ON-LINE TÁROLÓHELYEK BIZTONSÁGA

SECURITY IN CLOUD STORAGE

Wagner György[*]

ABSTRACT

The paper starts with the introduction of the different storage methods, which is followed by a detailed description of cloud based storage. The paper also highlights the dangers related to the utilization of the cloud. Later, the author proposes encryption-methods, during both the storage and transfer of data.

1. ADATTÁROLÁS A KEZDETEKTŐL

A számítógépek megjelenésétől kezdve fontos elvárás volt az, hogy a számításokhoz szükséges adatokat ne kelljen minden futtatás során kézzel megadni, valamint az is, hogy a számítások során keletkezett eredményeket el lehessen tárolni. Adatbevitel esetén megoldást jelentett, hogy lyukszalagon, lyukkártyán előzetesen rögzíteni lehetett az adatokat, és a tesztelés, hibakeresés során többszöri futtatásnál ugyanazokkal az adatokkal ellenőrizni lehetett a program helyes működését. A futás során előállt eredmények is rögzíthetők voltak ilyen módon. Ez (a lyukasztás, visszaolvasás) azonban viszonylag lassú volt, és adott esetben jelentős fizikai helyet is igényelt. Jelentős változást a mágneses elven történő adattárolás bevezetése jelentett. Az adatok tárolása eleinte mágnes kártyán, mágnes szalagon, majd különböző méretű és kapacitású hajlékony, illetve merev mágnes lemezeken valósult meg. Idővel elterjedtek az optikai elven működő tárolók (számítások során előálló adatok tárolására kevésbé jellemzők), illetve kevésbé elterjedve a magneto-optikai tárolók (ebben az esetben mágneses elv használatával változtatják meg az információt hordozó anyag optikai tulajdonságait, majd optikai módszerrel olvassák le az információt). A félvezetők árának jelentős esése után meglepő módon nem a számítóközpontokban és az ipari rendszerekben terjedtek el a flash memóriára épülő adattárolási megoldások (pendrive-ok), hanem a vállalati szférában és az otthoni használatban. Megbízhatóságuk az idő múlásával folyamatosan javult. Végül kb. 2010 után elterjedtek a szintén félvezető elven működő vállalati használatra szánt SSD meghajtók, amik már számos előnnyel rendelkeznek.

Bármelyik korszerűbb tárolási módot is vizsgáljuk, megállapítható, hogy bár egyes esetekben alkalmasak ugyan az adatok átvitelére egyik fizikai helyről a másikra (például mágnes lemezek, pendrive-ok), de az adatok mozgatásáról a felhasználónak kell gondoskodnia. Olyan esetekben, amikor viszonylag nagy távolságra levő telephelyeken közel azonos időben van szükség ugyanazokra az adatokra, ez csak olyan esetekben nyújt megoldást, ha statikus adatokról van szó. Ebben az esetben egyszerű többszörözéssel (másolással), és a másolatok fizikai utaztatásával a probléma áthidalható. Változó adatok esetében ez nem alkalmazható, mivel az adatok egyik helyről a másikra való eljuttatásához jelentős időre lehet szükség. A valós életben ilyen esetekben az a jól bevált módszer, ha az adatokat egy megbízható működésű szerveren tárolják, ami hálózaton keresztül elérhető, és ezeket az adatokat különböző felhasználók részére megfelelő hozzáférési engedélyek kialakítása után megosztják. Problémát okozhat, ha ugyanazt az adatot ugyanakkor akarják többen módosítani, de erre jól bevált, különböző szintű zárolásokkal fel lehet készülni.

