Élthes Zoltán[150]

Alternatív technológiák alkalmazásával alkotott biztonsági modell az interneten

A dolgozat egy olyan modell fejlesztését mutatja be, amely az interneten való alkalmazások biztonságát szavatolja, alternatív technológiák alkalmazásával. Az információ biztonsága, ennek szavatolása az emberi társrsadalom egyik legfontosabb követelménye. Jelen pillanatban, különböző klasszikus modellek vannak elterjedve, melyek magas komplexitású matematikai algoritmusokat tartalmaznak. Léteznek más modellek is, természeti jelenségekhez illeszkedő modellek, melyek új tudományos kutatási irányt jelenthetnek. A biotechnológiák, sőt a DNS információt alkalmazó módszerek, felhasználva a numerikus hybrid módszereket, olyan eredménnyek, melyeket érdemes alkalmazni, beépíteni bármelyik biztonsági információs rendszerbe.

Napjainkban, az informatikai biztonság nagyon fontos, mondhatjuk, hogy alapproblémájává vált minden internethasználónak, függetlenül, hogy szolgáltató vagy felhasználó. Egyre jobban nő a kommunikációs szükséglet, illetve az információk biztonságát szavatoló igény. Ezek olyan követelmények, melyeket bármilyen információs rendszernek vagy hállózatnak biztosittania kell.

Ha egy informatikai szervezet nem sajátítja el a számítógépes biztonság megteremtéséhez és fenntartásához szükséges legújabb ismereteket, könnyen a fehérgalléros bűnözők áldozatává válhat. Az üzleti titkok elveszítése, kiszivárgása, egy informatikai rendszer leállása, vagy az ügyfelek bizalmának elveszítése a kis- és nagyvállalatokat egyaránt megrendíti. Felmerül a kérdés, hogy honnan szerezhető naprakész tudás, és milyen módszerekkel tesztelhető hatékonyan a vállalati hálózat biztonsága. Ma már bevett gyakorlat, hogy a számítógépes hálózatok biztonságát etikus hackerek teszteljék. Az összes ismert támadási módszert részletesen kipróbálják, tesztelik a rendszer biztonságosságát, észreveszik a rendszer ellen irányuló támadásokat, és hatékonyan tudnak ellenük védekezni.

A dolgozat célja a létező biztonsági keretemodellek elemzése, melyek alapján egy biztonsági technologiát lehet fejleszteni a halózaton működő alkalmazások számára. Az elemzés

[150] A szerző egyetemi docens a Kolozsvári Babeş-Bolyai Tudományegyetem Közgazdaságtudományi Karán. E-mail: eltheszoltan@yahoo.com.

rávilágitott az alternativ technológiák implementálására, biótechnológián alapuló biztonsági elemek bevezetésének lehetőségére.

1. Biotechnológián alapuló biztonsági modell

Körülbelül 60 évvel ezelött fedezték fel a DNS kettős spirál struktúráját és azt, hogy az miképpen képes az örökítéshez szükséges információk tárolására. Ezzel a felfedezéssel vette kezdetét az a lassú, ám mára már igen előrehaladottabb állapotba jutó tudomány, amelyet genetika névvel illetnek, és amelynek leglátványosabb eredményeiről naponta olvasunk a híradásokban. Pedig sokak szerint az igazi nagy kaland még csak most kezdődik: a genetikus gyógyszerek, és a génkezelésen alapuló gyógyító és diagnosztikus eljárások új távolatokat nyithatnak meg az emberi betegségek kezelésében, és a biológiai fejlődés irányításában.

Egy dolog biztos: a DNS-ről még mindig nagyon sok dolgot nem tudunk. Ezen információk megszerzése a jövő kutatóinak feladata lesz, a megszerzett ismeretek felhasználási módjainak elfogadása vagy elutasítása pedig a jövő társadalmáé. Az élet titkainak teljes felfedezésére pedig egy darabig valószínűleg még várnunk kell.

