
Operații pe date encrypted la nivelul ORM-ului în contextul coregrafiilor encrypted

— Ioana - Maria Bogdan —
coord. Conf. dr. Lenuța Alboaie

Cuprins

1. Motivație
2. ORM & Apersistence
3. Modelul coregrafiilor executabile
4. Coregrafii encrypted
5. Use case
6. Contribuții
7. Concluzii

Motivație

Motivație

- fiecare utilizator de internet și-a furnizat o parte din datele personale cel puțin unui furnizor de servicii
- fiecare utilizator de internet are în medie 5.4 conturi pe rețelele de socializare și 40 de conturi online
- în acest moment se estimează că aproximativ 44 de înregistrări cu date private sunt copiate ilegal în fiecare secundă
- procentul de date criptate care au fost extrase ilegal din bazele de date este de 4.2%

Motivație

- fiecare utilizator de internet și-a furnizat o parte din datele personale cel puțin unui furnizor de servicii
- fiecare utilizator de internet are în medie 5.4 conturi pe rețelele de socializare și 40 de conturi online
- în acest moment se estimează că aproximativ 44 de înregistrări cu date private sunt copiate ilegal în fiecare secundă
- procentul de date criptate care au fost extrase ilegal din bazele de date este de 4.2%

Motivație

- fiecare utilizator de internet și-a furnizat o parte din datele personale cel puțin unui furnizor de servicii
- fiecare utilizator de internet are în medie 5.4 conturi pe rețelele de socializare și 40 de conturi online
- în acest moment se estimează că aproximativ 44 de înregistrări cu date private sunt copiate ilegal în fiecare secundă
- procentul de date criptate care au fost extrase ilegal din bazele de date este de 4.2%

Motivație

- fiecare utilizator de internet și-a furnizat o parte din datele personale cel puțin unui furnizor de servicii
- fiecare utilizator de internet are în medie 5.4 conturi pe rețelele de socializare și 40 de conturi online
- în acest moment se estimează că aproximativ 44 de înregistrări cu date private sunt copiate ilegal în fiecare secundă
- procentul de date criptate care au fost extrase ilegal din bazele de date este de 4.2%

Principalele tehnologii și modele arhitecturale utilizate

- apersistence
- coregrafii executabile

ORM & Apersistence

- modul *open source* de *npm* (node package manager)
- dezvoltat pentru proiectul *SwarmESB*, *PrivateSky*
- creează ORM-uri atât peste baze de date relaționale (*MySQL*) cât și nerelaționale (*Redis*)
- în modulul de baza s-a adăugat suport pentru criptarea datelor
- operațiile de criptare adăugate permit operații de egalitate și de comparare

ORM & Apersistence

- modul *open source* de *npm* (node package manager)
- dezvoltat pentru proiectul *PrivateSky* care se bazează pe *SwarmESB*
- creează ORM-uri atât peste baze de date relaționale (*MySQL*) cât și nerelaționale (*Redis*)
- în modulul de baza s-a adăugat suport pentru criptarea datelor
- operațiile de criptare adăugate permit operații de egalitate și de comparare

ORM & Apersistence

- modul *open source* de *npm* (node package manager)
- dezvoltat pentru proiectul *PrivateSky* care se bazează pe *SwarmESB*
- creează ORM-uri atât peste baze de date relaționale (*MySQL*) cât și nerelaționale (*Redis*)
- în modulul de baza s-a adăugat suport pentru criptarea datelor
- operațiile de criptare adăugate permit operații de egalitate și de comparare

