Privacy Preserving Multi Party Computation for Data-Analytics in the IoT-Fog-Cloud Ecosystem

Julio Lopez-Fenner, Samuel Sepulveda, Luiz Fernando Bittencourt, Fabio Moreira Costa, Nikolaos Georgantas

Privacy Preserving Multi Party Computation for Data-Analytics in the IoT-Fog-Cloud Ecosystem

Julio Lopez-Fenner[1], Samuel Sepúlveda[1], Luiz Fernando Bittencourt[2], Fabio Moreira Costa[3], and Nikolaos Georgantas[4]

[1] Departamento de Ciencias de la Computación e Informática,
Centro de Estudios en Ingeniería de Software
Universidad de La Frontera, Temuco, Chile
{julio.lopez, samuel.sepulveda}@ufrontera.cl
[2] Universidade Estadual de Campinas (UNICAMP), Brasil
bit@ic.unicamp.br
[3] Universidade Federal de Goiás, Brasil
[4] Inria Paris, France

Abstract. In this paper, we propose an architecture for privacy preserving protocols in an IoT-Fog-Cloud ecosystem computing hierarchy. We consider the paradigms of Fog and Edge computing, together with a multi-party computation mechanism that enables secure privacy-preserving data processing in terms of exchanged messages and distributed computing. We discuss the potential use of such an architecture in a scenario of pandemics where social distancing monitoring and privacy are pivotal to manage public health yet providing confidence to citizens.

Keywords: Secure Multi Party Computation · Internet of Things · Edge/Fog computing · Security and Trust

1 Introduction

The Internet of Things (IoT) is bringing countless ways of collecting and processing data as more and more smart devices and sensors (IoT devices, for short) are deployed and connected to the Internet.

IoT devices are scattered at the edge of the network. They produce vast amounts of heterogeneous data that does not generate value by itself by uploading it to a - say - database [28] but needs computing power to be either further processed in order to generate a desired output or to produce an immediate response for a data query, may be even to produce intermediate data results that need to be further acquired or with higher levels of processing.

Examples of these requirements can be easily found in smart agriculture domains [9], healthcare, industry and energy, transportation, and urban infrastructures, to name a few [23,22].

In this context, privacy concerns upon data being transmitted to and from the cloud arise naturally, as IoT devices and their data constitutes major targets

for security and privacy attacks, including data breaching, data integrity, and data collusion [35]. Moreover, very often the data collected - if leaked and not protected by suitable encryption - can breach the user's privacy and be used for non authorized virtual profiling [14].

On the other hand, however, data collected from IoT devices can also be used for the common good and social profitability, as knowledge gathered from those data sets can help in improving people's quality of life, for example, by offering personalised services, precise and up-to-date information about people's surroundings and interests, and information for improving planning and efficiency of cities as well as for policy making [38]. Therefore, there is ample need for the design and implementation of mechanisms for both, enabling and preserving privacy that still allows significant IoT data to be collected, distributed, and processed in a useful manner.

Currently, cloud computing has been used to store and process data collected by IoT devices. This well-established computing paradigm is very convenient for data processing applications that require large processing capacity, and it fits well to computing problems that use data collected from many sources regardless of their location. However, as IoT devices are located and scattered at the very edge of the network, they can easily be brought to consuming data from neighbouring counterparts, which then would not require further transfer to a centralised cloud for processing [40]. In this scenario, Fog Computing [13] has emerged to bring and distribute computing capacities closer to the edge. In this computing paradigm, micro data centres, or cloudlets, are deployed throughout the network (e.g. at access points or cellular base stations) to bring computing capacities closer to the IoT devices. Combined, all three layers of edge IoT devices, fog devices, and cloud computing, can provide a hierarchical ubiquitous-like infrastructure for processing IoT data. Notwithstanding, privacy concerns are still present in this scenario and should be addressed. Computational models for SMPC that fit the proposed hierarchical structure in terms of resource allocation need to ensure the privacy of individual users (parties) [17].