Az internet, az adatmenedzsment, a magas szinvonalú feldolgozás, új fejezetet nyitott a genetikában. Konkrétan lehetőség nyilt új gének azonositására, klonozására, fontos információkat szolgáltatva a különböző molekuláris hatásmechanizmusok megértésében. A bioinformatika infrastrukturális fejlődése lehetővé tette új szémitógéepes hállózat biztonságát szavatoló modellek megjelenését. Egy ilyen biztonsági modell fejlesztése egy nagyon komplex feladat. A modell lényege, újfajta kriptálási technikák bevezetése, biótechnológiát alkalmazva, ahol a személyes egészségügyi adatok DNS láncokba vannak kodolva, a mikrobiológia dogmái szerint.

2. Titkosított adatok tárolása mikrobákban

A biológiai tárolás, vagy biotárolás, igen fiatal tudományág, amely azt tűzte ki célul, hogy élő szervezetekben tároljanak és titkosítsanak információkat. A hongkongi Kínai Egyetem ifjú kutatói Aldrin Jim vezetésével egy új modszert dolgoztak ki, ahol a tároló az E. coli (Escherichia coli) baktérium DNS-molekulája. Mivel ezek a mikroorganizmusok folyamatosan szaporodnak, akár évezredekig is tárolhatjuk a bennük ma elrejtett információkat.[151]

[151] http://www.itp.net/583596-students-turn-ecoli-bacteria-into-data-storage [2013.03. 17.]

A csoport kidolgozta az adatok elrejtésének módszerét: darabokra vágják az információt, és különböző baktériumok sejtjeibe építik be azokat. Ehhez először eltávolítják a baktériumból a genetikai információt hordozó DNS-molekulát, majd azt enzimekkel úgy manipulálják, hogy a művelet után beépülve marad a többlet információ is. Az eljárás hasonlít a genetikai módosításhoz, amellyel például GM-növényeket állítanak elő. Mielőtt egy-egy változtatást elvégeznek a DNS-láncban, a meglévő adatbázisokban ellenőrzik, hogy az új betűsorrend, azaz változat nem hordoz-e káros mellékhatásokat.

Mivel az E.coli baktérium sejtjei igen kicsik, ezért ez a tárolási mód rendkívül kompakt. A kutatók szerint egy gramm baktérium 450 darab 2000 gigabájtos merevlemeznek megfelelő mennyiségű adatot képes tárolni. A kódolt, titkosított adatok megőrzésére három fokozatú biztonsági védelmet fejlesztettek ki.

3. DNS-alapú szteganográfia

Jelen pillanatban a titkositás legismertebb technikái a kriptográfia és a szteganográfia. Amig a kriptográfia célja, hogy a közölt információk módosítás nélkül, esetleg továbbra is bizalmasan érjenek célba, addig a szteganográfia célja, hogy maga az információközlés ténye rejtett maradjon, függetlenül attól, hogy védjük-e azt valamilyen technikával. Nyilvánvalóan, akár védhetjük is, kriptográfiai módszerekkel a küldött információt, ha biztosra szeretnénk menni.

Szteganográfia alatt az adatok valamilyen formában történő elrejtését értjuk, ahol a közlendő informació a kommunikáció soran ugyan lehet, de nem szükségképpen titkositott, ezért ertelmezéskor nem a kulcs fogalmárol, hanem az elrejtés módszereről beszélhetünk.

A szteganográfia alkalmazásának egyszerűsége a könnyen hozzáférhető, redundáns médiumokból fakad. E célra ugyanis bármely olyan közeg felhasználható, amely hibatűrés, vagy egyéb okok miatt redundanciát tartalmaz, vagy amely képi vagy hangos tartalommal rendelkezik és az emberi érzékszervek tehetetlensége miatt lehetséges néhány bitnyi plusz információ eltárolása. Például egy képből egy sort, vagy oszlopot levágva azt információ tárolására használjuk fel, hiszen jó eséllyel senkinek nem fog feltűnni, ha egy pár ezer soros képből eltűnik egy.

