Raport stiintific si tehnic in extenso pentru proiectul *Dezvoltarea de de tehnologii pentru securizarea datelor in Cloud – DTSDC*

Etapa I - Studii tehnice privind protectia informatiilor in cloud utilizand mecanisme criptografice

REZUMAT

Scopul proiectului pentru care este realizat prezentul raport il reprezinta dezvoltarea de tehnologii noi de protectie a informatiilor, tehnologii care sa permita asigurarea securitatii datelor atat din momentul in care acestea sunt migrate de pe sistemele de calcul clasice (calculatoare sau servere individuale) catre sisteme virtualizate sau de tip cloud cat si in situatia in care datele sunt create in astfel de sisteme inca de la inceput.

Cloud computing reprezinta un concept de prezentare a serviciilor ce tin de tehnologia informatiilor (IT) astfel incat utilizatorii nu trebuie sa detina resursele hardware si software pentru rularea serviciilor IT pe care le utilizeaza ci au acces la aceste resurse la distanta, peste Internet. Cloud computing nu este un domeniu nou din punct de vedere al serviciilor oferite dar acesta a cunoscut o expansiune importanta in ultimii ani si tinde sa devina mecanismul principal prin care serviciile IT sunt puse la dispozitia utilizatorilor. Acest lucru conduce practic la disparitia datelor stocate pe echipamente de calcul aflate sub controlul direct al utilizatorului, informatiile fiind pastrate la distanta, in centre de date asupra carora utilizatorul final nu detine niciun fel de control.

Utilizarea cloud reclama mecanisme de protectie a informatiilor adaptate acestui mod de lucru, astfel incat decizia privind modul de protectie si diseminare a informatiilor sa ramana sub controlul utilizatorului final. Chiar daca datele utilizatorului sunt copiate pe servere diverse, in centre de date distribuite la nivel mondial, aceste informatii nu trebuie sa poata fi accesate in mod neautorizat de catre terti iar elementele esentiale ce definesc protectia informatiilor trebuie sa fie asigurate cel putin la acelasi nivel de incredere ca atunci cand datele s-ar afla pe un sistem de calcul controlat in exclusivitate de catre utilizator:

- Autenticitate - se cunoaste cu siguranta sursa informatiilor
- Integritate - informatiile nu au fost modificate neautorizat fara a fi detectat acest lucru
- Non-repudiere - actiunile intreprinse nu pot fi negate
- Confidentialitate - este pastrat secretul informatiilor si acestea nu pot fi accesate neautorizat
- Disponibilitate – datele sunt accesibile utilizatorilor atunci cand au nevoie de ele

Etapele proiectului cuprind:

1. Studii tehnice privind protectia informatiilor in cloud utilizand mecanisme criptografice
2. Elaborarea si dezvoltarea modelelor experimentale
3. Proiectarea prototipurilor si elaborarea documentatiei tehnice de realizare
4. Dezvoltarea, testarea si validarea prototipurilor
5. Transferul tehnologic al rezultatelor de dezvoltare experimentala

1 Descrierea etapei si a activitatilor

Prima etapa a proiectului cuprinde Studii tehnice privind protectia informatiilor in cloud utilizand mecanisme criptografice. Etapa a cuprins 7 activitati si livrabilele aferente:

1. Activitatea I.1 Studiu de fezabilitate tehnica pentru cercetarea industriala asupra tehnologiilor de protectie a informatiilor in cloud, cu livrabilul:
    a. Studiu de fezabilitate tehnica pentru cercetarea industriala asupra tehnologiilor de protectie a informatiilor in cloud

In cadrul activitatii I.1 a fost realizat un studiu de fezabilitate tehnica pentru cercetarea industriala asupra tehnologiilor de protectie a informatiilor in cloud. Studiul a avut in vedere sistemele de operare cele mai raspandite precum si platformele utilizate ca si baza pentru tehnologia cloud la nivel global si a considerat ca, indiferent de tipul de cloud furnizat, cerintele si metodele de protectie sunt similare.

Din punct de vedere al cerintelor de securitate, acestea includ: stocarea datelor in cloud, autentificare utilizatorului la serviciile de tip cloud, E-mail, operarea de aplicatii in cloud, stergere datelor la distanta.

In acest moment piata tehnologiilor de protectie in cloud este neomogena si nu exista standarde care sa reglementeze modul de protectie a informatiilor in cloud.