In order to present our approach, we introduce next some concepts and discuss challenges in the study of the three components of the IoT-Fog-Cloud ecosystem with regard to privacy preserving algorithms and protocols considering secure multi-party interactions. Then, in section 3 we introduce our proposed architecture and discuss its instantiation. Section 4 presents preliminary results towards such an architecture implementation and in section 5 we discuss some available literature on these topics. Section 6 brings conclusions and remarks.

2 Background

2.1 IoT-Fog-Cloud ecosystem

The Internet of Things (IoT) consists of 'zillions' of (inter-) connected devices that can include sensors/actuators with communication capabilities, i.e., virtually any object with embedded micro-controller and antennae, which can be

highly heterogeneous at different levels, as for example energy consumption requirements, communications protocols, computing capacity, and mobility.

Therefore, IoT devices management becomes intrinsically challenging in terms of data communication and processing, while it requires significant processing and knowledge extraction capabilities in order to provide relevant insight and, hence, constitutes an ideal field for developing and testing of Big Data tools. The challenge is precisely to transform gathered data into actual information knowledge by (secure) privacy-preserving processing. Examples of data collected by IoT devices with such requirements are: location-based services, security cameras, personalised preference tracking mechanisms (e.g. for advertisement), medical data collected by body sensors or by professional equipment at hospitals and clinics, see for example [30].

Cloud computing represents nowadays a largely adopted computing paradigm servicing a variety of applications, providing dynamic configuration possibilities such as elasticity and pay-per-use. Resource virtualization allows providers to share slices of computing resources among users through the use of virtual machines and containers, where they appear to be logically isolated for each tenant. On-demand provisioning/de-provisioning, elasticity, ubiquitous access, lower upfront investments with reduced capital expenditures and faster time to market, are a few properties offered by cloud computing.

Clouds can partially fulfil applications requirements for IoT but may fall short for low latency, for example. Fog computing can be combined with the cloud to provide an ecosystem that furnishes full potential for IoT application deployments, as it introduces a hierarchy of computing capacity (fog nodes, cloudlets or micro data centres) between the edge and the cloud [13]. This hierarchy can provide a wider range of services that may not be supported solely by the cloud. Thus, a fog computing infrastructure can attend applications with a variety of Quality of Services (QoS) by using different hierarchical levels to meet latency and computing requirements.

A consequence of bringing processing closer to the edge with fog computing, as illustrated in Figure 1, is to reduce total bandwidth used in the network along the path between edge and cloud, as data can be aggregated at the edge before being transferred to the cloud. This computing hierarchy provided by the IoT-Fog-Cloud ecosystem enables thus processing to occur closer to where the data is being generated. This is useful for applications that depend upon very low delays or response times, but also for applications that only need data from constrained or specific geographic locations, as in this scenario the data does not need to be transferred all the way up to the cloud. Such a scenario demands the implementation of privacy-preserving mechanisms so that data shared from said IoT devices are not unintentionally available to third-parties.

Examples of such applications include real-time traffic estimation, autonomous cars traffic control, collision avoidance in non-signalised road intersections, localisation-based risk assessment, monitoring in disaster scenarios, actuators in dynamically changing environments, and so on.

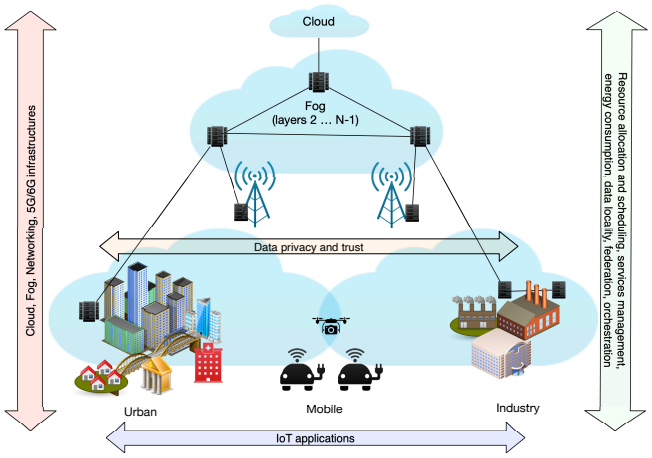

Fig. 1: Overview of the IoT-Fog-Cloud infrastructure (adapted from [4]).