Egy ilyen fájlszerver jelenthet tehát megoldást, ugyanakkor üzemeltetése költségekkel jár együtt. Az üzemeltetési költség egy része abból adódik, hogy az adatokat tároló szervernek a szükséges időben rendelkezésre kell állnia, másrészt adott időközönként az adatokat archiválni kell, harmadrészt (akár redundanciával) fel kell készülni arra is, ha a hálózat maga akadozik, esetleg teljesen leáll. Ezekre mind fel lehet készülni, de jelentős részben növelik az üzemeltetési költségeket. A költségek azonban csökkenthetők is. Ennek legegyszerűbb módja, ha valamilyen arányban osztódnak. Például egy helyen több fájlszervert üzemeltetnek, vagy egy fizikai szerveren több ügyfél adatai kerülnek tárolásra.

Fájlszerver használata esetén a felhasználó szinte minden esetben tudja, hol található fizikailag az a szerver. Ennek ismeretében képes számolni a biztonságot veszélyeztető faktorokkal, tudatosan fog vállalni kockázatokat. Információkat tud beszerezni a szolgál-

* egyetemi tanársegéd, Miskolci Egyetem, Általános Informatikai Tanszék

tatási helyre jellemző működtetési paraméterekről. Ha azonban (úgy véli, hogy) nincs szüksége a szerver helyének ismeretére, akkor lehetősége van arra, hogy egyszerűen csak tárolási szolgáltatást vegyen igénybe. Ebben az esetben a szervereket képletesen eltakarja egy felhő, mintha a felhőben lennének. Ezt felhő alapú tárolásnak (cloud based storage), a szolgáltatást pedig felhő alapú tárolási szolgáltatásnak (cloud based storage service) nevezzük.

Általában 4 tipikus felhasználási mód jellemző a felhő alapú tárolások használatára [1]. Ezek:

- copy
- backup
- synchronization
- sharing

Copy (másolás) esetében a felhasználó az általa kiválasztott fájlokat felmásolja a szolgáltató által biztosított tároló helyre. Ezt bárhol máshol, ahol szintén megfelelő eléréssel rendelkezik, onnan vissza tudja másolni egy számítógépre.

Backup (archiválás) esetében jellemző módon egy megadott tárterület (egy katalógus, vagy egy partíció) összes fájlja, vagy egy adott feltételnek megfelelő összes fájlja archiválásra kerül. Ezt bizonyos időközönként megismételve rendszer összeomlás, adatvesztés esetén a biztonsági másolatból a rendszer működőképessége helyreállítható.

Szinkronizáció esetében kiválasztott fájlok felkerülnek a felhőbe, majd adott időszakonként ellenőrzésre kerül (akár automatikusan), hogy történt-e változás a mentett változathoz képest. Amennyiben igen, az új változat felkerül a felhőbe. A módszer kiterjeszthető úgy is, hogy több számítógép vesz részt a szinkronizációban. Ennek segítségével minden gépen a legfrissebb változat áll rendelkezése.

Sharing (megosztás) esetében tulajdonképpen egy copy segítségével a fájlok felmásolásra kerülnek, majd megfelelő felhasználók létrehozása, és jogosultságok kiosztása után azt hozzáférhetővé teszik számukra. A megosztásnak 3 esetét szokás felhők esetében megkülönböztetni:

- fájlok megosztása ugyanazon szolgáltatón belüli más előfizetőkkel;
- fájlok megosztása zárt csoportba tartozó nem előfizetőkkel;
- fájlok megosztása bárkivel.

A szolgáltatás elérésére a következő módszerek terjedtek el[1]:

- egyedi kliens szoftver segítségével;
- Web böngészőn keresztül;
- API-n keresztül.

A felhasználó a legkényelmesebb az, amely számára transzparens. Ezt a legkönnyebben az API felhasználásával lehet megvalósítani. Ebben az esetben a fejlesztő olyan alkalmazásokat tud készíteni, amelyek közvetlenül érik el a tárolási felhő szolgáltatásait. Lehetőség van arra is, hogy ezek az alkalmazások az operációs rendszerbe beépüljenek, mintegy plug-inként. Ugyanakkor nem ez a legelterjedtebb [6] [7] [9], hanem az egyedi kliens szoftveres megoldás. Ennek oka valószínűsíthetően az, hogy a különböző operációs rendszert használó kliensek hasonlóképpen működjenek.

