

Az EgerFood élelmiszerbiztonsági nyomkövető rendszer informatikai megoldásai

IT solutions of EgerFood food safety tracking system

Radványi Tibor¹, Kusper Gábor²

INFO

Received 11 Oct. 2011

Accepted 31 Jan. 2012

Available on-line 15 Jun. 2012

Responsible Editor: Rajkai, K.

Kulcsszavak:

quality management,
meat industry,
food tracing,
information system

INFO

Beérkezés 2011.Okt. 11.

Elfogadás 2012.Jan. 31.

On-line elérés 2012. Jún. 15.

Felelős szerkesztő: Rajkai K

Kulcsszavak:

minőségmenedzsment,
húsipar,
élelmiszer nyomonkövetés,
információs rendszer

ABSTRACT

In this article we introduce the EgerFood food-safety tracing system, which has been developed in the Regional Knowledge Center at the Eszterházy Károly College. We have already reported on the applied methodologies on some conferences. This article gives a complete overview on the informatics system, on its features, and on our results. Our aim is that similar tracing system should be able to use this article as an example. The goal of the EgerFood system is to create a customer centric system, which deliver food-safety information in a cost effective and safe way to the customers, the food-producers, and the authorities. The developed information system uses at least a 2-tier architecture already at the site of the food-producers, which is connected to the main data warehouse server using VPN connection. We show how moves the data from its source to the buffer-servers, from that to the communication server and finally to the database server, and how it is encrypted on this way. We also approve the safety of data search, not only the safety of the data upload.

ÖSSZEFOGLALÓ

A cikkben bemutatjuk az Eszterházy Károly Főiskolán megalakult Regionális Tudásközpontban kutatott és kialakított EgerFood élelmiszer-biztonsági nyomkövető rendszert. A felhasznált informatikai megoldásokat már bemutattuk egy-egy konferencián. Ebben a cikkben áttekintjük az informatikai rendszert, annak feladatait és eredményeit, azzal a céllal, hogy hasonló nyomkövetési rendszerek példaként tudják használni. Az EgerFood rendszer célja egy olyan fogyasztó-központú rendszer kiépítése, mely gyors és költséghatékony információhoz juttatja a fogyasztókat, az élelmiszer termelőket és az érintett hatóságokat egy-egy élelmiszerről, mindezt magas fokú adatbiztonság garantálása mellett. A kialakított információs rendszer már a projektben résztvevő cégek telephelyein is minimum kétrétegű architektúra, ami VPN kapcsolaton keresztül kapcsolódik a központi kommunikációs szerveren keresztül a központi adattárházhoz. Bemutatjuk, hogy az adatok keletkezési helyétől kiindulva, hogyan biztosítjuk a megfelelő szintű titkosítást és adatbiztonságot a helyi puffer-szerverekig, majd onnan a kommunikációs szerveren keresztül az adattárházig. Az adatok feltöltése mellett biztosítottuk az adat visszakeresés biztonságát is.

1. Bevezetés

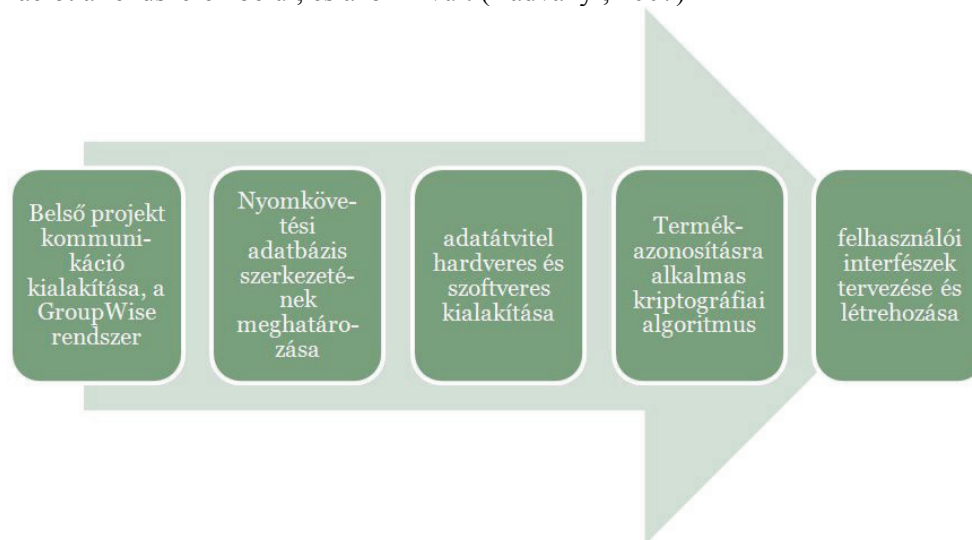
A kutatási-szolgáltatási tevékenységek fókuszában jelenleg környezetvédelmi és élelmiszeranalitikai munkák állnak, melyek közül kutatás-fejlesztési, valamint gazdasági és társadalmi aspektusból az élelmiszeranalitikával és élelmiszerbiztonsággal kapcsolatos tevékenységek a legjelentősebbek. Ebből következően a létesített élelmiszerbiztonsági és analitikai vizsgálati centrum az eddigi tevékenységek logikus folytatásának, bizonyos új fókuszpontok kialakításának és a gazdaságilag legrelevánsabb kutatási témák kiterjesztésének tekinthető.

¹ Radványi Tibor
Eszterházy Károly Főiskola, 3300 Eger, Leányka u. 4. C.ép.
dream@aries.ektf.hu

² Kusper Gábor
Eszterházy Károly Főiskola, 3300 Eger, Leányka u. 4. C.ép.
gkusper@aries.ektf.hu

Intézményünk, az Eszterházy Károly Főiskolán létrehozott Regionális Tudásközpont, komoly elhatározása az, hogy az Észak-Magyarországi Innovációs Stratégiával összhangban a K+F és innovációs képességek fejlesztésével, valamint a hazai élelmiszerbiztonsági kutatási tevékenységek összehangolásával és kiterjesztésével a gazdasági szféra szereplői számára is értékes eredmények szolgáltatásával járuljon hozzá a hazánkban előállított élelmiszerek versenyképességének növeléséhez.