We are interested in the modelling and design of efficient processing data protocols for applications in a privacy-preserving context. We posit that Secure Multi-Party Computation (SMPC) [16,19], understood as the joint computation of a desired function in terms of an appropriate splitting and distribution among a number of parties under the constraint that all data has to remain private, naturally furnishes a setting for privacy-preserving data processing and correctness:

- Privacy, in the sense that no party learns anything new other than its prescribed jointly computed output; and
- correctness, in the sense that parties can trust that the computed quantities are indeed correct.

This is useful, e.g., for the distributed evaluation of trust, as in [7], where parties or players compute a joint confidence level by combining their mutual degrees of trust. See the survey in [39] (and the references therein) for a nice description of the role of SMPC in the IoT field.

In view of potential applications, technologies should also consider, at least, designs providing Confidentiality, Integrity and Availability (CIA triad) [21]. Other requirements may be further imposed, for example on the side of independence of inputs, fairness, etc. (see [16]).

2.2 Privacy preservation in the IoT

Secure multiparty computations (SMPC) allows n players to compute together the output of some function, using private inputs without revealing them to other parties and without gaining access to knowledge entrusted to another party. This is useful, e.g., for distributed evaluation of trust. In this context, players compute a confidence level by combining their mutual degrees of trust. See for example

the survey in [39] (and the references therein) for a nice description of the role of SMPC in the IoT field.

Notice that while SMPC protocols have been present in the literature for more than thirty years, their application to a data streams in a hierarchy of IoT devices (in terms of computational power), which are continuously producing data worth analysing while preserving privacy, can be considered as a relatively recent development [15], in contrast to the more typical reception, storage and analysis of source data by a third-party centralised server that is not under the administrative control of the smart environment and hence potentially untrustworthy.

In the proposed architecture, the server should not obtain access to the raw data of the sources; it only fulfils management and orchestration purposes to carry out SMPC computations that are executed by the sources themselves [19]. This enables privacy-preserving data processing while the sources can be dynamic. The role of an edge-IoT gateway, understood as middle-ware between IoT devices and the cloud that facilitates computations and is a communication gateway as well [25], may be further extended to be able to receive queries regarding the outcomes of the computations still without revealing any private information about the sources.

Performance and resource consumption characteristics of SMPC methods are key limitations for their application in resource constrained environments. A detailed assessment of these characteristics is carried out in [20]. The authors reach the conclusion that SMPC methods can be applied, in practice, in Intranet environments, but with limitations in Internet settings. This shows the need for new SMPC-based solutions where the resource environment performs in close collaboration with privacy-preserving mechanisms.

3 Privacy towards the Edge

This section describes an overview for the proposed privacy-preserving multi-party computation architecture for IoT using fog computing.

3.1 Hypotheses and Objectives

In order to develop a framework of theoretical nature and a test pilot for the hierarchical architecture in layers: from IoT to Edge and from Edge to Fog computing, in which multi party protocols can be proposed, we first consider current techniques and methods for Fog/Edge technologies and Multi party computations.

Since cloud computing cannot rely exclusively upon cryptographic protocols alone [37] and, furthermore, the data collected by cyber-physical (IoT) sensors is known to be securely (and privately) processed using zero-knowledge proofs, as in [12], we propose to undertake our approach of Privacy Preserving Multi Party Computation for Data Analytic in the Iot-Edge-Fog ecosystem by first establishing a hierarchy of devices, as in Figure 2 and then to follow the lines proposed by [33] and [24].

