hang-See, O.: Research article. A review on smart home based on ambient intelligence, contextual awareness and Internet of Things (IoT). In: Constructing Thermally Comfortable and Energy Aware House (2016)
22. Panarello, A., et al.: Blockchain and IoT integration, a systematic survey. Sensors **18**(8), 2575 (2018)
23. Dorri, A., Kanhere, S. S., Jurdak, R.: Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187 (2016)

24. Pahl, C., El Ioini, N., Helmer, S.: A decision framework for blockchain platforms for IoT and edge computing. In: International Conference on Internet of Things, Big Data and Security (2018)
25. Egyptian Electric Utility and Consumer Protection Regulatory Agency (EgyptERA). http://egyptera.org/ar/. Accessed 1 Oct 2018
26. Dorri, A., et al: Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623. IEEE (2017)