BU Department of Computer Science

Soham Sinha, Clare Bornstein, John Spinelli, Robin Kurosawa

Security Analysis: jet

Introduction:

Jet.com is an up and coming American e-commerce site founded in 2014. The company is similar to Amazon, selling a variety of home goods, electronics, and fresh groceries. Jet.com's shopping experience is defined by a unique pricing structure that allows customers to save money by eliminating some of the traditional overheads of online commerce. After selecting an item for purchase, other items that can be discounted as a result of that purchase are suggested to the user. These discounts are primarily achieved by ordering multiple items from the same distributor, paying by debit card and opting out of return eligibility.

Site Security:

Jet uses certificates with the highest level signed by Verisign Class 3. The certificate signature algorithm is PKCS #1 SHA-1 with RSA. SHA-1 is recently discovered to have collisions in hashing. Therefore, it would be better to upgrade the service to SHA-256. However, the lower level is signed by Symantec which uses PKCS #1 SHA-256 with RSA.

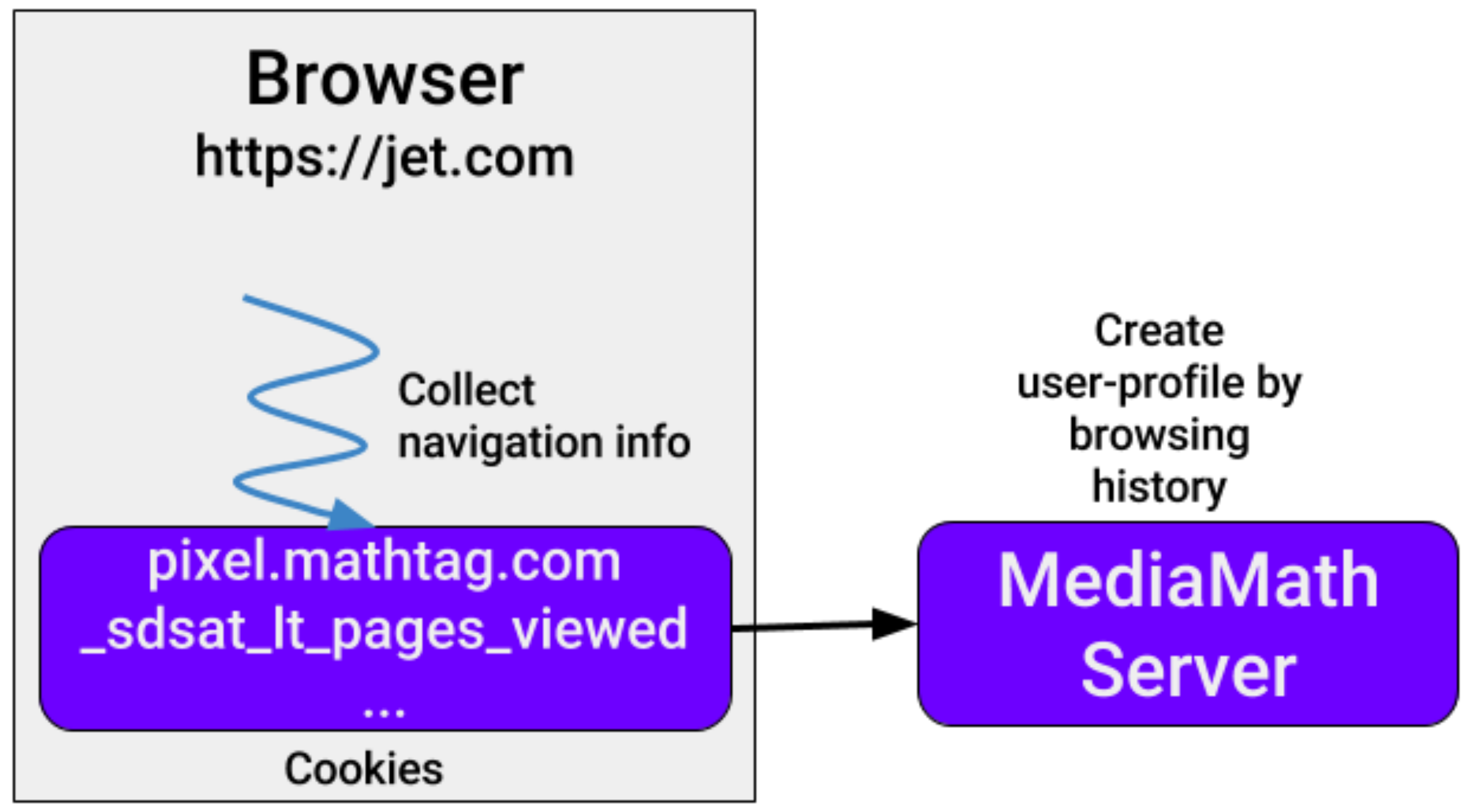
Cookies:

There are two main cookies that Jet uses to hold user information:

1. jet – this cookie is quite big (1/2 a kb)
2. jid – this cookie is small (only about 39 bytes)

Both cookies are http only and secure.

The pixel.mathtag.com cookie along with jet.com site-specific cookies is used to send information related to the browsing history of a user / an IP-address to a third-party advertising platform, namely MediaMath.



