The Quest for Secure and Privacy-preserving Cloud-based Industrial Cooperation

Martin Henze
Cyber Analysis & Defense
Fraunhofer FKIE
Wachtberg, Germany
martin.henze@fkie.fraunhofer.de

***Abstract*—Industrial cooperation promises to leverage the huge amounts of data generated by and collected in industrial deployments to realize valuable improvements such as increases in product quality and profit margins. Cloud computing with its adjustable resources is a prime candidate to serve as the technical foundation for industrial cooperation. However, cloud computing further exaggerates existing security and privacy concerns of industrial companies, leading them to refrain from participating in cloud-based industrial cooperation. To overcome these concerns and thus allow companies to benefit from its advantages, we identify and discuss different aspects of secure and privacy-preserving cloud-based industrial cooperation, ranging from securing industrial devices and networks to secure storage and processing of industrial data in the cloud. By discussing already usable and emerging technical approaches as well as identifying open research challenges, we contribute to realizing the vision of secure and privacy-preserving industrial cooperation.**

***Index Terms*—Cloud computing, Industrial cooperation, Industrial Internet of Things, Internet of Production, Security, Privacy**

I. Introduction

The amount of industrial data generated and collected, e.g., in the context of the Industrial Internet of Things (IIoT), the Internet of Production, or the envisioned Industry 4.0 [1]–[4], steadily increases. Such data encompasses everything concerning a specific manufactured product during its development, production, and customer usage [5]. Although this data is extremely valuable, especially for outside entities, it often resides in isolated silos, mainly because industrial companies are reluctant to share details on their processes in fear of accidentally disclosing valuable trade secrets [2], [6].

Yet, if this data could be shared across factories or even companies, effectively breaking up institutional boundaries, manifold benefits such as increases in product quality and profit margins as well as reductions in time to market and development costs could be realized [7]. Ultimately, this would allow to create a global platform for industrial cooperation across all relevant stakeholders, where data from all stages of a product (development, production, customer usage) could be combined [5], [7]. Given the reluctance of industrial companies to open their data silos, realizing this vision requires approaches to ensure corporate secrecy and secure information sharing between industrial corporations [8], which we call secure and privacy-preserving industrial cooperation [2], [9].

One natural solution to meet the huge storage and processing demands of industrial cooperation is cloud computing. Most importantly, cloud computing provides high usability through transparent and efficient network access, realizes high availability through redundant storage and computing resources, charges based on usage without upfront investment, and makes own infrastructure unnecessary. These advantages are especially important in industrial settings, where devices are often limited w.r.t. computing, storage, and potentially energy resources [10]. Consequently, there are clear incentives to realize industrial cooperation based on cloud resources.

However, the adoption and acceptance of cloud computing is hindered by security and privacy concerns, especially in corporate settings [11], [12]. Most importantly, companies lose control over their data when it is outsourced to the cloud, thus negatively impacting confidentiality, integrity, and availability. These concerns are not restricted to industrial data, but also concern, e.g., interaction patterns of different companies to optimize industrial processes. As a result, basing industrial cooperation on cloud computing even further fuels industrial companies' reluctance to open their data silos. Overcoming these challenges is key to secure the success of cloud-based industrial cooperation and hence to allow a wide range of corporate users to benefit from the advantages of cooperation without having to sacrifice security and privacy requirements.

In this paper, we discuss the different aspects that are important for secure and privacy-preserving cloud-based industrial cooperation (§II), i.e., we identify and discuss different approaches to ***1)*** empower industrial devices to perform the necessary steps to provide security and privacy (§III), ***2)*** securing industrial networks in the face of increased cloud connectivity (§IV), ***3)*** securing the storage of industrial data in the cloud (§V), and ***4)*** realizing secure and privacy-preserving processing and computations in the cloud (§VI). Besides discussing the current state-of-the-art and promising emerging approaches, we also identify open challenges that demand for further research in this field. With this paper, we move an important step forward in the quest to turn secure and privacy-preserving cloud-based industrial cooperation into reality.

II. Security & Privacy in Industrial Cooperation

Industrial cooperation allows all entities involved in the creation of products to improve said products and the underlying

Author's version of a manuscript accepted for publication in the proceedings of the 6th International Workshop on Security and Privacy in the Cloud (SPC).

production processes by exchanging knowledge [2]. For example, sharing characteristics of parts and products along supply chains allows to minimize production interruptions, increase product quality, and improve the development process [2], [7], [13]. Similar benefits can be achieved for predictive maintenance and collaborative agile production [7]. Most importantly, however, industrial cooperation allows previously unaffiliated companies, e.g., those using the same machines or material, to exchange knowledge, e.g., on how to best parameterize a machine [7]. Quantifying these benefits, McKinsey predicts increases in profit margins by 2–3% as well as reductions in time to market and development costs by 25–50% [6].

