VirtualIdentity:
a Privacy-Preserving User Profiling Service

Sisi Wang
sisiwang@uw.edu
M.S. in Computer Science

Faculty Advisors:
Dr. Martine De Cock & Dr. Anderson Nascimento
The Secure ML team:
Wing-Sea Poon, Golnoosh Farnadi, Caleb Horst,
Kebra Thompson, Michael Nickels, Chris Allan Vishoot & Such Kamal
http://secureml.insttech.washington.edu/

UNIVERSITY of WASHINGTON | TACOMA
Institute of Technology

facebook

Search for people, places and things

SORT

American Express

Taking advantage of post-holiday sales? Use Membership Rewards points for Mobile Gift Cards to select retailers right on your smartphone! http://aexp.co/ruY

Like · Comment · Share · 4,014 53 115 · Sponsored

Sponsored Create an Ad

American Express

Taking advantage of post-holiday sales? Use Membership Rewards points for Mobile Gift Card...

4,014 53 115

Fresno All Laser LASIK

fresnolasikeyesurgery.com

With LASIK, you won't have to worry about painful surgery or lengthy recovery times.

Meet Singles On Facebook

Interested Single Women. Sign up and see pics on Facebook. It's 100% free to look!

Free Cab Fare For A Year!

Share your safe alternative to driving

User Profiling

Machine Learning

Gender, Age,

Personality,

Religion, Sexual

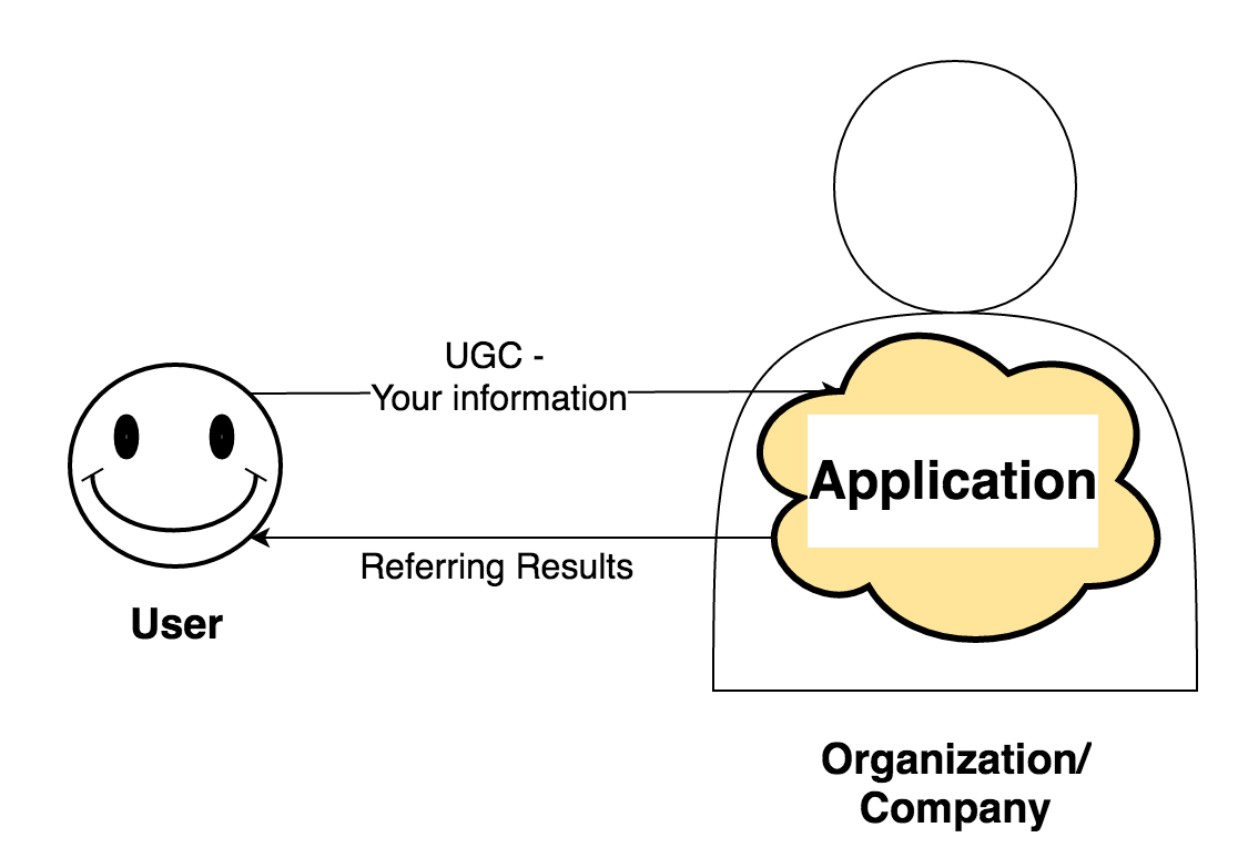
Orientation,

Interest,...

