Zaštita u oblaku

Ilija Bašičević

- Zaštita u oblaku je složeniji problem nego u tradicionalnom računarskom okruženju
- Razlog je dinamika sa kojom se obrađuju informacije u okruženju oblaka i fluidnost informacija
- Resursi su visoko centralizovani, i usluga čuvanja podataka je zasnovana na virtuelizaciji
- Zaštita u oblaku nije samo tehnički, već i društveni problem

Tradicionalni pristup zaštiti

- Dolazi iz fizičkog sveta i koncepta ključ-brava koji se u računarskom svetu preslikava na zaštitu nosioca (eng. container security)
- Ne štiti se informacija nego njen nosilac

Zaštita u oblaku

- Zbog složenost obrada u okruženju oblaka, tradicionalni ima-nema (on-off) pristup zaštiti (ima pristup ili nema pristup) nije pogodan
- Zaštita se posmatra kao niz (kontinuum) opcija koje obuhvata tzv. upravljanje rizicima (eng. risk mitigation)
- Opcije se odnose na mogućnost pristupa i treba da očuvaju fleksibilnost u obradi podataka koju nudi oblak

Još o tradicionalnom pristupu

- Tradicionalni pristup zaštite podataka jednog preduzeća je tzv. zaštita granične linije (eng. perimeter protection) izložena u MRKRM1.
- Najjednostavnije je opisati kao zaštitu granice mreže preduzeća prema okruženju (javnom Internetu).
- Oko mreže preduzeća se uspostavlja zid (koji čine zaštitni zid - firewall, IDS sistemi itd.) i podaci preduzeća se čuvaju unutar tog zida
- Izazov za ovaj koncept predstavljaju zaposleni koji rade od kuće jer se nalaze izvan zida (udaljeni pristup mreži preduzeća), kao i situacije kada dva preduzeća rade na zajedničkom projektu

Zaštita orijentisana na sadržaj

- Eng. content-centric protection, a koristi se i naziv egn. information-centric protection
- Novi koncept zaštite informacija
- Ne štiti se granica mreže preduzeća, već se štiti granica svakog objekta podataka
- Zaštita objekta podataka se kreće (pomera) sa samim objektom
- Nema potreba da objekat podataka bude čuvan u okviru granične linije preduzeća

Slučaj upotrebe: podaci u oblaku

- Rizici zaštite podataka koji postoje u tradicionalnom računarskom okruženju, postoje i u oblaku, ali postoje i neki novi
- Podaci se generišu u oblaku (ili se podižu „upload“ na oblak) i čuvaju u centru podataka (eng. data center)

Čuvanje podataka

- Odmah se uočava rizik vezan za čuvanje podataka
- Podatke koje korisne generiše u oblaku ili podigne na oblak, čuva preduzeće koje realizuje uslugu oblaka (eng. cloud provider)
- U stvari tu ima više rizika

1. Rizik – podizanje podataka

- Neophodno je obezbediti da podaci ne budu ukradeni (eng. hijacked) tokom podizanja na oblak

2. Rizik – čuvanje podataka

- Potrebna je garancija da će podaci celo vreme čuvanja biti šifrovani

3. Rizik – pristup podacima

- Pristup podacima mora biti kontrolisan uključujući i pristup od strane administratora centra podataka
- Takođe je bitna zaštita podataka za vreme obrade, tj. njihovog korišćenja
- Još jedan bitan aspekt je korišćenje podataka od strane korisnika nakon pristupa (nakon što su pristupili podacima). Kako sprečiti nekontrolisanu distribuciju podataka ? (ovaj problem postoji i u tradicionalnom računarskom okruženju)

Kontrola pristupa orijentisana na informacije

- Eng. Information-centric access control
- Povezivanje pravila pristupa sa objektima podataka

Mešanje podataka kao izvor rizika

- Eng. data-centric mashups
- Mešanje podataka je tehnologija koja integriše raznovrsne izvore podataka i pojednostavljuje neke vrste obrada nad podacima na taj način što sakriva od korisnika odredjene operacije
- Najčešće je to veb stranica ili veb aplikacija koja integriše različite izvore podataka u novu uslugu sa jednom grafičkom spregom
- Problem je što ako ne postoji dobro definisana politika kontrole pristupa podacima i distribucije podataka, privatnost korisnikovih podataka može biti ozbiljno narušena.