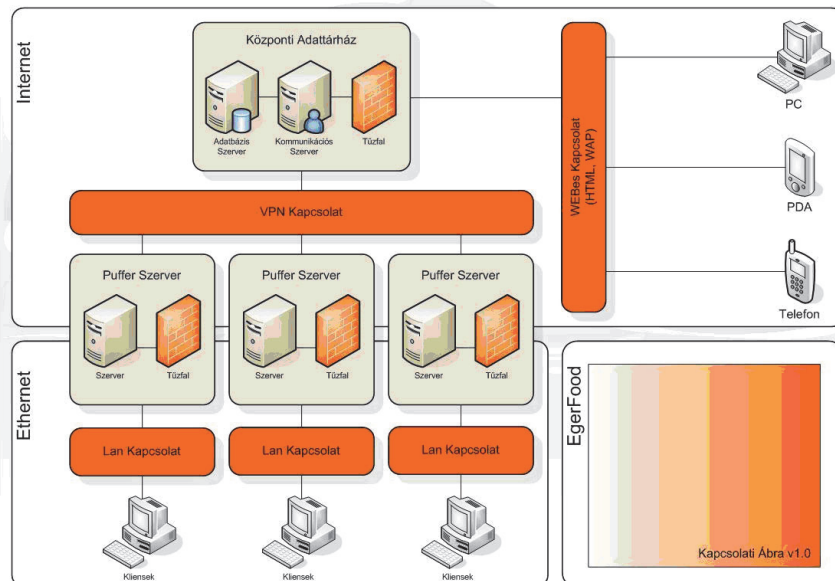
A projektben az informatika platform felé több feladatot fogalmaztak meg. Ezekből több érintette a kommunikációt a rendszeren belül, és azon kívül. (Radványi, 2007)



1. ábra. Projekt feladatok

- A projekt belső kommunikációját működtető web rendszer elkészítése és folyamatos működtetése. A célja a projektben dolgozók közötti információáramlás biztosítása.
- A nyomkövetési adatbázis szerkezetének meghatározása, az adatátvitel hardveres és szoftveres kialakítása.
- Az informatikai rendszer gerincét a nyomkövetési rendszer adatbázisa képezi. A begyűjtött adatokat, követelményeket elemeztük, és ezek alapján megalkottuk az információs rendszer adatmodelljét.
- A nyomkövetési rendszer hosszú távú fejlesztési stratégiájának figyelembe vételével kidolgoztunk egy termékazonosításra alkalmas algoritmust és kódrendszert, amellyel született kódot a terméken a nyomkövetési rendszerben való szereplést igazoló garanciajegy hordoz. Fontos hogy az adatok megfelelő kriptográfiai eljárással titkosítva kerüljenek tárolásra és mozgásra.
- Feladatunk felhasználói interfészek tervezése és létrehozása a különböző adatgyűjtő és lekérdezési tevékenységekhez.
- Kialakítottuk a fogyasztókkal WAP-on, ill. interneten való kommunikáció tartalmi szempontjait. Megtörtént az általános élelmiszerbiztonsági információk különböző részletességű platformokon való megjelenítése.
- Megterveztük és megvalósítottuk a teljes információs rendszer biztonsági követelményeit és a biztonsági eljárásokat.

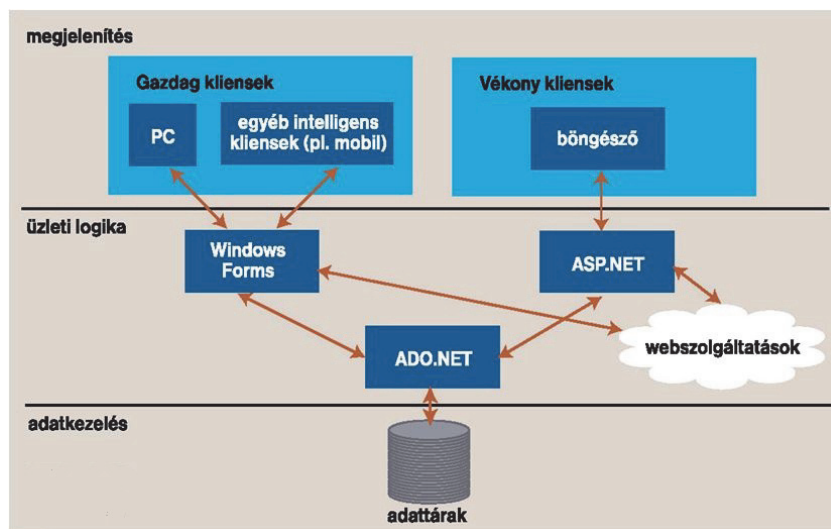
A rendszer vázlatos felépítését az 2. ábra mutatja.



2. ábra. A kommunikációs rendszer

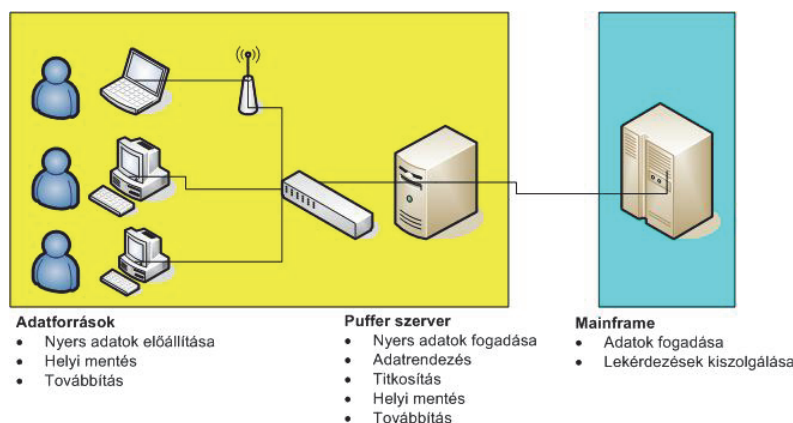
A központi tárház vállalja az adatok végleges tárolását és a lekérdező, megjelenítő modulok kiszolgálását. Az első kérdés a termelési folyamatban kinyert adatok eljuttatása a tárházba. Erre több lehetőség is kínálkozik, melyek közül az első, hogy a kiépített hálózati rendszer segítségével on-line kapcsolatban lévő adatforrások folyamatosan szolgáltatják az adatokat közvetlenül a központ felé. Nézzük meg az adatforrásokat.

