Reputation Systems for Supply Chains: The Challenge of Achieving Privacy Preservation

✉ Lennart Bader[1]*, ✉ Jan Pennekamp[2]*, Emildeon Thevaraj[2], Maria Spiß[3], Salil S. Kanhere[4], and Klaus Wehrle[2]

[1] Cyber Analysis & Defense, Fraunhofer FKIE, Germany
[2] Communication and Distributed Systems, RWTH Aachen University, Germany
[3] Institute for Industrial Management at RWTH Aachen University, Germany
[4] School of Computer Science and Eng., University of New South Wales, Australia

Abstract. Consumers frequently interact with reputation systems to rate products, services, and deliveries. While past research extensively studied different conceptual approaches to realize such systems securely and privacy-preservingly, these concepts are not yet in use in business-to-business environments. In this paper, (1) we thus outline which specific challenges privacy-cautious stakeholders in volatile supply chain networks introduce, (2) give an overview of the diverse landscape of privacy-preserving reputation systems and their properties, and (3) based on well-established concepts from supply chain information systems and cryptography, we further propose an initial concept that accounts for the aforementioned challenges by utilizing fully homomorphic encryption. For future work, we identify the need of evaluating whether novel systems address the supply chain-specific privacy and confidentiality needs.

Keywords: SCM · confidentiality · anonymity · voter · votee · FHE

1 Introduction and Motivation

In contrast to historically long-living business relationships, today's supply chain networks are much more volatile [47]. This shift manifests in both (i) the demand for more flexible, spontaneous and short-lived business agreements and (ii) a growing demand for digitized relationship establishments and management. While these aspects are well-known influencing factors for traditional supply chain management (SCM) [48], where various tracing systems tailored to the specific privacy and transparency needs of businesses within and along supply chain structures have been proposed [6,22], these solutions are not applicable for easing the business partner selection processes in such volatile supply chains.

For spontaneously establishing new relationships, potential business partners are in need of reliably assessing the credibility, i.e., *reputation*, of each other. Similarly, they have an incentive to advertise their own business and services to potential partners, where a well-built reputation might attract further business

* The authors contributed equally to this work.

and sales. Since these use cases require businesses to transparently provide insights into their operations and potentially their former business relationships, confidentiality concerns on business and production secrets must be considered at all times when discussing and proposing respective technical solutions [48].

The concept of measuring a business' or product's reputation and granting access to it to potential customers or partners is well-established [28], e.g., for online sellers and their offered articles. However, since such reputations are mostly based on non-verifiable reviews, they can neither guarantee reliability nor accuracy, limiting their value for customers and the businesses themselves.

Hence, business-to-business (B2B)-focused reputation systems, as prevalent in the context of supply chains, exhibit a distinct set of requirements regarding (1) the reliability of ratings and the resulting reputation, (2) the transparency properties, (3) the privacy of involved stakeholders, and (4) the confidentiality of business information. Even though related work studies reputation systems [24,27], they largely fail to consider the specific needs of B2B settings. In this paper, we thus raise the awareness for this research gap by identifying and discussing respective requirements along with potential conflicts. Moreover, we propose a first concept for a privacy-preserving multi-agent B2B reputation system that combines well-established concepts from supply chain information systems and cryptography for a flexible trade-off between these requirements.

2 Reputation Systems

Information *transparency* is an important aspect of today's supply chain networks [48]. Businesses have identified the various benefits of inter-business transparency for enhancing their collaboration for increased success of both their individual business and their supply chain as a whole [6]. However, *privacy* preservation is an equally important aspect as businesses want to keep their business relationships a secret. Consequently, generally maintaining the *confidentiality* of information (except for deliberately shared slices) as well as sufficient *security* mechanisms (e.g., to protect against unauthorized access as well as manipulation) are fundamental requirements for supply chain-oriented information systems.

2.1 Related Work: The Diversity in Today's Reputation Systems

The universal benefits of reputation systems have resulted in diverse approaches for various domains. Due to our focus on privacy preservation and confidentiality in supply chains, we study relevant approaches from two well-known surveys [24,27] in light of these requirements, i.e., we omit inapplicable approaches from our analysis. We augment this foundation with a selection of recent papers [36,64,50,3] to provide an up-to-date overview. In Table 1 (Appendix), we detail the specific features of these approaches, which serve as the basis for our own design. Just like previous conclusions [24], we confirm that today's systems are unable to satisfy all desirable combinations of properties. Especially privacy properties often depend on the inclusion of at least one trusted third party, which is a challenging and potentially unrealistic assumption for supply chain settings.