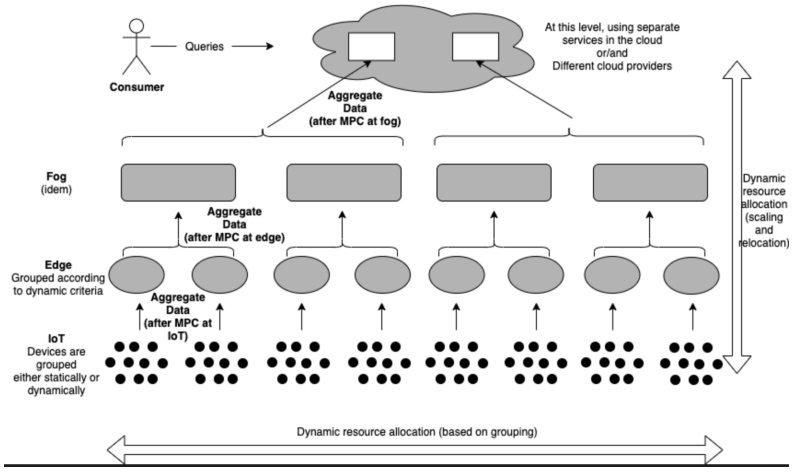

Fig. 2: Edge/Fog Computing hierarchy together with secure multi-party computation brings resource allocation challenges.

3.2 Architectural Principles

At the edge, we propose that IoT devices are grouped, either statically or dynamically, to be considered as data generators for a specific application or user query. Grouping is based on criteria such as resource allocation (at the fog), scalability and geographic location. These devices are assumed to be capable of executing SMPC in the context of the group which they currently belong to. The output of such computation may either be used immediately, to answer localised queries posed by users/consumers, or sent up (to services running in the same or a different micro-datacenter in the fog) as intermediate outputs that in turn are used in conjunction with outputs from other SMPC computations performed by other IoT device groups. This pattern of dynamically grouping SMPC parties that receive inputs from SMPC groups located underneath in the hierarchy repeats at the fog and cloud levels to produce intermediate outputs and/or to answer user queries.

To illustrate how this works, we consider the current pandemic scenario: Consider an end-user who is willing to know how safe it is to go to a specific place. Assume we can come up with a safety metric based on several pieces of information from the neighbourhood and/or place where this user is willing to go. A combination of data from IoT devices at the location of interest can be used to compute such safety metric and respond to the user query. However, it is clear that such information can often include personal data that raises privacy concerns, as for example medical conditions of people in that area, real-time and accurate information about people's location, data on how those people interact or have interacted on that location, information collected from cameras about the amount of people wearing masks, and so on. A privacy-preserving mechanism using multi-party computation would need to first choose sources to obtain all

that data to be processed, and this is an example of how devices are to be grouped into sets that are able to generate data in response to a query. Then, the data set obtained from those devices can be first processed using multi-party computation protocols, and then be further moved to the closest cloudlet/micro data center at the fog level for further processing. With privacy already in place, it remains to aggregate the data and compute the necessary safety metrics of interest to that query.

Note that more complex scenarios, with more data or data from multiple geographic locations, can involve multiple cloudlets at the fog level or even involve the cloud to provide enough capacity or enough data sets to allow a proper computation of the desired metric.

To enable SMPC in the discussed scenario, many challenges arise. First, a candidate set of SMPC protocols must be identified, studied, and potentially adapted for the proposed infrastructure. Second, the composition of IoT device groups should be enabled by distributed computing mechanisms. Third, once these groups have been defined for a specific application or query, data processing should occur in an efficient manner throughout the system through proper resource allocation and scheduling mechanisms.

