|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ITU Logo | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2017-2020 | | | FG-AI4H-F-040 |
| **ITU-T Focus Group on AI for Health** |
| **Original: English** |
| **WG(s):** | | Plenary | | Zanzibar, 3-5 September 2019 |
| **DOCUMENT** | | | | |
| **Source:** | | FG-AI4H WG-DASH Chair | | |
| **Title:** | | LS/r on AI (Artificial Intelligence)/ML (Machine Learning) and security (SG17-LS142) [to ITU-T SG17] | | |
| **Purpose:** | | Approval | | |
| **LIAISON STATEMENT** | | | | |
| **For action to:** | | | ITU-T SG17 | |
| **For comment to:** | | | - | |
| **For information to:** | | | ITU-T SG16 | |
| **Approval:** | | | FG-AI4H meeting (Zanzibar, 5 September 2019) | |
| **Deadline:** | | | 1 July 2020 | |
| **Contact:** | | Thomas Wiegand Chair, FG-AI4H HHI Fraunhofer, Germany | | Email: [thomas.wiegand@hhi.fraunhofer.de](mailto:thomas.wiegand@hhi.fraunhofer.de) |
| **Contact:** | | Marc Lecoultre Chair, FG-AI4H WG-DASH ML Lab, Switzerland | | Email: [ml@mllab.ai](mailto:ml@mllab.ai) |

|  |  |
| --- | --- |
| **Abstract:** | FG-AI4H thanks SG17 for its LS, notes interest in material provided and requests studies in SG17 that would lead to the standardization of homomorphic encryption techniques. |

The Focus Group on AI4H thanks ITU-T SG17 for its LS on (ours [FGAI4H-F-023](https://extranet.itu.int/sites/itu-t/focusgroups/ai4h/docs/FGAI4H-F-023.docx), yours [SG17-LS142](http://handle.itu.int/11.1002/ls/sp16-sg17-oLS-00142.zip)).

We found the attachment with the Contribution from Symantec of particular interest.

We have received in a previous meeting a proposal to use homomorphic encryption to assist in protecting user data in the context of the benchmarking we are developing for health solutions that use AI (found in document [FGAI4H-B-016](https://extranet.itu.int/sites/itu-t/focusgroups/ai4h/docs/FGAI4H-B-016.docx), [https://extranet.itu.int/sites/itu-t/focusgroups/ai4h/docs/‌FGAI4H-B-016.docx](https://extranet.itu.int/sites/itu-t/focusgroups/ai4h/docs/FGAI4H-B-016.docx)). Homomorphic encryption would allow computation to be performed on data without needing to decrypt it. After discussions, we found that homomorphic encryption is a promising technique that might facilitate the identification of datasets that would be provided to the FG-AI4H to progress its work. However, we recognize the lack of existing standards and libraries that would allow us to use it currently.

The FG-AI4H would therefore be grateful and encourage SG17 to define standards covering homomorphic encryption, as this has great potential to facilitate data protection and "safe" sharing that is needed for many AI-based techniques, even beyond the health field.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_