2.2 Requirements for Privacy-preserving Reputation Systems

The desire for inter-business transparency, aiming at an accountable selection of new business partners and increasing their own business' visibility, leads to the research area of privacy-preserving reputation systems [24,27]. These reputation systems adduce customer and business feedback in the form of *votes* to derive a business' *reputation* as a measure of its trustworthiness, quality of offered services, and ability to cooperate. Other customers and businesses can then request this reputation as a foundation for their follow-up decision-making.

Hence, businesses can take the role of a *voter* when submitting a vote or rating, a *votee* when receiving such ratings, or a *requester* when requesting access to the derived reputation score, as formalized by Gurtler and Goldberg [24]. Each business taking one or multiple roles introduces specific requirements to the reputation system. Straightforward requirements, i.e., the reliability and accountability of the reputation, the security and flexibility of submitted ratings, and the possibility for access control for reputation requests, are complemented by the demand for the complex trade-off between privacy and transparency [6], especially since "privacy" can have different notions depending on a business' role [24]. Common privacy requirements for voters are related to their anonymity and the anonymity of individual (*voter-vote privacy*) and even multiple (*two-vote privacy*) votes [24]. Further, votees might require privacy (confidentiality) regarding their reputation, either by proving their current reputation without the need to link themselves to a long-term history (*reputation-usage unlinkability*) or by providing meta-information on their current reputation, e.g., threshold-based, instead of their plain reputation score (*exact reputation blinding*) [24], raising reputation reliability challenges. Similarly, requesters might want to hide their identity when requesting another business' reputation, which, among other aspects, might contradict the votees' demand for sophisticated access control.

The variety of contradicting requirements poses a significant challenge for researchers when designing appropriate and practical reputation systems. Each assessment of the importance or trade-off weights of these requirements leads to different potential designs, such that a wide range of systems has been proposed.

3 Reputation and Privacy Preservation in Supply Chains

The lack of widely-used reputation systems in supply chain settings hints at issues with today's technical approaches (cf. Table 1 for general academic concepts). To better assess this inadequate situation, we now explore the circumstances of deploying and developing supply-chain-focused reputation systems.

3.1 Supply Chain-induced Requirements

In contrast to commonly studied consumer-oriented reputation systems, e.g., seller or product ratings on online platforms, reputation systems for B2B use and supply chains face specific confidentiality and privacy needs, which render the application of existing reputation systems difficult or simply infeasible.

First, supply chains induce new *information flow dimensions* [48]. Combining subjective ratings with contract-based information and objective production- or service-related information for computing a reputation score requires suitable reputation functions, authenticity checks, and verification mechanisms.

Second, the volatility of modern supply chain networks is a big challenge because, e.g., systems with *votee-owned* [24] scores are not applicable when participants go out of business or just decide to stop participating. Likewise, selecting a trusted third party for managing the businesses' reputations that all participants agree on represents a significant challenge for globalized supply chains.

3.2 Research Gap: Domain-specific Realization

Existing (privacy-preserving) reputation systems (cf. Section 2.1) fail to consider the previously outlined requirements regarding privacy, availability, and the supported data dimensions. For a formal definition of these dimensions in supply chains, we refer to Pennekamp et al. [48]. Hence, developing a sophisticated privacy-preserving design for all involved parties that does not require well-established trust between participants while also accounting for volatile structures remains an open issue in research. In the following, we outline promising design decisions for such a reputation system and detail its conceptual design.

4 Toward a Comprehensive Design

Based on the general requirements for privacy-preserving reputation systems and the additional challenges arising from the specifics of modern supply chain networks, we now derive a comprehensive design for a reputation system tailored to these challenging needs. Given our business focus, we know that all entities (operators, participants, and users) are bound by legislation and to specific jurisdictions. Hence, for this work, we consider malicious-but-cautious attackers [52] who can misbehave in all possible ways while trying to not leave any verifiable evidence of their misbehavior. With this attacker model, we have to include more attacks than with honest-but-curious (semi-honest) attackers since it explicitly allows for local deviation from protocols unless they are provable by third parties. Consequently, collusion attacks are possible but attackers would have to make sure to not leave any (public) traces to comply with the attacker model.

4.1 Design Decisions

Achieving a reasonable trade-off between reputation privacy and the desired degree of transparency while maintaining a secure operation and accounting for volatile supply chain structures calls for (1) a sophisticated encryption scheme, (2) verifiable reputation computations, and (3) a distribution of competences to multiple independent entities (as we assume malicious-but-cautious adversaries).