However, due to security and privacy concerns, current industrial deployments confine knowledge in stakeholder-specific data silos, which makes any exchange of data and thus industrial cooperation impossible [7]. Pennekamp et al. [7] provide a comprehensive survey of the underlying security and privacy concerns in industrial cooperation. Concerns they identify are fear of losing intellectual property or business secrets, e.g., through reverse engineering, receiving falsified or incorrect information, e.g., regarding the properties of a product, transferring knowledge to competitors, e.g., through maintenance contracts, and tracking and tracing based on usage information, e.g., on the utilization of products [7], [14].

Realizing industrial cooperation on top of cloud infrastructure further exaggerates these concerns [11], [12], [15]. Most importantly, cloud computing is more complex and less transparent than traditional IT outsourcing, since cloud providers often subcontract or utilize other cloud providers [12], [16], [17]. In such settings, companies have to trust an unidentified number of third parties with their sensitive industrial data, obliterating which jurisdiction applies to data and thus offering only limited legal protection [12], [18]. Likewise, companies using cloud services might not even be aware that and which cloud services they are using [19]. Finally, cloud computing centralizes data at a comparatively small number of entities, making those valuable attack targets [12].

Secure and privacy-preserving cloud-based industrial collaboration promises to overcome these concerns, thus making it possible to combine the advantages of industrial cooperation *and* cloud computing by providing strong security and privacy functionality. As shown in Figure 1, realizing secure and privacy-preserving cloud-based industrial collaboration requires ***1)*** empowering industrial devices to be able to realize security and privacy protection such as object and transport security (§III), ***2)*** monitoring and securing industrial networks in the face of increased communication with Internet and cloud endpoints (§IV), ***3)*** protecting industrial data during cloud storage (§V), and ***4)*** realizing secure and privacy-preserving processing and computations on industrial data in the cloud (§VI).

In the following, we discuss each of these categories in more detail. Thereby, we survey for each category of approaches the state-of-the-art as well as promising emerging research directions. Furthermore, we identify open challenges that provide exciting potential for further research efforts.

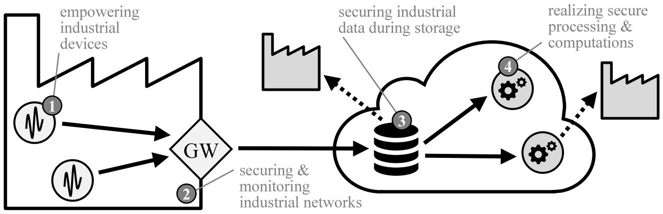
empowering industrial devices
securing industrial data during storage
realizing secure processing & computations
1
2
3
4
GW
securing & monitoring industrial networks

Fig. 1. Turning secure and privacy-preserving cloud-based industrial collaboration into reality requires technical approaches to 1) empower industrial devices, 2) secure and monitor industrial networks, 3) secure industrial data during storage, and 4) realize secure processing and computations.

III. Empowering Industrial Devices

Industrial devices often operate for decades and were often not designed with security and privacy functionality in mind [20], as, e.g., required to realize object and transport security for cloud-based industrial cooperation. Furthermore, these existing devices are often limited w.r.t. their computing, storage, and potentially energy resources, making it difficult to apply resource-expensive security functionality such as public-key cryptography [10]. We identify two approaches to still empower existing industrial devices to participate in secure and privacy-preserving cloud-based industrial collaboration: ***1)*** adapting security mechanisms and ***2)*** gateway support.

Adapting security mechanisms mainly aims at tailoring existing and well-proven security protocols and cryptographic primitives to the specifics of resource-constrained industrial devices [4]. For example, slightly adapting protocol encoding and pre-computing cryptographic operations allows resource-constrained devices to meet low-latency requirements of industrial settings while using transport security [21]. Especially when using public-key cryptography, careful selection of ciphers allows to reduce computation time and energy consumption. For example, elliptic curves reduce computation time and energy consumption for setting up transport security on resource-constrained devices by one order of magnitude compared to RSA [4], [22]. When two communication partners repeatedly have to establish security sessions, session resumption allows to omit public-key operations in successive connections establishments [4]. Especially in the context of cloud computing, session sharing additionally allows to resume security sessions across different industrial applications to further reduce overheads for establishing transport security [23].