A DNS hatalmas mennyiségű információt tud tárolni. Például egyetlen gram DNS-molekula több milliárd gigabájt adat tárolására képes. Több kutatócsoport próbálkozott már információt tárolni sejten belül a DNS-ben, de ennek a módszernek két komoly hátulütője van: egyik, hogy a sejt elpusztul, a másik, hogy osztódáskor mutációk rongálhatják a tárolt adatot. George Church, a bostoni Harvard Medical School biológusa azonban sikerrel fejlesztett ki egy eljárást, mely adatok tárolására és visszanyerésére képes sejtek használata nélkül is. A

módszer lényege, hogy üvegszeletkékre egy tintasugaras nyomtatóval mesterségesen létrehozott DNS-töredékeket juttat, melyek hasonlóan a 2-es számrendszer 0-1 jeleihez a DNS "nyelvén" A, C, G és T szimbólumokban kódolja az adatokat. Minden adattöredék több ezerszer kerül rögzítésre, valamint egy pozícióinformációt is tartalmaz. Az eljárással mindössze 2 hiba/millió bit mellett sikerült egy teljes könyvet kódolni és visszaállítani.[152]

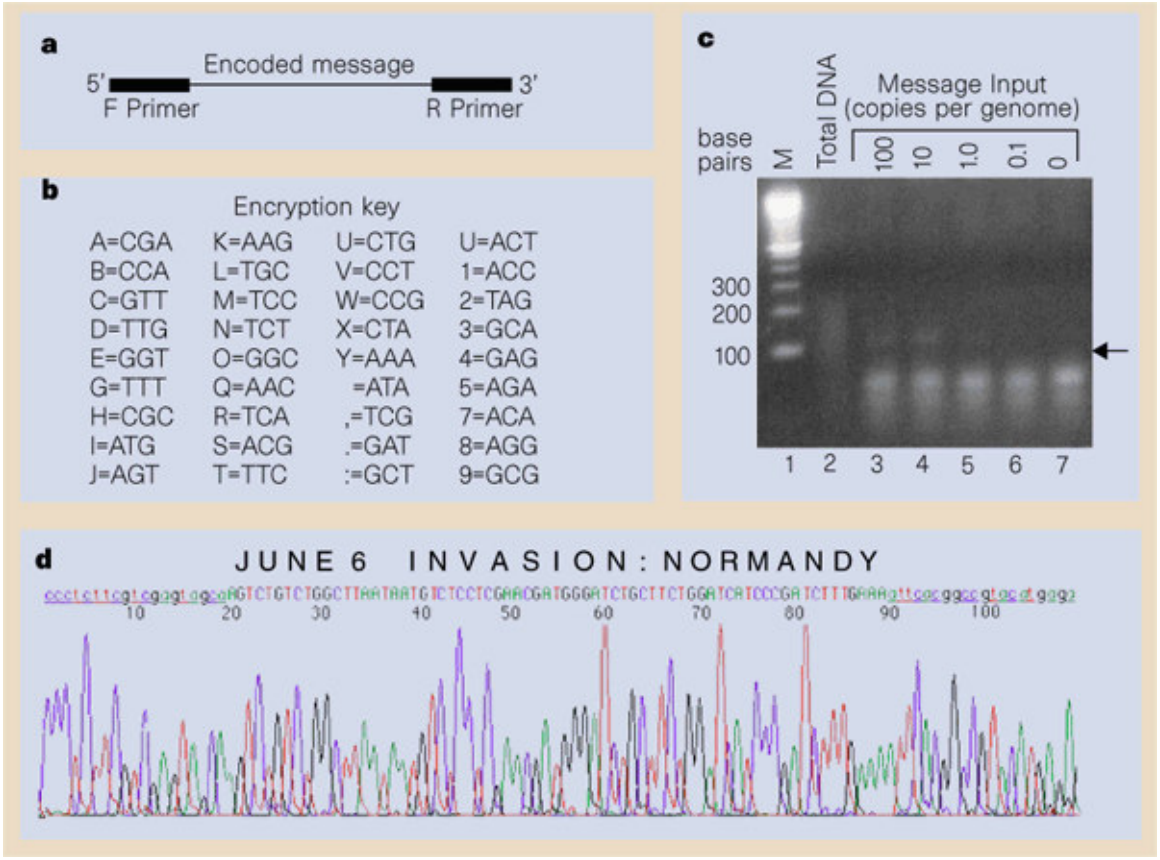
Az adatok DNS-ben történő archiválása rendkívüli előnyökkel jár, így mindenképp érdemes lesz az adatátvitel sebességén és a költségek leszorításán dolgozni. Az óriási adatsűrűségen túl a módszer másik lényeges tulajdonsága, hogy valóban hosszú távú adatmegőrzést tesz lehetővé: a DNS-molekula akár több tízezer évig is képes változatlan formában tárolni a belé kódolt információkat.