First, we identify a *ticket-based* [24] voting process as well suited for combining privacy preservation with rating reliability: A business should be authorized

to submit a vote for another business only if a (recent) business relationship existed. Hence, voting tickets can be issued as soon as a business relationship has been established, i.e., a new contract has been signed. The tickets can either be issued by the businesses themselves or by a third entity that reviews relationships within an already-deployed supply chain information system, such as the privacy-preserving realizations ProductChain [37] or PrivAccIChain [6].

Second, to account for the challenge of dealing with volatile supply chain structures (especially, defunct, i.e., departing, businesses), we assess that a *centralized* approach fits best to ensure a reliable operation of the system (availability of reputation scores). With a (conceptual) central and static entity, departing or non-collaborative nodes do not negatively affect the reputation system's operation. Using multiple entities for different roles and potentially splitting a single role onto multiple entities further reduces the risk of operational deficiencies.

Third, as we already encourage the use of *multiple independent entities* for different roles, we reduce the trust in a single entity and limit its ability to compromise information privacy and security, i.e., preventing the threat and impact of collusion attacks. While such an approach already achieves full collusion resistance, increasing the number of central entities further distributes critical responsibilities, which allows for a tunable degree of collusion resistance.

Fourth, to achieve privacy-preserving voting and request processes, we propose the use of *pseudonyms*. Instead of authorizing themselves to other businesses or the reputation engine, voters and requesters receive a (temporary) pseudonym from an independent or government-run entity to authorize their requests. Thus, individual requests cannot be linked to a specific business, and multiple requests from the same business appear as if they were coming from different entities, such that the businesses' privacy as well as privacy of relationship can be achieved, accounting for the needs of (volatile) supply chain networks.

Finally, the use of a (conceptually) central entity mandates an elaborate data security concept. Specifically, we propose to base the voting process as well as the reputation function on *fully homomorphic encryption* (FHE) [38]. In particular, voters encrypt their votes under FHE before submitting them to an available reputation engine, which is unable to decrypt or tamper with individual votes. The reputation engine then computes the reputation score under FHE while offering a verification mechanism to both voters and votees. Since the result remains encrypted, the reputation engine does not learn the actual, potentially sensitive reputation score, ensuring the desired votee privacy.

To quickly explore the feasibility of FHE for our use in reputation systems, we measured the runtime of the basic operations needed in our design using Pyfhel [30], which is a Python library for Microsoft SEAL [40], utilizing the CKKS [16] scheme. We extrapolated these numbers to realistic scenarios, and after discussions with our applied partner, we concluded that FHE is suitable.

4.2 The Rating Process on a High-level

To illustrate our design and the interaction of its entities, we now present the rating process consisting of multiple steps (cf. Figure 1). For the rating, we com-

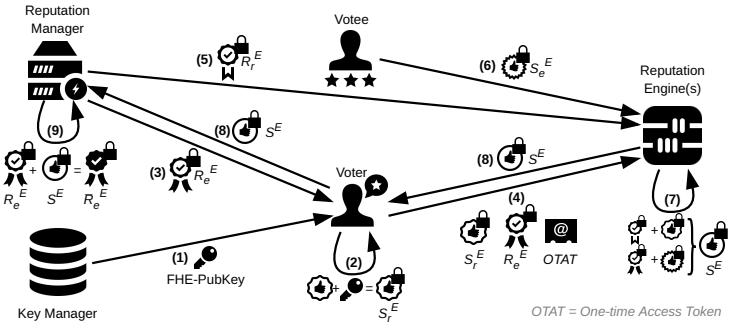

Fig. 1. The reputation calculation is shielded using FHE to ensure confidentiality.

bine and weigh subjective ratings with a rating based on objective information on the business relationship.

During the rating process, both the *voter* and the *votee* use (temporary) pseudonyms for their interactions. The *voter* (1) retrieves the *votee*-specific FHE key from the *key manager* and (2) encrypts its rating with this key under FHE as S_r^E. The voter then (3) receives the (FH-encrypted) current reputation R_e^E of the *votee* from the *reputation manager* to (4) forward S_r^E, R_e^E, and a one-time *access token* to one of the available *reputation engines*. The *reputation engine* then (5) uses the access token to receive the *voter's* current reputation R_r^E from the *reputation manager* and (6) optionally receives a data-backed (which ideally is verifiable, e.g., since it has been processed using trusted computing [46]) self-rating S_e^E from the *votee* to (7) combine S_r^E and S_e^E into the final rating S^E. Here, the current reputations R_r^E and R_e^E can be used as weights for the ratings. The *reputation engine* then (8) signs and submits the new rating to the *voter*, who forwards the rating S back to the *reputation manager*. Here, the new reputation (9) is calculated as $\bar{R}_e^E$ using R_e^E and S^E.