3.3 Architecture Instantiation

It is known that effective mechanisms addressing stacked fog layers (cloudlets) constitutes still a challenge and open issue [4], since a universal standard of multi-layered fog computing architecture has not yet been adopted. We address this issue by considering data privacy aspects as inherent to a multi-layered fog architecture, in which resource allocation mechanisms are needed to efficiently process privacy-sensitive information.

Indeed, Fog computing technology enables the deployment of cloud-like computing services at the edge of the network. Fog-aware mechanisms and procedures to implement efficient resource management for applications with different levels of latency requirements remains a non trivial challenge [18]. Several efforts have addressed this body of work to provide a latency-driven fog computing environment for IoT applications using only one fog layer (i.e. *cloudlets*, *micro data centres*, or *fog nodes*) between the edge and the cloud (as illustrated in the proposed fog-cloud topology in Figure 1) [32,3,34,26].

Next, it is common knowledge that some architectures [27] for IoT assume that infrastructural elements in fog and edges are trusted entities. Thus, to preserve data privacy, those architectures may adopt data randomisation techniques such as differential privacy [8] based on a trust curator model [29]. But, in a complete untrustworthy component model, which is at the centre of our considerations, infrastructural components are not necessarily assumed to be trusted entities, so they should not access sensible data. We propose hence that our model should adopt techniques of secure multi-party computation to preserve data privacy.

Adoption of these techniques will have a direct impact on resource usage adequacy for IoT, in terms of processing power and exchanged messages among

devices. In particular, they produce a huge increase in both the length and the number of messages, so they should be adapted to large-scale scenarios with IoT.

Finally, for the deployment of these protocols, end-to-end automated systems for deploying large-scale SMPC protocols between end users, called MPSaaS (acronym for system-as-a-service) have been designed and tested [2].

4 Preliminary Results and Discussion

In the field of smart homes with IoT, secure communications between smart devices endowed with low computational capabilities and a home gateway are frequently established via unsecured wireless communication channels. In [5] we explored secure data transfer generated by IoT using standard Diffie-Hellman secret sharing which can be applied via buffering to higher throughput communications. Our assumptions were that at setup both the user and the gateway have enough processing power to perform - say - one time secured RSA encrypted communication, hence relaxing the need for a trusted secure server outside the domain, and that the protocol should at least be secure for a range of known attacks, as replay or DoS attacks. In turn, the approach failed impersonation attacks via Man in the Middle (MiM) so that a possible way out may lie in the implementation of SMPC as proposed in the architecture proposed here, since authentication would require a consensus (for example defined using Shamir's secret schem) to be build upon trusted devices. Hence, as mentioned above, joint computation of trust among parties can be performed by matrix multiplication, as in [6], where we proposed an *ad hoc* Strassen-Winograd multiplication protocol that use a combination of partial homomorphic encryption schemes and additive masking techniques together with a (novel) schedule for the location and encryption layout of all intermediate computations, such that privacy is preserved. It turned out that the asymptotic communication volume and computational time was reduced from $O(n^3)$ to $O(n^{2.81})$.

Thus, the main challenge now is to incorporate the developed protocols to the proposed computing hierarchy. This involves the prior study of performance of devices from the edge to the cloud to evaluate the possible ways of allocating resources for protocol processing and also assess communication costs. As a second step, evaluating the performance of the protocols in a real-world scenario, considering requirements as the amount of data inputs and needed response time (e.g. in the pandemics scenario described in Section 3), is key for establishing limitations and pinpoint where research must be focused to enable performance-effective multiparty computation at the edge.

This involves developing optimization algorithms for dynamic grouping or clustering, as presented in Figure 2, which should consider multiparty computation aspects both in terms of privacy and response times: a too large set of IoT devices may impair performance for response time, while a too small set may result in poor output for the application requiring data collection and processing.