2. JELLEMZŐ BIZTONSÁGI KOCKÁZATOK

Az egyes országok törvényi előírásainak megfelelően a biztonsági problémák eltérőek. Létezik olyan biztonsági probléma, amely az egyik országban nem is értelmezhető. Mivel egy felhő esetében a szolgáltatást igénybevevő felhasználó gyakorlatilag nem tudja, hogy melyik országban levő szerveren tárolódnak fizikailag az adatai, adott esetben előfordulhat, hogy az ottani üzemeltető információkat nyer ki a felhasználó adataiból, esetleg saját céljaira rendszeresen lemásolja azokat, és a felhasználó semmilyen jogi lépést nem tehet, mivel az adott országban ez nem számít bűncselekménynek. A felhasználó anyaországában természetesen cél a felhasználó adatainak (személyi adatok, banki adatok, stb.) védelme jogi következményekkel. A tapasztalat azonban azt mutatja, hogy ezek egy már meglévő jogrendszerbe épülnek bele, azok sajátosságainak következményeivel [1].

Elterjedt felhőalapú tárolás biztosító szolgáltatók listája az 1-es táblázatban következik:

CloudMe
CrashPlam
Dropbox
Mozy
TeamDrive
UBUNTU ONE
Wuala
Syncplicity
AVG LiveKive
SpiderOak
Apple iCloud
LogMeIn Cubby
Google Drive
Microsoft SkyDrive
SugarSync
Insync
Boksz

1. táblázat

A felhő alapú szolgáltatásnak sok esetben létezik ingyenes változata. Ennek célja vagy az, hogy megis-

mertessék a szolgáltatást, és így később fizetős ügyfelekké váljanak, vagy eleve ingyenesnek szánják a szolgáltatást, aminek költségét reklám bevételekből fedezik. Az ingyenesnek induló szolgaáltatás használat később átminősíthető fizetőssé, az adatatok megmaradnak, csak a használható tárhely mérete nő meg, illetve a szolgáltatás minősége javul, és újabb funkciók érhetők el. Ez felveti a kérdést, hogy milyen módon történik egy ingyenes szolgáltatásba való regisztrálás. Korrekt esetben a regisztráció során meg kell adni egy e-mail címet, amelyre elküldésre kerül egy aktivációs kód. Ennek visszaküldésével az ügyfél (még akkor is, ha most az ingyenes részét használja a szolgáltatásnak) igazolja az e-mail cím valódiságát, és ezzel valamilyen szinten személyazonosságát. Mivel meglehetősen gyorsan lehet létrehozni nem ellenőrzött ingyenes e-mail címet, ezért ez nem teljes ellenőrzésnek számít. Ellenőrzött esetben (regisztráció és a használathoz szükséges bejelentkezés) a kötelezően teljesítendő elvárások a következők [2] [4]:

- bizalmasságnak és integritásnak eleget tevő kommunikáció;
- erős jelszavak;
- szerver oldali azonosítás;
- account aktíválás;
- jelszó alaphelyzetbe állításhoz megerősítés;
- védelem a próbálkozásos elven történő név-jelszó feltörés ellen.
-

A tipikus biztonsági problémák közé tartozik [1]:

- az azonosítási probléma;
- a szállítási rétegbeli probléma;
- a titkosított adattárolás hiánya;
- a megosztási probléma.

Regisztrációkor szükséges visszaazonosítás esetén egyes szolgáltatók elfogadják azt is, ha nem ellenőrzött e-mail címmel történik a regisztráció. Ez lehetőséget ad arra, hogy egy rosszindulatú felhasználó olyan néven regisztráljon be, amely egy céghez, vagy egy másik személyhez köthető, és így felmerül a megszemélyesítés, vagy a személyazonosság lopásának lehetősége.