Identitet korisnika

- Da bi se realizovala prilagodiva zaštita podataka, neophodna je podrška za digitalni identitet korisnika
- Tri ključna koncepta u zaštiti podataka su identitet, pristup i rizik
- Sa povećanjem prava pristupa, povećava se i rizik
- Da bi se kontrolisao pristup, neophodno je postojanje digitalnog identiteta, koji se programski povezuje sa politikama zaštite

Identitet 2

- Da bi sve ovo funkcionisalo, digitalni identitet mora biti proveren od strane trećeg lica (eng. trusted third party)
- Pri korišćenju identiteta, treba voditi računa o privatnosti
- Potrebno je napraviti uravnoteženje između ova dva. Korisnik treba da ima mogućnost da upravlja svojim identitetom (eng. user-centric identity), ali identitet mora biti ustanovljen od strane treće strane (na primer banka) koja može da potvrdi taj identitet.

Nivoi zaštite podataka

- Koje su bitne osobine podataka (ili objekta podataka) ?
- Postojanje podataka nije ograničeno graničnom linijom mreže preduzeća.
- Mogu biti korišteni od strane više korisnika.
- “Podaci su objekti koji treba da se slobodno kreću”

- Da bi zaštita podataka bila uspešna, politika zaštite mora postati ugrađeni, suštinski (eng. intrinsic) deo samog objekta podataka.
- Zaštitu možemo posmatrati kroz nekoliko koncentričnih nivoa.

Nivoi 2

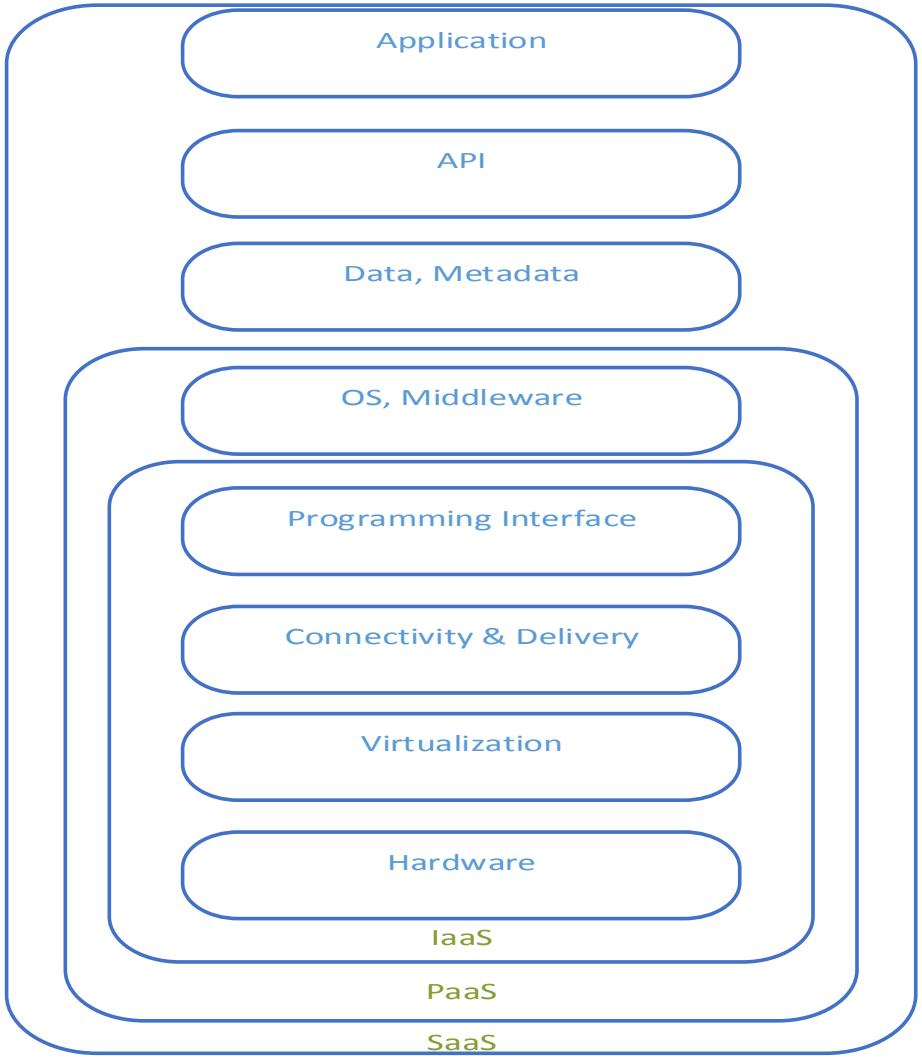
- Nivo 1 – zaštićeni prenos datoteke
- Nivo 2 – kontrola pristupa datoteci, bez šifrovanja sadržaja
- Nivo 3 – kontrola pristupa datoteci sa šifrovanjem sadržaja
- Nivo 4 – upravljanje pravima pristupa (na primer kontrola kopiranja ili štampanja sadržaja datoteke)