Gateway support leverages the gateway device often used to connect industrial devices to the Internet and thus cloud services (cf. Figure 1) to reduce the overhead for individual devices [4]. For example, such a gateway can establish secure connections on behalf of a resource-constrained device or translate between different transport security protocols without losing end-to-end security properties [24]. Likewise, a gateway can apply fine-grained object security measures to data collected by industrial devices and manage access control, e.g., using public-key cryptography [25] (cf. §V).

Open Challenges: With increasing cooperation and coordination across companies, access control decisions eventually will have to be taken dynamically and automatically, increasing the burden put on industrial devices. Thus, further research is required for dealing with this increasing complexity, e.g., by securely offloading parts of access control to the cloud and further leveraging the capabilities of gateways [26]. Similar considerations hold in preparation for quantum technology, where it will likely become necessary to replace public-key ciphers with less storage and computation efficient ones as well as increase the key length for symmetric encryption [27]. Increasingly deploying security functionality furthermore comes with the challenge of having to ensure that security settings are configured correctly, especially for complex novel industrial protocols such as OPC UA [28].

IV. Securing & Monitoring Industrial Networks

Cloud-based industrial cooperation leads to increased communication of industrial devices with Internet hosts such as cloud services, potentially increasing attack surfaces. Consequently, we need mechanisms for ***1)*** securing industrial networks to prevent unauthorized communication and ***2)*** monitoring industrial networks to detect suspicious network activity.

Securing industrial networks aims at preventing unauthorized communication, e.g., between industrial devices or with unpermitted cloud services. Traditionally, to prevent unauthorized communication within industrial networks, these networks can be separated using demilitarized zones and virtual networks. Likewise, firewalls can be used to restrict communication, e.g., to blacklist communication with certain cloud services. However, such systems are typically configured manually during the setup of a network and cannot be adapted automatically during operation. To address this issue and provide support for dynamically changing security requirements, software-defined networking allows to quickly perform changes in the configuration of network separation, e.g., to enforce compliance with communication rules continuously updated by the operator of the industrial network [29].

Monitoring industrial networks allows to uncover suspicious activities, e.g., resulting from inadequately implemented security measures or exploitation of zero-day vulnerabilities. While intrusion detection is the standard approach to perform this task in traditional networks [30], applying it to industrial networks requires further work [31], e.g., to account for real-time requirements and resource constraints. Interestingly, the characteristics of industrial networks such as rather well-defined traffic that potentially influences the physical state of the controlled process also open new opportunities for intrusion detection: Process-aware intrusion detection also incorporates information on the industrial process and environment and thus is able to monitor compliance of transmitted data with physical constraints and safety requirements [20], [31], [32].

Open Challenges: Industrial cooperation significantly increases the dynamics of communication patterns in industrial networks. As such, further research is required to (semi-) automatically (little to no manual effort) derive allowed communication rules, e.g., which industrial devices are allowed to communicate with which cloud services, as well as process information such as physical constraints. Such anomaly detection approaches based on artificial intelligence or machine learning show huge potential, but come with their own challenges, especially with respect to the high costs associated with false classifications [33], [34]. Furthermore, with an increasing trend to secure communication within industrial networks (cf. §III), it remains open how monitoring approaches that rely on process information within communication payload can be enhanced to also operate on encrypted data.

V. Securing Industrial Data During Storage

To protect industrial data during storage in the cloud, the most prominent approach is object-level security for individual data items [4], [25]. For industrial cooperation, this entails ***1)*** encrypting industrial data and ***2)*** realizing access control.

Encrypting industrial data ensures that access to confidential industrial data is restricted to authorized parties. The main challenge of encryption in the context of industrial cooperation is the huge heterogeneity of industrial data, which originates from various sources and can thus be structured nearly arbitrarily [4]. To realize applicability of object security to various forms of industrial data, SenML [35] standardizes a unified representation of industrial data using JSON, CBOR, or XML. As SenML splits up data into individual data fields, it lays the basis for fine-grained object security to realize access control per data field or optionally keeping meta data unencrypted for efficient indexing [4]. Actual encryption of data fields is typically realized using symmetric encryption due to superior performance [25], [36]. Still, asymmetric encryption can provide more functionality, e.g., to directly process on encrypted data without prior decryption (cf. §VI).