Szállítási rétegbeli probléma esetében az alapvető gondot az okozza, ha a szolgáltatás használata során nem titkosított útvonalat (csatornát) használ az ügyfél, így lehetőség van arra, hogy jogosulatlan támadó ezeket az adatokat eközben saját célra ellopja. Ez a támadás viszonylag jól ismert, ezért a fejlesztők erre felkészülve sok esetben használnak titkosított adatátvitelt. A tapasztalatok azonban arra utalnak, hogy két jellemző hibát követnek el:

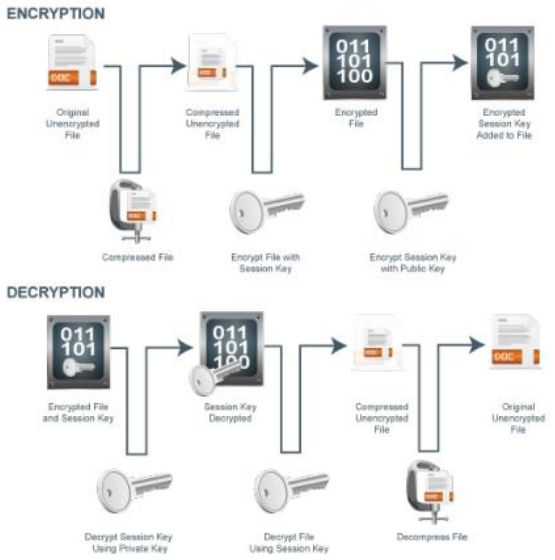
- a titkosítás nem megfelelő szintű. Vagy gyenge az algoritmus, vagy kisméretűek a titkosításhoz használt kulcsok, és így gyorsan kitalálhatók;
- saját titkosítást építenek be az alkalmazásba, amely nem rendelkezik megfelelő védettséggel. Ez utóbbi esetre vonatkozik egyébként a Kerckhoff-elv, amely (leegyszerűsítve) azt mondja ki, hogy nem a titkosítási algoritmus titkossága nyújt megfelelő védelmet, hanem a titkosításhoz használt kulcs titkossága.

A felhasználótól nem csak az előző biztonsági problémákra való felkészülés várható el, hanem az is, hogy adatait olyan módon tárolja a számára biztosított tárhelyen, hogy aza szolgáltató számára ne legyen felhasználható. Ha SSL-t, vagy https-t használ az adatátvitel során, de az adatok (fájlok) nincsenek titkosítva, akkor a szolgáltató (egy alkalmazottja) ezzel visszaélve az adatokból mások számára eladható információkat nyerhet ki. Az irodalomkutatás során felhasznált szinte összes forrás szerint [1] [2] [3] [4] [5] ez jelenti a legnagyobb biztonsági problémát. A felhasználó elemi érdeke, hogy adatai biztonságban legyenek. Erre megoldást jelenthet az, ha fájljait egy tömörítő program segítségével tömörítés közben jelszómegadással védi. Ennek a módszernek hátránya az, hogy a felhasználó számára nem transzparens, kevésbé képzett alkalmazottak számára nehezen kezelhető. Tisztább, és egyszerűbb, ha maguk az alkalmazások, vagy az operációs rendszer maga oldja meg a titkosítást, illetve visszafejtést. Ebben az esetben kevesebb a hibázási lehetőség, kisebb a biztonsági kockázat.

Megosztás esetében problémát az okozhat, hogy sok szolgáltató biztosít egy olyan lehetőséget, hogy a tároló helyen levő adatokhoz a felhasználó egy URL-t (linket) készítsen, és ezt másoknak elküldve hozzáférjenek az ott található fájlokhoz. Ezeket a linkeket a kereső motorok (google, bing, stb.) sok esetben megtalálják, és így a fájlokhoz jogosulatlanok is hozzáférhetnek teljesen véletlenszerűen.