ORM & Apersistence

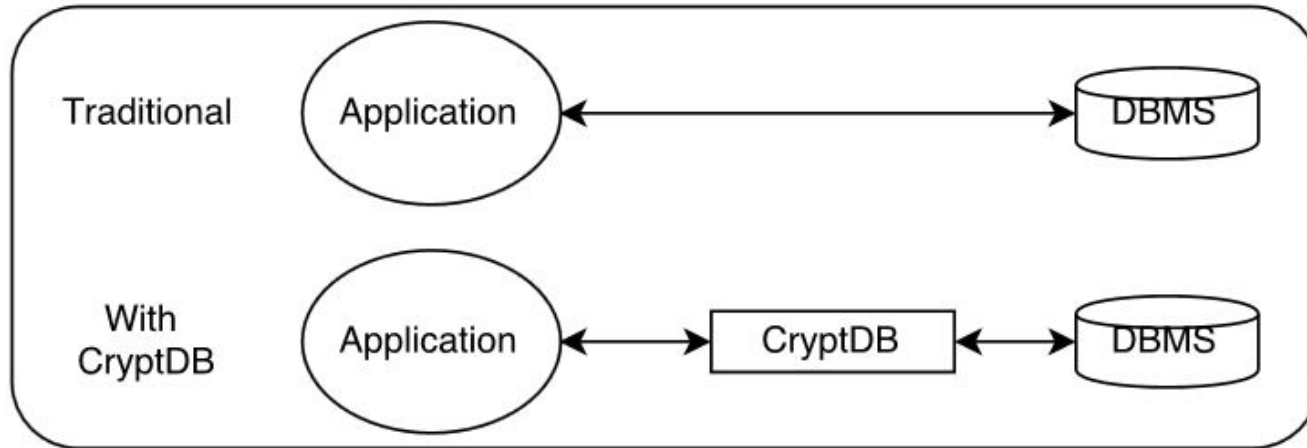
- modul *open source* de *npm* (node package manager)
- dezvoltat pentru proiectul *PrivateSky* care se bazează pe *SwarmESB*
- creează ORM-uri atât peste baze de date relaționale (*MySQL*) cât și nerelaționale (*Redis*)
- în modulul de baza s-a adăugat suport pentru criptarea datelor
- operațiile de criptare adăugate permit operații de egalitate și de comparare

ORM & Apersistence

- modul *open source* de *npm* (node package manager)
- dezvoltat pentru proiectul *PrivateSky* care se bazează pe *SwarmESB*
- creează ORM-uri atât peste baze de date relaționale (*MySQL*) cât și nerelaționale (*Redis*)
- în modulul de baza s-a adăugat suport pentru criptarea datelor
- operațiile de criptare adăugate permit operații de egalitate și de comparare

ORM & Apersistence

- model inspirat din *CryptDB*



<http://web-in-security.blogspot.ro/2015/12/analysis-of-encrypted-databases-with.html>

Apersistence - use case

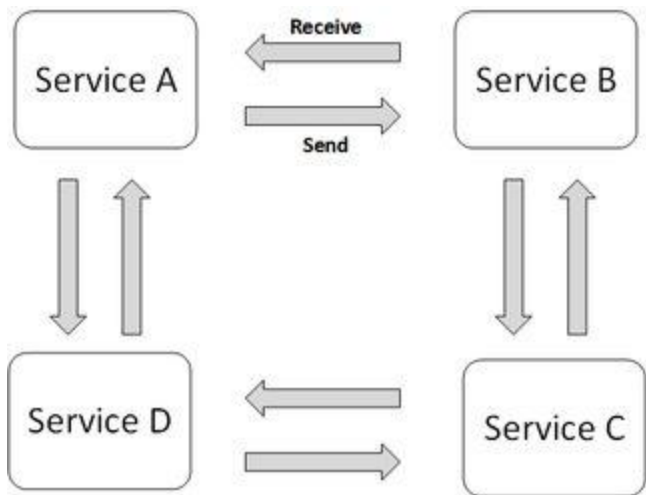
```
{ __meta:
  { typeName: 'Person',
    freshRawObject: true,
    savedValues: { name: 'ana',
                  lastName: 'popescu' },
    getPK: [Function: bound ],
    getPKField: [Function],
    loadLazyField: [Function],
    loadLazyFields: [Function] },|
  assign: [Function: bound castAssign],
  name: 'ana',
  lastName: 'popescu' }
```

Înregistrare care nu folosește beneficiile de securitate adăugate în *apersistence*

```
{ __meta:
  { typeName: 'Person',
    freshRawObject: true,
    savedValues:
      { name: 'f458cb536c4eb9ee749dbaa3e67144fc',
        lastName: '0ce8612d92e708fb5247235378b37582' },
    getPK: [Function: bound ],
    getPKField: [Function],
    loadLazyField: [Function],
    loadLazyFields: [Function] },
  assign: [Function: bound castAssign],
  name: 'f458cb536c4eb9ee749dbaa3e67144fc',
  lastName: '0ce8612d92e708fb5247235378b37582' }
```