- Ovde se vidi zbog čega tradicionalni „ima-nema“ pristup zaštiti podataka nije pogodan u okruženju oblaka

Tehnička realizacija zaštite u oblaku

- Fizička zaštita u centrima podataka, koja uključuje biometrijske čitače, close-circuit TV (CCTV), detekciju pokreta itd.
- Zaštita mreže koja uključuje spoljašnje sisteme zaštitnog zida, sisteme za detekciju upada, procenu slabosti od strane treće strane (eng. third party vulnerability assessment)
- Zaštita platforme koja uključuje SSL, šifrovanje podataka, politike korišćenja lozinki, i sertifikaciju sistema (eng. system trust certification)

Modeli usluge u oblaku



Infrastruktura kao usluga i zahtevi u pogledu zaštite

- Skladištenje i obrada podataka: HIPS, HIDS, zaštitni zid na jednom računaru, šifrovanje , zaštita integriteta datoteka
- Bezbedna obrada podataka (eng. trusted computing): tehnologija koju razvija konzorcijum Trusted Computing Group i koja omogućuje određeni nivo sigurnosti da hardver i softver nisu zlonamerno menjani
- Umrežavanje: NIDS, NIPS, zaštitni zid, sistemi za zaštitu od napada odbijanjem usluge

Platforma kao usluga i zahtevi u pogledu zaštite

Upravljanje identitetima i pristupom

Programska podrška kao usluga i zahtevi u pogledu zaštite

Podaci: zaštita od gubitka podataka, nadzor aktivnosti baze podataka, šifrovanje, vodeni žig, bojenje podataka
Aplikacija: aplikativni zaštitni zid (eng. app firewall), zaštita prava kopiranja

Tehnike koje se koriste u oblaku

- Digitalni vodeni žig (eng. digital watermarking)
- Bojenje podataka (eng. data coloring)

Digitalni vodeni žig

To je tehnologija zaštite prava kopiranja (eng. copyright protection) koja se zasniva na ugrađivanju (eng. embed) informacije o pravima kopiranja u digitalne podatke.
Male slike ili obrasci se ubacuju u digitalne podatke na način koji ne ometa njihovo normalno korišćenje.
Ako dodje do ilegalnog kopiranja podataka, legitimni vlasnik podataka može proveriti postojanje vodenih oznaka u podacima, i na taj način potvrditi svoje vlasništvo nad podacima.