The use of FHE ensures that neither the reputation engine nor the reputation manager can access individual ratings or a business' plain reputation. By distributing the reputation computation to multiple entities, i.e., *reputation engines*, we maintain privacy of relationship between voter and votee toward the *reputation manager*. The use of the one-time *access token* further prevents the *reputation manager* from linking *voter* and *votee* by request analyses, as the current reputations are requested by different entities.

5 Conclusion and the Road Ahead

In this paper, we have highlighted the lack of reputation systems in B2B settings and volatile supply chain networks despite the availability of technical approaches, indicating a mismatch between offered features and set requirements.

Evaluation Challenges. Generally, this research is hindered by the lack of evaluation data and realistic supply chain models [48]. While our applied partner (Institute for Industrial Management) can provide us with real-world data, its scale and the complexity of business relationships represent only the tip of the

iceberg. Specifically, at this point, we rely on data from ERP systems that cover the order and delivery of goods. Moreover, we have access to monitoring data of production machines that allow us to incorporate such data into the calculation of reputation. Regardless, we are interested in acquiring additional datasets to extensively evaluate reputation systems for volatile supply chain networks.

Future Work. In addition to evaluating our proposed approach, we further identify three crucial research directions: (1) Assessing whether multi-key FHE can offer confidentiality benefits, (2) studying how to better utilize existing supply chain information systems, and (3) investigating the implications of dealing with E2E-secured supply chains [46], i.e., incorporating trusted sensors into the reputation computation and capitalizing on their reliability benefits.

Conclusion. The lack of deployed reputation systems in B2B environments encouraged us to look into the respective reasons since reliable reputation scores are beneficial for businesses when managing both short- and long-term operations. Even though privacy-preserving concepts are available, their use is hindered by volatile supply chain networks and differing data dimensions. Addressing this research gap, we are proposing an FHE-based design that accounts for the transparency, confidentiality, and privacy requirements of participating businesses while being compatible with existing supply chain information systems.

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

References

1. Anceaume, E., Guette, G., Lajoie-Mazenc, P., Sirvent, T., Viet Triem Tong, V.: Extending Signatures of Reputation. In: PrimeLife (2014)
2. Androulaki, E., Choi, S.G., Bellovin, S.M., Malkin, T.: Reputation Systems for Anonymous Networks. In: PETS (2008)
3. Arshad, J., Azad, M.A., Prince, A., Ali, J., Papaioannou, T.G.: REPUTABLE–A Decentralized Reputation System for Blockchain-Based Ecosystems. IEEE Access **10** (2022)
4. Azad, M.A., Bag, S., Hao, F.: M2M-REP: Reputation of Machines in the Internet of Things. In: ARES (2017)
5. Azad, M.A., Bag, S., Hao, F.: PrivBox: Verifiable decentralized reputation system for online marketplaces. Future Gener. Comput. Syst. **89** (2018)
6. Bader, L., Pennekamp, J., Matzutt, R., Hedderich, D., et al.: Blockchain-Based Privacy Preservation for Supply Chains Supporting Lightweight Multi-Hop Information Accountability. Inf. Process. Manag. **58**(3) (2021)
7. Bag, S., Azad, M.A., Hao, F.: A privacy-aware decentralized and personalized reputation system. Comput. Secur. **77** (2018)
8. Bakas, A., Michalas, A., Ullah, A.: (F)unctional Sifting: A Privacy-Preserving Reputation System Through Multi-Input Functional Encryption. In: NordSec (2021)

