Enkripcija nije dovoljna za očuvanje privatnosti

Danas je nedvojbeno prevladavajući trend distribucija informacija putem pohrane u oblaku, pri čemu se koriste vanjski poslužitelji za upravljanje i jednostavan pristup podacima. Istraživači iz Microsofta u suradnji sa znanstvenicima s tri sveučilišta (California, Irvine i Brown) predložili su tehnologiju koja bi u budućnosti trebala otežati izvlačenje vrijednosti iz podataka pohranjenih u oblaku.

Takve usluge mogu pobuditi zabrinutost zbog ugrožavanja privatnosti, jer pružatelji ove usluge obavljaju automatsko pretraživanje i analiziranje korisničkih podataka čak i kada su oni kriptirani, pa postoji mogućnost da u nekim slučajevima takvi podaci budu predmet istraživanja i od strane vlasti. Zbog toga znanstvenici predlažu algoritamska rješenja koje će očuvati poželjne osobine pohrane u oblaku, a istovremeno pružiti zaštitu privatnosti korisničkih podataka. Njihovo je rješenje nazvano Melbourne Shuffle, a znanstveni rad je dostupan u repozitoriju arXiv [1].

„Sama enkripcija danas više nije dovoljna za zaštitu privatnosti, jer se analizom obrazaca pristupanja podacima mogu otkrivati informacije o sadržaju podataka“, ističu znanstvenici.

Znanstvenici su objasnili kako jedno rješenje za ovaj problem mogu biti „zaboravljivi“ algoritmi pohrane, koji mogu sakriti slijed podatkovnog pristupa. Takvi algoritmi rade dobro, ali su označeni kao „računalno skupi“. Zbog toga znanstvenici predlažu alternativu - “Melbourne Shuffle” – tehnika izvedena iz miješanja karata kako bi se prikrila prava priroda podataka kojima se pristupa u oblaku. Ovo naizgled nasumično miješanje podataka može obavljati softver, ali i hardver, na primjer u obliku dodatnog *chipa* koji bi se ugrađivao u sustave za pohranu.

Drugim riječima, znanstvenici su otkrili novu metodu koja doprinosi anonimnosti bez usporavanja rada sustava za pohranu podataka u oblaku i to na dvostruki način - koristeći se mamcima, a dijelom i zbog premještanja podataka koja mogu biti predmet analize njuškala. Znanstvenici smatraju kako “Melbourne Shuffle” neće zahtijevati dodatne kapacitete potrebne za pohranu, ni dodatno opterećivati servere.

Za sve one koji žele proučiti ovaj vrijedan znanstveni rad, preporuča se upotreba znanstvenog kalkulatora i prilično napredno matematičko znanje.

Ako tehnologija bude prihvaćena bit će dobrodošla u ovim post-Snowdenovim vremenima kada se prelako postaje predmet analize najviših državnih struktura s nesagledivim posljedicama za zaštitu privatnosti.

Izvori:

http://www.itdirection.net/it-news-0020/022814-00548-it-news.shtml [2]

http://thejournal.com/articles/2014/03/11/researchers-recommend-data-shuffling-technique-to-secure-cloud-activity.aspx [3]

uto, 2014-03-11 20:46 - Uredništvo**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1365

Links
[1] http://arxiv.org/abs/1402.5524
[2] http://www.itdirection.net/it-news-0020/022814-00548-it-news.shtml
[3] http://thejournal.com/articles/2014/03/11/researchers-recommend-data-shuffling-technique-to-secure-cloud-activity.aspx