Két nagy területről érkeznek adatok: a főiskolai kutató laborok vizsgálati eszközeinek mért eredményei, illetve a távoli felhasználók, az ipari telephelyeken, a termelés során mért adatok. Ezek az adatok napi 24 órán keresztül, folyamatosan érkehetnek, míg a laborok eredményei szakaszosan, a mérési kísérleteknek megfelelően. A külső telephelyek hat különböző élelmiszeripari cég termelési helyei, ezeknek teljesen különböző a földrajzi elhelyezkedésük, az informatikai felszereltségük, és lehetőségeik. Az általuk előállított élelmiszeripari termékek is különbözőek, azaz gyártási technológiájuk eltéréséből adódóan a termékpályákban különböző a vizsgált adatok összetétele, és keletkezésük időintenzitása. Ezen eltérésekből adódik, hogy a hálózat és az adatok tárolását megvalósító informatikai rendszernek fel kell erre készülni. Látható, hogy az adatok várható mennyisége megköveteli a nagyméretű központi tárház megépítését. Az érkező adatok időintenzitása pedig a nagy hálózati keresztmetszetet. (Radványi, 2004)



3. ábra. A rendszer rétegei

Az ipari cégekhez kihelyezett helyi szerverek, nevezzük ezeket puffer-szervereknek, feladata, hogy a tartományukba tartozó gépek és mérőműszerek adatait előfeldolgozzák, és megfelelő rendszerbe csoportosítva küldik tovább a központi szerver felé. Az adatok továbbtitkosítását is ezeken a számítógépeken futó szoftverek végzik el. Fontos kérdés, hogy az adatvesztést hogyan lehet a legnagyobb valószínűséggel elkerülni. Ennek két oldalát kell megvizsgálni. Ez egyik a bekerült adatok hosszú távú védelme, melyet a jól átgondolt és kidolgozott archiválási rend hivatott biztosítani. A másik az adatforrásoknál előállított, de a központi szerverre még be nem került adatok rövid és hosszú távú védelme. A rövid távú védelem alatt értsük azt a lehetőséget, hogy az adat keletkezés pillanatához minél közelebb kell az első biztonsági mentést megtenni. Majd az előfeldolgozott, titkosított, a továbbításra felkészített adatokat újra menteni szükséges. Így a központi szerver adattárházába való bekerülés előtt az adatok már két, egymástól független helyen tárolásra kerülnek. Ilyen mértékű adat redundancia igen erőforrás-igényesnek tűnik, de a követelmények teljesítésére ezek az intézkedések szükségesnek tűnnek.



4. ábra. Kommunikációs vonal egy cégtől

2. A kapcsolódó irodalom áttekintése

A munka elkezdésekor három nagy csomópont köré csoportosítottuk a kutatás irányát. Az első az adatbázissal kapcsolatos eredmények, melyek felhasználásával, és továbbfejlesztésével kívántunk eredményeket elérni. Másodsorban az adatok titkosítása, a kommunikáció az egyes telephelyek között. Azokat az eredményeket kerestük, melyek ebben a munkában segítenek. A harmadik csoport a szoftverfejlesztés, a felhasználói interfészek kialakítása, az objektum orientált programozási módszerek használata volt.

2.1. Az adatbázis fejlesztéshez tartozó előzmények

Nagyon fontos kérdés volt az adatbázis-kezelő rendszer vizsgálatánál, hogy milyen lehetőségek vannak. A DBMS értékesítők milyen kínálatot biztosítanak a felhasználóknak, és milyen feltételekkel.

A (Zolotova, 2005) cikk áttekinti, hogy milyen lehetőségek vannak az ipari adatbázis-rendszerek használatára elosztott ellenőrzési rendszerekben. Megtalálhatjuk benne, hogy milyen fontos szoftverfejlesztési és adatbázis tervezési kérdések merülnek fel a fejlesztés során. Áttekinti a lehetőségek széles tárházát annak, hogy a korszerű, cégen belüli ellenőrző rendszerek mögött milyen adatbázis-kezelő rendszerek állhatnak. Hogyan tudják a mobilitást és a rugalmasságot biztosítani a modularitás segítségével. Megtaláljuk annak az elemzését, hogy milyen elterjedt ipari platformok vannak. Segítséget nyújtott a cikk az előttünk álló feladatok és lehetőségek pontosabb körülhatárolásában. A lehetőségeink felmérésében.

Hasonló vizsgálatot végeztek Malajziában. Ennek eredményét írja le (Hamid, 2003) cikk.

A kis- és középvállalatok szintjén fontos annak a megvilágítása, hogy az informatikai eszközök, köztük az adatbázis-alkalmazások, illetve adatbázis-kezelők technológiai szintjének növelése előnyös a profittermelésben, és az üzletmenet javításában.

Az adatbázis-alkalmazások (mint például adatbázis-kezelő rendszer, adattárház és az adatbányászat) alkalmasak az információk hatékony eszközökkel való tárolására, kezelésére, így hasznos információkat nyújt az üzleti tevékenységről, mint a vásárlói számlák, szállítói kapcsolatok, mozgás leltár, beszerzés, marketing tervezés és egyéb üzleti tevékenység.

Felismerve a potenciális lehetőséget az adatbázis technológiában, a cégek már most kihasználhatják ezeket az információkat annak érdekében, hogy hatékonyan kezeljék a beszállítói lánc tevékenységét.

A tanulmány kimutatta, hogy ha a gyártó pozitív hozzáállást mutatott az adatbázis technológia iránt, akkor az ellátási láncban részt vevő cégek tevékenységét is befolyásolni tudta.

Bár általában kis-közepes vállalatok között a rendszerek elfogadása korai szakaszában jár, az eredmények azt mutatják, hogy a malajziai gyártók lelkesednek az adatbázis-technológia előnyeire. Röviden, a tendencia az, hogy a cégek dinamikus adatbázist használnak az adatok kezelésének javítására a stratégiai tervezésben és az ellátási láncban.

Fontos kérdés volt az adatbázis logikai tervezése. Nagy relációs adatbázisok tervezést valamely adatbázis tervezési módszertan segítségével oldhatjuk meg (Teorey, 1986). Először is az ER modellt használhatjuk a követelményelemzéskor felderített rendszer megjelenítésére. Majd transzformálhatjuk ezt a kiterjesztett EER modellé, és végül normalizálhatjuk a logikai tervet.