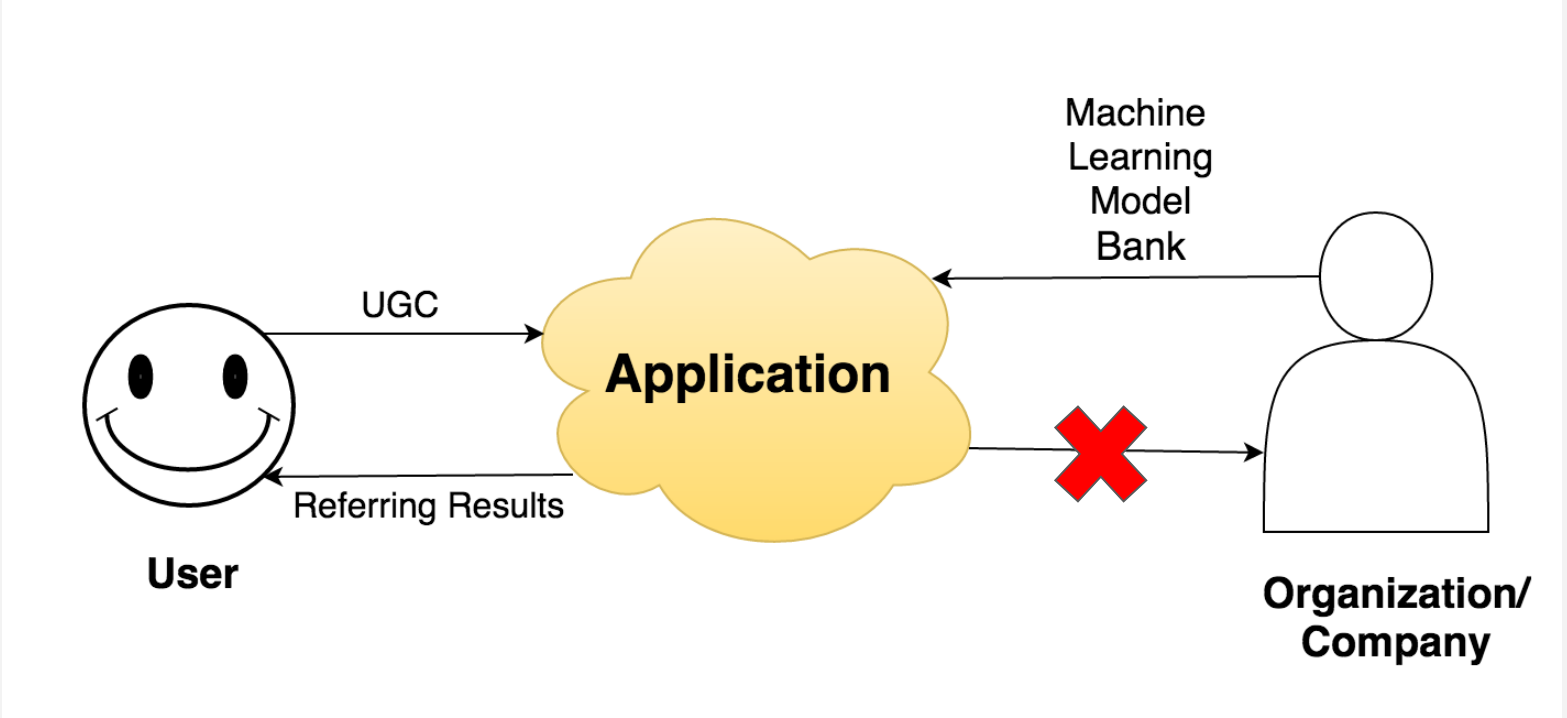
Image Credit: The New Yorker cartoon modified by Eric Blattberg / VentureBeat