Realizing access control then is a matter of providing all entities that should have access to specific data with the corresponding keying material [37]. Typical current approaches rely on an existing public-key infrastructure and separately encrypt keying material with the public key of each intended recipient, possibly periodically changing keying material to realize time-based access control [25]. More advanced approaches rely on attribute-based encryption where everyone assigned a certain cryptographic attribute can decrypt keying material [38], [39]. This allows to realize scenario where everyone who fulfills a certain property can access certain industrial data. Here, security depends on a trusted party which assigns attributes.

Open Challenges: To fully embrace the advantages of industrial cooperation, as many companies as possible have to participate, opposing the use of a single trusted public-key infrastructure and thus demanding for innovative approaches to access control. Additionally, further research is required on how to automatically assign attributes for attribute-based encryption at large scales when access control decisions have to be taken dynamically, e.g., in settings where industrial data itself is used to reveal who should cooperate with whom. When sharing data across industrial companies, one important challenge concerns safety considerations to ensure that externally acquired data, e.g., used to parameterize a production line, does not cause any harm to humans or machinery.

VI. Realizing Secure Processing & Computations

To remedy security and privacy concerns (cf. §II), one key aspect is to perform processing and computations on industrial data in the cloud such that the cloud provider cannot access the data. Two orthogonal approaches to achieve this goal are ***1)*** trusted hardware components and ***2)*** secure computations.

Trusted hardware components such as ARM TrustZones, Intel SGX, or TPM provide a hardware root of trust and can be used to ensure that the cloud provider cannot access otherwise encrypted data during processing. In the context of cloud computing, they can be used to realize storage and processing of confidential data in secure execution environments [40], perform trustworthy data analytics in which computing instructions and data remain secret [41], ensure confidentiality and integrity for third-party coordination services [42], and realize secure and privacy-preserving decentralized cloud services [43]. For cloud-based industrial cooperation, trusted hardware could be used to guarantee integrity and authenticity of measured industrial data provided by companies.

Secure computations in contrast realize a software-based approach for untrusted cloud services to directly operate on encrypted data [4]. They can be applied to protect computing instructions and data during execution on untrusted cloud infrastructure [36], perform de-duplication of encrypted data [44], securely outsource lookup operations on encrypted data [45], and support SQL queries over encrypted databases [46]. Considering cloud-based industrial cooperation, secure computations could, e.g., be used to securely realize privacy-preserving performance benchmarking, which would allow companies to compare their production output against competitors without the need to disclose confidential data. Likewise, secure computations provide the technical foundation to realize secure end-to-end sensing in supply chains [47].

Open Challenges: While certain use cases for cloud-based industrial cooperation can already be realized with sufficient efficiency today, further research is required to make secure computations *generally* applicable [48], especially considering limited storage and processing resources of industrial devices (cf. §III). Similar considerations hold regarding the use of trusted hardware components, which today often require industrial devices to perform costly verification operations locally. Again, when combining data from different industrial companies during processing, ensuring safety when using the computed results such as crowd-sourced parameter configurations in industrial processes is of paramount importance to prevent harm to humans and machinery.

VII. Conclusion

Cloud computing provides a promising foundation for industrial cooperation and thus realizing sought after improvements such as increases in product quality and profit margins. Still, realizing industrial cooperation using cloud computing further amplifies already existing concerns of industrial companies regarding the security and privacy of their confidential data and knowledge, negatively impacting adoption and acceptance of cloud-based industrial cooperation.

In this paper, we identified and discussed different aspects of secure and privacy-preserving cloud-based industrial cooperation to address these concerns. To this end, we presented approaches to empower resource-constrained industrial devices to perform security and privacy operations, secure and monitor industrial networks bearing increased cloud connectivity, realize secure cloud-based storage of industrial data, as well as perform secure and privacy-preserving processing and computations in the cloud. While different approaches to address these aspects already exist, we also identified open challenges that demand for further research in the intersection of cloud computing, industrial cooperation, and security/privacy. Thus, we make great strides forward in our quest to realize secure and privacy-preserving cloud-based industrial cooperation.

References

[1] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, “Industry 4.0,” *Business & Information Systems Engineering*, vol. 6, no. 4, 2014.

[2] J. Pennekamp, R. Glebke, M. Henze, T. Meisen, C. Quix, R. Hai, L. Gleim, P. Niemietz, M. Rudack, S. Knape, A. Epple, D. Trauth, U. Vroomen, T. Bergs, C. Brecher, A. Bührig-Polaczek, M. Jarke, and K. Wehrle, “Towards an Infrastructure Enabling the Internet of Production,” in *Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, 2019.