Figyelembe véve azt is, hogy várhatóan elosztott adatbázisrendszert kell kialakítani, és ennek a replikációját is meg kell oldani (Holliday, 1999; Ceri, 1987). Ez mutatta meg, hogy alkalmazható a pesszimista, az optimista illetve a félig optimista megközelítése a problémának. Mivel a rendszerünkben nem feltétlenül elsődleges szempont a replikációkor a gyors válaszadás, ezért a konkurens hozzáférést többszörös próbálkozással javíthatjuk. Választhatjuk az optimista megközelítést is.

A (Iyer, 2004) cikkben elemzik a szerzők, hogy milyen kérdések merülnek fel az adattárolás és adatbiztonság területén. Milyen kompromisszumokra kényszerülünk, ha az adatbiztonságot és a hatékonyságot állítjuk mérlegre. Javaslatot tesznek egy hatékony kulcskezelési protokollra, mely lehetővé teszi a biztonságos adattárolást.

2.2. A kriptográfiai előzmények

A biztonság a számítógép és a számítógépes kommunikációs alapú információs rendszerek elengedhetetlen része és feltétele. Az ipari vagy részben ipari környezetben működő rendszerekkel szemben kiemelten magas a biztonsági elvárások szintje, hiszen a hálózati kommunikációban ipari titoknak minősülő adatok vesznek részt. Így a gazdasági résztvevők alapvető elvárása, hogy az adataik megfelelő szinten védve legyenek.

Ezek a kérdések nem csak tisztán technikai jellegű elvárások. Kiderült, hogy az emberi tényező legalább annyira fontos, mint a megfelelő kriptográfiai eljárások alkalmazása. (Trcek, 2003)

A cikk ebből a szempontból vizsgálja a problémát, ad egy lehetséges megközelítést, melyet mind a fejlesztők, mind a cégvezetők követhetnek.

A technikai tényezők is összetettek. A biztonsági megfontolások során figyelembe kell venni az információs rendszer minden részterületét, szakaszát. Kezdve ott, ahol az adatok keletkeznek, áthaladva az átviteli közegeken és csatornákon, kiterjesztve a biztonsági módszereket az adatok tárolásának helyeire is.

A (Diaa, 2009) cikkben a szerzők egy fontos kérdést járnak körbe. Megvizsgálják, hogy a wireless hálózatokon belül milyen hatékonysággal lehet alkalmazni a különböző kriptográfiai eljárásokat. (Hardjono, 2005) Ezt teszik mind a 2,4GHz, mind az 5GHz hálózati frekvenciákon. Fontos a vizsgálat, hiszen ezek a kriptográfiai eljárások jelentős erőforrást fogyasztanak, úgy mint CPU időt, memóriát, mobil eszközöknél akkumulátor töltést.

A cikkben a szerzők összehasonlítanak 6 különböző titkosítási algoritmust, úgy mint AES (Rijndael), DES, 3DES, RC2, Blowfish, és RC6 (Rijndael, 2001; Coppersmith, 1994; Schneier, 2008; Fishawy, 2007).

A vizsgálatok azt mutatták, hogy több esetben a Blowfish algoritmus teljesített a legjobban, de a változó adatmennyiséget és a változtatható kommunikációs protokollt figyelembe véve nem volt jelentős eltérés az egyes algoritmusok között. Amennyiben a jelerősség csökken a hálózaton belül, megnőhet a szükséges idő. A szerzők javasolnak egy újabb megközelítési módot is az algoritmusok és a protokollok kiválasztására. Ebben a megközelítésben a felhasznált energia minimalizálása az elsődleges szelekciós szempont. Ez fontos olyan rendszerek esetében, ahol a rendszer hardver elemei akkumulátoros energiaellátást használnak.

A fenti algoritmusok közül választunk mi is egy megfelelő, a fejlesztő eszköz által támogatott algoritmust, melynek a segítségével az adatokat már a keletkezésük helyén kódolhatjuk.

Az adatáramlás biztonságát jól tudja biztosítani a megfelelően kiépített VPN hálózat (Ferguson, 1998). Nem csak az oktatás a kutatás, hanem a nagyvállalati szférában is kielégítő adatbiztonságot tud biztosítani.

A (Ferguson, 2000) cikkben leírja a szerző az IPsec értékelését, komoly kritikai megfogalmazásokat téve. Ezeket szem előtt kell tartani egy VPN hálózat tervezésekor. Túl bonyolultnak minősíti a részrendszert, nehezen kezelhető, és nem elég biztonságos. Lehetőségként megfogalmazza a következtetésben, hogy az új AES algoritmus használatával egyszerűbbé és hatékonyabbá tehető a titkosítás. Ezt szem előtt tartottuk, amikor az információs rendszer kriptográfiai rendszere került tervezésre. Így az AES algoritmust használjuk, mintegy kiegészítésként a VPN hálózaton belül.

2.3. A kliensszoftverek fejlesztésének előzményei

A szoftverfejlesztéshez több irányból kellett közelíteni, hiszen egyrészt feladat volt a kliensszoftver megírása, a megfelelő fejlesztőeszköz kiválasztása, a fejlesztési stratégia eldöntése. Másrészt a kommunikációt kiszolgáló szerver oldali programok megírása, és tesztelése.

A szoftver fejlesztésekor sok feladat, és sok protokoll együttes kezelését, integrációját kellett megvalósítani. A (Shakhgeldyan, 2004) cikkben a szerzők az egyetemi infrastruktúra kialakításakor vizsgálják az integráció lehetőségeit, és tanulságait. Fontos megállapításuk, hogy az integrációs problémákat webservice-ek alkalmazásával kívánják megoldani. A gondolat nagyban befolyásolta az EgerFood szoftver köztes rétegének kialakítását.

