Security for Deep Learning

Opportunity for a 6-month internship

Security Research @ SAP Labs France
Sophia-Antipolis – France

SAP's security vision is built on 5 ideals to secure business: Defendable Application, Zero-Knowledge, Zero-Vulnerability, Security by Default, and Transparency.
SAP's security research group lays the foundation for realising the vision: The 30+ researchers of the Security Research unit focus on security engineering (e.g., the automation of the secure software development lifecycle), secure business execution (e.g., business process security and security in cloud based business applications) and secure operations (e.g., secure maintenance and support of complex and heterogeneous cloud IT landscapes).

Security Research proposes a 6-month internship in its Sophia-Antipolis offices (Mougins, France).

INTERNSHIP TOPIC

This internship is based in the SAP Labs France Research Lab, in Sophia-Antipolis. The work will be performed in the context of the Research Program "Security & Trust", and deals with secure integration of Internet of Things with SAP HANA applications. The Internet of Things (IoT) is expected to grow to 50 billion connected devices and $14.4 trillion in value at stake until 2020. SAP is exploiting this trend and centers its IoT development on the SAP HANA Cloud Platform IoT Service.

Benefiting from the latest technological advances of GPUs, **deep learning** *has dramatically improved the state-of-the-art in speech recognition, visual object recognition, object detection and many other domains such as drug discovery and genomics. Deep learning discovers intricate structure in large data sets by using the backpropagation algorithm to indicate how a machine should change its internal parameters that are used to compute the representation in each layer from the representation in the previous layer. Deep convolutional nets have brought about breakthroughs in processing images, video, speech and audio, whereas recurrent nets have shone light on sequential data such as text and speech.* [1]

Applying **deep learning** to a problem involving medical, financial, personal sensitive data requires not only accurate predictions, but also a careful attention to data privacy and security, in conformity and compliance with regulation on data protection. In that context, crypto-nets [2] have been developed for *"cloud service […] capable of applying the neural networks to encrypted data to make encrypted predictions."*

In addition, following on the Machine Learning trend, several approaches [3], [4] have been proposed for ML over encrypted data enabling privacy-preserving training and classification. Their approach is based on a homomorphic public key based encryption, evaluated on Linear Means (LM) and Fisher's Linear Discriminant (FLD) classifiers.

The goal of this internship is two-fold:

1. State of the art on deep learning training and learning over encrypted data
2. Implementation of a PoC demonstrating the feasibility of such approach in an industrial use case

We expect that 60% of time will be dedicated to development and 40% to research activities.

[1] Yann LeCun, Yoshua Bengio, Geoffrey Hinton, *Deep Learning*, Nature, 2015
[2] Dowlin, Gilad-Bachrach, Laine, Lauter, Naehrig, Wernsing, *Cryptonets applying-neural-networks-to-encrypted-data-with-high-throughput-and-accuracy*, technical report, 2016
[3] Graepel, Thore, Kristin Lauter, Michael Naehrig. *"ML confidential: Machine learning on encrypted data."* International Conference on Information Security and Cryptology. Springer Berlin, Heidelberg, 2012.
[4] Raphael Bost, Raluca Ada Popa, Stephen Tu, Shafi Goldwasser. *"Machine Learning Classification over Encrypted Data."* Network and Distributed System Security (NDSS) Symposium. San Diego, 2015.

CANDIDATE PROFILE

- University Level: Last year of MSc in Computer Science or beyond
- XSJS (SAP HANA language), C, Java
- Experience on Internet of Things and embedded systems
- Fluency in English (working language)
- Abilities in organizing meeting and contacting people
- Good oral and written communication skills
- Capacity to write documents in English, ability to synthesize

INTERNSHIP CONTEXT

SAP

Over the past 45 years, SAP has grown to become the world's leading provider of business software solutions. With 12 million users, 96,400 installations, and more than 1,500 partners, SAP is the world's largest inter-enterprise software company and the world's third-largest independent software supplier, overall. SAP solutions help enterprises of all sizes around the world to improve customer relationships, enhance partner collaboration and create efficiencies across their supply chains and business operations. SAP group includes subsidiaries in over 180 countries and employs more than 84 000 people.

Security Research at SAP Labs France, Sophia Antipolis

Based at SAP Labs France Mougins, Security Research Sophia-Antipolis addresses the upcoming security needs, focusing on increased automation of the security life cycle and on providing innovative solutions for the security challenges in networked businesses, including cloud, services and mobile.

STANDARD INTERNSHIP PACKAGE

- *Salary*: depending on the length of the internship and your diploma.
- *Lunch*: SAP Labs France has a local cafeteria; interns contribute 2,40 €uro/lunch, like other SAP employees.
- *Holidays*: French Bank Holidays
  - January 1st; April 2nd, May 1st, May 8th, May 10th, May 21st, July 14th; August 15th , Nov 1st and 11th; December 25th
- *Travel*: no trip will be paid by SAP.
- *Accommodation*: SAP can propose an accommodation for the duration of your internship. The accommodation is subsidized by SAP: the intern pays half of the rental cost: 342€ for a 1-room apartment or 442€ for a 2-room apartment (Choice depending on the availability).

CONTACTS AND PROCEDURE

Please send **in English** your CV, a cover letter and any relevant documents to the following persons stating the title of the Internship in the subject: [Internship Application] **Secure Integration of Internet of Things**.

Supervisor
Laurent Gomez
laurent.gomez@sap.com
Tel. +33-(0)4-92286346

Administrative point of contact
Sylvine Eusebi
sylvine.eusebi@sap.com
Tel. +33-(0)4-92286477