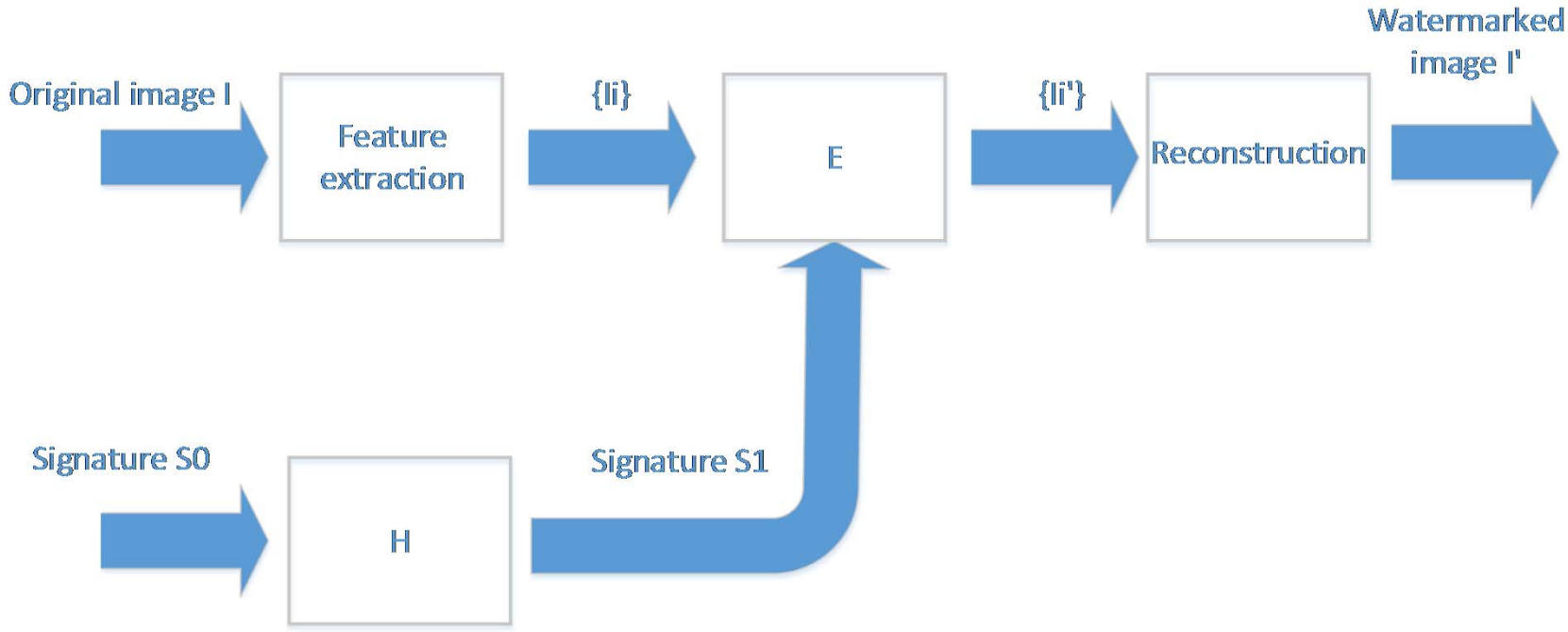
Na prethodnom slajdu je pomenuto samo utvrđivanje vlasništva nad podacima, ali u opštem slučaju detekcija odnosno izdvajanje potpisa iz podataka zaštićenih žigom omogućuje da se:

- Identifikuje vlasnik podataka,
- Identifikuje predviđeni primalac odnosno korisnik nosioca podataka, kao i
- Autentičnost samih nosilaca podataka