5 Related work

A set of requirements for privacy preservation mechanisms in the context of distributed and ubiquitous environments, such as in the IoT, was presented in [1]. Among those requirements, they highlight the importance of ensuring privacy of the outputs of SMPC, which may be as important as the privacy of the inputs (as normally targeted in SMPC approaches), since data profiling might be used to de-anonymize the inputs or obtain sensitive information about the parties.

We address this issue to some extent, as the outputs at a lower level of the hierarchy are handled as inputs to the immediate upper level, and thus are subject to the usual privacy requirement. It remains to assess the effects of such privacy handling in relation to the use of the intermediate outputs for answering localised queries in a multi-layered fog architecture.

Some architectures for IoT assume that infrastructural elements in fog and edges are trusted entities [27]. Thus, to preserve data privacy, those architectures adopt data anonymization techniques such as differential privacy [8] based on a trust curator model [29]. In an untrusted component model, which is the center of this proposal, infrastructural components are not assumed as trusted entities so they should not access sensible data. This model usually adopts techniques of secure multi-party computation to preserve data privacy.

In IoT, the adoption of those techniques differs in terms of the mechanism for privacy preservation, resource usage adequacy and the architectural-style for IoT platforms. The mechanisms for privacy preservation vary from differential privacy [8], homomorphic encryption (partial or full) [10] and secure multi-party computation. Adoption of those techniques have a direct impact on resource usage adequacy for IoT, but also in terms of requirements of processing power and exchanged messages among devices. In particular, they produce a huge increase in the length and number of messages, so they should be adapted (e.g. [2]) to be applied in large-scale scenarios of IoT. Section 2.2 above discusses relevant approaches for privacy preservation in the IoT.

The architectural-style of an IoT platform may be exploited to satisfy resource limitations (e.g., processing power) or to decrease the number of disseminated messages, by transferring processing from devices or servers to intermediary components. Approaches of privacy preservation for IoT assume architectures such as cloud-based [2] platforms, mixed-mesh [36] networks, edge networks [11], fog [31], and mixed architectures with trusted entities [1]. In particular, fog and edge-fog architectures allow multiple levels of processing and they are more adaptable to the dynamicity and diversity of IoT devices. We hypothesize that fog-edge architectures allow the development of efficient privacy preservation techniques, in terms of exchanged messages and distributed processing power.

6 Conclusions and future work

This work presented the main concepts and initial findings about the design and evaluation of privacy preserving protocols in an IoT-Fog-Cloud ecosystem

computing hierarchy. We briefly discussed how this can be applied in a scenario as the present times of pandemics, but also covered general aspects that need attention for a generalized application of privacy-preserving mechanisms at the edge of the network.

We considered the paradigms of Fog and Edge computing, together with a multi-party computation mechanism to enable secure privacy-preserving data processing at the edge. The proposed architecture demands further developments in terms of understanding performance limitations and also in terms of resource allocation for data collection and processing of multiparty computation protocols, which can be the focus for further research. Also, the formalization of the proposal, with the modeling of inputs and outputs for multiparty computation at the edge, is a key future work to enable proper evaluation of efficiency and limitations of the proposal.

Acknowledgments

This work was partially funded by the São Paulo Research Foundation (FAPESP), grants #2018/23126-3 and #2015/24494-8, CAPES, and CNPq, Brazil, grants 432943/2018-8 and 309562/2019-8. Partial support from Universidad de La Frontera, Vicerrectoría de Investigación grant DI20-0060 is also acknowledged.

