frontiers | Frontiers in Computer Science

MINI REVIEW
published: 07 July 2022
doi: 10.3389/fcomp.2022.930741

Trusted Execution Environments: Applications and Organizational Challenges

Tim Geppert[1]*, *Stefan Deml*[2], *David Sturzenegger*[2] and *Nico Ebert*[1]

[1] School of Management and Law, Institute for Business Information Technology, ZHAW Zurich University of Applied Sciences, Winterthur, Switzerland, [2] dq technologies AG, Zurich, Switzerland

A lack of trust in the providers is still a major barrier to cloud computing adoption – especially when sensitive data is involved. While current privacy-enhancing technologies, such as homomorphic encryption, can increase security, they come with a considerable performance overhead. As an alternative Trusted Executing Environment (TEE) provides trust guarantees for code execution in the cloud similar to transport layer security for data transport or advanced encryption standard algorithms for data storage. Cloud infrastructure providers like Amazon, Google, and Microsoft introduced TEEs as part of their infrastructure offerings. This review will shed light on the different technological options of TEEs, as well as give insight into organizational issues regarding their usage.

Keywords: trusted execution environment, TEE, confidential computing, SGX, cloud computing

OPEN ACCESS

Edited by:
Zarina Shukur, National University of Malaysia, Malaysia

Reviewed by:
Maxime Puys, CEA LETI, France

***Correspondence:**
Tim Geppert
gepp@zhaw.ch

Specialty section:
This article was submitted to Computer Security, a section of the journal Frontiers in Computer Science

Received: *28 April 2022*
Accepted: *10 June 2022*
Published: *07 July 2022*

Citation:
Geppert T, Deml S, Sturzenegger D and Ebert N (2022) Trusted Execution Environments: Applications and Organizational Challenges. Front. Comput. Sci. 4:930741. doi: 10.3389/fcomp.2022.930741

INTRODUCTION

Over the last two decades, the adoption of cloud computing by organizations has increased steadily (Mell and Grance, 2011; Gartner, 2020). The economic and technological benefits of pay-as-you-go pricing and elasticity have resulted in outsourcing infrastructure to on-site and public cloud services (Hsu and Lin, 2016). As cloud computing systems are complex and draw on diverse technologies, gaining a sufficient understanding of how to secure such systems can be a significant challenge (Venters and Whitley, 2012; Fernandez et al., 2016). Furthermore, organizations that use cloud computing services have only weak guarantees (e.g., legal contracts) concerning the tamper resistance of hardware, the virtualization layer, the operating system, or the applications that may be executed (Kelbert et al., 2017). The EU General Data Protection Regulation (GDPR) has further increased the legal obligations of organizations and their cloud service providers when handling customer data (Russo et al., 2018). Therefore, the fear of losing control over the data processed by a cloud service provider remains a significant adoption barrier to outsourcing data processing (Senyo et al., 2018).

A trusted execution environment (TEE) is a new security technology that promises to mitigate attacks on cloud systems (Sehgal et al., 2020) and therefore lower the barriers to cloud computing adoption by organizations. TEEs use a hardware root of trust to enable data processing with fine-grained access control and protection of the executed code, runtime state, and memory of cloud systems (Birrell et al., 2018; Sehgal et al., 2020).

As processor manufacturers have already provided TEE capabilities for several years, large cloud providers have started to provide TEEs for their customers to provide additional security guarantees and ease the concerns about cloud computing. In 2019, industry participants, such as Intel, AMD, Microsoft, and Google, founded a new Linux foundation consortium, which coined the term "confidential computing" as an umbrella term for their TEE services (Rashid, 2020).

TRUSTED EXECUTION ENVIRONMENT

Security guarantees provided through the hardware have been a subject of discussion for over 20 years (Pearson and Balacheff, 2003). The early hardware-security modules were used to secure the BIOS and boot code but were not programmable and did not encrypt the computing process or protect the data (Garfinkel et al., 2003; Abera et al., 2016). TEEs overcome these shortcomings and are defined as "tamper-resistant processing environments that run on a separation kernel" (Sabt et al., 2015). Remote verification makes the technology suitable for cloud environments (Chen et al., 2019). It is a mechanism proving to an organization that uses the services of a cloud provider that the specified software runs on the predefined hardware even if the organization does not have direct access to this hardware.