Bitne osobine tehnike digitalnog vodenog žiga

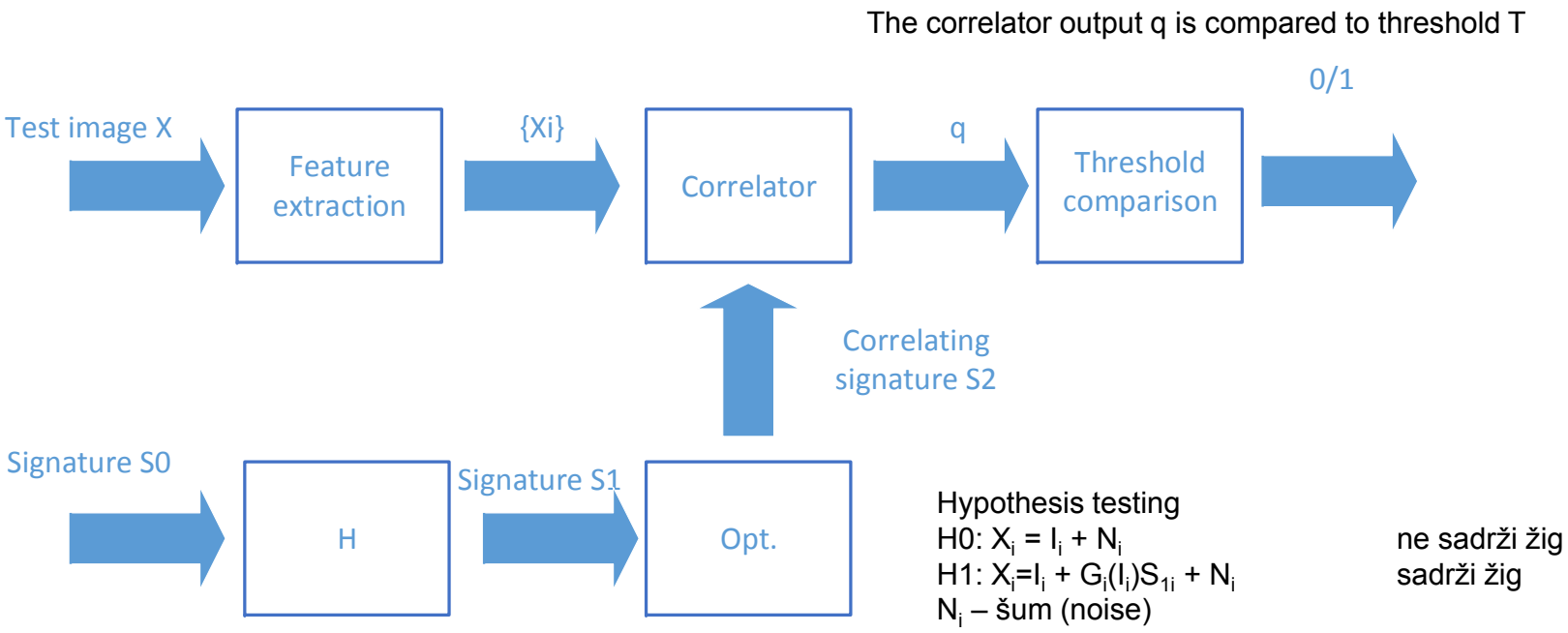
Robustnost – gubitak (malog) dela poruka ne treba da spreči prepoznavanje žiga
Detektabilnost – žig se datom tehnikom uvek prepoznaje
Očuvanost signala – degradacija osnovne poruke ugradnjom žiga treba da bude minimalna ili je u nekim slučajevima ne sme uopšte biti
Veličina žiga u bajtima – veći žig sprečava mogućnost da dva različita žiga budu prepoznata kao isti, ali ne sprečava izmene žiga od strane napadača
Trošak ugradnje žiga – treba da bude minimalan

Koder vodenog žiga (eng. watermark encoder)



Encoding process on feature I_i: $I_i' = I_i + G_i(I_i)S_{1i}$
The watermarked image is constructed based on modified features set $\{I_i'\}$ and unmodified data.