9. Bazin, R., Schaub, A., Hasan, O., Brunie, L.: A Decentralized Anonymity-Preserving Reputation System with Constant-time Score Retrieval. Cryptology ePrint Archive 2016/416 (2016)
10. Bazin, R., Schaub, A., Hasan, O., Brunie, L.: Self-reported Verifiable Reputation with Rater Privacy. In: IFIPTM (2017)
11. Bemmann, K., Blömer, J., Bobolz, J., Bröcher, H., et al.: Fully-Featured Anonymous Credentials with Reputation System. In: ARES (2018)
12. Bethencourt, J., Shi, E., Song, D.: Signatures of Reputation. In: FC (2010)
13. Blömer, J., Eidens, F., Juhnke, J.: Practical, Anonymous, and Publicly Linkable Universally-Composable Reputation Systems. In: CT-RSA (2018)
14. Bo, Y., Min, Z., Guohuan, L.: A Reputation System with Privacy and Incentive. In: ACIS SNPD (2007)
15. Busom, N., Petrlic, R., Sebé, F., Sorge, C., Valls, M.: A privacy-preserving reputation system with user rewards. J. Netw. Comput. Appl. **80** (2017)
16. Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic Encryption for Arithmetic of Approximate Numbers. In: ASIACRYPT (2017)
17. Christin, D., Roßkopf, C., Hollick, M., Martucci, L.A., Kanhere, S.S.: IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications. Pervasive Mob. Comput. **9**(3) (2013)
18. Clark, M.R., Stewart, K., Hopkinson, K.M.: Dynamic, Privacy-Preserving Decentralized Reputation Systems. IEEE Trans. Mob. Comput. **16**(9) (2016)
19. Clauß, S., Schiffner, S., Kerschbaum, F.: k-Anonymous Reputation. In: ACM ASIACCS (2013)
20. Dolev, S., Gilboa, N., Kopeetsky, M.: Efficient private multi-party computations of trust in the presence of curious and malicious users. J. Trust Manag. **1** (2014)
21. Gal-Oz, N., Grinshpoun, T., Gudes, E.: Sharing reputation across virtual communities. Journal of theoretical and applied electronic commerce research **5**(2) (2010)
22. Gonczol, P., Katsikouli, P., Herskind, L., Dragoni, N.: Blockchain Implementations and Use Cases for Supply Chains-A Survey. IEEE Access **8** (2020)
23. Gudes, E., Gal-Oz, N., Grubshtein, A.: Methods for Computing Trust and Reputation While Preserving Privacy. In: DBSec (2009)
24. Gurtler, S., Goldberg, I.: SoK: Privacy-preserving reputation systems. Proc. Priv. Enhancing Technol. **2021**(1) (2021)
25. Hao, L., Lu, S., Tang, J., Zhang, A.: A Low Cost and Reliable Anonymity Scheme in P2P Reputation Systems with Trusted Third Parties. In: IEEE GLOBECOM (2008)
26. Hao, L., Yang, S., Lu, S., Chen, G.: A Dynamic Anonymous P2P Reputation System Based on Trusted Computing Technology. In: IEEE GLOBECOM (2007)
27. Hasan, O., Brunie, L., Bertino, E.: Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey. ACM Comput. Surv. **55**(2) (2022)
28. Hendrikx, F., Bubendorfer, K., Chard, R.: Reputation systems: A survey and taxonomy. J. Parallel Distrib. Comput. **75** (2015)
29. Hussain, M., Skillicorn, D.B.: Mitigating the linkability problem in anonymous reputation management. J. Internet Serv. Appl. **2** (2011)
30. Ibarrondo, A.: Pyfhel. https://github.com/ibarrond/Pyfhel (2017)
31. Kerschbaum, F.: A Verifiable, Centralized, Coercion-Free Reputation System. In: ACM WPES (2009)
32. Kinateder, M., Pearson, S.: A Privacy-Enhanced Peer-to-Peer Reputation System. In: EC-Web (2003)