A DNS-alapú adattárolásnak persze megvannak a hátrányai is. Egyrészt egyelőre rettenetesen lassú a kiolvasás sebessége: a kódolt 739,3 kilobájtnyi adat dekódolásához és rekonstrukciójához két hétre volt szükségük a szakértőknek, bár elmondásuk szerint ma már léteznek olyan berendezések is, amelyekkel ez egy nap alatt megoldható lehet. Gyakorlati használathoz ez persze még mindig nagyon lassú, de ahogy fejlődik a szekvenálás sebessége, idővel ez is megvalósulhat.

Viviana Risca, Amerikában tanuló, román egyetemi hallgató, Junior Nobel dijat kapott a DNS-alapú szteganográfiáért. A „DNA-based Steganography” nevű projektje ötvözi a kriptográfia, szteganográfia és molekuláris számítástechnika tudományágait.

„DNA-based Steganography” nevű projektben, Viviana Risca egy egyszerű kodot alkalmazott, amely képes konvertálni az ABC betűit egy alapkombinációba, melyek alkotják a DNS molekulát.Viviana kodolásra a következő üzenetet alkalmazta: „June 6 Invasion Normandy”, Bancroft professzor katonai karierje tiszteletére. Ezt követően elhelyezte a kodot egy mesterségesen létrehozott, egyszerű DNS molekulába.

[152] Risca, V.: *DNA-based steganography*. Publisher Taylor & Francis, Inc. Bristol, 2001/1. sz. 37–49.



DNS szteganográfia[153]

Ezt a molekulát a többi DNS molekulák közé rakta. Következett egy sajátos biókémiai folyamat, melynek következtében sikeresen tudta olvasni a dekodolt üzenetet.

4. DNS kodolás

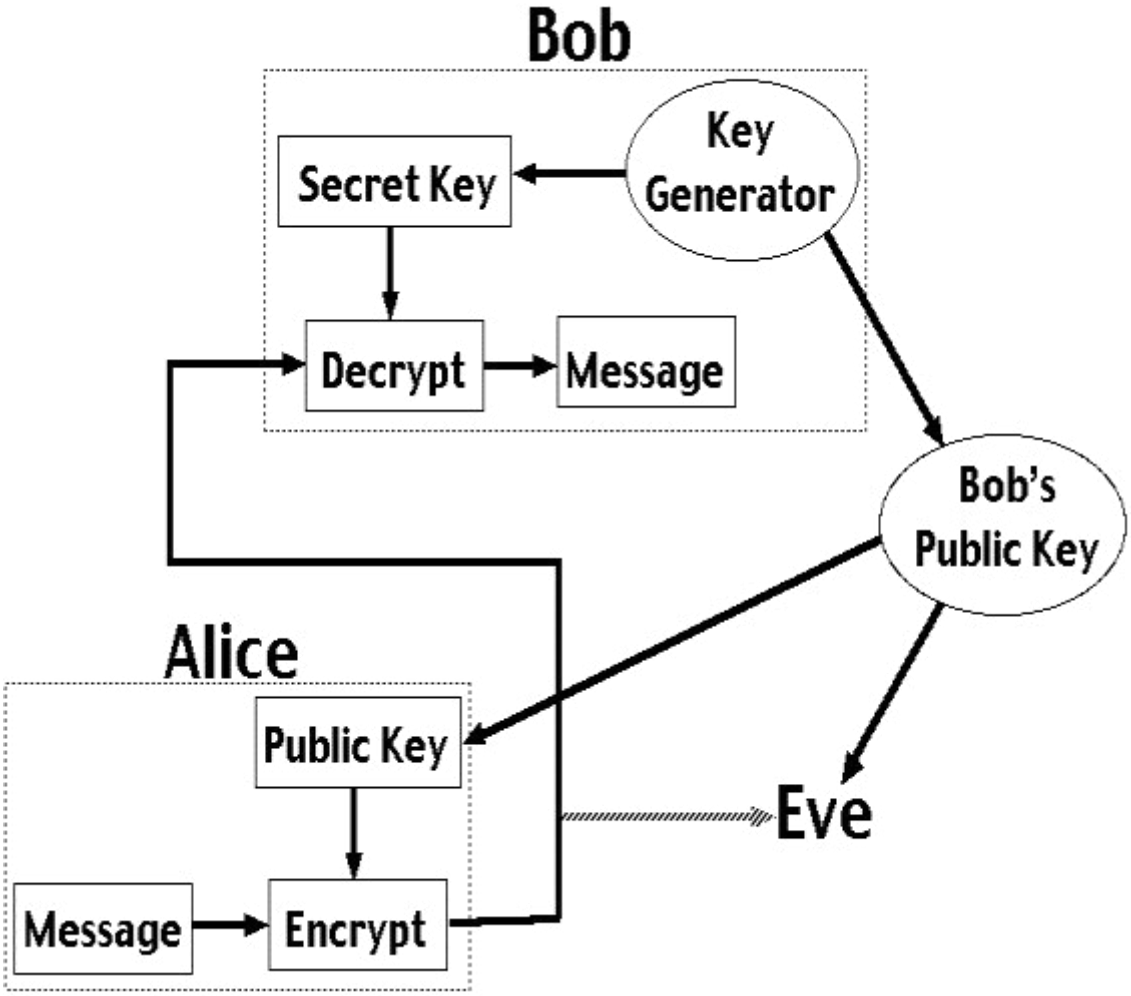
A DNS kodolás alkalmazásának koncepciója a titkositás területén egy új lehetséges technológia megjelenését tette lehetővé, amely eredményezheti a feltétel nelküli algoritmusok létrehozását. Fontos megismerni a genotipus ée a fenotipus közti complex relációt. Genotípusnak nevezik az egyed által hordozott géneket (alléleket). Fenotípusnak pedig a genotípus által meghatározott külső tulajdonságokat. A genotipust örököljük mint egy kodot, a fenotipus ennek a kodnak a fizikai megnyilvánulása. Alapvetően, a kod és a kifejezési szabályok tökéletes megismerése, illetve a környezeti információk elégségesek kell legyenek a fenotipus predikciójához.

