SecureDataCloud: Introducing Secure Computation in ATM

Massimiliano Zanin, David Pérez
Innaxis Foundation & Research Institute, Madrid, Spain
{mz, dp}@innaxis.org

Gokhan Inalhan
Istanbul Technical University, Istanbul, Turkey
inalhan@itu.edu.tr

Cengiz Paşaoğlu
Devlet Hava Meydanlari Işletmesi, Istanbul, Turkey
cengiz.pasaoglu@dhmi.gov.tr

Emilio Álvarez Pereira
Telenium, Madrid, Spain
ealvarez@telenium.es

The achievement of an efficient information sharing and coordination between the different stakeholders involved in air transport and ATM is nowadays considered one of the most important priorities in aviation, with potential benefits ranging from improved safety, reduced delays, up to more environmental-friendly operations. In spite of this, the management of the different types of information is at present split among different compartments, mostly isolated and with little cross-integration, due to organizational and institutional barriers that prevent the timely and free flow of relevant data.

In order to improve such situation, SESAR is currently developing the System Wide Information Management (SWIM) [1], a new information infrastructure which will connect all ATM stakeholders, aircraft as well as all ground facilities. In spite of the improvements that SWIM will provide on this aspect, still information flow will not be completely free, as most ATM data is considered in Europe as confidential and sensitive and, hence, private – both for its commercial value, and for the political or social consequence some of the analyses may cause. Confidentiality will be tackled in SWIM by means of strict access regulations to certain types of data: while in the short term these types of policies might be effective, in the long run it will make European air transport lag beyond other countries, such as the USA, where the publicity of data is considered an essential element of development.

In the recently launched WP-E project *SecureDataCloud*, a new paradigm is proposed to deal with confidentiality issues without limiting the ability of performing relevant computation of private data: the use of secure computation techniques. Secure computation is the field of cryptology devoted to the study of performing a computation while preserving the privacy of the inputs of any party. One example, known as *the millionaires problem*, may help clarifying this concept: two millionaires are interested in knowing which of them is richer, but they do not want to reveal their actual wealth to the other, nor to an external trusted party. Such problem was introduced by Andrew Yao, a prominent computer scientist and computational theorist, and is considered as the first solved example of secure computation [2], [3].

From a more general point of view, a secure computation problem deals with computing any function on any input in a distributed system where each participant holds a part of the information, even in a cloud environment [4]. This must be achieved ensuring the correctness of the computation while no additional information is revealed to any participant other than strictly the information inferred from that participant's input and output. Clearly, this can always be solved by assuming the existence of a trusted third party; yet, in real applications, this requirement is not always feasible. Secure computation techniques can enable business models in those cases where trusted parties are difficult or impossible to designate, and, specific secure computation algorithms and protocols have been developed for these cases.

Nowadays, there are several problems tackled using a secure computation approach, with applications spanning from secure sealed-bid auction, elections with an electronic voting scheme [5], and stock transactions, up to defense applications in military operations [6].

The use of this technology would enable the improvement of uncountable applications within Air Traffic Management, starting with actual research activities. Among others, these include safety, allowing analysts to mine some specific pattern inside historical data, without actually accessing the data sets and thus ensuring confidentiality; understanding global properties of air transport, as for instance the number of passengers in a given route, or actual fuel consumptions; or improving the cooperation between airlines, fostering mechanisms such as slot bidding.

References

[1] J. S. Meserole and J. W. Moore, *What is System Wide Information Management (SWIM)?*. Aerospace and Electronic Systems Magazine, IEEE, 22(5), pp. 13–19, 2007.

[2] A. C. Yao, *Protocols for Secure Computations.* In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, 1982.

[3] A. C. Yao, *How to generate and exchange secrets.* In Proceedings of the 27th Annual Symposium on Foundations of Computer Science, 1986.

[4] A. López-Alt, E. Tromer and V. Vaikuntanathan, *On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption.* In Proceedings of the 44th symposium on Theory of Computing, 2012.

[5] H. Vegge, *Realizing Secure Multiparty Computations.* 2009.

[6] R. Pathak and S. Joshi, *Secure Multi-party Computation Protocol for Defense Applications in Military Operations Using Virtual Cryptography.* Communications in Computer and Information Science 40 (8), pp. 389–399, 2009.