As shown in **Figure 1**, there are two conceptually different TEE models for cloud computing (Mofrad et al., 2018). The virtual machine-based model dynamically encrypts the whole system memory of a virtual machine (Hetzelt and Buhren, 2017), and the process-based model provides only an encrypted memory area within the virtual machine (Zhang and Zhang, 2016). While all of an application's memory is encrypted by default in the virtual machine-based model, in the process-based model, the application developer must selectively decide which code to execute in the encrypted section and which calculations to perform in the unencrypted section of the system memory. In the process-based model, the encrypted part of the memory is also referred to as an "enclave."

Owing to its current popularity, we are providing a conceptual overview of the creation of a TEE and its validation for the process-based model. The hardware vendor (e.g., Intel) takes the certificate authority (CA) role, providing a private/public key pair for the unique hardware. The private key is embedded into the hardware during manufacturing ("root of trust"), while the public key is signed using the CA's private key, building a chain of trust back to the CA.

In the first phase, the TEE is created using platform-specific microcode instructions provided by the hardware (**Figure 2A**). In the first step of the TEE setup (**Figure 2A**, 1), a user-defined amount of system memory is encrypted using a symmetric encryption schema (Costan and Devadas, 2016) and is granted access to the private key embedded in the hardware. Therefore, this TEE is protected from the cloud service provider or any other adversary accessing the system (Sobchuk et al., 2018). Next, a part of the application is loaded into the encrypted memory of the TEE (**Figure 2A**, 2), and in the final stage of TEE creation, a unique identifier of the running TEE is calculated and reported back to the user of the TEE for later validation (**Figure 2A**, 3).

In the second phase, the TEE validation is conducted, which is required because the user who created the TEE in a cloud environment does not have access to the physical hardware. Therefore, it is necessary to verify that (i) the TEE was created on the vendor-provisioned hardware (as only this guarantees the integrity of the encryption) and (ii) the TEE contains the expected application code. Both requirements are solved by using a remote CA validation service (**Figure 2B**). In the first step, the user retrieves a certificate from the TEE (**Figure 2B**, 1). The certificate is then signed using the TEE sealed private validation key (see above) and contains the unique ID from the creation process, information about the specific application code executed within the TEE, and the underlying hardware. Next, the user can confirm that the TEE is running the anticipated application code by sending the certificate to the CA (**Figure 2B**, 2). Following successful validation (**Figure 2B**, 3), the user can execute the application code within the TEE with the prescribed security guarantees.

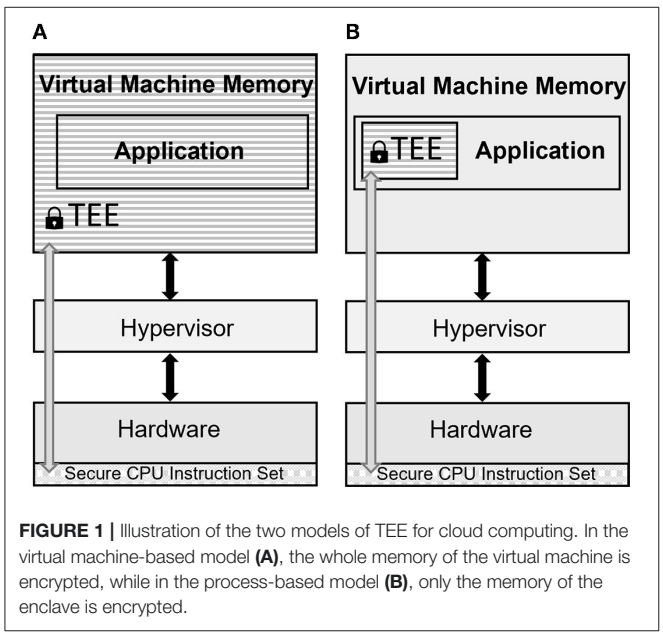

FIGURE 1 | Illustration of the two models of TEE for cloud computing. In the virtual machine-based model **(A)**, the whole memory of the virtual machine is encrypted, while in the process-based model **(B)**, only the memory of the enclave is encrypted.