[153] Clelland, C.T.–Risca, V.–Bancroft, C.: Hiding messages in DNA microdots. *Nature International,* 1999/399. sz. 533–534.

Az utóbbi idöben, a biólogia és az orvostudomány összefonódásának köszönhetően két új tudomány született: a komputacionális biológia (computational biology) és az orvosi informatika (medical informatics). A komputacionális biológia felulmulja a hagyományos bioinformatikát, mivel magában foglal új technikai kezdeményezéseket, mint pl.a silico molekuláris modellezés (silico molecular modeling) a proteinek szerkezetének tanulmányozása.

Egy ember személyes egészségügyi adatjait DNS láncokba kodoljuk, amelyek elejét és végét egy egységes elsődleges (primer) szekvencia jelöli. Ezeket a primereket a vér analizis DNS kulcsok deriválási folyamatából kapjuk. Összekeverjük egyébb DNS láncokkal és elküdjük a cimzethez. Bevezetjük a DNS kodolást a nyilvános kulcsú infrastruktúrába (PKI) és igy lehetségesé válik, hogy követve a PKI strukturát illetve felhasználva a DNS párhuzamos feldolgozás tulajdonságait, megoldjuk a kulcsok kódolását és dekódolását. A tranzakcióban alkalmazott algoritmusok sokkal komplexebbek lesznek mint a konvenciónális módszerek által alkalmazott algoritmusok. A következő ábrán bemutatunk egy DNS kodolású, biztonságos adatküldési eljárást Bob és Alice között, ahol Bob átadja Alice-nek a nyilvános kulcsot, melynek alapja az egyén vér mintavétele, DNS kdolás alkalmazásával.

Bob felhasználja ezt a kulcsot egy általa titkositott üzenet továbbküldésére. Egy ilyen DNS titkos üzenet tartalmazza a DNS láncokba kodolt információt, ahol a üzenet elejét és végét egy egységes primer szekvencia jelzi. A cimzett azonositja a titkos DNS sorozatot egy olyan program segitségével amely hozzárendeli a nukleotidok szekvenciáját egy specifikus mintavételhez, melyet az egyén vérvételéből származtatunk. Igy kapunk egy egységes primer szekvenciát, amely jelzi annak a DNS titkos sorozatnek az elejét és végét, amely más DNS sorozatokban van elrejtve. Utolsó lépéskénz alkalmazunk egy konverziós programot, melynek segitségével értelmezhetjük az orvosi eredményeket.