[3] R. Glebke, M. Henze, K. Wehrle, P. Niemietz, D. Trauth, P. Mattfeld, and T. Bergs, “A Case for Integrated Data Processing in Large-Scale Cyber-Physical Systems,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS)*, 2019.

[4] M. Henze, J. Hiller, R. Hummen, R. Matzutt, K. Wehrle, and J. H. Ziegeldorf, “Network Security and Privacy for Cyber-Physical Systems,” in *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications*, H. Song, G. A. Fink, and S. Jeschke, Eds. Wiley-IEEE Press, 2017.

[5] T. Stock and G. Seliger, “Opportunities of Sustainable Manufacturing in Industry 4.0,” in *Proceedings of the 13th Global Conference on Sustainable Manufacturing (GCSM)*, ser. Procedia CIRP, vol. 40, 2016.

[6] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. Hung Byers, “Big data: The next frontier for innovation, competition, and productivity,” McKinsey Global Institute, 2011.

[7] J. Pennekamp, M. Henze, S. Schmidt, P. Niemietz, M. Fey, D. Trauth, T. Bergs, C. Brecher, and K. Wehrle, “Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective,” in *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC)*, 2019.

[8] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and Privacy Challenges in Industrial Internet of Things,” in *Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015.

[9] J. Pennekamp, R. Matzutt, S. S. Kanhere, J. Hiller, and K. Wehrle, “The Road to Accountable and Dependable Manufacturing,” *Computer*, 2020.

[10] J. Hiller, J. Pennekamp, M. Dahlmanns, M. Henze, A. Panchenko, and K. Wehrle, “Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments,” in *Proceedings of the IEEE 27th International Conference on Network Protocols (ICNP)*, 2019.

[11] S. Pearson and A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing,” in *Proceedings of the IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, 2010.

[12] M. Henze, “Accounting for Privacy in the Cloud Computing Landscape,” Ph.D. dissertation, RWTH Aachen University, 2018.

[13] K. Liere-Netheler, S. Packmohr, and K. Vogelsang, “Drivers of Digital Transformation in Manufacturing,” in *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)*, 2018.

[14] C. Yin, J. Xi, R. Sun, and J. Wang, “Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, 2018.

[15] M. Henze, M. Großfengels, M. Koprowski, and K. Wehrle, "Towards Data Handling Requirements-aware Cloud Computing," in *Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2013.

[16] T. F. J.-M. Pasquier and J. E. Powles, "Expressing and Enforcing Location Requirements in the Cloud Using Information Flow Control," in *Proceedings of the 2015 IEEE International Conference on Cloud Engineering (IC2E)*, 2015.

[17] M. Henze, R. Matzutt, J. Hiller, E. Mühmer, J. H. Ziegeldorf, J. van der Giet, and K. Wehrle, "Practical Data Compliance for Cloud Storage," in *Proceedings of the 2017 IEEE International Conference on Cloud Engineering (IC2E)*, 2017.

[18] P. De Filippi and S. McCarthy, "Cloud Computing: Centralization and Data Sovereignty," *European Journal of Law and Technology*, vol. 3, no. 2, 2012.

[19] M. Henze, J. Pennekamp, D. Hellmanns, E. Mühmer, J. H. Ziegeldorf, A. Drichel, and K. Wehrle, "CloudAnalyzer: Uncovering the Cloud Usage of Mobile Apps," in *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, 2017.

[20] D. van der Velde, M. Henze, P. Kathmann, E. Wassermann, M. Andres, D. Bracht, R. Ernst, G. Hallak, B. Klaer, P. Linnartz, B. Meyer, S. Ofner, T. Pletzer, and R. Sethmann, "Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures," in *Proceedings of the 6th IEEE International Energy Conference (ENERGYCon)*, 2020.

[21] J. Hiller, M. Henze, M. Serror, E. Wagner, J. N. Richter, and K. Wehrle, "Secure Low Latency Communication for Constrained Industrial IoT Scenarios," in *Proceedings of the IEEE 43rd Conference on Local Computer Networks (LCN)*, 2018.

[22] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," in *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2005.

[23] J. Hiller, M. Henze, T. Zimmermann, O. Hohlfeld, and K. Wehrle, "The Case for Session Sharing: Relieving Clients from TLS Handshake Overheads," in *Proceedings of the IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium)*, 2019.

[24] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, 2015.

[25] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, "A Cloud Design for User-controlled Storage and Processing of Sensor Data," in *Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2012.