Cota de piata cea mai mare este ocupata de de marii producatori de software: Microsoft, Apple, Google, IBM, de companii ce activeaza in comertul online precum Amazon precum si de mari producatori in domeniu solutiilor de securitate gen Symantec sau McAfee. Au fost analizate mecanismele de protectie atat din punct de vedere al functionalitatilor oferite nativ de fiecare producator cat si din perspectiva posibilitatii de a dezvolta aplicatii care sa se integreze nativ in platformele cloud puse la dispozitie. Astfel, exista posibilitatea de autentificare a utilizatorilor pentru in cloud, stergerea la distanta a datelor sau criptarea continutului stocat cu decriptare la utilizator sau prin mecanismele de securitate ale furnizorului de cloud. In prezent, una din problemele majore care impiedica adoptarea tehnologiei cloud la nivel global este data de faptul ca, in marea majoritate a cazurilor si in special in ceea ce priveste prelucrarea datelor in cloud, nu exista mecanism de securitate care sa impiedice accesul furnizorului de cloud la datele stocate.

2. Activitatea I.2 Studiu de fezabilitate tehnica pentru dezvoltarea experimentala a tehnologiilor de protectie a informatiilor in cloud, cu livrabilul:
    a. Studiu de fezabilitate tehnica pentru dezvoltarea experimentala a tehnologiilor de protectie a informatiilor in cloud

In cadrul activitatii I.2 s-a realizat un studiu de fezabilitate tehnica cu privire dezvoltarea experimentala a tehnologiilor de criptare in cloud cu accent pe mecanismele de criptare homomorfica, a posibilitatilor de aplicare a acestora in practica, dar si din punctul de vedere al avantajelor obtinute prin implementarea acestora. In cadrul studiului s-au avut in vedere aspecte cum ar fi elemente de teoria numerelor aplicabile in criptografie si in special in criptarea homomorfica, rezultatele obtinute in cadrul implementarilor realizate dea lungul timpului in literatura de specialitate (*state of the art*), algoritmii de calcul si mecanismele principale folosite in cadrul acestor implementari, securitatea si vulnerabilitatile schemelor de criptare homorfice.

Au fost analizate rezultatele obtinute in domeniul criptografiei homomorfice pe doua paliere:

- Criptosisteme partial homomorfice: Unpadded RSA, ElGamal, Goldwasser-Micali, Benaloh, Paillier
- Criptosisteme full homorfice. Au fost analizate in special schemele propuse de Craig Gentry bazate pe latici. In acest caz problemele majore identificate au fost in special cele legate de aplicabilitatea unei asemenea scheme, avand in vedere faptul ca, datorita puterii de calcul existente, nu pot fi utilizate polinoame cu grad mare deoarece zgomotul rezultat in urma procesului de criptare/decriptare face practic sistemul indescifrabil. Au fost retinute totusi o serie de elemente ce pot constitui o baza in cercetarea stiintifica ulterioara.

3. Activitatea I.3 Studiu privind implementarea si utilizarea mecanismelor de criptare homomorfica cu livrabilul:
    a. Studiu privind implementarea si utilizarea mecanismelor de criptare homomorfica

I n cadrul activitatii I.3 a fost realizata analiza pentru implementarea si utilizarea mecanismelor de criptare homomorfica.

Asa cum a reiesit din activitatile anterioare, intrebararea principala atunci cand se pune problema migrarii informatiilor in cloud este „Este posibil sa delegi procesarea datelor tale fara sa delegi si controlul asupra acestora?". Aceasta intrebare a fost dintotdeauna importanta insa acum, o data cu extinderea cloud computingului devine din ce in ce mai importanta. Raspunsul la aceasta intrebare este mecanismul de tip „criptare complet homorfica" (FHE), care este o modalitate foarte puternica de criptare ce permite unui server care nu este de incredere sa proceseze datele unui client.

Schema initiala pentru criptarea homorfica a fost introdusa de catre R. Rivest, L. Adleman, and M. Dertouzos. in lucrarea „ On data banks and privacy homomorphisms.". Aceasta schema a ramas deschisa pana in anul 2009, atunci cand Gentry a reusit realizarea unei scheme FHE bazata pe teoria laticelor ideale. In acest sens, studiul din aceasta activitate si-a propus sa prezinte si sa studieze cele mai importante scheme FHE.