Nyílt/nyilvános kulcsú rejtjelezés vagy titkosítás[154]

5. A keretmodell bemutatása

Az ajánlott keretmodell támogat bármilyen Interneten futó alkalmazást. A keretmodell alapján kifejlesztett szoftvertermék lehetővé teszi a weboldalak biztos és biztonságos integrálását, függetlenül, hogy látogatók vagy regisztrált felfasználókról van szó. Támogatja a távadminisztrálási eszközöket (CMS, Content Management System), melyek lehetővé teszik:

- Az alkalmazás összes adatbázissainak kezelését
- A lehivott site-ok multimedia tartalmának kezelését

Az alkalmazás háromszintű kliens/szerver megvalósítás, mely lehetővé teszi a teljesítményelosztást az egyes szintek szerverei között. A háromrétegű architektúra az alkalmazást három különálló szintre osztja fel. E rétegek/szintek komponensei önállóan

[154] Ashish, G.–Reif, T.: *DNA-Based Cryptography*. Department of Computer Science. Duke University, 1999.

létez Adatbázis működésü GUI kezelésének modulja nböz Felhasználói interfész ei lehetnek.A szintek a következők:

- Első szint: grafikus felhasználói felület vagy grafikus felhasználói interfész (GUI, Graphical User Interf Logika implementálásának modulja feladata az ügyviteli logika által küldött adatok formázása és megjelenítése. Biztosítja a felhasználó hozzáférését az ügyviteli logika szolgáltatásaihoz. Sohasem kerül közvetlen kapcsolatba az adatbázissal, és nem atokon."
- Másadik szint: az üz Adatok hatékony összekapcsolását biztositó modul ely meghatározza az alkalmazás működésének logikáját.
- Harmadik szint: adatbázis amely az adatok nyers tárolását végzi. Semmilyen információval nem rendelkezik az adatok feldolgozásával vagy megjelenítésével kapcsolatban.

A másadik szintnek 3 komponense van:

- A felhasználói interfész kezelésének a modulja
- A működési logika implementálásának a modulja
- Az adatok hatékony összekapcsolását biztositó modul