Dekoder vodenog žiga (eng. watermark decoder)



Legenda

Extraction of multiresolution watermark images for resolving rightful ownership
Wenjun Zeng, Bede Liu, Shawmin Lei

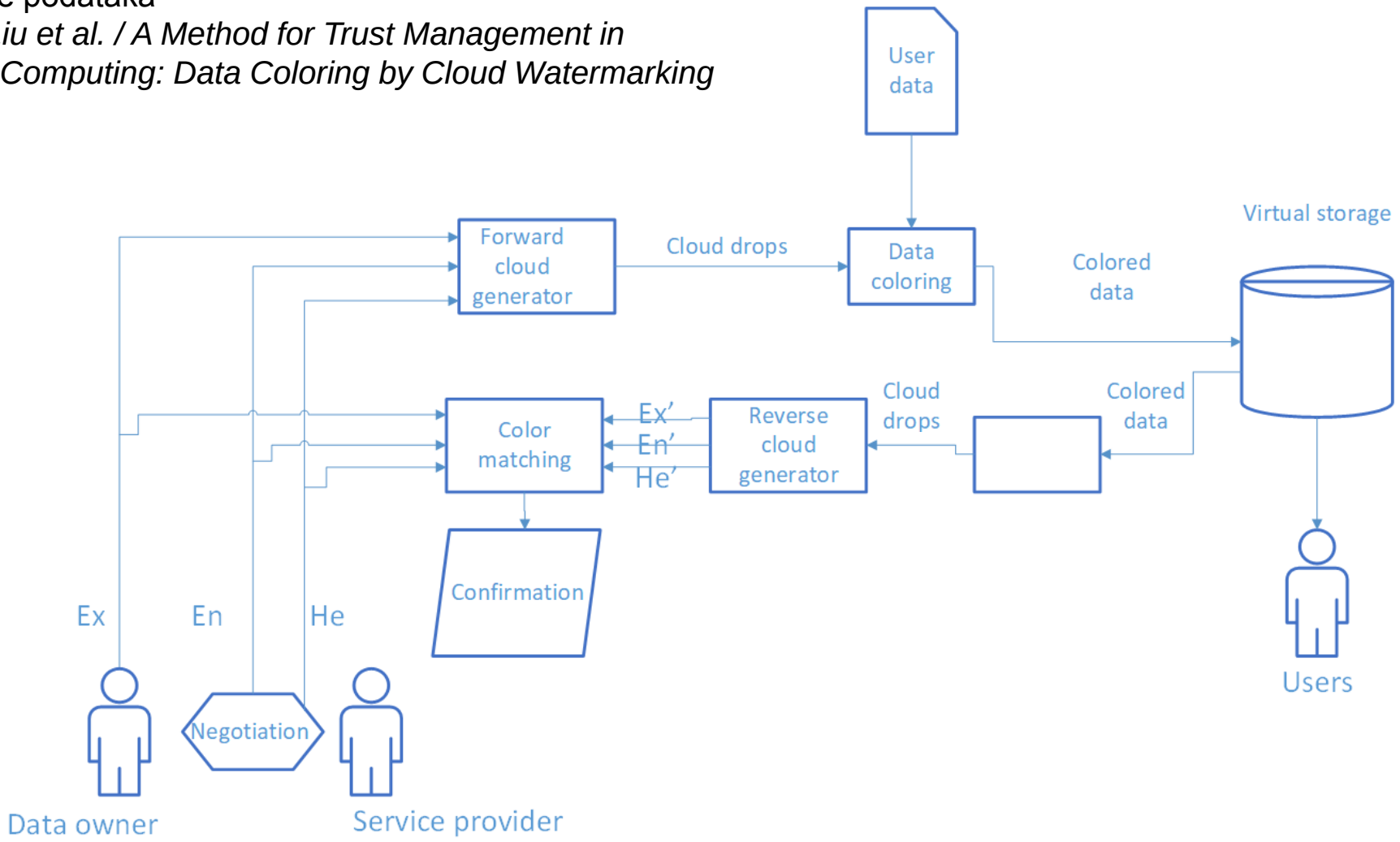
H – deterministička funkcija sa jednim prolazom (eng. one way)
S0 – potpis sa realnim značenjem – na primer registrovani identitet korisnika
S2 – pseudoslučajan niz visoko korelisan sa *S1*, optimizovan tako da poboljša performansu detektora. Treba da bude nekorelisan sa originalnom slikom *I*. Srednja vrednost *S2i* = 0.
S1 – i.i.d (independent identically distributed) pseudoslučajan niz. Moduliše se sa slikom vodenog žiga, pre ugrađivanje u originalnu sliku.
Ii – skup osobina, može biti naprimer podskup DCT koeficijenata 8x8 blokova u originalnoj slici