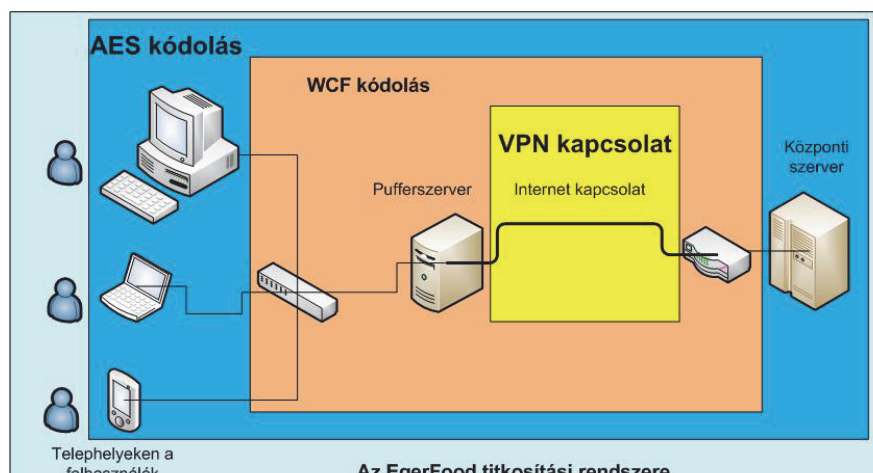
A (Colafigli, 2001) cikkben a szerzők egy információs rendszert mutatnak, melyet turisztikai célból hoztak létre. Elsősorban a WEB és a WAP technológiákat használták. Különböző hozzáférési jogosultságokat alakítottak ki, így mindkét technológia adatait mind statikusan, mind dinamikusan szolgáltatni tudták. Nagy hangsúly került a mobil interfészek használatára.

Részletesen elemzik a szerzők a WAP használat nehézségeit. Kiemelik a készülékek korlátozott tudását, az erősen szűkös sáv szélességet, a relatív nagy költséget, mely a WAP eléréssel jár együtt.

3. A kódolás

Tekintsük át, hogy a rendszerben hogyan biztosítjuk az adatok biztonságos kódolását, oly módon, hogy ne menjen az algoritmusok alkalmazása a kommunikáció hatékonyságának rovására. Amellett, hogy teljesíti a megfogalmazott és elvárt magas szintű titkosítást és biztonságot.

A projekt információs rendszerének kialakításakor kiemelt szerepet kapott a megfelelő adatbiztonság biztosítása. Ennek érdekében egy háromszintű titkosítási rendszer került kialakításra. Így az adatok keletkezésének pillanatától kezdve minden adat AES-128 algoritmus szerint kerül kódolásra (Liptai, 2007), az adattovábbításakor a szoftvertechnológiában legmodernebb „windows communication foundation” módszert használjuk, mely önmagában is titkosítottan végzi a kommunikációt. A hálózati adatforgalom VPN hálózaton keresztül történik, így a VPN routerek által biztosított titkosítást is ki tudjuk használni.



5. ábra. A titkosítási rendszer sémája

Az 5. ábra szemlélteti az általunk használt titkosítási rendszert. Az ábrán található fogalmakat a következő alfejezetekben fejtjük ki.

3.1. Az AES kódolásról

A Rijndael titkosítási eljárást, mint Advanced Encryption Standardot (AES) az USA Szabványügyi Intézete (NIST) 2001-ben fogadta el, lecserélve ezzel az addigi, már elavult DES titkosítási eljárást.

Az AES kiválasztását széles körben meghirdetett verseny előzte meg. A NIST olyan szimmetrikus kulcsú blokk kódolót keresett, amely 128 bites adatblokkok kódolására képes, és ehhez háromféle kulcsméret használatát teszteli lehetővé: 128, 192 és 256 biteset. A kiválasztás szempontjai voltak a kicsi méret, nehéz törhetőség, a gyorsaság és a kis eszközökben való alkalmazhatóság.

1999 augusztusában a kiválasztási verseny második fordulójában mindössze öt algoritmus maradt: a MARS, az RC6TM, a Rijndael, a Serpent és a Twofish. A győztes végül a Rijndael lett, amely eredeti nevét kitalálóiáról (Vincent Rijmen és Joan Daemen) kapta – továbbiakban ezt nevezzük AES-nek.

Az AES kódolóban a kódolást és dekódolást különböző eljárások végzik. A kódolás négy különböző transzformáció többszöri megismétlése, míg a dekódolás az egyes transzformációk inverzének megfelelő sorrendben történő végrehajtása.

3.2. A WCF (Windows Communication Foundation)

A .NET Framework 3.0 részeként megjelent Windows Communication Foundation (WCF, előző nevén Indigo) a Windows platform újgenerációs technológiája elosztott alkalmazások fejlesztéséhez. A legnagyobb előnye, hogy egységes programozási modellt nyújt, legyen szó egyszerű vagy biztonságos webszolgáltatásról, rendkívül hatékony bináris formátumú üzenetsorról vagy akár peer-to-peer alapú kommunikációról. Ennek következtében a fejlesztők a jövőben egyetlen kommunikációs technológia ismeretével és jelentősen kevesebb kód megírásával, vagyis a korábbinál egyszerűbben és hatékonyabban, készíthetnek elosztott alkalmazásokat.

A WCF egyik fontos tulajdonsága, hogy szolgáltatások közötti kommunikációt valósít meg. Ez a technológia túlmutat a webszolgáltatások nyújtotta lehetőségek kihasználásán, hiszen célja egy, a webszolgáltatások képességeit felülmúló funkcionalitásokat összegző szolgáltatás orientált API megvalósítása. A szolgáltatás és webszolgáltatás korábban még egy és ugyanazon fogalom megnevezésére volt használatos, ma már azonban nem csak szótani különbségek vannak a két megnevezés között:

1. A webszolgáltatásokat csak HTTP protokollon keresztül lehet meghívni. A szolgáltatások esetén viszont ilyen szempontból nincsenek korlátok, tetszőleges transzport protokoll használatával valósítják meg az adattovábbítást.

2. A webszolgáltatások ma csupán kérés-válasz jellegű kommunikációt képesek megvalósítani. Ezzel ellentétben a szolgáltatások számos egyéb üzenetküldési minta használatát is lehetővé teszik.
3. A webszolgáltatásokkal ellentétben a szolgáltatások rugalmasabbak, agilisek és jobban közelítik a szolgáltatás orientált paradigma szemléletmódját.

3.3. A VPN kapcsolat

Az adatgyűjtő szervert a legbiztonságosabban egy router mögé helyezhetjük el, amelyik fogadja a VPN kapcsolatokat, akár komplett hálózatoktól, akár egyedi munkaállomásoktól. A router feladata lehet igény szerint az adatgyűjtő szerver internet-kapcsolatának biztosítása egy NAT-olt hálózaton keresztül. A router feladat ellátására egy Cisco 1812-as routert alkalmaznánk két darab LAN port-tal. Az egyik port kapcsolódna az internethez, és NAT-olná a másik portja felé, amelyhez kapcsolódik az adatgyűjtő szerver. A router belső portjának a 192.168.0.254/24 IP-cím van megadva, mely tetszőlegesen és célszerűen változtatható a privát IP-címek tartományából. A router külső IP címének fix publikus IP-címnek kell lennie.