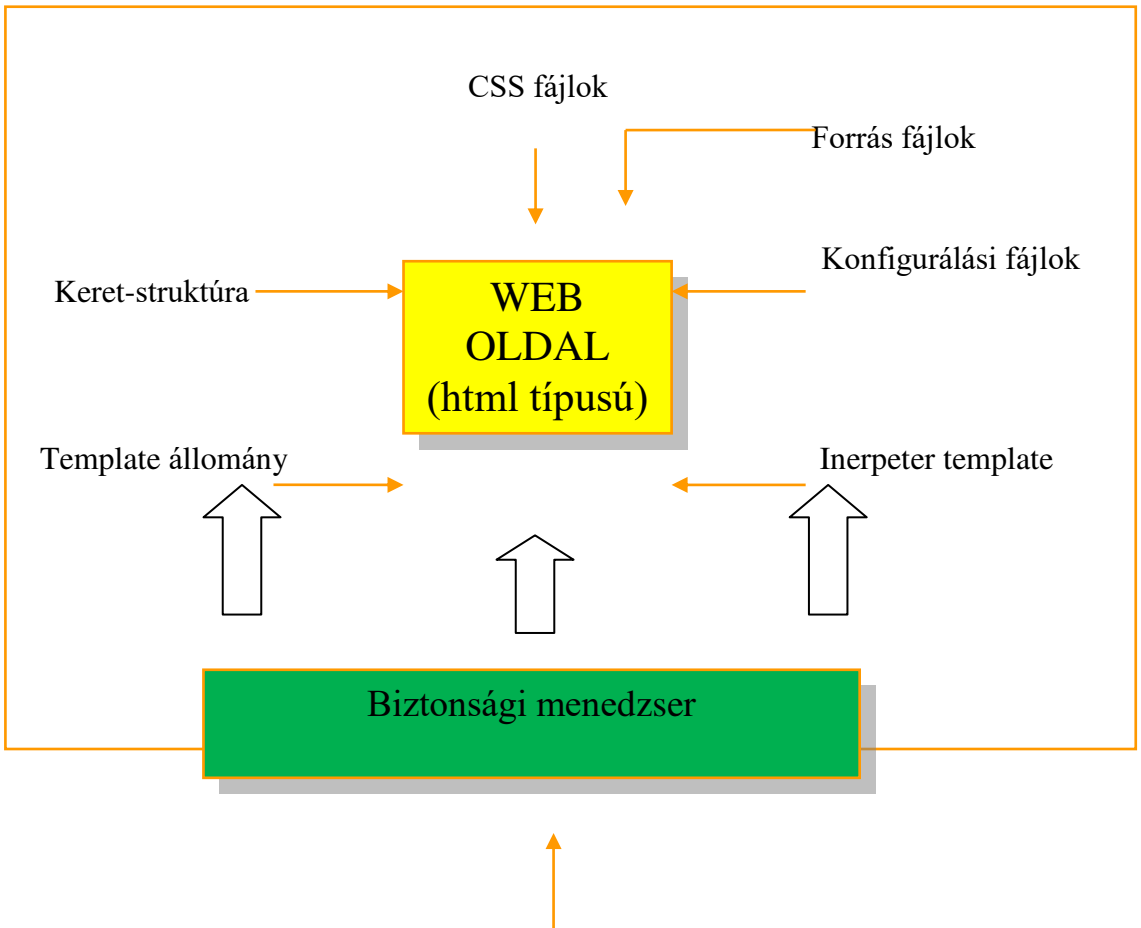
Első szint Második szint Harmadik szint

A modulok szerkezete

A keretmodell moduljait kizárólag külső deszkriptor állományok ellenőrzik. Ezek több csoportba oszthatók:

- GUI-t ellenörző állományok, melyek tartalmazzák a site leirását, a HTML programot illetve a site-nak megfelelő táblázatokat, képeket, szövegrészeket.
- A logikai analizátor állományok. Ezekben konfiguréljuk az adatbázishoz való hozzáférést, definiáljuk a könyvtárak elérési útjait, a biztonsági metódusokat.
- A működési logikát támogató állományok, Tartalmaznak osztálykönyvtárakat mint pl. az XML osztály.
- A működési logikát implementáló állományok, melyek olyan programsorokat tartalmaznak amelyek konkrétan definiálják a site működési módját.

A keretmodell strukturájának megfelelően, a browser által megjelenitett weboldal a következő:



Konfigurálási állomány

A weblapok tartalma a keretmodellnek megfelelően

A keretmodell portabilitásával kapcsolatban két fontos tényezőt érdemes kiemelni:

- Könyvtárak közti átvihetőség, amely biztositja az alkalmazás helyének változtatását a lemezen belül. Ez lehetséges mivel a könyvtárban lévő fájlra mutató linket a jelenlegi dokumentumhoz képesti relatív uttal adjuk meg. Egyik file-t sem hivunk meg az abszolut hivatkozás alapján.
- Rendszerek közti átvihetőség, amikor a az alkalmazás működik bármilyen serveren, függetlenül az operációs rendszertől.

Összefoglaló

Az információ biztonságának megtervezése elengedhetetlenül fontos bármilyen gazdasági tevékenység részére. Az információkat védeni kell, függetlenül attól, hogy milyen formában vannak. A biztonsági politika nagyon lényeges bármilyen cég részére. Kell tartalmazzon bizonyos szabályokat amelyek meghatározzák a felhasználók hozzáférési módját az erőforásokhoz, biztosítják a tevékenység folytonosságát illetve az esetleges megkárosodott adatok visszanyerését. Ha megtervezzük az adataink biztonságát akár szélsőesetekre is, kevésbé leszünk kitéve egy esetleges külső támadásnak.

A DNS kodolás alkalmazásának koncepciója a titkosítás területén egy új lehetséges technológia megjelenését tette lehetővé, amely eredményezheti a feltétel nelküli algoritmusok létrehozását.