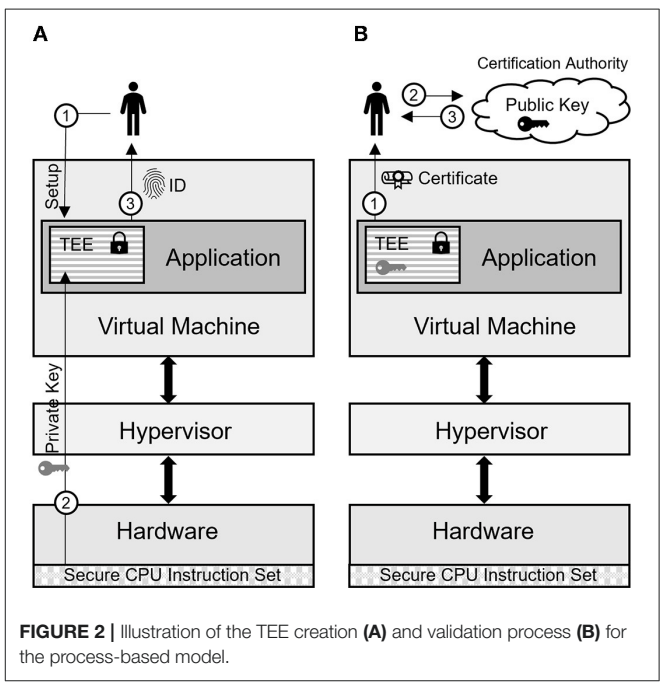

FIGURE 2 | Illustration of the TEE creation **(A)** and validation process **(B)** for the process-based model.

EXAMPLE APPLICATIONS OF TEE

Use cases for TEEs start evolving in the areas of cloud computing, the Internet of Things (IoT), multi-party computation (MPC), and artificial intelligence.

Cloud computing is currently the primary use case for TEEs. It is driven by features like pay-as-you-go pricing and dynamic scaling possibilities but also has to address the security and trust requirements of organizations (Coppolino et al., 2017). TEEs promise to add the same security properties to cloud computing that organizations are familiar with from on-premises environments (Barbosa et al., 2016). This shall allow using TEE-based cloud computing also in sensitive areas.

Trusted execution environments are also applied to support the IoT. Since IoT devices typically have low processing power, they send the collected sensor data to a central public cloud component. As these data can be highly sensitive, TEEs can improve the security guarantees of the processing cloud environment (Gremaud et al., 2017). Furthermore, the correct code must be executed in IoT scenarios where processing is already done within the IoT device (e.g., in automotive or healthcare applications). TEEs can be used on the device to protect the execution code and increase trust by attesting correctness to the backend system (Pettersen et al., 2017; Valadares et al., 2021).

Another TEE application domain is MPC. Collaborative work on private data sets by mutually distrusting parties—referred to as MPCs—often rely heavily on non-technical solutions such as trusted third parties or legal contracts. Data leakages or misuse within such setups are still possible. TEEs can increase the trust in collaborative work and provide a secure and efficient technical solution to MPC problems as an alternative or addition to current MPC solutions (Koeberl et al., 2015). In such MPCs, collaborative data analytics can be executed within the TEE. Each collaboration partner can validate the code executed within the TEE, provide raw input data, and collect the aggregated output data (Ohrimenko et al., 2016; Kaissis et al., 2020).

Artificial intelligence and privacy-preserving data mining are use cases for TEEs, too. Both approaches often rely on datasets, which have to be trustfully shared between domain and data modeling experts (Kaissis et al., 2020). Especially in the area of medical data, collaborations must take data confidentiality into account. Ohrimenko et al. described a machine learning protocol for collaborative data analytics using TEE (Ohrimenko et al., 2016). All involved organizations profit from the pooling of private datasets by training machine learning models on the aggregated data. Possible applications are the aggregation of disease diagnosis data from different hospitals and the pooling of customer attributes from complementary companies (Ohrimenko et al., 2016). In a study by Luo et al., a TEE-based system was developed, which can securely calculate the similarity of customer attributes. The system can be used to recommend potential friends within a social network while preserving data confidentiality (Luo et al., 2020). Another example is the Genie platform, which can be used to securely train AI models based on medical data. All data is uploaded into a TEE and within this security boundary used for training and statistical modeling (Zhang et al., 2020). As an alternative one can also use the TensorSCONE system, which integrates the TensorFlow library within a trusted execution environment using SCONE (Kunkel et al., 2019). It enables the training and usage of TensorFlow models for arbitrary AI tasks (Kunkel et al., 2019). In the case of machine learning, it is also important to protect the trained model, as it can give a competitive advantage. Ács and Coleşa designed a system for securely loading machine learning models within a TEE. They also provided a trusted web API for querying the loaded models (Ács and Coleşa, 2019).