[26] M. Henze, B. Wolters, R. Matzutt, T. Zimmermann, and K. Wehrle, "Distributed Configuration, Authorization and Management in the Cloud-based Internet of Things," in *Proceedings of the 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2017.

[27] M. Kaiiali, S. Sezer, and A. Khalid, "Cloud Computing in the Quantum Era," in *Proceedings of the 5th IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2019.

[28] L. Roepert, M. Dahlmanns, I. B. Fink, J. Pennekamp, and M. Henze, "Assessing the Security of OPC UA Deployments," in *Proceedings of the 1st ITG Workshop on IT Security (ITSec)*, 2020.

[29] M. Serror, M. Henze, S. Hack, M. Schuba, and K. Wehrle, "Towards In-Network Security for Smart Homes," in *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES)*, 2018.

[30] L. Pham, M. Albanese, and S. Venkatesan, "A quantitative risk assessment framework for adaptive intrusion detection in the cloud," in *Proceedings of the 2nd IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.

[31] C. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, and X. Li, "Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, 2015.

[32] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel, "Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes," in *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*, 2014.

[33] M. Mantere, I. Uusitalo, M. Sailio, and S. Noponen, "Challenges of Machine Learning Based Monitoring for Industrial Control System Networks," in *Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2012.

[34] T. Cruz, J. Barrigas, J. Proença, A. Graziano, S. Panzieri, L. Lev, and P. Simões, "Improving Network Security Monitoring for Industrial Control Systems," in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2015.

[35] C. Jennings, Z. Shelby, J. Arkko, A. Keranen, and C. Bormann, "Sensor Measurement Lists (SenML)," RFC 8428, Internet Engineering Task Force, 2018.

[36] S. Bugiel, S. Nürnberger, A.-R. Sadeghi, and T. Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency," in *Proceedings of the 12th IFIP International Conference on Communications and Multimedia Security (CMS)*, 2011.

[37] P. Samarati and S. C. de Vimercati, "Access Control: Policies, Models, and Mechanisms," in *Proceedings of the International School on Foundations of Security Analysis and Design (FOSAD)*, 2000.

[38] J. Pennekamp, L. Bader, R. Matzutt, P. Niemietz, D. Trauth, M. Henze, T. Bergs, and K. Wehrle, "Private Multi-Hop Accountability for Supply Chains," in *Proceedings of the IEEE ICC Workshop on Blockchain for IoT and Cyber-Physical Systems (BIoTCPS)*, 2020.

[39] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," in *Proceedings of the 14th International Conference on Financial Cryptography and Data Security Workshops (FC Workshops)*, 2010.

[40] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," in *Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC)*, 2009.

[41] F. Schuster, M. Costa, C. Fournet, C. Gkantsidis, M. Peinado, G. Mainar-Ruiz, and M. Russinovich, "VC3: Trustworthy Data Analytics in the Cloud Using SGX," in *Proceedings of the 2015 IEEE Symposium on Security and Privacy (S&P)*, 2015.

[42] S. Brenner, C. Wulf, D. Goltzsche, N. Weichbrodt, M. Lorenz, C. Fetzer, P. Pietzuch, and R. Kapitza, "SecureKeeper: Confidential ZooKeeper using Intel SGX," in *Proceedings of the 17th International Middleware Conference (Middleware)*, 2016.

[43] M. Henze, J. Hiller, O. Hohlfeld, and K. Wehrle, "Moving Privacy-Sensitive Services from Public Clouds to Decentralized Private Clouds," in *Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshops (IC2EW)*, 2016.

[44] W. K. Ng, Y. Wen, and H. Zhu, "Private Data Deduplication Protocols in Cloud Storage," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing (SAC)*, 2012.

[45] J. H. Ziegeldorf, J. Pennekamp, D. Hellmanns, F. Schwinger, I. Kunze, M. Henze, J. Hiller, R. Matzutt, and K. Wehrle, "BLOOM: BLoom filter based oblivious outsourced matchings," *BMC Medical Genomics*, vol. 10, no. 2, 2017.

[46] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (SOSP)*, 2011.

[47] J. Pennekamp, F. Alder, R. Matzutt, J. T. Mühlberg, F. Piessens, and K. Wehrle, "Secure End-to-End Sensing in Supply Chains," in *Proceedings of the 5th International Workshop on Cyber-Physical Systems Security (CPS-Sec)*, 2020.

[48] J. H. Ziegeldorf, J. Metzke, M. Henze, and K. Wehrle, "Choose Wisely: A Comparison of Secure Two-Party Computation Frameworks," in *Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW)*, 2015.