Confidential Computing-Induced Privacy Benefits for the Bootstrapping of New Business Relationships

Jan Pennekamp*, Frederik Fuhrmann*, Markus Dahlmanns*, Timo Heutmann†, Alexander Kreppein†, Dennis Grunert†, Christoph Lange¶,‡, Robert H. Schmitt§,†, and Klaus Wehrle*
*Communication and Distributed Systems, ¶Information Systems, §Machine Tools and Production Engineering, *,¶,§ All affiliated to: RWTH Aachen University, Germany · †Production Quality, Fraunhofer IPT, Aachen, Germany
‡Data Science and Artificial Intelligence, Fraunhofer FIT, Sankt Augustin, Germany
{lastname}@comsys.rwth-aachen.de · {firstname.lastname}@ipt.fraunhofer.de · {christoph.lange-bever}@fit.fraunhofer.de

ABSTRACT

In addition to quality improvements and cost reductions, dynamic and flexible business relationships are expected to become more important in the future to account for specific customer change requests or small-batch production. Today, despite reservation, sensitive information must be shared upfront between buyers and sellers. However, without a trust relation, this situation is precarious for the involved companies as they fear for their competitiveness following information leaks or breaches of their privacy. To address this issue, the concepts of confidential computing and cloud computing come to mind as they promise to offer scalable approaches that preserve the privacy of participating companies. In particular, designs building on confidential computing can help to technically enforce privacy. Moreover, cloud computing constitutes an elegant design choice to scale these novel protocols to industry needs while limiting the setup and management overhead for practitioners. Thus, novel approaches in this area can advance the status quo of bootstrapping new relationships as they provide privacy-preserving alternatives that are suitable for immediate deployment.

KEYWORDS

bootstrapping procurement; business relationships; secure industrial collaboration; privacy; Internet of Production

ACM Reference Format:
Jan Pennekamp, Frederik Fuhrmann, Markus Dahlmanns, Timo Heutmann, Alexander Kreppein, Dennis Grunert, Christoph Lange, Robert H. Schmitt, and Klaus Wehrle. 2021. Confidential Computing-Induced Privacy Benefits for the Bootstrapping of New Business Relationships. To be presented at *2021 Cloud Computing Security Workshop, November 14, 2021, Seoul, Korea.*

1 ESSENTIAL PRIVACY NEEDS

Novel paradigms, such as the Internet of Production [4], envision the increase of short-lived and flexible business relationships to achieve enhanced product quality, a reduction in costs, and improved sustainability. However, buyers are notoriously cautious when sharing sensitive information with third parties [5], such as details on products they intend to purchase, especially without an established trust or business relationship. Likewise, sellers might want to keep their capabilities and price expectations a secret. For example, this information could leak insights into new product models, made technical advances, or their current workload.

During the procurement process, a buyer is interested in selecting a suitable (and cheap) seller. Today, companies rely on inflexible strategies during procurement: Due to the lack of suitable privacy-preserving approaches, buyers usually resort to their existing network of suppliers, i.e., they immediately exclude a large number of other, potentially superior suppliers. Alternatively, they employ time-consuming methods, such as signing non-disclosure agreements (NDAs) early on. However, these approaches have in common that (i) they limit their relations in terms of quality, functionality, innovation, and costs, and (ii) they contradict the idea of dynamically establishing short-lived relations as needed.

To tackle the lack of privacy-preserving approaches when bootstrapping business relationships, two promising concepts come to mind. First, confidential computing offers building blocks to protect the participants' privacy, even in industrial settings [6]. Second, cloud computing can easily deal with the (extreme) scalability needs of industrial applications [2]. So far, to the best of our knowledge, research has neglected the privacy of this essential step in business. However, the combination of both concepts has been successfully applied in several industrial use cases, such as company benchmarking [7] (e.g., to identify the need for new, more suitable suppliers) and when exchanging information along [1] or across [3] supply chains. Thus, we intend to apply these concepts for the privacy-preserving bootstrapping of relationships as well.

ACKNOWLEDGMENTS

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Production – 390621612.

REFERENCES

[1] Lennart Bader, Jan Pennekamp et al. 2021. Blockchain-Based Privacy Preservation for Supply Chains Supporting Lightweight Multi-Hop Information Accountability. *Inf. Process. Manag.* 58, 3. https://doi.org/10.1016/j.ipm.2021.102529
[2] Martin Henze. 2020. The Quest for Secure and Privacy-preserving Cloud-based Industrial Cooperation. In *IEEE SPC*. https://doi.org/10.1109/CNS48642.2020.9162199
[3] Jan Pennekamp, Erik Buchholz et al. 2020. Privacy-Preserving Production Process Parameter Exchange. In *ACSAC*. https://doi.org/10.1145/3427228.3427248
[4] Jan Pennekamp, René Glebke et al. 2019. Towards an Infrastructure Enabling the Internet of Production. In *IEEE ICPS*. https://doi.org/10.1109/ICPHYS.2019.8780276
[5] Jan Pennekamp, Martin Henze et al. 2019. Dataflow Challenges in an *Internet* of Production: A Security & Privacy Perspective. In *ACM CPS-SPC*. https://doi.org/10.1145/3338499.3357357
[6] Jan Pennekamp, Martin Henze et al. 2021. Unlocking Secure Industrial Collaborations through Privacy-Preserving Computation. *ERCIM News* 126.
[7] Jan Pennekamp, Patrick Sapel et al. 2020. Revisiting the Privacy Needs of Real-World Applicable Company Benchmarking. In *WAHC*. https://doi.org/10.25835/0072999