ORGANIZATIONAL ISSUES REGARDING TEE ADOPTION

In the context of cloud computing, TEEs raises many questions. Most importantly, these are related to the role TEEs might play in the adoption of cloud computing by organizations. While academics currently focus on technical discussions regarding the security properties of TEEs (Nilsson et al., 2020), other aspects such as the organizational potential of TEEs or TEE governance are currently driven by a few prominent industry players. One example is the Confidential Computing Consortium, which focuses on accelerating TEE adoption and is an industry-driven governance project. In addition, rigorous empirical and theory-driven information systems (IS) research on TEE remains scarce but is necessary to understand the potential of the technology better and, most importantly, promote its organizational adoption (Gallivan, 2001).

From the ongoing technical discussion surrounding TEEs, it is evident there are several possible attack vectors undermining TEE security guarantees (Nilsson et al., 2020). These open gaps are being addressed by security researchers or vendors (Fei et al., 2021). These attacks rely on the assumption that the attacker has full control over the platform. Successful mitigations for these attacks implement additional security primitives to guard memory and I/O accesses (Chandra et al., 2017; Sasy et al., 2018). Remote attestation is another attack vector of TEEs. SGX uses an Intel service for attestation, which has been criticized within the literature as it puts Intel in a dominant position within the Confidential Computing space (Costan and Devadas, 2016). The attestation process can also leak sensitive information; for example, information about the signing party and the signed content (Sardar et al., 2020). In the case of a high number of attestations, it can also be an infrastructure bottleneck (Abera et al., 2016). Possible solutions are open attestation services, third-party attestation solutions, or attestation of groups (Scarlata et al., 2018; Chen et al., 2019). As security gains can be an important driver for the general adoption of security technologies (Herath et al., 2020), future research first needs to investigate TEE implementations by organizations to understand the real-world security and trust benefits of TEE.

This potential added security has also been discussed as a way of reducing sensitive data leakages and could therefore be an appropriate technology to address legal requirements when processing personal data in the cloud (e.g., GDPR or the California Consumer Privacy Act). These laws mandate

data protection by design and require that the level of security is appropriate to the risk (Singh et al., 2020). TEEs could potentially help organizations using cloud systems to process personal data in a way that not only enforces security through legal contracts between organizations and cloud service providers but also provides technical security measures controlled by the organization. However, this might not fundamentally change the legal nature of the relationship between organization and cloud service provider, as scholars have discerned no difference between processing personal data with TEEs and using traditional encryption mechanisms to protect personal data (Singh et al., 2020). Nevertheless, scholars conclude that TEEs can still help in "reducing the compliance barriers for cloud adoption" (Singh et al., 2020). Therefore, an organization that uses cloud systems may still benefit from the additional security of a cloud service provider that offers TEE-based services. The latter not only reduces the risk of data leakages but demonstrates compliance with tenants and auditors.

From an organizational perspective, compatibility with current systems is also essential for the further adoption of TEEs for cloud computing (Herath et al., 2020). While the currently popular process-based model requires existing applications that are supposed to run in the cloud to be partly rewritten for TEEs (Sobchuk et al., 2018), the virtual machine-based model does not need refactored applications and could be more readily adopted. The first research to improve the compatibility gap has been undertaken, and the Horizon 2020 project SecureCloud resulted in an abstraction layer on top of the process model to reduce refactoring needs (Kelbert et al., 2017). As a drawback of an abstraction layer, it was noted that an adversary or malware within a TEE cannot be detected by current standard security measures (Costan and Devadas, 2016). A solution for this problem is currently not known and is a topic for further research (Schwarz et al., 2019). Major hardware vendors are also focusing on closing the compatibility gap with current systems in their upcoming releases of AMD's Secure Nested Paging and Intel's Trusted Domain Extension. All these steps could improve the integration into existing IT landscapes. The situation will be further eased by the evolving ready-to-use cloud products offered by major providers like Microsoft, Amazon, and Google. However, Geppert et al. (2022) could show that organizations perceive a lack of knowledge regarding TEEs, which points to low organizational market readiness. The research community could therefore help to improve organizational understanding of TEEs.