33. Lajoie-Mazenc, P., Anceaume, E., Guette, G., Sirvent, T., Tong, V.V.T.: Efficient Distributed Privacy-Preserving Reputation Mechanism Handling Non-Monotonic Ratings. hal-01104837 (2015)
34. Liu, D., Alahmadi, A., Ni, J., Lin, X., Shen, X.: Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain. IEEE Trans. Industr. Inform. **15**(6) (2019)
35. Liu, J., Manulis, M.: pRate: Anonymous Star Rating with Rating Secrecy. In: ACNS (2019)
36. Malik, S., Dedeoglu, V., Kanhere, S.S., Jurdak, R.: TrustChain: Trust Management in Blockchain and IoT supported Supply Chains. In: IEEE Blockchain (2019)
37. Malik, S., Kanhere, S.S., Jurdak, R.: ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains. In: IEEE NCA (2018)
38. Marcolla, C., Sucasas, V., Manzano, M., Bassoli, R., et al.: Survey on fully homomorphic encryption, theory, and applications. Proc. IEEE **110**(10) (2022)
39. Melchor, C.A., Ait-Salem, B., Gaborit, P.: A Collusion-Resistant Distributed Scalar Product Protocol with Application to Privacy-Preserving Computation of Trust. In: IEEE NCA (2009)
40. Microsoft, Inc.: Microsoft SEAL. https://github.com/Microsoft/SEAL (2018)
41. Miranda, H., Rodrigues, L.: A Framework to Provide Anonymity in Reputation Systems. In: MobiQuitous (2006)
42. Nithyanand, R., Raman, K.: Fuzzy Privacy Preserving Peer-to-Peer Reputation Management. Cryptology ePrint Archive 2009/442 (2009)
43. Owiyo, E., Wang, Y., Asamoah, E., Kamenyi, D., Obiri, I.: Decentralized Privacy Preserving Reputation System. In: IEEE DSC (2018)
44. Pavlov, E., Rosenschein, J.S., Topol, Z.: Supporting Privacy in Decentralized Additive Reputation Systems. In: iTrust (2004)
45. Peng, H., Lu, S.n., Zhao, D.d., Zhang, A.x.: Low cost and reliable anonymity protocols in P2P reputation systems. J. Shanghai Jiaotong Univ. (Sci.) **15** (2010)
46. Pennekamp, J., Alder, F., Matzutt, R., Mühlberg, J.T., et al.: Secure End-to-End Sensing in Supply Chains. In: IEEE CPS-Sec (2020), proceedings of the 5th International Workshop on Cyber-Physical Systems Security (CPS-Sec '20)
47. Pennekamp, J., Henze, M., Schmidt, S., Niemietz, P., et al.: Dataflow Challenges in an *Internet* of Production: A Security & Privacy Perspective. In: ACM CPS-SPC (2019)
48. Pennekamp, J., Matzutt, R., Klinkmüller, C., Bader, L., et al.: An Interdisciplinary Survey on Information Flows in Supply Chains. ACM Comput. Surv. **56**(2) (2024)
49. Petrlic, R., Lutters, S., Sorge, C.: Privacy-Preserving Reputation Management. In: ACM SAC (2014)
50. Putra, G.D., Kang, C., Kanhere, S.S., Hong, J.W.K.: DeTRM: Decentralised Trust and Reputation Management for Blockchain-based Supply Chains. In: IEEE ICBC (2022)
51. Ries, S., Fischlin, M., Martucci, L.A., Muuhlhauser, M.: Learning Whom to Trust in a Privacy-Friendly Way. In: IEEE TrustCom (2011)
52. Ryan, M.D.: Enhanced Certificate Transparency and End-to-end Encrypted Mail. In: NDSS (2014)
53. Schaub, A., Bazin, R., Hasan, O., Brunie, L.: A Trustless Privacy-Preserving Reputation System. In: SEC (2016)
54. Schiffner, S., Clauß, S., Steinbrecher, S.: Privacy and Liveliness for Reputation Systems. In: EuroPKI (2009)
55. Schiffner, S., Clauß, S., Steinbrecher, S.: Privacy, Liveliness and Fairness for Reputation. In: SOFSEM (2011)

56. Singh, A., Liu, L.: TrustMe: Anonymous Management of Trust Relationships in Decentralized P2PSystems. In: P2P (2003)
57. Soska, K., Kwon, A., Christin, N., Devadas, S.: Beaver: A Decentralized Anonymous Marketplace with Secure Reputation. Cryptology ePrint Archive 2016/464 (2016)
58. Steinbrecher, S.: Design Options for Privacy-Respecting Reputation Systems within Centralised Internet Communities. In: SEC (2006)
59. Voss, M.: Privacy preserving online reputation systems. In: SEC (2004)
60. Wei, Y., He, Y.: A Pseudonym Changing-Based Anonymity Protocol for P2P Reputation Systems. In: ETCS (2009)
61. Yang, X., Yang, X., Luo, J., Yi, X., et al.: Towards Sustainable Trust: A Practical SGX Aided Anonymous Reputation System. IEEE Trans. Sustain Comput. (2023)
62. Yao, D., Tamassia, R., Proctor, S.: Private Distributed Scalar Product Protocol With Application To Privacy-Preserving Computation of Trust. In: IFIPTM (2007)
63. Zhang, K., Li, Z., Yang, Y.: A Reputation System Preserving the Privacy of Feedback Providers and Resisting Sybil Attacks. Int. J. Multimedia Ubiquitous Eng. **9**(2) (2014)
64. Zhou, Z., Wang, M., Yang, C.N., Fu, Z., et al.: Blockchain-based decentralized reputation system in E-commerce environment. Future Gener. Comput. Syst. **124** (2021)

A Appendix: Comparing Reputation Systems in Detail

As a foundation of our work (cf. Section 2.1), we have analyzed various reputation systems, especially those covered in previous surveys [24,27], regarding their system architecture and their properties for both feedback provision and the reputation itself. In Table 1, we summarize the corresponding results.