KDnuggets Cartoon by Jon Carter

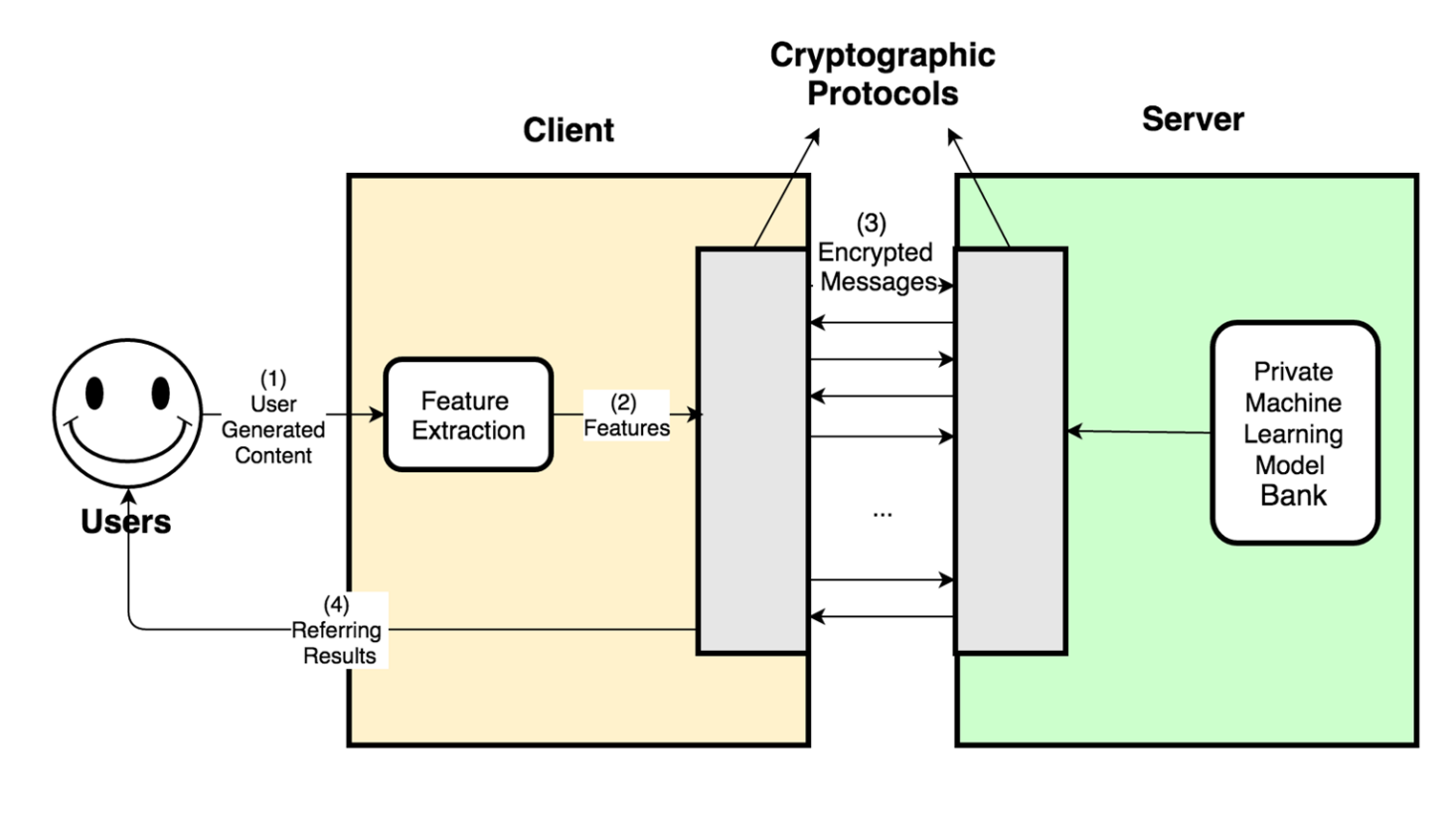
Problem?