4. Activitatea I.4 Studiu privind integrarea mecanismelor de protectie a informatiilor in servicii cloud oferite de terti, cu livrabilul:
    a. Studiu privind integrarea mecanismelor de protectie a informatiilor in servicii cloud oferite de terti

In cadrul activitatii I.4 a fost realizat un studiu privind integrarea mecanismelor de protectie in servicii cloud oferite de terti. In cadrul acestui studiu s-au analizat doua directii:

- Utilizarea de algoritmi de criptare clasici pentru operatiunile de stocare in cloud oferite de terti
- Utilizarea de scheme FHE.

In primul caz s-a studiat posibilitatea utilizarii solutiilor existente de criptare pentru protectia datelor in sistemele de cloud existente. O prima concluzie a studiului a fost aceea ca marea majoritate a furnizorilor de cloud nu ofera in acest moment mecanisme puternice de criptare a datelor stocate in cloud. Acestea au la baza solutii de autentificare bazate pe nume utilizator si parola sau anumite tipuri de criptari hibride bazate pe chei publice. In acest ultim caz insa cheile sunt sub controlul furnizorului de cloud ceea ce ridica probleme serioase de siguranta in ceea ce il priveste pe utilizatorul final.

Analiza a fost realizata in principal pe aplicatiile oferite de Microsoft prin Office 365 si de Google prin GoogleDocs.

5. Activitatea I.5 Studiu privind mecanisme de securitate existente la nivelul tehnologiilor cloud, cu livrabilul:

a. Studiu privind mecanisme de securitate existente la nivelul tehnologiilor cloud

In cadrul activitatii I.5 a fost realizat un studiu privind mecanismele de securitate existente la nivelul tehnologiilor cloud.

Pentru inceput, s-a incercat definirea riscurilor de acces din urmatoarele perspective:

- Stocarea datelor – este necesara evaluarea politicii de securitate precum si ale mecanismelor existente pentru evalua cat de bine sunt protejate datele ce sunt stocate pe serverele furnizorului de cloud.
- Transfer de date – in ce masura datele sunt criptate intre utilizator si centrul de date din cloud
- Segregarea datelor – in ce masura compromiterea datelor unui utilizator afecteaza si pe alti utilizatori

Au fost analizate o serie de lucrari in domeniu, in special, cele elaborate de Cloud Security Alliance (CSA). Pentru a intelege mecanismele de securitate este necesar sa faci o evaluare a principalelor amenintari existente.

Pe primul loc se afla incalcarea securitatii datelor. In cazul datelor in cloud, securitatea este asigurata de cele mai multe ori de furnizor.

Un alt risc este reprezentat de pierderea datelor. Pot fi cazuri in care datele sunt sterse accidental de catre furnizorul de cloud sau de catre un atacator rau intentionat. De asemenea sunt cazuri in care utilizatorii isi stocheaza datele in mod criptat in cloud insa isi pierd cheia de criptare, fapt care duce la pierderea definitiva a acestora.

Alte riscuri legate de pastrarea datelor in cloud mai sunt: atacarea si compromiterea contului detinut in cloud, interfete si API nesigure si care sunt puse la dispozitie de catre furnizorul de cloud, lipsa de acces la serviciu, abuzul furnizorilor de servicii de tip cloud, vulnerabilitatile tehnologice.

6. Activitatea I.6 Studiu privind evaluarea si certificarea produselor de securitate a informatiilor in cloud, cu livrabilul:
    a. Studiu privind evaluarea si certificarea produselor de securitate a informatiilor in cloud

Divulgarea, modificarea, distrugerea sau deturnarea neautorizata a informatiilor duc la prejudicii care pot induce consecinte nefaste pentru cel are este detinatorul de drept al acelor informatiilor. De aceea primul obiectiv al unui produs sau sistem de securitate IT trebuie sa fie acela de a reduce la un nivel acceptabil pentru organizatia interesata, riscurile asociate. Acest obiectiv se atinge prin alegerea caracteristicilor si functiilor de securitate pentru sistemul IT care minimalizeaza riscurile.

La indeplinirea obiectivului de securitate a produselor sau sistemelor IT contribuie diverse procese. Acestea sunt ilustrate in figura 1. Aceasta figura prezinta contextul ideal in care se inscrie evaluarea securitatii IT. Sagetile indica faptul ca fiecare proces furnizeaza datele pentru prelucrarea ulterioara de catre celalalt proces. Procesele pot sa se suprapuna partial. Inlantuirea prelucrarilor este cel mai frecvent ciclica si iterativa.