A távoli adatgyűjtő munkaállomások kétféle módon kapcsolódhatnak az adatgyűjtő szerverhez:

- VPN routeren keresztül a helyi hálózat összes számítógépe elérheti a szervert.
- A helyi hálózat internet routerén keresztül VPN Client program segítségével kapcsolódhatnak a kijelölt munkaállomások a szerverhez.

Az első megoldás csak abban az esetben alkalmazható, ha nem jelent biztonsági kockázatot a helyi hálózat összes munkaállomásának a kapcsolódási lehetősége az adatgyűjtő szerverhez. A második megoldás viszont minden más esetben alkalmazható, viszont ilyenkor a munkaállomás processzorát terheli meg a titkosítási procedúra. Mindkét megoldásnál ügyelni kell arra, hogy az adatgyűjtő szerver, és az adatgyűjtő, valamint adatfeldolgozó munkaállomások ne kerüljenek azonos IP tartományba. A központi router megfelelő konfigurációjával el tudja szeparálni egymástól az egyes VPN hálózatok és VPN Client-ek hálózati forgalmát úgy, hogy közben a szervert mindenki lássa.

4. Szerkezeti felépítés

A rendszer felépítését a 2. és 4. ábra szemlélteti. Ezeket fejtjük ki a következő alfejezetekben.

4.1. A központi adattárház

A központi adattárház tűzfal védi a külvilágtól. A tűzfalon kizárólag azok a portok vannak nyitva, amelyek a webes eléréshez és a VPN kapcsolat felépítéséhez szükségesek.

Az adattárházban két szerver található, az adatbázis szerver és a kommunikációs szerver.

Az Adatbázis szerver feladata:

- A Konzorciumi tagok által szolgáltatott adatok biztonságos tárolása.

A Kommunikációs szerver feladatai a következők:

- Adatok fogadása a Konzorciumi tagoknál elhelyezett Puffer szerverektől.
- Az érkezett adatok feldolgozása (dekódolás, mentés az Adatbázis szerverre).
- Az adatok publikálása a végfelhasználók felé.

Az adatbázis szerver védelme érdekében az adatbázis és a kommunikációs program különálló gépeken helyeztük el. Ez megnöveli az adatbázisban lévő adatok tárolásának biztonságát. Az adatbázis kizárólag a kommunikációs szerveren keresztül érhető el.

4.2. A puffer szerverek

A puffer szerver VPN kapcsolaton keresztül csatlakozik a Központi adattárházhoz.

Feladatai a következők:

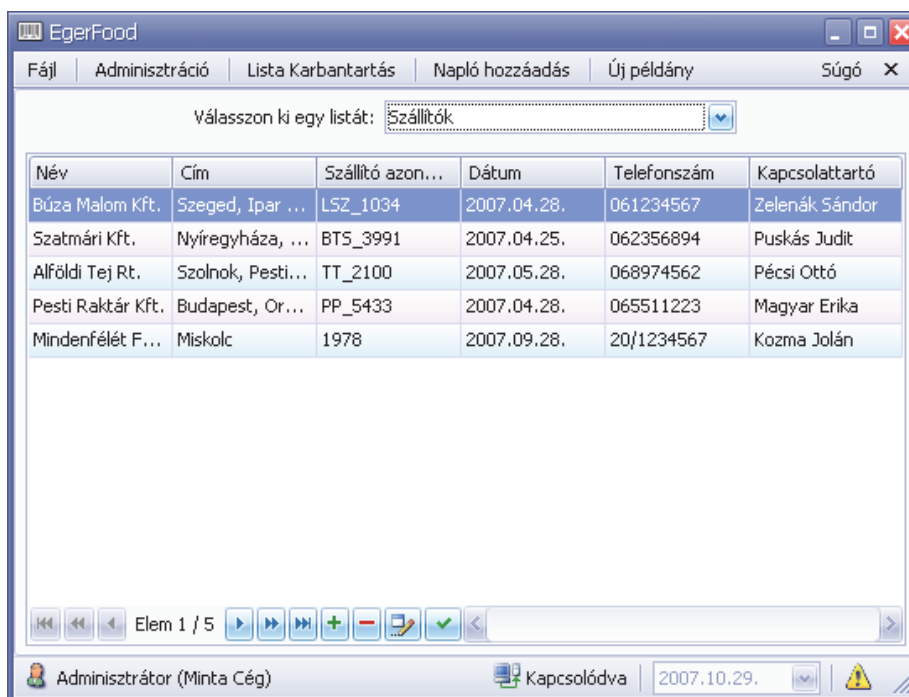
- A tagok EgerFood projekthez tartozó összes adatának tárolása (például törzsadatok, mérési eredmények stb.).
- A beérkező adatok dekódolása.
- A beérkező adatok feldolgozása és letárolása.
- A kimenő adatok titkosítása és elküldése meghatározott időnként a központi adattárház felé (VPN kapcsolaton keresztül).
- Biztonsági mentések megvalósítása.

4.3. A kliens gépek

A kliens gépek feladatai:

- Az egyes Konzorciumi tagok rendszerének konfigurálása, menedzselése.
- Törzsadatok (például beszállítók, nyersanyagok adatai) felvitele.
- Mérési adatok felvitele.
- Adatok titkosítása és továbbítása a puffer szerver felé.

A program eszközt nyújt a céges adminisztrációs adatok tárolásához is. Ezek az adatok összekötöttek a termékek adataival. Az adatok beviteli módja a legnagyobb mértékben automatizált: minimális a hibázás lehetősége és az adatok közötti kapcsolat biztosított. Az ablakok létrehozása automatikus, nincsenek kötött elrendezések, beépített vezérlők. Minden cég személyre szabott arculatot kap. A program arculata ízlés szerint változtatható, de a témák használata akár le is tiltható. Így a kisebb teljesítményű klienseken sem tapasztalható sebességcsökkenés.



6. ábra. Kliens program

4.4. A puffer szerver és a kliensek közötti kapcsolat

A kliens gépek VPN kapcsolaton keresztül érik el a puffer szerveret. Ez a megoldás lehetővé teszi a puffer szerver elérését a kliensek számára abban az esetben is, amikor egy Konzorciumi tag több olyan

telephellyel rendelkezik, ahonnan mérési adatokat szeretne rögzíteni, illetve menedzselni szeretné rendszerét.

