


Eventually Consistent Access Control: Thinking in Two Orders


Florian Jacob ¹

Abstract: In terms of access control, we are used think in the conventional model of a single, append-only total order of all actions as basis for authorization decisions, formed by a trusted central entity or by consensus of a set of distributed entities. However, this model inherently limits availability and Byzantine fault tolerance: entities depend on coordination with other entities to ensure safety and liveness of authorization decisions. Systems that cannot afford dependencies among entities, like conflict-free replicated data types (CRDTs, [Al24]), must break with the conventional model, but gain fundamental advantages in availability and Byzantine fault tolerance. In line with eventually consistent replication in CRDTs, we define “eventually consistent access control” as an alternative conceptual model that does not depend on coordination with others, and present its consequences. Our model postulates thinking in two orders of access control actions: a partial order for storage, where the past of an action is final, and a total order for execution, where the past of an action is grow-only.

Coordination takes time, and results in dependencies to other entities. Therefore, system designers often strive to make time-critical actions independent of the latency to other entities. Coordination-avoiding [Ba14] or wait-free [He91] systems follow this design principle, which can be said to follow the famous quote “It’s easier to ask forgiveness than it is to get permission.”, popularized by Grace Hopper [Ha86; OT18]. In the realm of data consistency, this limits achievable consistency to models like eventual consistency [Al24], but enables to tolerate an arbitrary number of Byzantine-faulty Sybill entities taking part in the system [Kl22]. But what does this principle mean for access control?

In context, Hopper’s quote is specifically on reducing coordination and latency of (organizational) access control decisions: she advised the interviewer to act now, to their best of knowledge and belief, and to reconcile later, instead of coordinating on and waiting for an up-front authorization decision. Access control found in group communication and collaboration systems based on Byzantine-tolerant CRDTs [Kl22], like Matrix [Th23] or Beehive [GMZ24], follows this idea. While Beehive is still a research project, access control in Matrix has grown to be a security-critical topic: Matrix deployments gained significant traction in the public sector, e.g., the United Nations International Computing Center has switched to Matrix as communication platform provided to UN organizations [Lo24], and in Germany, the German public sector has the “BundesMessenger” [BW24], and German healthcare standardized the “TI-Messenger” [ge24].

At the example of Matrix, we present our work on understanding and formalizing the conceptual model we called eventually consistent access control [Ja21; JH24]. In our model, entities replicate all access control actions in storage order, i.e., a partial, append-only order

¹ Karlsruhe Institute of Technology, Decentralized Systems and Network Services, Karlsruhe, Germany, florian.jacob@kit.edu,  <https://orcid.org/0000-0002-5739-8852>

where the immutability of an action’s past ensures an immutable authorization decision, and thereby eventual consistency. Then, entities derive the execution order of actions by performing topological sorting. While the execution order is total and grow-only, it is not append-only: new actions can appear at any point in the order. Our core finding is that eventually consistent access control implies authorization to the best of knowledge and belief: an entity *stores* an action only if the action is authorized by *immutable knowledge* derived from its *append-only partial* order of actions, and *executes* an action only if it is also authorized by the entity’s *mutable beliefs* derived from the *grow-only total* order of actions.

References

- [Al24] Almeida, P. S.: Approaches to Conflict-free Replicated Data Types. *ACM Comput. Surv.* 57 (2), 51:1–51:36, 2024, ISSN: 0360-0300, DOI: 10.1145/3695249, URL: <https://dl.acm.org/doi/10.1145/3695249>, visited on: 12/12/2024.
- [Ba14] Bailis, P.; Fekete, A.; Franklin, M. J.; Ghodsi, A.; Hellerstein, J. M.; Stoica, I.: Coordination Avoidance in Database Systems. *Proceedings of the VLDB Endowment* 8 (3), pp. 185–196, 2014, ISSN: 2150-8097, DOI: 10.14778/2735508.2735509.
- [BW24] BWI: IT Für Deutschland: BundesMessenger: Souveränität und Sicherheit und Freiheit. Freier Messenger für die öffentliche Hand. 2024, URL: <https://messenger.bwi.de/bundesmessenger>.
- [ge24] gematik: TI-Messenger: Schnelle und sichere Echtzeit-Kommunikation auch im Gesundheitswesen, 2024, URL: <https://www.gematik.de/anwendungen/ti-messenger>.
- [GMZ24] Good, A.; Mumm, J.; Zelenka, B.: Beehive: Local-first Access Control, 2024, URL: <https://www.inkandswitch.com/beehive/>.
- [Ha86] Hamblen, D.: Only the Limits of Our Imagination: An exclusive interview with RADM Grace M. Hopper. *Chips Magazine*, 1986, URL: https://web.archive.org/web/20090114165606/http://www.chips.navy.mil/archives/86_jul/interview.html.
- [He91] Herlihy, M.: Wait-free synchronization. *ACM Trans. Program. Lang. Syst.* 13 (1), pp. 124–149, 1991, ISSN: 0164-0925, DOI: 10.1145/114005.102808, URL: <https://doi.org/10.1145/114005.102808>.
- [Ja21] Jacob, F.; Beer, C.; Henze, N.; Hartenstein, H.: Analysis of the Matrix Event Graph Replicated Data Type. *IEEE Access* 9, pp. 28317–28333, 2021, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2021.3058576.
- [JH24] Jacob, F.; Hartenstein, H.: To the Best of Knowledge and Belief: On Eventually Consistent Access Control, tech. rep., 2024, 13 pp., DOI: 10.5445/IR/1000176494.
- [Kl22] Kleppmann, M.: Making CRDTs Byzantine Fault Tolerant. In: *Proceedings of the 9th Workshop on Principles and Practice of Consistency for Distributed Data. PaPoC ’22, Association for Computing Machinery, Rennes, France*, pp. 8–15, 2022, ISBN: 978-1-4503-9256-3, DOI: 10.1145/3517209.3524042.
- [Lo24] Loynes, S.: UNICC Selects Element for Secure Communications, 2024, URL: <https://element.io/blog/unicc-selects-element-for-secure-communications/>.
- [OT18] O’Toole, G.: It’s Easier To Ask Forgiveness Than To Get Permission, 2018, URL: <https://quoteinvestigator.com/2018/06/19/forgive/>.
- [Th23] The Matrix.org Foundation CIC: Matrix Specification v1.9, tech. rep., 2023.