References

1. Ankele, R., Küçük, K.A., Martin, A., Simpson, A., Paverd, A.: Applying the trustworthy remote entity to privacy-preserving multiparty computation: Requirements and criteria for large-scale applications. In: 2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld). pp. 414–422 (2016)
2. Barak, A., Hirt, M., Koskas, L., Lindell, Y.: An end-to-end system for large scale p2p mpc-as-a-service and low-bandwidth mpc for weak participants. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 695–712 (2018)
3. Bittencourt, L., Diaz-Montes, J., Buyya, R., Rana, O., Parashar, M.: Mobility-Aware Application Scheduling in Fog Computing. IEEE Cloud Computing **4**(2), 26–35 (March 2017)
4. Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., Villas, L., DaSilva, L., Lee, C., Rana, O.: The internet of things, fog and cloud continuum: Integration and challenges. Internet of Things **3-4**, 134 – 155 (2018), `http://www.sciencedirect.com/science/article/pii/S2542660518300635`
5. Díaz Arancibia, J., Ferrari Smith, V., López Fenner, J.: On-The-Fly Diffie-Hellman for IoT. In: 2019 38th International Conference of the Chilean Computer Science Society (SCCC). pp. 1–5. IEEE (2019)
6. Dumas, J.G., Lafourcade, P., Lopez Fenner, J., Lucas, D., Orfila, J.B., Pernet, C., Puys, M.: Secure multiparty matrix multiplication based on strassen-winograd algorithm. In: International Workshop on Security. pp. 67–88. Springer (2019)

7. Dumas, J.G., Lafourcade, P., Orfila, J.B., Puys, M.: Dual protocols for private multi-party matrix multiplication and trust computations. Computers & security **71**, 51–70 (2017)
8. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Halevi, S., Rabin, T. (eds.) Theory of Cryptography. pp. 265–284. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
9. Elijah, O., Rahman, T.A., Orikumhi, I., Leow, C.Y., Hindia, M.N.: An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges. IEEE Internet of Things Journal **5**(5), 3758–3773 (2018)
10. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. p. 169–178. STOC '09, Association for Computing Machinery, New York, NY, USA (2009)
11. Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C., Tan, K.L.: Private queries in location based services: Anonymizers are not necessary. In: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data. p. 121–132. SIGMOD '08, Association for Computing Machinery, New York, NY, USA (2008)
12. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM Journal on computing **18**(1), 186–208 (1989)
13. Group, O.C.A.W., et al.: Openfog reference architecture for fog computing. OPFRA001 **20817**, 162 (2017)
14. Hossain, E., Khan, I., Un-Noor, F., Sikander, S.S., Sunny, M.S.H.: Application of big data and machine learning in smart grid, and associated security concerns: A review. IEEE Access **7**, 13960–13988 (2019)
15. Kerschbaum, F.: Privacy-preserving computation. In: Annual Privacy Forum. pp. 41–54. Springer (2012)
16. Lindell, Y.: Secure multiparty computation for privacy preserving data mining. In: Encyclopedia of Data Warehousing and Mining, pp. 1005–1009. IGI Global (2005)
17. Liu, W., Luo, S.s., Wang, Y.b., Jiang, Z.t.: A protocol of secure multi-party multi-data ranking and its application in privacy preserving sequential pattern mining. In: 2011 Fourth International Joint Conference on Computational Sciences and Optimization. pp. 272–275. IEEE (2011)
18. Mahmud, R., Ramamohanarao, K., Buyya, R.: Latency-Aware Application Module Management for Fog Computing Environments. ACM Trans. Internet Technol. **19**(1), 9:1–9:21 (Nov 2018)
19. von Maltitz, M., Bitzer, D., Carle, G.: Data Querying and Access Control for Secure Multiparty Computation . In: 2019 IFIP/IEEE International Symposium on Integrated Network Management. Washington, DC, USA (2019)
20. von Maltitz, M., Carle, G.: A performance and resource consumption assessment of secret sharing based secure multiparty computation. In: Data Privacy Management Workshop '18. Springer International Publishing (2018)
21. von Maltitz, M.L.: Secure and Privacy-preserving Services Based on Secure Multiparty Computation. Network Architectures and Services NET (2019)
22. Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., Marrs, A.: Disruptive technologies: Advances that will transform life, business, and the global economy, vol. 180. McKinsey Global Institute San Francisco, CA (2013)
23. Mohammadi, M., Al-Fuqaha, A., Sorour, S., Guizani, M.: Deep learning for iot big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials **20**(4), 2923–2960 (2018)
24. Pallas, F., Raschke, P., Bermbach, D.: Fog computing as privacy enabler. IEEE Internet Computing (2020)