OUTLOOK

Previous research on cloud computing has shown that privacy, security, and availability are crucial to organizations adopting this technology (Venters and Whitley, 2012). As TEE could improve the security and privacy of cloud computing, it is important to reevaluate previous research related to organizational cloud security risk and trust perception (Legner et al., 2017). Further research in this area could improve the understanding of TEE-based cloud adoption and how cloud providers use this technology as strategic signaling to assure product security and trust to customers. As a future managerial issue, IT organizations must evaluate where TEE gives additional value with regard to trust, security, and confidentiality and where its use is not justified. This future research must also consider performance overheads, added complexity, and post-adoption support by providers. To conclude, the current observation of this rapidly developing field suggests that TEE research may bear more fruit in years to come and could influence the cloud-adoption strategy of many organizations.

AUTHOR CONTRIBUTIONS

TG and NE conducted the scientific literature evaluation and writing. SD and DS provided technical insights. All authors contributed to the article and approved the submitted version.

FUNDING

The authors of this research paper were supported by Innosuisse, Grant Nr: 48335.1 IP-ICT. Open access funding provided by Zurich University of Applied Sciences (ZHAW).

REFERENCES

Abera, T., Asokan, N., Davi, L., Koushanfar, F., Paverd, A., Sadeghi, A.-R., et al. (2016). "Invited - things, trouble, trust: on building trust in IoT systems", in *Proceedings of the 53rd Annual Design Automation Conference* (New York, NY: Association for Computing Machinery), 1–6. doi: 10.1145/2897937.2905020

Ács, D., and Coleşa, A. (2019). "Securely Exposing Machine Learning Models to Web Clients using Intel SGX", in *2019 IEEE 15th International Conference on Intelligent Computer Communication and Processing (ICCP)* (Cluj-Napoca: IEEE), 161–168. doi: 10.1109/ICCP48234.2019.8959635

Barbosa, M., Portela, B., Scerri, G., and Warinschi, B. (2016). "Foundations of Hardware-Based Attested Computation and Application to SGX," in *2016 IEEE European Symposium on Security and Privacy (EuroSandP)*. p. 245–260. doi: 10.1109/EuroSP.2016.28

Birrell, E., Gjerdrum, A., van Renesse, R., Johansen, H., Johansen, D., and Schneider, F. B. (2018). SGX enforcement of use-based privacy. *Proc. 2018 Workshop Privacy Electronic Society – WPES.* 18, 155–167. doi: 10.1145/3267323.3268954

Chandra, S., Karande, V., Lin, Z., Khan, L., Kantarcioglu, M., and Thuraisingham, B. (2017). "Securing data analytics on sgx with randomization," in *Computer Security - ESORICS 2017*, eds S. N. Foley, D. Gollmann, and E. Snekkenes (Springer International Publishing), 352–369. doi: 10.1007/978-3-319-66402-6_21

Chen, G., Zhang, Y., and Lai, T.-H. (2019). "OPERA: open remote attestation for intel's secure enclaves," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London: ACM), 2317–2331. doi: 10.1145/3319535.3354220

Coppolino, L., D'Antonio, S., Mazzeo, G., and Romano, L. (2017). Cloud security: emerging threats and current solutions. *Comput. Electr. Eng.* 59, 126–140. doi: 10.1016/j.compeleceng.2016.03.004

Costan, V., and Devadas, S. (2016). *Intel SGX Explained. IACR Cryptol. ePrint Arch.* San Diego, CA: IACR.

Fei, S., Yan, Z., Ding, W., and Xie, H. (2021). Security vulnerabilities of SGX and countermeasures: a survey. *ACM Computing Surv.* 54, 1–36. doi: 10.1145/3456631

Fernandez, E. B., Monge, R., and Hashizume, K. (2016). Building a security reference architecture for cloud systems. *Requirem. Eng.* 21, 225–249. doi: 10.1007/s00766-014-0218-7

Gallivan, M. J. (2001). Organizational adoption and assimilation of complex technological innovations: development and application of a new framework. *ACM SIGMIS Database.* 32, 51–85. doi: 10.1145/506724.506729

Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., and Boneh, D. (2003). Terra: a virtual machine-based platform for trusted computing. *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles* (Boltan Landing, NY: ACM Press), 14. doi: 10.1145/945445.945464

Gartner (2020). *2020-11-17_Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3_ in 2020*. Available online at: https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020 (accessed November 17, 2020).

