

Privacy Preserving Stream Analytics

Tech ID: 29845 / UC Case 2016-806-0

SUMMARY

UCLA researchers in the Department of Computer Science have developed a new privacy preserving mechanism for stream analytics.

BACKGROUND

Computers and smartphones not only serve as a means of communication and computation, but also include a variety of sensors (e.g., proximity, accelerometer, gyroscopic, GPS, etc.). Various data analysts perform data aggregation studies and try to extract meaning from this sensor and user data. However, with this wide array of sensors comes serious privacy concerns with the large amount of real-time personal data that is collected without individual's consent or knowledge. Of the more serious privacy violations is with regards to location data. While location based services are rising in popularity, the concerns of being constantly tracked require proportional privacy-preserving mechanisms. There needs to be a mechanism by which the data analysts should be able to receive the aggregated data in order to perform analysis but simultaneously preserve the user's privacy at the same time.

INNOVATION

Researcher Josh Joy and colleagues at UCLA have developed a novel privacy preserving tool for stream analytics that allows the user to control and privatize their data without the need for a 'trusted' third party. Additionally, this allows users to share their private data without actually being linked to the data, thereby preserving privacy. This allows the data analysts to make conclusions with aggregate data in real-time all while preserving end-user data privacy. This innovation streamlines data privacy management as the user privatizes the data, as opposed to a single data-owner, allowing for scalability of the service.

APPLICATIONS

- ▶ Large scale data collection where individuals currently do not share due to privacy concerns. This ranges from location data, financial data, and health data.
- ▶ Current geo-location services only collect data. They are not able to publicly disclose the data due to privacy concerns, and this technique enables real-time private data collection and disclosure.

ADVANTAGES

- ▶ Allows user to privatize data before transmission, removing the need for 'trusted' third parties.
- ▶ Allows for analysis of real-time private data
- ▶ Highly scalable as user generates private data, and not housed by a single data owner.
- ▶ Existing techniques either do not have strong anonymous data uploads and sacrifice security for speed. This method would enable high-speed transmission of privatized data.

STATE OF DEVELOPMENT

This technology has been validated with vehicle tracking data

RELATED MATERIALS

- ▶ J. Joy and M. Gerla, PAS-MC: Privacy-preserving Analytics Stream for the Mobile Cloud, in *Cryptography and Security*, 2016.
- ▶ J. Joy, S. Rajwade, and M. Gerla, Participation Cost Estimation: Private Versus Non-Private Study, in *Cryptography and Security*, 2016.

PATENT STATUS

CONTACT

UCLA Technology Development
Group
ncd@tdg.ucla.edu
tel: 310.794.0558.



INVENTORS

- ▶ Joy, Joshua

OTHER INFORMATION

KEYWORDS

Cyber security, data encryption, encryption, privacy, data privacy, stream analytics, PAS-MC, location services, GPS tracking, location data, location tracking

CATEGORIZED AS

- ▶ **Communications**
 - ▶ Internet
 - ▶ Other
 - ▶ Wireless
- ▶ **Computer**
 - ▶ Other
 - ▶ Security
- ▶ **Security and Defense**
 - ▶ Cyber security

RELATED CASES

2016-806-0

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	10390220	08/20/2019	2016-806

Gateway to Innovation, Research and Entrepreneurship

UCLA Technology Development Group

10889 Wilshire Blvd., Suite 920, Los Angeles, CA 90095

tdg.ucla.edu

Tel: 310.794.0558 | Fax: 310.794.0638 | ncd@tdg.ucla.edu

© 2018 - 2019, The Regents of the University of California

[Terms of use](#)

[Privacy Notice](#)