25. Papcun, P., Kajati, E., Cupkova, D., Mocnej, J., Miskuf, M., Zolotova, I.: Edge-enabled iot gateway criteria selection and evaluation. Concurrency and Computation: Practice and Experience p. e5219 (2020)
26. Peterson, L., Anderson, T., Katti, S., McKeown, N., Parulkar, G., Rexford, J., Satyanarayanan, M., Sunay, O., Vahdat, A.: Democratizing the Network Edge. SIGCOMM Comput. Commun. Rev. **49**(2), 31–36 (May 2019)
27. Pinto, S., Gomes, T., Pereira, J., Cabral, J., Tavares, A.: Iioteed: An enhanced, trusted execution environment for industrial iot edge devices. IEEE Internet Computing **21**(1), 40–47 (2017)
28. Raafat, H.M., Hossain, M.S., Essa, E., Elmougy, S., Tolba, A.S., Muhammad, G., Ghoneim, A.: Fog intelligence for real-time iot sensor data analytics. IEEE Access **5**, 24062–24069 (2017)
29. Rao, F.Y., Bertino, E.: Privacy techniques for edge computing systems. Proceedings of the IEEE **107**(8), 1632–1654 (2019)
30. Reddy, K.U.K., Shabbiha, S., Kumar, M.: Design of High Security Smart Health Care Monitoring System using IoT. International Journal of Emerging Trends in Engineering Research **8**(6), 2259–2265 (June 2020)
31. Saleem, A., Khan, A., Malik, S.U.R., Pervaiz, H., Malik, H., Alam, M., Jindal, A.: Fesda: Fog-enabled secure data aggregation in smart grid iot network. IEEE Internet of Things Journal pp. 1–1 (2019)
32. Shah-Mansouri, H., Wong, V.W.S.: Hierarchical Fog-Cloud Computing for IoT Systems: A Computation Offloading Game. IEEE Internet of Things Journal **5**(4), 3246–3257 (2018)
33. Sousa, P.R., Antunes, L., Martins, R.: The present and future of privacy-preserving computation in fog computing. In: Fog Computing in the Internet of Things, pp. 51–69. Springer (2018)
34. Souza, V.B.C., Ramírez, W., Masip-Bruin, X., Marín-Tordera, E., Ren, G., Tashakor, G.: Handling service allocation in combined Fog-cloud scenarios. In: IEEE International Conference on Communications (ICC). pp. 1–5 (2016)
35. Tao, H., Bhuiyan, M.Z.A., Abdalla, A.N., Hassan, M.M., Zain, J.M., Hayajneh, T.: Secured data collection with hardware-based ciphers for iot-based healthcare. IEEE Internet of Things Journal **6**(1), 410–420 (2018)
36. Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A.S., Nojoumian, M.: Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems. Future Generation Computer Systems **78**, 547–557 (2018)
37. Van Dijk, M., Juels, A.: On the impossibility of cryptography alone for privacy-preserving cloud computing. HotSec **10**, 1–8 (2010)
38. Vorakulpipat, C., Rattanalerdnusorn, E., Thaenkaew, P., Hai, H.D.: Recent challenges, trends, and concerns related to iot security: An evolutionary study. In: 2018 20th International Conference on Advanced Communication Technology (ICACT). pp. 405–410. IEEE (2018)
39. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for internet of things. Journal of network and computer applications **42**, 120–134 (2014)
40. Zhang, Y., Ren, J., Liu, J., Xu, C., Guo, H., Liu, Y.: A survey on emerging computing paradigms for big data. Chinese Journal of Electronics **26**(1), 1–12 (2017)