UGC -
Your information
Application
Referring Results
User
Organization/
Company

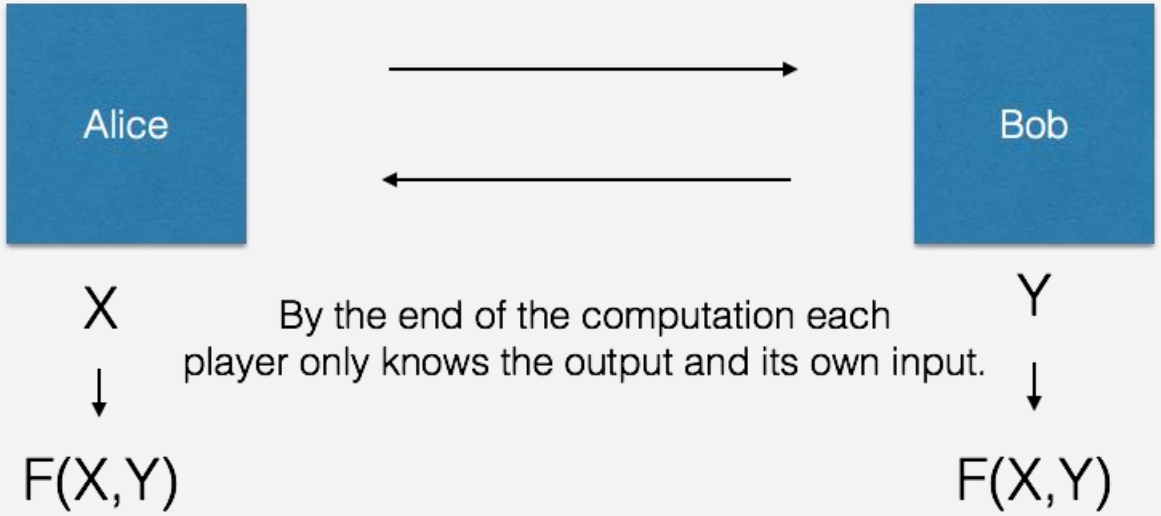
Privacy-Preserving



VirtualIdentity -- Overview

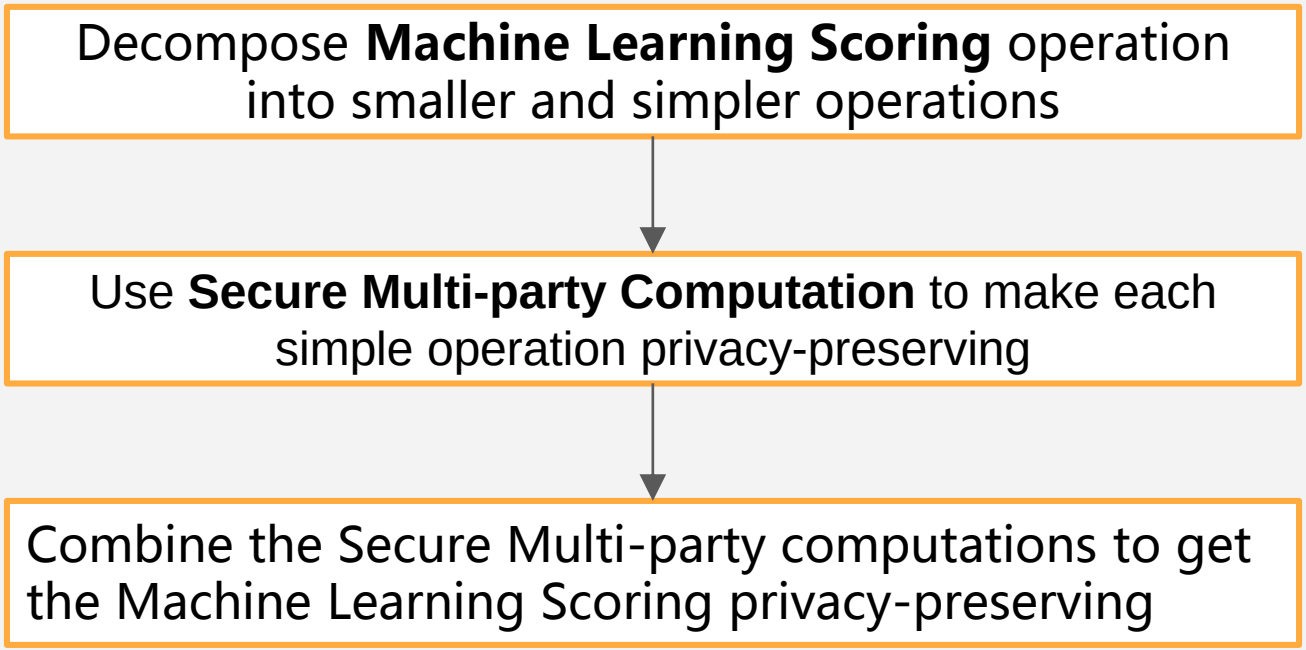


Secure Two Party Computations

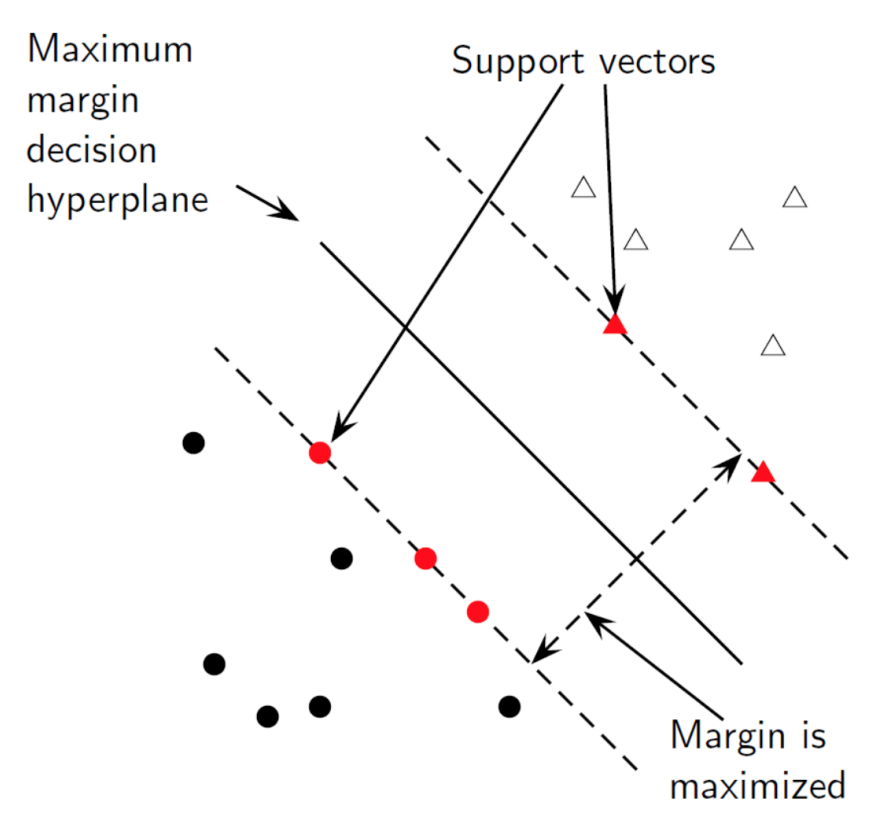


A. Yao. How to Generate and Exchange Secrets. In 27th FOCS, pages 162–167, 1986.

Cryptographic Protocols



Support Vector Machine Scoring



Scoring for new instance x_q:

$$f(x_q) = \text{sign}\left(\sum_i \alpha_i y_i K(x_q, x_i)\right)$$

- Multiplication
- Addition
- Comparison
- ...

Privacy-Preserving Comparison
-- by Multi-party Computation

Let ℓ be the bit length of the integers to be compared. The trusted initializer pre-distributes the correlated randomness necessary for the execution of all instances of the distributed multiplication protocol. The parties have as inputs shares $[\![x_i]\!]_2$ of each bit of x and shares $[\![y_i]\!]_2$ of each bit of y. The protocol proceeds as follows:

1. For $i = 1, \ldots, \ell$, compute $[\![d_i]\!]_2 \leftarrow [\![y_i]\!]_2 \, (1 - [\![x_i]\!]_2)$ using the multiplication protocol π_{DM} and locally compute $[\![e_i]\!]_2 \leftarrow [\![x_i]\!]_2 + [\![y_i]\!]_2 + 1$.

2. For $i = 1, \ldots, \ell$, compute $[\![c_i]\!]_2 \leftarrow [\![d_i]\!]_2 \prod_{j=i+1}^{\ell} [\![e_j]\!]_2$ using the multiplication protocol π_{DM}.

3. Compute $[\![w]\!]_2 \leftarrow 1 + \sum_{i=1}^{\ell} [\![c_i]\!]_2$ locally.

We hope to achieve highly practical results that allow the benefits of machine learning to be unlocked without the cost of individual privacy.

Check our website: http://secureml.insttech.washington.edu/

Sisi Wang
M.S. in Computer Science
sisiwang@uw.edu

UNIVERSITY of WASHINGTON | TACOMA
Institute of Technology