Geppert, T., Anderegg, J., Frei, L., Moeller, S., Deml, S., Sturzenegger, D., et al. (2022). "Overcoming cloud concerns with trusted execution environments? Exploring the organizational perception of a novel security technology in regulated swiss companies", in *Proceedings of the 55nd Hawaii International Conference on System Sciences* (Manoa, HI: Hamilton Library). doi: 10.24251/HICSS.2022.824

Gremaud, P., Durand, A., and Pasquier, J. (2017). "A secure, privacy-preserving IoT middleware using intel SGX", in *Proceedings of the Seventh International Conference on the Internet of Things - IoT'17*. p. 1–2. doi: 10.1145/3131542.3140258

Herath, T. C., Herath, H. S. B., and D'Arcy, J. (2020). Organizational adoption of information security solutions: an integrative lens based on innovation adoption and the technology- organization- environment framework. *ACM SIGMIS Database.* 51, 12–35. doi: 10.1145/3400043.3400046

Hetzelt, F., and Buhren, R. (2017). Security Analysis of Encrypted Virtual Machines. *ArXiv:1612.01119 [Cs]*. Available online at: http://arxiv.org/abs/1612.01119 (accessed October 02, 2020).

Hsu, C.-L., and Lin, J. C.-C. (2016). Factors affecting the adoption of cloud services in enterprises. *Inf Syst E-Bus Manag.* 14, 791–822. doi: 10.1007/s10257-015-0300-9

Kaissis, G. A., Makowski, M. R., Rückert, D., and Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. *Nat. Mach. Intell.* 2, 305–311. doi: 10.1038/s42256-020-0186-1

Kelbert, F., Gregor, F., Pires, R., Köpsell, S., Pasin, M., Havet, A., et al. (2017). SecureCloud: Secure big data processing in untrusted clouds. *DATE.* 2017, 282–285. doi: 10.23919/DATE.2017.7926999

Koeberl, P., Phegade, V., Rajan, A., Schneider, T., Schulz, S., and Zhdanova, M. (2015). "Time to rethink: trust brokerage using trusted execution environments", in *Trust and Trustworthy Computing,* Conti, M., Schunter, M., Askoxylakis, I. Springer International Publishing. p. 181–190. doi: 10.1007/978-3-319-22846-4_11

Kunkel, R., Quoc, D. L., Gregor, F., Arnautov, S., Bhatotia, P., and Fetzer, C. (2019). TensorSCONE: A Secure TensorFlow Framework using Intel SGX. *ArXiv:1902.04413 [Cs]*. Available online at: http://arxiv.org/abs/1902.04413

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., et al. (2017). Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. *Bus. Inf. Syst. Eng.* 59, 301–308. doi: 10.1007/s12599-017-0484-2

Luo, J., Yang, X., and Yi, X. (2020). "SGX-based Users Matching with Privacy Protection", *Proceedings of the Australasian Computer Science Week Multiconference*. p. 1–9. doi: 10.1145/3373017.3373021

Mell, P., and Grance, T. (2011). *The NIST Definition of Cloud Computing*. p. 7. doi: 10.6028/NIST.SP.800-145

Mofrad, S., Zhang, F., Lu, S., and Shi, W. (2018). A comparison study of intel SGX and AMD memory encryption technology. *Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy*. p. 1–8. doi: 10.1145/3214292.3214301

Nilsson, A., Bideh, P. N., and Brorsson, J. (2020). *A Survey of Published Attacks on Intel SGX*. Lund University. p. 12.

Ohrimenko, O., Schuster, F., Fournet, C., Mehta, A., Nowozin, S., Vaswani, K., et al. (2016). Oblivious Multi-Party Machine Learning on Trusted Processors. *Proceedings of the 25th USENIX Security Symposium*. Austin, TX: 25th USENIX Security Symposium.

Pearson, S., and Balacheff, B. (2003). *Trusted Computing Platforms: TCPA Technology in Context*. Prentice Hall Professional.