7. Activitatea I.7 Diseminarea rezultatelor, cu livrabilele:
    a. Site web de prezentare a proiectului
    b. Realizare articol de cercetare

c. Participare la conferinta cu participare internationala

In cadrul activitatii I.7 a fost realizata diseminarea rezultatelor astfel:

- Un site web al proiectului In aceasta etapa a fost demarata implementarea pe site –ul web al CertSIGN (www.certsign.ro), o sectiune speciala dedicata prezentarii cerintelor si rezultatelor obtinute in cadrul proiectului. In acest moment exista pe site –ul certSIGN un link de acces catre acesta sectiune unde sunt prezentate elementele de identificare ale proiectului, obiectivele proiectului, atat cele strategice cat si cele specifice, precum si rezultatele preconizate ale proiectului. Pe masura avansarii activitatilor cuprinse in etapele proiectului vor fi adaugate noi elemente privitoare la rezultatele obtinute precum si actualizari periodice privind stadiul proiectului.
- Realizarea unui articol referitor la analiza schemelor FHE (FULL HOMMOMORPHIC ENCRYPTION) ce urmeaza a fi transmis spre diseminare si in reviste de specialitate.
- Prezentarea articolului la conferinta internationala Cyber Security desfasurata in perioada 21-22 octombrie 2013 si organizata de Universitatea National de Aparare. Prezentarea a atins subiecte de interes, subliniind aspectele ce trebuie avute in vedere inainte de migrarea datelor si aplicatiilor in cloud: Cine opereaza serviciul cloud, Unde se afla centrul de date, Exista sprijin legislativ competent care sa asiste semnarea contractelor cu furnizorul cloud, Cine controleaza securitatea datelor migrate, Este oportuna migrarea datelor guvernamentale/ ale sectorului de aparare in cloud.

- Participarea la Workshop-ul privind "Identificarea electronica si serviciile de incredere" organizat de Comisia Europeana din perspectiva adoptarii noului Regulament al Uniunii Europene cu privire la identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna. Evenimentul a acoperit aspecte privind identificarea utilizatorilor, conceptul „privacy by design", supervizarea serviciilor de incredere. Aceste elemente au legatura directa cu securitatea informatiilor procesate in sistemele de tip cloud, constituind practic cerintele de baza ce urmeaza a fi puse in practica la nivelul Uniunii Europene cu privire la identitatea utilizatorilor, protectia datelor personale ale acestora precum si evaluarea nivelului d eincredere al furnizorilor de servicii electronice. Workshop-ul a fost un eveniment interactiv ce a permis participantilor sa exprime punctele de vedere si informatiile pe care le detin cu privire la subiectele discutate.
- Promovarea solutiilor si studiilor realizate in cadrul unor intalniri cu mediul de afaceri, prin constientizarea acestuia in raport cu riscurile existente in cloud si necesitatea de a implementa solutii care sa asigure confidentialitatea datelor. In acest sens, au fost prezentate solutii care implementeaza pe de o parte anumite elemente de criptare homomorfica, solutii care implementeaza elemente de PKI precum si bune practici in domeniu.In acest sens au fost realizate peste 10 intalniri cu factori de decizie din companii mari ce activeaza in domeniul telecom si energie.
- Realizarea unui workshop in cadrul certSIGN cu studenti din mediul academic (Academia Tehnica Militara si Universitatea Politehnica Bucuresti) in care a fost prezentat stadiul actual al securitatii in cloud, schemele de criptare homorfice existente precum si directiile viitoare de dezvoltare. Seminarul a fost unul interactiv si considerat interesant de studenti si mediul academic.
- Participarea la „Conferinta Internațională: Protecţia infrastructurilor critice din sectoarele energetic şi comunicaţii" organizata de Transelectrica. In cadrul acestei conferinte au fost prezentate riscurile la care se expun sistemele nationale de distribuire a energiei electrice, necesitatea implementarii unui cloud la nivel nationale precum si solutii si proceduri necesare asigurarii securitatii acestuia. Prezentarea a fost sustinuta in prezenta unui auditoriu de peste 100 de persoane din mediul energetic, academic, aparare si privat.
- Participare la conferinta Cyberthreats organizata de Institutul Bancar Roman unde au fost prezentate directiile viitoare de dezvoltare in ceea ce priveste asigurarea confidentialitatii in cloud si evolutia sistemelor de criptare homomorfica. La conferinta au fost prezenti peste 200 de participanti din mediul bancar, IT si servicii.

Director proiect

Adrian Floarea