Open PhD position in IoT data integrity

As IoT device deployment increases for smart homes, smart cities, and industrial settings, data integrity and the security of IoT deployment becomes more and more important. Often intelligence at the edge or in the cloud determines how to act upon such data feeds. Erroneous data may lead to taking the wrong decisions such as stopping a production line if jamming indicators are falsely transmitted. Such falsified data may be the result of an IoT device infection or the impersonation of such devices.

Traditional centralized architectures struggle to cope with the sheer amount of data and the need for real-time verification. Blockchain approaches are proposed to remove the need to rely on Third Party Auditors[1]. Blockchain technology provides a secure, decentralized and transparent framework [2, 3] for data authentication that can address the evolving needs of IoT environments. The nature of IoT devices demands a scalable and efficient solution to ensure trust and reliability. However, blockchains still struggles with scalability. There are approaches that improve scalability through distribution of the transactions and/or state, like sharding [4, 5]. Other approaches, such as Non-interactive proofs of Proof-of-Work (NIPoPoWs) [6] aim to reduce storage and communication complexity.

This thesis aims at proposing scalable and secure solutions for the real-time verification of large amounts of IoT generated data while enforcing data privacy. The thesis will consider sharding [4, 5], relying on proof-of-interactions [7] and Non-interactive proofs of Proof-of-Work (NIPoPoWs) [6] as building blocks for the online data verification. We will also consider alternative data structures [8, 9]. While significant contributions have been done to reduce the load on the blockchain, there is little support for the interaction of IoT objects with blockchain solutions. A key aspect of the thesis will be to consider the objects and their edge as an integral part of the solution to provide end-to-end security of IoT deployments. The proposed solutions in the thesis will be tested on real smart building deployments.

Work environment

The thesis will take place at the University of Strasbourg, in the Networking research team[1], in the ICube laboratory. Created in 2013, ICube is a multidisciplinary research laboratory of 17 teams which gathers researchers from

[1] https://reseaux.icube.unistra.fr/index.php/Accueil

the university of Strasbourg, the French National Center for Scientific Research (CNRS), ENGEES and also INSA of Strasbourg. The networking team has a long experience in IoT research and contributions to scalable blockchain approaches. The team hosts and operates the FIT Iot-Lab testbed in Strasbourg [10][2], the LRP-IoT testbed [3] (a city scale LoRaWAN deployment) and iBat (a smart building testbed)[4], which will be used for this research.

The PhD supervision team is composed of Loïc Miller (IMT Atlantique) Anissa Lamani (U. Strasbourg), Pascal Mérindol (U. Strasbourg) and Cristel Pelsser (UCLouvain and U. Strasbourg).

Expected background and skills

The candidate possesses a master in computer science with a solid background in computer networking. A combination of technical, theoretical, and practical skills are required from the applicants, namely:

- The interdisciplinary nature of this field requires that the applicant is able to quickly deepen their knowledge in the areas of IoT, security and blockchain to be able to tackle complex challenges in these areas.
- Proficiency in conducting literature reviews, strong critical thinking skills for identifying research problems, formulating, ability to design and execute experiments, collect data, and analyze results.
- Strong foundation in mathematics and statistics.
- Solid programming skills.
- Proven proficiency in English (reading, writing and speaking).

Contact

Interested candidates can apply by sending a detailed CV to the following address: iotdata-thesis@icube.unistra.fr

References

[1] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for iot data," in *2017 IEEE International Conference on Web Services (ICWS)*, 2017, pp. 468–475.

[2] https://www.iot-lab.info

[3] https://inetlab.icube.unistra.fr/index.php/LRP_IoT

[4] https://inetlab.icube.unistra.fr/index.php/IBat

[2] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: Analysis and applications,” in *Annual international conference on the theory and applications of cryptographic techniques.* Springer, 2015, pp. 281–310.

[3] ——, “The bitcoin backbone protocol with chains of variable difficulty,” in *Annual International Cryptology Conference.* Springer, 2017, pp. 291–323.

[4] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 17–30.

[5] Y. Li, J. Wang, and H. Zhang, “A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces,” *Journal of Network and Computer Applications*, p. 103686, 2023.

[6] A. Kiayias, N. Leonardos, and D. Zindros, “Mining in logarithmic space,” in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS).* New York, NY, USA: Association for Computing Machinery, 2021, p. 3487–3501. [Online]. Available: https://doi.org/10.1145/3460120.3484784

[7] J.-P. Abegg, Q. Bramas, and T. Noël, “Blockchain using proof-of-interaction,” in *Networked Systems: 9th International Conference, NETYS 2021, Virtual Event, May 19–21, 2021, Proceedings.* Springer, 2021, pp. 129–143.

[8] E. Anceaume, A. Guellier, R. Ludinard, and B. Sericola, “Sycomore: A permissionless distributed ledger that self-adapts to transactions demand,” in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA).* IEEE, 2018, pp. 1–8.

[9] A. Djari, E. Anceaume, and S. Tucci-Piergiovanni, “Sycomore++, un registre distribué orienté graphe auto-adaptatif,” in *AlgoTel 2022-24èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, 2022, pp. 1–4.

[10] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele, and T. Watteyne, “Fit iot-lab: A large scale open experimental iot testbed,” in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 459–464.