A kliensek és a puffer szerverek között minden adat titkosított formában kerül továbbításra.

5. Információ szolgáltatás a felhasználók felé

A rendszerből a fogyasztók interneten vagy WAP-on keresztül kérhetnek le információt. Internet esetén legalább InternetExplorer 5.5, Firefox 1.5, vagy ezzel egyenértékű böngésző szükséges, amiben engedélyezni kell a JavaScript és a cookie-k használatát. WAP esetén legalább 1.2-es WAP böngésző szükséges.

A böngészőbe gépeljük be a következő címet: <http://193.225.33.32/egerfood>

A megjelenő oldal felső mezőjébe írjuk be a kérdéses termék csomagolásán található termékkódot (egy élő kód például: 110007112313). A beviteli mező alatt egy biztonsági ellenőrző kód látható, amely a rosszindulatú internetes támadások ellen véd. Ha létező kódot adtunk meg és az ellenőrző mezőt is helyesen adtuk meg, akkor egy hasonló képernyőt láthatunk:



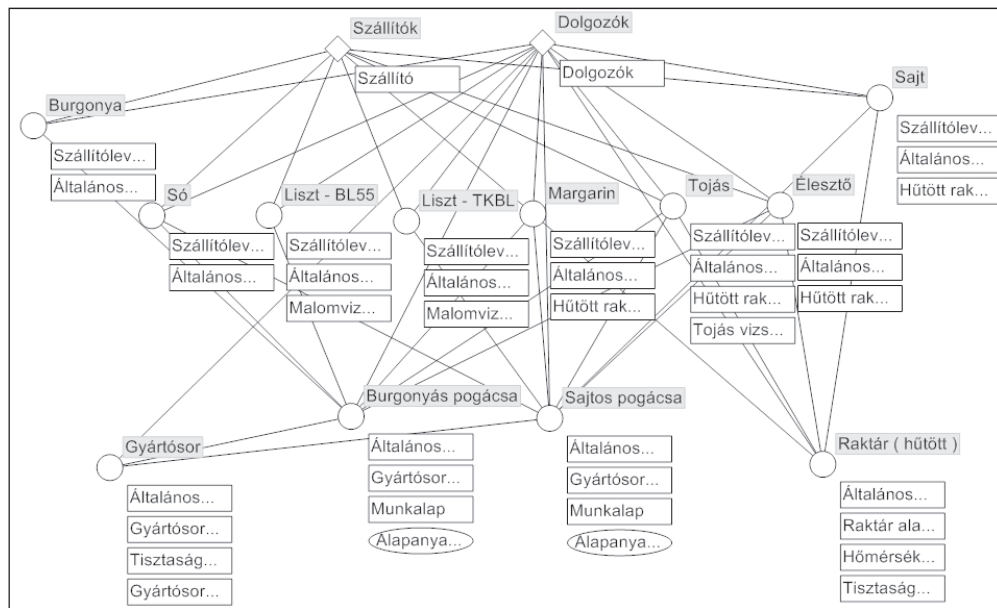
7. ábra. Egy lekérdezés az EgerFood adatbázisából

A megjelenő lapon az adatbázisban az adott terméken keresztül elérhető összes nyilvános adathoz hozzáférhetünk. Ezt úgy képzelhetjük el, hogy minden termékhez kapcsolódik egy munkafolyamat gráf, amelyben a rendszer tárolja, hogy az adott termékhez milyen naplókat kell vezetni. A konkrét termékhez tartozik egy konkrét munkalap, ami a legalapvetőbb információkat tartalmazza, valamint amin keresztül eljuthatunk a konkrét termékhez kapcsolódó többi konkrét naplóhoz is.

6. Belső felépítés

Hogyan képes az EgerFood mindezeket a képességeket nyújtani? Tekintsünk a rendszer mélyére!

Az egyedülálló képességek kulcsa a munkafolyamat-gráf (Kusper, 2007). A gráf segítségével minden cég egyedi módon modellezheti a gyártási folyamatait. Ez a modell vezérli a kliens program és az adatbázis működését. A modell szinte végtelen lehetőségeket nyújt és nem mellékesen összetett képet ad a cég működéséről is. Megtervezéséhez ezért a cég képviselőjének és a beüzemelést végző szakemberek közös munkájára van szükség.



8. ábra. Munkafolyamat gráf

A termék előállítását felfoghatjuk egy irányított gráfnak, amelynek csúcsai a termékek (vagy nyersanyagok), az élei pedig a munkafolyamatok, az élek kiindulási pontja a nyersanyagból az elkészült termékbe vezetnek. Ez a felfogás szükségessé teszi nem-nevesített termékek kezelését, mint például a massa, amely áll lisztből, sóból, vízből, élesztőből. Tehát ekkor ebből a négy nyersanyagból megy el a masszába. Ebben a felfogásban ez idáig így egy fa, de megengedjük azt is, hogy egy terméket részre szedjünk szét, így visszafelé vezető nyílak is lehetségesek, illetve lehetséges olyan folyamat is (pl.: tárolás), ami nem változtatja meg a terméket, illetve egy termékhez több odavezető utat is tárolhat.

A megvalósítás során kiderült, hogy a naplók élehez rendelése nehezebben megvalósítható, mint a csomópontokhoz rendelése. Ezért minden naplót termékhez, félkész termékhez rendelünk.

A gráf csomópontjai lehetnek csúcs és lista típusúak. A listákat csúcsokra állított négyzetek, a csúcsokat körök ábrázolják. A gráf élei az aktuális csomópontból kiinduló gyártási folyamatokat modellezik. Minden csomópont egy-egy entitást jelképez az adatbázisban. Látható, hogy a szállítók csomópontból származnak az alapanyagok, amelyekből a késztermékek készülnek. A dolgozók csomópont az alapanyagokra és a gyártósorra van hatással, a gyártósor szintén részt vesz a késztermék elkészülésében. A négyzetek a csomópontokhoz tartozó naplót reprezentálják. A példányosító naplók ebben a nézetben nem jelöltek speciális módon az ábrán. A szállítók és dolgozók csomópont lista típusú, ami azt jelenti, hogy törzsadatokat tárolnak, vagyis szállítók-, dolgozók-, műszakok-adatait, illetve ezekhez hasonló adatokat. A naplót egy szerkesztő modul segítségével lehet összeállítani.

