Blockchain-based solutions for privacy in Internet of Things smart environment

Author: Shubhankar Darbari (S.Darbari@student.tudelflt.nl) | Supervisors: Dr. Z. Erkin & M. Ayşen | CSE3000 | Delft University of Technology

Delft University of Technology

1. Introduction

- The use of the **Internet of Things** (IoT) has increased significantly over the years.
- Personal data and information are often stored, mishandled, and misused, posing a threat to user data *privacy.*
- State of the art technology uses a centralized approach. Is decentralization the solution?

2. Privacy in Smart Home System

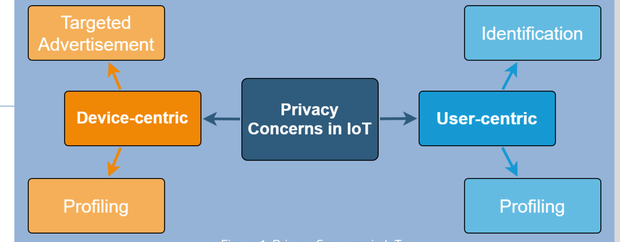

Figure 1: Privacy Concerns in IoT

3. Decentralizing IoT

"How can Blockchain-based IoT serve as a viable solution to the user and device-centric privacy along with the hardware-based limitations of IoT devices?"

- Blockchain is an immutable shared ledger with features that can be essential to solving challenges faced by IoT devices [15].
- Defining the privacy requirements in IoT.
- Investigation to the extent to which privacy can be enhanced in a smart home system.

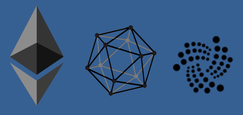

Figure 2: Ethereum, Hyperledger, and IOTA

4. Methodology

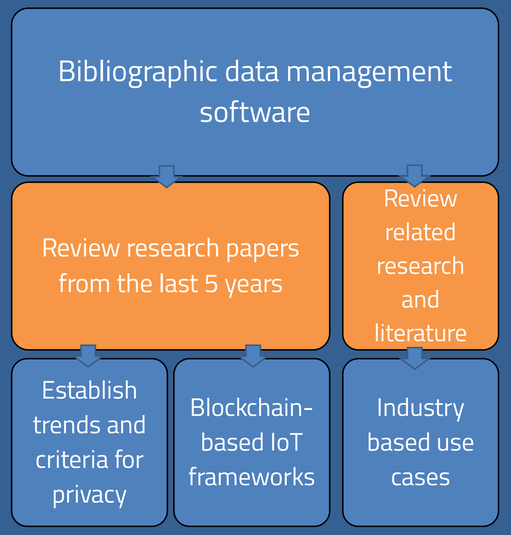

Figure 3: Methodology

5. Results [1-14]

Table 1: Comparison of the aforementioned mechanisms

Privacy mechanism	Proposed solution/platform(s)	Feature(s)	Risk(s)
One-time address	[1], Ethereum [2]	• User Anonymity • Untraceable data	• Computational burden • Unencrypted data
Mixing technique	[3], IOTA [4]	• Untraceable data	• Increased complexity • Low anonymity
Ring signature	[5]	• User Anonymity • Untraceable data • Encrypted data	• Signature reuse • Address correlation
Homomorphic encryption	[6], Ethereum [2]	• User Anonymity • Untraceable data • Encrypted data	• Computational burden
Zero-knowledge proof	[7], Ethereum [2], Fabric [8]	• User Anonymity • Untraceable data • Encrypted data	• Data misrouting • Computational burden
Differential privacy	[9]	• Lightweight • Confidential data	• Trade-off b/w privacy & accuracy
Off-chain mechanism	[10], [11], IOTA [4], Fabric [8]	• User Anonymity	• Linkable data • Traffic correlation
Partner matching	[12]	• User Anonymity • Confidential data	• Address correlation
Secret sharing	[13]	• User Anonymity • Confidential data	• High memory usage • Computational burden
Editable blockchain	[14]	• Blockchain features • Right to be forgotten	• Still in development

- Privacy mechanisms in addition to the anonymity of blockchain.
- Mechanisms can be categorized into three types based on their functionalities.
- *Data manipulation* solutions provide an effective utility solution.

5. Conclusions & Future work

- Blockchain can enhance privacy in an IoT environment along with additional advantages.
- Combing data manipulation solutions is an effective solution. For example, Monero.
- Future work
  - Differential privacy.
  - Ring signature scheme for smart homes.
  - Quantitative vs Qualitative data.
  - Moving towards efficient solutions/devices.

6. References

[1] X. Fan, "Faster dual-key stealth address for blockchain-based internet of things systems," 2018.
[2] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis,and S. Shiaeles, "On the suitability of blockchain platforms for iot applications: Architectures, security, privacy, and performance,"
Computer Networks, vol. 191, p. 108005, 2021.
[3] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coin-shuffle: Practical decentralized coin mixing for bitcoin,"in Computer Security - ESORICS 2014 (M. Kutyłowski and J. Vaidya, eds.), (Cham), pp. 345–364, Springer International Publishing, 2014.
[4] I. Foundation, "Introducing masked authenticated messaging," Dec 2020.
[5] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," Sensors, vol. 19, no. 2, p. 326, 2019.
[6] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, and W. Liu, "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving," IEEE Access, vol. 7, p. 62058–62070, 2019.
[7] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza,
"Zerocash: Decentralized anonymous payments from bitcoin," in 2014 IEEE Symposium on Security and Privacy, pp. 459–474, 2014.
[8] "Private and confidential transactions with hyperledger fabric."
[9] M. Ul Hassan, M. H. Rehmani, and J. Chen, "Differential privacy in blockchain technology: A futuristic approach," Journal of Parallel and Distributed Computing, vol. 145, p. 50–74, 2020.
[10] S. Zhao, B. Wang, Y. Li, and Y. Li, "Integrated energy transaction mechanisms based on blockchain technology," Energies, vol. 11, no. 9, p. 2412, 2018.
[11] I. Kotsiuba, A. Velivkzhanin, Y. Yanovich, I. S. Bandurova, Y. Dyachenko, and V. Zhygulin, "Decentralized e-health architecture for boosting healthcare analytics," In 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp. 113–118, 2018.
[12] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," Ad Hoc Networks, vol. 90, p. 101730, 2019.
[13] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, p. 11676–11686, 2018.
[14] D. Grigoriev and V. Shpilrain, "Rsa and redactable blockchains," 2020.
[15] Y. Yu, Y. Li, J. Tian, and J. Liu. "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things", IEEE Wireless Communications, vol. 25, no. 6, pp. 12–18, 2018.