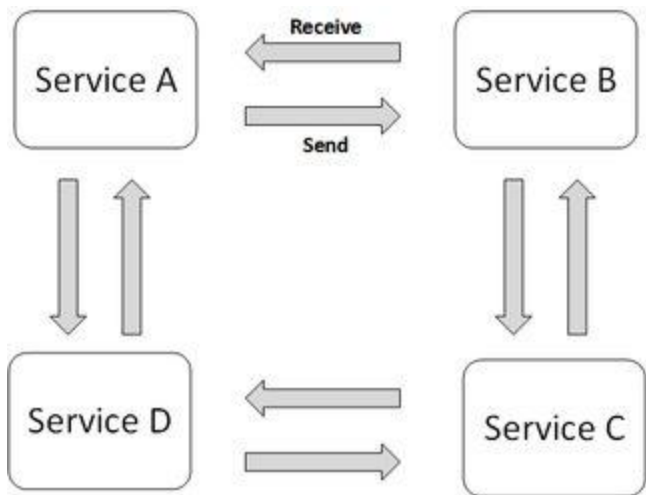
Înregistrare care folosește beneficiile de securitate adăugate în *apersistence*

Modelul coregrafiei executabile



- coregrafia se caracterizează printr-o descriere globala a serviciilor și reguli de interacțiune dintre acestea
- modelul **coregrafiei executabile** aduce ca noutate faptul că interacțiunile nu sunt globale, ci sunt învățate pe parcurs

Modelul coregrafiei executabile



- coregrafia se caracterizează printr-o descriere globala a serviciilor și reguli de interacțiune dintre acestea
- modelul **coregrafiei executabile** aduce ca noutate faptul că interacțiunile nu sunt globale, ci sunt învățate pe parcurs

Model propus

coregrafii encrypted

Coregrafii encrypted

- propun un model care ajută la mitigarea impactului scurgerii de date
- cripteaza datele sensibile la nivelul ORM-ului (folosind *Apersistence*)
- folosesc un sistem de gestionare a cheilor de criptare care se bazeaza pe coregrafii executabile (*Private Data System*)
- coreografiile criptate (*encrypted choreographies*) se bazează pe existența unor mijloace de control a cheilor de criptare (*PDS*) și mecanisme de identificare și autentificare (*apersistence*) ce permit crearea de coregrafii sigure din punct de vedere al datelor criptate între două sau mai multe organizații.

Coregrafii encrypted

- propun un model care ajută la mitigarea impactului scurgerii de date
- cripteaza datele sensibile la nivelul ORM-ului (folosind *apersistence*)
- folosesc un sistem de gestionare a cheilor de criptare care se bazeaza pe coregrafii executabile (*Private Data System*)
- coreografiile criptate (*encrypted choreographies*) se bazează pe existența unor mijloace de control a cheilor de criptare (*PDS*) și mecanisme de identificare și autentificare (*apersistence*) ce permit crearea de coregrafii sigure din punct de vedere al datelor criptate între două sau mai multe organizații.

Coregrafii encrypted

- propun un model care ajută la mitigarea impactului scurgerii de date
- cripteaza datele sensibile la nivelul ORM-ului (folosind *apersistence*)
- folosesc un sistem de gestionare a cheilor de criptare care se bazeaza pe coregrafii executabile (*Private Data System*)
- coregrafiile criptate (*encrypted choreographies*) se bazează pe existența unor mijloace de control a cheilor de criptare (*PDS*) și mecanisme de identificare și autentificare (*apersistence*) ce permit crearea de coregrafii sigure din punct de vedere al datelor criptate între două sau mai multe organizații.

Coregrafii encrypted

- propun un model care ajută la mitigarea impactului scurgerii de date
- cripteaza datele sensibile la nivelul ORM-ului (folosind *apersistence*)
- folosesc un sistem de gestionare a cheilor de criptare care se bazeaza pe coregrafii executabile (*Private Data System*)
- coreografiile criptate (*encrypted choreographies*) se bazează pe existența unor mijloace de control a cheilor de criptare (*PDS*) și mecanisme de identificare și autentificare (*apersistence*) ce permit crearea de coregrafii sigure din punct de vedere al datelor criptate între două sau mai multe organizații.

Private Data System

- sistem distribuit care permite stocarea si redistribuirea datelor private via internet
- sistem format din noduri distribuite care sunt folosite pe post de baze de date locale de tipul *key-value*
- datele private sunt impartite in *chunk*-uri indecifrabile si distribuite in retea
- *PDS* propune moduri de gestionare (*create, read, update, share access, revoke access*) a datelor private
- propunere DAIS2017 (*International Conference on Distributed Applications and Interoperable Systems*)