Egy napló legegyszerűbben név-érték párosként fogható fel. A naplószerkesztő modul segítségével lehet megadni a neveket és a hozzájuk rendelhető értékek típusát. A szerkesztő csoportok definiálására is lehetőséget ad. A típusok általában egyszerű típusok (szám, szöveg, dátum, idő), amelyekhez megadható riasztás is. A listákhoz csak ilyen egyszerű típusú mezők adhatók. A csúcsokhoz viszont jóval bonyolultabb típusok rendelkezésre állnak a következő okok miatt: a legegyszerűbb esetben a burgonyás pogácsa elkészítéséhez sok összetevőre van szükség. Minden összetevőből több példány található a rendszerben. Tekintsük csak a lisztet, amiből több szállítmány is lehet a raktárakban. Egy-egy szállítmány új példányként jelenik meg, mert amikor megérkezik, példányosító naplót kell létrehozni hozzá. Amikor egy pogácsát sütnek, szükséges tudni, hogy melyik szállítmányból készült (hiszen erre szolgál az egész rendszer). Erre szolgál a csúcs típus. Ennél a típusnál meg lehet adni, hogy melyik csúcsról van szó. A kliens majd a napló kitöltésénél megjeleníti a megadott csúcs példányait, vagyis példánkban a liszt szállítmányait. A naplót kitöltő felhasználó kiválasztja a megfelelő példányt. Ez a módszer más esetekben is nagyon hasznos lehet.

Egy entitáshoz ún. dinamikus listát is létre lehet hozni. A gráfon ezt ovális alakzat jelképezi. A dinamikus listához tetszőleges csomópontokat lehet rendelni. Arra szolgál, hogy az ott lévő naplók közös részét kiemeljük, így a redundancia csökkenthető.

7. Összefoglalás

Az adatbázisok programozása, elérése felhasználói programokból napjainkban egy elterjedt, az élet minden területén megjelenő, sok helyen vezető szerepet betöltő problémakör. Az adatok kezelésének első lépése, azok tárolása, mely művelet minden rendszerben megjelenik, helyenként jelentős erőforrásokat felemésztve a rendelkezésre álló keretből.

Belátható, hogy a fent részletezett kriptográfiai eszközök alkalmazása megfelelően erős titkosítást és így biztonságot ad az ipari titkokat is tartalmazó adatoknak.

A rendszer továbbfejlesztési lehetősége a modern, emberi hibát egyre jobban kiküszöbölő automatikus azonosítás felé mozdulhat. Ezért az RFID technológia integrálása fontos előrelépést jelenthet.

Hivatkozások

- Abdul D. S., Hatem E. M., Abdul K., Hadhoud M. M. 2009. Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices, *International Journal of Computer Theory and Engineering*, Vol. 1, No. 4
- Ceri, S., Pernici, B., Wiederhold, G. 1987. Distributed database design methodologies, *Proceedings of the IEEE*, vol.:75, num.: 5, pp: 533-546
- Colafigli, C., Inverardi, P., Matricciani R. 2001. InfoParco: an experience in designing an information system accessible through WEB and WAP interfaces, *PROCEEDINGS OF THE ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES*,
- Coppersmith D. 1994. The Data Encryption Standard (DES) and Its Strength against Attacks. *IBM Journal of Research and Development*, vol. 38, num. 3, pp. 243 -250
- Ferguson, N., Schneier, B. 2000. *A cryptographic evaluation of IPsec*, Counterpane Internet Security, Inc.
- Ferguson, P., Huston, G. 1998. *What is a VPN?*, Citeseer
- Fishawy N. E. 2007. Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms, *International Journal of Network Security*, pp.241-251.
- Hamid, N.R.A. 2003. Database imperatives in managing supply chain: an empirical study, *WSEAS Transactions on Computers*, vol.:2, num.: 2, pp: 379-385
- Hardjono, T., Dondeti L.R. 2005. *Security in Wireless LANS and MANS (Artech House Computer Security)*, Artech House, Inc. Norwood, MA, USA
- Holliday, J.A., Agrawal, D., Abbadi, A.E. 1999. The performance of database replication with group multicast, In *Proceedings of IEEE International Symposium on Fault Tolerant Computing (FTCS29)*
- Iyer, B., Mehrotra, S., Mykletun, E., Tsudik, G., Wu, Y. 2004. A framework for efficient storage security in rdbs, *Lecture Notes in Computer Science*, pp:147-164
- Kusper G., Radványi T. 2007. Requirement Analyzes and a Database Model for the Project EGERFOOD Food Safety Knowledge Center, , 7th International Conference on Applied Informatics, Eger, Hungary, January 28 - 31, 2007, plenáris előadás page 15-25
- Liptai K., Kusper G., Radványi T. 2007. Cryptographycal Protocols in the Egerfood Information System, (Eger, Hungary), *Annales Mathematicae et Informaticae*, 61-70 p.
- Radvanyi T. 2004. Examination of the MSSQL server from the user's point view considering data insertion, (Eger, Hungary), *Acta Academiae Pedagogicae Agriensis*, 69-77 p.
- Radványi T., Kusper G. 2007. Az EGERFOOD élelmiszerbiztonsági tudásközpont projekt információs rendszerének kialakítása, *NetworkShop 2007 Eger*, 2007. április 11-13.
- Rijndael V., Daemen, J., Rijmen 2001. The Advanced Encryption Standard. *D r. Dobb's Journal*, PP. 137-139.

Schneier B. 2008. The Blowfish Encryption Algorithm, Retrieved October 25, 2008, <http://www.schneier.com/blowfish.html>

Shakhgeldyan, C., Kryukov, V. 2004. Integration of University Information Resources into the Unified Information Environment, Proceedings of the 10-th International Conference of European University Information Systems (ENUS 2004). Slovenia, pp.: 321-327

Teorey, T.J., Yang, D., Fry, J.P. 1986. A logical design methodology for relational databases using the extended entity-relationship model, ACM Computing Surveys (CSUR) vol.:18, num.: 2, pp.: 197-222

Treck, D., Kandus, G. 2003. Security Policy - Human Factor Modeling and Simulation, WSEAS Transactions on Computers, vol. 2, pp.: 339-342

Zolotova, I. and Flochova, J., Ocelnia, E. 2005. Database technology and real time industrial transaction techniques in control, Journal of Cybernetics and Informatics, vol.:5, pp: 18-23