3. TITKOSÍTÁS AZ ADATTÁROLÁS SORÁN

Az előző pontban rövidebben megemlítésre került, hogy az adatokat titkosítással kell védeni (1. ábra). Az is felmerült, hogy egy rosszul kivitelezett titkosítás hamis biztonságérzetet kelthet a felhasználóban. Valójában nem elég annyi, hogy az adatok titkosítva vannak, minden esetben ügyelni kell a szokásos titkosításos veszélyforrásokra is. Az egyik legismertebb kockázatot az jelenti, ha a felhasználó ugyanazzal a kulccsal titkosít el több fájlt. Ilyen esetben a támadó az algoritmus ismeretében az ismétlődés miatt sokkal könnyebben vissza tudja fejteni a kulcsot, és hozzá tud jutni a fájl eredeti tartalmához.



1. ábra A titkosítás, megfejtés általános menete

Ha a kliens programnak, illetve az operációs rendszer egy megfelelő plug-in-jának kell a titkosítást, megfejtést feltöltés előtt elvégeznie, akkor az a legtöbb esetben nem érzékelhető lassulást eredményezhet. Több olyan vizsgálat is készült [3], amely különböző méretű fájlok esetében tételesen mérte a titkosításhoz, és a feltöltéshez szükséges időt különböző méretű fájlok esetében. A mérések szerint 1 MB méret alatt ezredmásodperc időigénye volt a titkosításnak. A méret növekedésével nem csak az időigény nőtt meg, hanem a teljes időigényhez képesti százalékos mértéke is. 10 MB-os fájlméret esetében 1.3 %-ra a korábbi (százalékosan) szinte mérhetetlen 0.0 – 0.1 %-os értékről. A mérésekhez AES+HMAC került használatra, 256 bites kulcsokat használva. A mérések eredménye az, hogy ha a felhasználó az elvárható szintű titkosítást használja, és azt automatikusan (transzparens módon), akkor a felhő használatának sebességét csak nagyon kis mértékben lassítja.

4. ÖSSZEFOGLALÁS

A publikáció célja az, hogy felhívja a figyelmet a Magyarországon is egyre nagyobb mértékben terjedő felhőalapú tárolási rendszerek használatának veszélyére. Tudatosítja azt, hogy a szolgáltatók sok esetben nem biztosítanak vagy egyáltalán semmilyen védelmet, vagy annak szintje nem megfelelő. Ilyen esetekben azt a felhasználónak kell arra ügyelnie, hogy megfelelő alkalmazásokat, megfelelő üzemeltetési körülmények között dolgozzon. Cél volt az is, hogy bemutassa, a titkosítás használata nem lassítja le (érezhető mértékben) a használatot, így az megfelelő titkosítás kötelező használata erősen javasolt, cégek esetében a céges policy részévé kell tenni.

KÖSZÖNETNYILVÁNÍTÁS

A bemutatott kutató munka a TÁMOP-4.2.1.B-10/2/KONV-2010-0001 jelű projekt részeként az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

IRODALOMJEGYZÉK

[1] Borgman, Hahn, Herfert, Kunz, Richter, Viebeg, Vowe: On the Security of Cloud Storage Services, Fraunhofer SIT, (2012)
[2] Understanding Security in Cloud Storage, Nasuni White paper, (2010)
[3] Tang, Lee, Lui, Perlman: FADE: Secure Overlay Cloud Storage with File Assured Deletion, Chinese University of Hong Kong, (2010)
[4] Grant Bugher: Secure use of Cloud Storage, Microsoft, (2010)
[5] Wang, Wang, Ren, Lou: Ensuring Data Storage Security in Cloud Computing, (2008)
[6] Mika Turim-Nygren: 7 top Cloud Storage Services compared, Digital Trends, (2012)
[7] Balaji: Top Cloud Storage Providers in the Consumer Segment, Gartner Report, (2012)
[8] Cloud Tweeks: The Future of Cloud Storage and Sharing, Gartner Report, (2011)
[9] Ellis Hamburger: Google Drive vs. Dropbox, SkyDrive, SugarSync, and others: a Cloud Sync Storage face-off, Gartner Report, (2012)