For the architecture, we distinguish between *centralized* (C), *decentralized* (D), and *hybrid* (H) approaches. Additionally, depending on the system, voters can provide feedback values from different sets or value ranges. Here, we indicate the set of available values either as a set (e.g., $\mathbb{R}$ or $\{1, ..., 5\}$) or as an interval. Some systems also allow text and vectors as feedback. Moreover, the feedback granularity indicates whether feedback is provided for a *single* (S) interaction between voter and votee or over *multiple* (M) ones.

For reputation, we further cover six distinct properties per approach. While the set or range is equivalent to the respective feedback property, liveliness [54] indicates whether negative ratings are allowed by the system. This aspect is also related to monotonicity, which indicates that a votee's reputation can only increase over time. Hence, non-monotonicity allows for reputations to decrease over time or when negative ratings are submitted. Some reputation systems provide *global* (G) visibility, while others offer *local* (L) visibility. With global visibility, all requesting parties receive the same response to a reputation query. With local visibility, different requesters can receive different results. The durability indicates whether ratings are stored locally or whether the reputation has to be recalculated on every request, resulting in a trade-off between storage and computation requirements. Finally, a reputation system's aggregation model indicates how feedback is aggregated into a final reputation score.

Table 1. We analyzed privacy-preserving reputation systems that are promising for use in supply chains regarding nine distinct properties. We represent no level of fulfillment of the respective property by ○ while ● shows fulfillment of the property. For entries labeled with "?", we cannot reliably identify the corresponding aspect.

Publication	Architecture	Set / Range	Granularity	Set / Range	Liveliness	Visibility	Durability	Non-Monotonicity	Aggregation Model
System		**Feedback**		**Reputation**					
SMPC-based Systems									
Pavlov et al. (2004) [44]	D	$\mathbb{R}$	M	$\mathbb{R}$ $[0, 1]$	●	L	○	●	Sum, Beta reputation
Yao et al. (2007) [62]	D	$\mathbb{Z}$	M	$\mathbb{Z}$	●	L	○	○	Weighted average
Gudes et al. (2009) [23]	D	$\mathbb{R}$	M	$\mathbb{R}$	●	L	○	●	Weighted sum, Mean
Melchor et al. (2009) [39]	D	$\mathbb{Z}$	M	$\mathbb{Z}$	●	L	○	○	Weighted average
Nithyanand and Raman (2009) [42]	D	$\mathbb{R}$ $\{0, 1\}$	M	$\mathbb{R}$	●	L	○	●	Ordered weighted average
Gal-Oz et al. (2010) [21]	D	$\mathbb{R}$	M	$\mathbb{R}$	●	L	○	●	Weighted sum, Mean
Dolev et al. (2014) [20]	D	$\{1, \ldots, 10\}$	M	$\mathbb{R}$	●	L	○	●	Weighted mean
Clark et al. (2016) [18]	D	$[0, v_{max}]$	M	$[0, v_{max}]$	●	L	○	●	Mean
Azad et al. (2018) [4]	D	$\{-1, 0, 1\}$	M	$\{-1, 0, 1\}$	●	G	●	●	Weighted sum
Bakas et al. (2020) [8]	D	$\{1, \ldots, 5\}$	M	$\mathbb{Z}$	●	G	○	○	Weighted sum
Token-based Systems									
Singh and Liu (2003) [56]	H	?	M	?	?	G	●	?	?
Voss (2004) [59]	C	$\mathbb{Z}$	S	$\mathbb{Z}$	●	G	●	●	Sum
Androulaki et al. (2008) [2]	C	$\{0, 1\}$	S	$\mathbb{Z}$	○	G	●	○	Sum
Kerschbaum (2009) [31]	C	$\{0, 1\}$	S	$[0, 1]$	●	G	●	●	Beta reputation
Schiffner et al. (2009) [54]	C	$\{-1, 1\}$	S	$\mathbb{Z}$	●	G	●	●	Sum
Hussain and Skillicorn (2011) [29]	C	?	M	?	?	G	●	?	Open
Schiffner et al. (2011) [55]	C	$\{-, +\}$	S	$\mathbb{R}$	●	G	●	●	Open
Zhang et al. (2014) [63]	H	?	S	$\mathbb{R}$	●	G	●	●	Open
Bazin et al. (2016) [9]	H	?	S	?	?	G	●	?	Open, Beta reputation
Busom et al. (2017) [15]	C	Text	S	?	●	G	●	●	Union
Blömer et al. (2018) [13]	C	?	S	?	?	G	?	?	Open
Liu and Manulis (2019) [35]	C	$\{1, \ldots, 5\}$	M	$\mathbb{Z}$	●	G	●	○	Sum
Proxy-based Systems									
Ries et al. (2011) [51]	C	$\{0, 1\}$	M	$[0, 1]$	●	L	○	●	Beta reputation
Petrlic et al. (2014) [49]	C	Vector $\{0, 1\}$	S	$\mathbb{Z}$	●	G	●		Sum