Bojenje podataka

Bojenje podataka u oblaku je proširenje gornje tehnike tako što svaki korisnik dobija svoju boju, i svi njegovi podaci se boje (pored ugrađivanja vodenih oznaka).
Boja se generiše na osnovu nekoliko komponenti od kojih neke zavise od objekta podataka, a neke su poznate samo korisniku i specifične za njega
Proces poređenja boja (eng. color matching) obezbedjuje da boje korišćene u identifikaciji korisnika odgovaraju bojama podataka.
Na taj način, legitimni vlasnici jedini imaju pristup svojim objektima podataka.

Bojenje podataka

Y. C. Liu et al. / A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking



Prikazan je sistem bojenja koji omogućuje korisniku da proveri da li su njegovi podaci “procureli” iz oblaka.
Predloženi sistem je nepotpun, ali može da bude osnova za dalji rad.

Legenda

Ex očekivana vrednost (eng. expected value), izvor je korisnik
En entropija, rezultat pregovaranja korisnika i uslužioca
He hiper entropija, rezultat pregovaranja korisnika i uslužioca

Cilj predloga

Za razliku od tradicionalnog vodenog žiga gde se samo ugrađuje korisnikov žig u podatke, ovde se boje svi njegovi podaci.
Svaki fragment korisnikovih podataka je obeležen.
Svaki korisnik dobija specifičnu boju koja ne ometa normalno korišćenje podataka.

Generator kapi za bojenje

eng. Forward cloud drop generator

Korak 1: generisanje slučajnog broja po normalnoj raspodeli

$$En_i' = \mathrm{NORM}(\mathrm{En}, He^2)$$

Korak 2: generisanje slučajnog broja po normalnoj raspodeli

$$x_i = NORM(Ex, {En'}_i^2)$$

Korak 3:

$$\mu_i = e^{\frac{-(x_i - E_x)^2}{2(En_i')^2}}$$

Korak 4: xi sa stepenom sigurnosti μi je kap za bojenje

Inverzni generator kapi za bojenje

eng. Reverse cloud drop generator

Korak 1: sračunati aritmetičku sredinu $\bar{X} = \frac{1}{n}\sum_{i=1}^{n} x_i$ i varijansu

$$S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{X})^2$$

Korak 2: $Ex' = \bar{X}$

Korak 3: $En' = \sqrt{\frac{\pi}{2}} \times \frac{1}{n}\sum_{i=1}^{n}|x_i - E_x|$

Korak 4: $He' = \sqrt{S^2 - En'^2}$

Korišćenje jednokratnog ključa (eng. one time pad)

Jednokratni ključ je dugo poznat koncept zaštite komunikacije, gde se poruka koja se šalje šifruje (logičko ILI) sa slučajno generisanim nizom podataka iste dužine.
Pretpostavke su da se jedan slučajni niz koristi samo za jednu poruku (za svaku se generiše novi), da je niz stvarno slučajan, i da se slučajni niz prenese primaocu odvojenim putem
Korišćen je za zaštitu komunikacija između Čerčila i Ruzvelta 1944 (SIGSALY) kao i tokom kubanske krize za komunikacije između vlada SSSR i SAD


1943 SIGSALY 1946
SPEECH ENCIPHERMENT SYSTEM

Paul Tobin i kolege sa Dublinskog instituta za tehnologiju su nedavno predložili korišćenje jednokratnog ključa za zaštitu ličnih podataka u oblaku (naprimer zdravstvenih).

U tom slučaju korisnik će čuvati slučajni niz na fleš memoriji ili sličnom uređaju, i pošto sadržaju pristupa samo on (ili naprimer njegov lekar), problem distribucije ključa (eng. key distribution problem) je praktično izbegnut.