Pettersen, R., Johansen, H. D., and Johansen, D. (2017). Secure Edge Computing with ARM TrustZone. *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security* (Porto: Science and Technology Publications), 102–109. doi: 10.5220/0006308601020109

Rashid, F. Y. (2020). The rise of confidential computing: Big tech companies are adopting a new security model to protect data while it's in use - [News]. *IEEE Spectrum*. 57, 8–9. doi: 10.1109/MSPEC.2020.9099920

Russo, B., Valle, L., Bonzagni, G., Locatello, D., Pancaldi, M., and Tosi, D. (2018). Cloud computing and the new EU general data protection regulation. *IEEE Cloud Computing*. 5, 58–68. doi: 10.1109/MCC.2018.064181121

Sabt, M., Achemlal, M., and Bouabdallah, A. (2015). Trusted execution environment: what it is, and what it is not. *2015 IEEE Trustcom/BigDataSE/ISPA*. 1, 57–64. doi: 10.1109/Trustcom.2015.357

Sardar, M. U., Quoc, D. L., and Fetzer, C. (2020). "Towards formalization of enhanced privacy ID (EPID)-based remote attestation in intel SGX.," *2020 23rd Euromicro Conference on Digital System Design (DSD)*. p. 604–607. doi: 10.1109/DSD51259.2020.00099

Sasy, S., Gorbunov, S., and Fletcher, C. W. (2018). *ZeroTrace: Oblivious Memory Primitives from Intel SGX. Proceedings 2018 Network and Distributed System Security Symposium.* San Diego, CA: Network and Distributed System Security Symposium. doi: 10.14722/ndss.2018.23239

Scarlata, V., Johnson, S., Beaney, J., and Zmijewski, P. (2018). *Supporting Third Party Attestation for Intel® SGX with Intel® Data Center Attestation Primitives* Santa Clara, CA: Intel Corporation.

Schwarz, M., Weiser, S., and Gruss, D. (2019). "Practical Enclave Malware with Intel SGX", in *Detection of Intrusions and Malware, and Vulnerability Assessment,* Perdisci, R., Maurice, C., Giacinto, G., Almgren, M. (eds). Springer International Publishing. p. 177–196. doi: 10.1007/978-3-030-22038-9_9

Sehgal, N. K., Bhatt, P. C. P., and Acken, J. M. (2020). "Future trends in cloud computing", in *Cloud Computing with Security,* Sehgal, N. K., Bhatt, P. C. P., Acken, J. M. Springer International Publishing. p. 235–259. doi: 10.1007/978-3-030-24612-9_13

Senyo, P. K., Addae, E., and Boateng, R. (2018). Cloud computing research: a review of research themes, frameworks, methods and future research directions. *Int. J. Informat. Manag.* 38, 128–139. doi: 10.1016/j.ijinfomgt.2017.07.007

Singh, J., Cobbe, J., Quoc, D. L., and Tarkhani, Z. (2020). Enclaves in the clouds: legal considerations and broader implications. *Queue*. 18, 78–114. doi: 10.1145/3442632.3448126

Sobchuk, J., O'Melia, S., Utin, D., and Khazan, R. (2018). "Leveraging Intel SGX Technology to Protect Security-Sensitive Applications", *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)* (Cambridge, MA: IEEE), 1–5. doi: 10.1109/NCA.2018.8548184

Valadares, D. C. G., Will, N. C., Caminha, J., Perkusich, M. B., Perkusich, A., and Gorgônio, K. C. (2021). Systematic literature review on the use of trusted execution environments to protect cloud/fog-based internet of things applications. *IEEE Access*. p. 1–1. doi: 10.1109/ACCESS.2021.3085524

Venters, W., and Whitley, E. A. (2012). A critical review of cloud computing: Researching desires and realities. *J. Informat. Technol.* 27, 179–197. doi: 10.1057/jit.2012.17

Zhang, F., and Zhang, H. (2016). "SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security", *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016 on - HASP 2016*. p. 1–8. doi: 10.1145/2948618.2948621

Zhang, S., Kim, A., Liu, D., Nuckchady, S. C., Huang, L., Masurkar, A., et al. (2020). Genie: A secure, transparent sharing and services platform for genetic and health data. *arXiv [Preprint]*. arXiv:1811.01431. Available online at: http://arxiv.org/abs/1811.01431

Conflict of Interest: SD and DS are employed by dq technologies AG.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.