Continues on next page

Continued from previous page

Publication	Architecture	Feedback: Set / Range	Feedback: Granularity	Reputation: Set / Range	Reputation: Liveliness	Reputation: Visibility	Reputation: Durability	Reputation: Non-Monotonicity	Reputation: Aggregation Model
System		**Feedback**		**Reputation**					
Signature-based Systems									
Bethencourt et al. (2010) [12]	H	$\{0, 1\}$	S	$\mathbb{Z}$	●	G	●	○	Sum
Lajoie-Mazenc et al. (2015) [33]	H	$\{-, +\}$ $\mathbb{Z}$	S	$\mathbb{R}$	●	G	●	●	Open
Transitory Pseudonym-based Systems									
Miranda and Rodrigues (2006) [41]	C	?	S	?	●	G	●	●	Open
Steinbrecher (2006) [58]	C	?	S	?	●	G	●	●	Open
Hao et al. (2007) [26]	D	$\{-1, 1\}$	S	$\mathbb{Z}$	●	G	●	●	Sum
Hao et al. (2008) [25]	C	$\{-1, 1\}$	M	$\mathbb{R}$	●	G	●	●	Sum, Average
Wei and He (2009) [60]	C	$\{-1, 1\}$	M	$\mathbb{R}$	●	G	●	●	Sum, Average
Peng et al. (2010) [45]	C	?	S	?	?	G	●	?	Open
Anceaume et al. (2013) [1]	D	$[0, 1]$	S	$[0, 1]$	●	G	?	●	Beta reputation
Christin et al. (2013) [17]	C	?	S	?	●	G	●	●	Open
Clauß et al. (2013) [19]	?	$[1, \ldots)$	M	$[1, \ldots)$	?	G	?	?	Open
Blockchain-based Systems									
Schaub et al. (2016) [53]	D	$\mathbb{Z}$	S	$\mathbb{R}$	●	G	○	●	Open
Soska et al. (2016) [57]	D	Text $\mathbb{Z}$	M	?	?	G	●	?	Open
Bazin et al. (2017) [10]	D	$\mathbb{Z}$	S	$\mathbb{R}$	●	G	●	●	Open
Azad et al. (2018) [5]	D	$\{-, +\}$	S	$\mathbb{Z}$	●	G	○	●	Beta reputation
Bag et al. (2018) [7]	D	$\{0, 1\}$	M	$[1, 10]$	○	L	○	●	Mean
Bemmann et al. (2018) [11]	C	$\{0, 1\}$	M	?	?	G	●	?	?
Owiyo et al. (2018) [43]	D	?	S	?	?	G	●	?	Open
Liu et al. (2019) [34]	C	$[1, 10]$	S	$\mathbb{N}$	●	G	●	○	Sum
Malik et al. (2019) [36]	D	?	M	?	?	G	●	?	Mean, Median, Beta reputation
Zhou et al. (2021) [64]	D	$[-5, -1]$, $[1, 5]$	M	$[0, 1]$	○	G	●	●	Weighted sum
Arshad et al. (2022) [3]	D	$\{0, 1\}$	M	$\mathbb{R}$	○	G	●	●	Beta reputation, Open
Putra et al. (2022) [50]	D	$\{-1, 1\}$	M	$\mathbb{R}$	●	G	●	●	Weighted average
Other Systems									
Kinateder and Pearson (2003) [32]	D	$[0, 1]$	S	$\mathbb{R}$	●	L	○	●	Open
Bo et al. (2007) [14]	H	?	S	?	●	G	●	●	Open
Yang et al. (2023) [61]	C	$\{-1, 1\}$	M	$\mathbb{Z}$	●	G	●	●	Sum