PAPAYA

PlAtform for PrivAcY preserving data Analytics

Data analytics provide valuable insights and new opportunities to businesses who often resort to **third-party services or data processors** (such as clouds) to perform all these operations. Nevertheless, data analytics may jeopardize data **confidentiality** and data subjects' **privacy**, while companies and cloud providers must **comply with GDPR obligations**.

In this context, the **PAPAYA** project aims at enabling data processing and analytics on **encrypted and/or anonymized data**. This will ensure that data subjects' privacy is preserved while companies are still able to extract **valuable and meaningful information** from analyzed data.

[Key Facts]

Project ID:	786767
Start Date:	May 1, 2018
Duration:	3 years
Coordinator:	EURECOM

[Objectives]

- ✓ Develop **privacy-preserving data analytics modules** within different settings (single/multiple owners). Analytics ranging from simple statistics to more complex operations such as machine learning, etc.
- ✓ Design and develop **an integrated platform** that can be used in an **interoperable** manner.
- ✓ Enable **risk management and user control** of data disclosure.

[Use Case 1]

e-Health

Thanks to the **PAPAYA platform**, a healthcare institution can **delegate** the processing of the tremendous amount of (sensitive) data collected by wearable devices and biomedical sensors to a **third-party processor** (e.g., a cloud). In a first scenario (Fig. 1.a), the healthcare institution (a **single data owner**) will encrypt the data and delegate the data analytics tasks to the cloud. The second scenario (Fig. 1.b) considers **several data owners** that collaborate to perform the analytics **without compromising data confidentiality and privacy**.

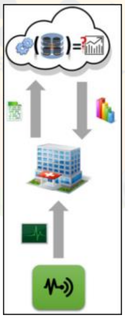

Fig. 1.a

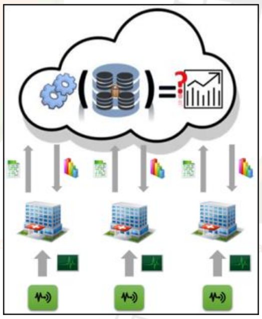

Fig. 1.b

[Use Case 2]

Web & Mobile data

Web browsing and mobile data are useful for industries such as tourism to analyze tourists' flow. PAPAYA will be useful to extract such information in a privacy-preserving way. The first usage scenario (Fig. 2.a) considers a **single data owner** which **aggregates encrypted data** and allows a **third-party querier** to perform data analytics requests. In a second scenario (Fig. 2.b), **end-to-end privacy** will be ensured by **encrypting these data directly in users' mobile phones/devices**

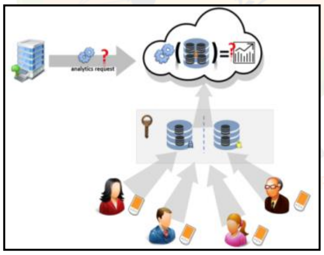

Fig. 2.a

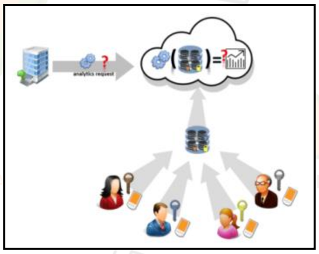

Fig. 2.b

EURECOM Sophia Antipolis · IBM · Karlstads Universitet · MEDIACLINICS Wearable Health Applications · orange · Atos

www.papaya-project.eu · @ProjectPapaya · PAPAYA Project · papaya@eurecom.fr

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, through the PAPAYA project, under Grant Agreement No. 786767. This flyer reflects the view of the consortium only. The Research Executive Agency is not responsible for any use that may be made of the information it contains.

PAPAYA

PlAtform for PrivAcY preserving data Analytics

Data analytics provide valuable insights and new opportunities to businesses who often resort to **third-party services or data processors** (such as clouds) to perform all these operations. Nevertheless, data analytics may jeopardize data **confidentiality** and data subjects' **privacy**, while companies and cloud providers must **comply with GDPR obligations**.

In this context, the **PAPAYA** project aims at enabling data processing and analytics on **encrypted and/or anonymized data**. This will ensure that data subjects' privacy is preserved while companies are still able to extract **valuable and meaningful information** from analyzed data.

[Key Facts]

Project ID:	786767
Start Date:	May 1, 2018
Duration:	3 years
Coordinator:	EURECOM

[Objectives]

- ✓ Develop **privacy-preserving data analytics modules** within different settings (single/multiple owners). Analytics ranging from simple statistics to more complex operations such as machine learning, etc.
- ✓ Design and develop **an integrated platform** that can be used in an **interoperable** manner.
- ✓ Enable **risk management and user control** of data disclosure.

[Use Case 1]

e-Health

Thanks to the **PAPAYA platform**, a healthcare institution can **delegate** the processing of the tremendous amount of (sensitive) data collected by wearable devices and biomedical sensors to a **third-party processor** (e.g., a cloud). In a first scenario (Fig. 1.a), the healthcare institution (a **single data owner**) will encrypt the data and delegate the data analytics tasks to the cloud. The second scenario (Fig. 1.b) considers **several data owners** that collaborate to perform the analytics **without compromising data confidentiality and privacy**.

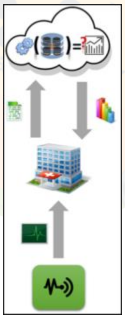

Fig. 1.a

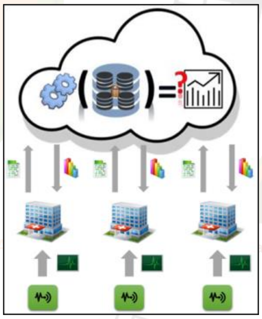

Fig. 1.b

[Use Case 2]

Web & Mobile data

Web browsing and mobile data are useful for industries such as tourism to analyze tourists' flow. PAPAYA will be useful to extract such information in a privacy-preserving way. The first usage scenario (Fig. 2.a) considers a **single data owner** which **aggregates encrypted data** and allows a **third-party querier** to perform data analytics requests. In a second scenario (Fig. 2.b), **end-to-end privacy** will be ensured by **encrypting these data directly in users' mobile phones/devices**

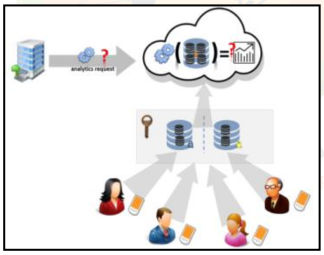

Fig. 2.a

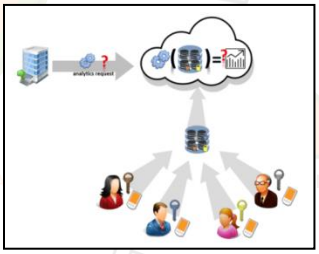

Fig. 2.b

EURECOM IBM KARLSTADS UNIVERSITET MEDIACLINICS Wearable Health Applications orange™ Atos

www.papaya-project.eu @ProjectPapaya PAPAYA Project papaya@eurecom.fr

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, through the PAPAYA project, under Grant Agreement No. 786767. This flyer reflects the view of the consortium only. The Research Executive Agency is not responsible for any use that may be made of the information it contains.