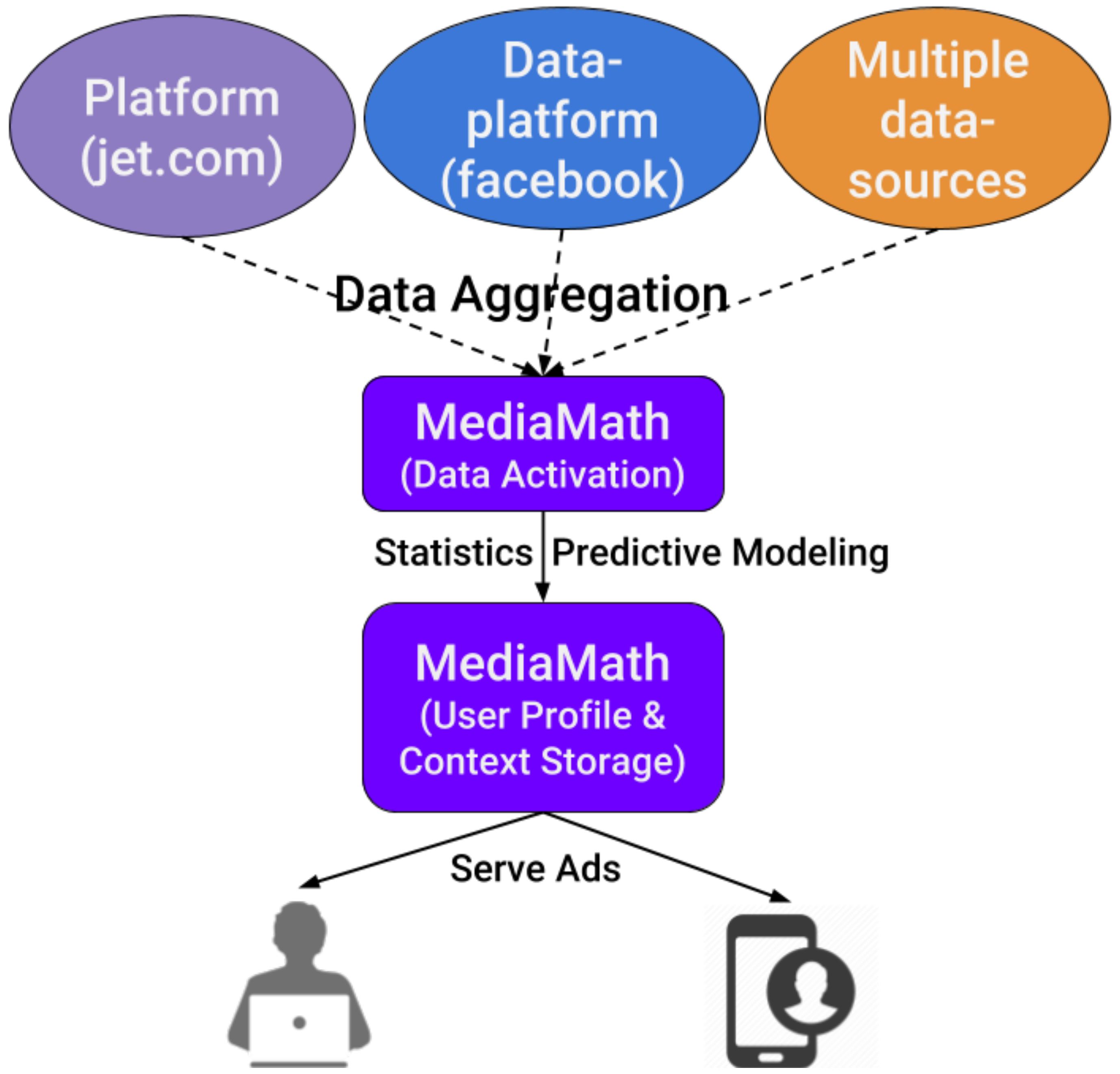
Browser
https://jet.com

Collect navigation info

pixel.mathtag.com
_sdsat_lt_pages_viewed
...
Cookies

Create user-profile by browsing history

MediaMath Server



Platform (jet.com)

Data-platform (facebook)

Multiple data-sources

Data Aggregation

MediaMath (Data Activation)

Statistics | Predictive Modeling

MediaMath (User Profile & Context Storage)

Serve Ads

Advertising and Third Party Content:

MediaMath is an advertising platform used by many other websites. MediaMath collects useful information from different websites and then create user-profile based on the relevant information. For example, MediaMath may collect a user's browser name, version, IP address, Facebook user-id, and create a user-profile based on the various available data-sources on the platform. MediaMath carries out extensive statistical analysis on the data they collect to churn out useful information about users and also display targeted ads

Privacy Policy:

Jet's privacy policy fundamentally absolves them from responsibility and is blatantly stated as in Jet's best interests. By accessing any of Jet's sites, according to Jet's terms of service, the user is explicitly agreeing to Jet's privacy policy.

They outline both what information they collect (name, address, telephone number, email, credit card/banking, etc.) and also how they may share this data. In both respects, they allow themselves very little limitations on whom they may share with and what they may share, especially when it comes to aggregated data.

Vulnerabilities:

Jet.com employs excellent security standards to protect user interactions on the site. Some information is still leaked during normal use:

- jid – jet's user tracking cookie
- https headers
- Browsing location
- Pages viewed
- Traffic source
- Cart total
- Number of items in cart

bu.edu/cs

@BUCompSci