Private Data System

- sistem distribuit care permite stocarea si redistribuirea datelor private via internet
- sistem format din noduri distribuite care sunt folosite pe post de baze de date locale de tipul *key-value*
- datele private sunt impartite in *chunk*-uri indecifrabile si distribuite in retea
- *PDS* propune moduri de gestionare (*create, read, update, share access, revoke access*) a datelor private
- propunere DAIS2017 (*International Conference on Distributed Applications and Interoperable Systems*)

Private Data System

- sistem distribuit care permite stocarea si redistribuirea datelor private via internet
- sistem format din noduri distribuite care sunt folosite pe post de baze de date locale de tipul *key-value*
- datele private sunt impartite in *chunk*-uri indecifrabile si distribuite in retea
- *PDS* propune moduri de gestionare (*create, read, update, share access, revoke access*) a datelor private
- propunere DAIS2017 (*International Conference on Distributed Applications and Interoperable Systems*)

Private Data System

- sistem distribuit care permite stocarea si redistribuirea datelor private via internet
- sistem format din noduri distribuite care sunt folosite pe post de baze de date locale de tipul *key-value*
- datele private sunt impartite in *chunk*-uri indecifrabile si distribuite in retea
- *PDS* propune moduri de gestionare (*create, read, update, share access, revoke access*) a datelor private
- propunere DAIS2017 (*International Conference on Distributed Applications and Interoperable Systems*)

Private Data System

- sistem distribuit care permite stocarea si redistribuirea datelor private via internet
- sistem format din noduri distribuite care sunt folosite pe post de baze de date locale de tipul *key-value*
- datele private sunt impartite in *chunk*-uri indecifrabile si distribuite in retea
- *PDS* propune moduri de gestionare (*create, read, update, share access, revoke access*) a datelor private
- propunere DAIS2017 (*International Conference on Distributed Applications and Interoperable Systems*)

Use case

aplicație proof of concept

- DEMO

Concluzii

- s-a prezentat un sistem care permite interogări pe date criptate
- interogările sunt procesate la nivelul bazei de date si nu este nevoie de decriptare
- față de alte abordări, cum ar fi CryptDB, modelul de față constă în modificarea ORM-ului pentru a suporta operații de criptare
- modul de gestionare a parolelor se bazează pe coregrafii executabile

Concluzii

- s-a prezentat un sistem care permite interogări pe date criptate
- interogările sunt procesate la nivelul bazei de date si nu este nevoie de decriptare
- față de alte abordări, cum ar fi CryptDB, modelul de față constă în modificarea ORM-ului pentru a suporta operații de criptare
- modul de gestionare a parolelor se bazează pe coregrafii executabile

Concluzii

- s-a prezentat un sistem care permite interogări pe date criptate
- interogările sunt procesate la nivelul bazei de date si nu este nevoie de decriptare
- față de alte abordări, cum ar fi CryptDB, modelul de față constă în modificarea ORM-ului pentru a suporta operații de criptare
- modul de gestionare a parolelor se bazează pe coregrafii executabile


Concluzii

- s-a prezentat un sistem care permite interogări pe date criptate
- interogările sunt procesate la nivelul bazei de date și nu este nevoie de decriptare
- față de alte abordări, cum ar fi CryptDB, modelul de față constă în modificarea ORM-ului pentru a suporta operații de criptare
- modul de gestionare a parolelor se bazează pe coregrafii executabile

Contribuții

Contribuții

- Modelul descris a fost propus la ICCP 2017

| Paper 83 | |
|------------------|--|
| Title: | Operations on encrypted data in an ORM made for encrypted choreographies |
| Paper: |  |
| Author keywords: | encrypted database encrypted choreography executable choreography Private Data System |

| Authors | | | | | | |
|------------|-----------|---------------------------|---------|--|----------|----------------|
| first name | last name | email | country | organization | Web page | corresponding? |
| Alboaie | Sînică | salboaie@gmail.com | Romania | Faculty of Computer Science Alexandru Ioan Cuza University of Iasi | | ✓ |
| Ioana | Bogdan | ioana.bogdan@info.uaic.ro | Romania | Faculty of Computer Science Alexandru Ioan Cuza University of Iasi | | |
| Alboaie | Lenuța | adria@info.uaic.ro | Romania | Faculty of Computer Science Alexandru Ioan Cuza University of Iasi | | ✓ |

Concluzii

- s-a prezentat un sistem care permite interogări pe date criptate
- interogările sunt procesate la nivelul bazei de date și nu este nevoie de decriptare
- față de alte abordări, cum ar fi CryptDB, modelul de față constă în modificarea ORM-ului pentru a suporta operații de criptare
- modul de gestionare a parolelor se bazează pe coregrafii executabile