Utjecaj primjene kriptografije na performanse sistema s akcentom na okruženje MySQL

Mahir Zajmović
Fakultet informacionih tehnologija
Sveučilište/Univerzitet "Vitez"
Vitez, BiH
mahir.zajmovic@unvi.edu.ba

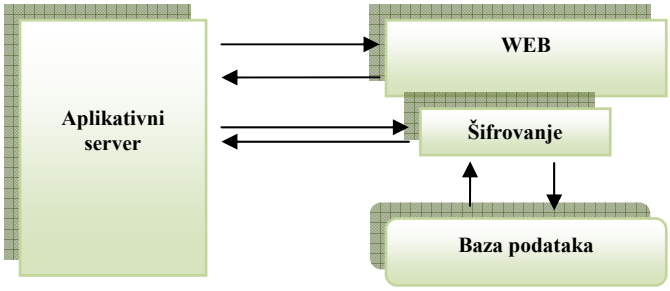
Siniša Minić
Fakultet informacionih tehnologija
Sveučilište/Univerzitet "Vitez"
Vitez, BiH
sinisa.minic@unvi.edu.ba

Sadržaj—**U ovom radu prikazana je komparativna analiza primjene kriptografskih algoritama u bazama podataka, gdje je izvršeno testiranje ponašanja baza podataka ukoliko se primjenjuju kriptografski algoritmi i dokazana činjenica koliko primjena kriptografije utiče na same performanse sistema. Testiranje je izvršeno u sistemu za upravljanje bazama podataka MySQL.**

Ključne riječi - kriptografija, simetrični algoritmi, asimetrični algoritmi, performanse sistema, baze podataka, MySQL

I. UVOD

Kriptografija je nauka koja se bavi metodima očuvanja tajnosti informacija. Kada se lične, finansijske, vojne ili informacije državne bezbjednosti prenose sa mjesta na mjesto, one postaju ranjive na napadačke taktike. Ovakvi problemi se mogu izbjeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim neželjenoj strani. Šifra i digitalni potpis su kriptografske tehnike koje se koriste da bi se implementirali bezbjednosni servisi. Osnovni element koji se koristi naziva se šifarski sistem ili algoritam šifrovanja. Za realizaciju ovog rješenja lokalne zaštite korišćena je MySQL baza podataka. Izvorni kod nekih od realizacija je dostupan i/ili postoji mogućnost proširenja dok su neke realizacije potpuno zatvorene. MySql SUBP (Sistem za upravljanje bazom podataka) ne posjeduje sve funkcionalnosti kao sistemi tipa Oracle, ali dovoljan skup funkcionalnosti i povoljna cijena su pozitivno uticali na prihvatanje ovog softvera od strane tržišta. Danas većina programskih jezika posjeduje biblioteke za korišćenje MySQL-a, a postoji i ODBC (Open Database Connectivity) interfejs za jezike za koje nije ugrađena podrška. Mjesto modula za šifrovanje kod lokalne zaštite baze prikazano je na slici 1.



Slika 1. Mjesto modula za šiftovanje kod lokalne zaštite baze

MySQL u svom kriptografskom modulu koristi dva najpoznatija algoritma za šifrovanje AES (Advanced Encryption Standard) i DES (Data Encryption Standard). U eksperimentalnoj analizi izabran je AES algoritam ("Rijnda-el") koji koristi funkcije AES_ENCRYPT() i AES_DECRYPT() za šifrovanje i dešifrovanje podataka. U ovom modulu MySQL može da koristi dužinu ključa od 128 ili 256 bita. U radu korišćen je ključ od 256 bita zbog povećanja sigurnosti što se odražava na performanse sistema. Funkcija AES_ENCRYPT() kao rezultat vraća binarni string (šifrat), a funkcija AES_DECRYPT() vraća originalni string (otvoreni tekst). U slučaju da se proslijede pogrešni argumenti funkcijama, obje funkcije vraćaju kao rezultat nulu.

Za realizaciju funkcije AES_ENCRYPT() kao argumente funkciji prosljeđujemo tekst za šifrovanje i ključ algoritma dužine 128 ili 256 bita sa kojim šifrujemo, a za realizaciju funkcije AES_DECRYPT() kao argumente prosleđujemo šifrat i ključ koji smo koristili kod funkcije AES_ENCRYPT() pri šifrovanju.

Navedene su prednosti i mane ovog koncepta zaštite:

- Prednosti:
  - realizacija AES algoritma u C programskom jeziku,
  - podaci se u bazi čuvaju u šifrovanom obliku.
- Mane:
  - nedostupnost izvornog koda,
  - ključ se nalazi zajedno sa šifrovanim podacima,
  - promjena ključa (proces koji zahtijeva dešifrovanje i ponovno šifrovanje kompletne baze podataka),
  - podaci nisu zaštićeni u toku komunikacije sa bazom.

II. ŠIFROVANJE NA APLIKATIVNOM SERVERU

Ovaj vid lokalne zaštite se postiže na klijent / server arhitekturi instalacijom kriptografskog modula na aplikativnom serveru. Komponente klijent / server arhitekture moraju se povinovati nekim osnovnim principima kako bi međusobno djelovale ispravno. Ovi principi moraju biti jednoznačno upotrebljivi u komponentama klijenta, servera i komunikacionog posrednika.

Principi koji moraju biti ispunjeni su:

- hardverska nezavisnost,
- softverska nezavisnost,
- otvoreni pristup za servise,
- distribucija procesa.

U izradi kriptografskog modula za kompletnu funkcionalnost AES algoritma korišćen je PHP programski jezik zbog svojih sve naprednijih mogućnosti i zato što pripada grupi open source jezika.

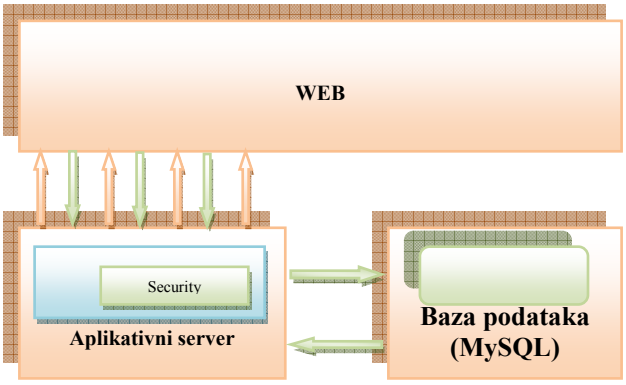
Algoritam je napisan prema standardima propisanim od strane FIPS-a (Federal Information Processing Standards). Navedeni AES algoritam ima podršku za tri dužine ključa (128, 192, 256). Mogućnost korišćenja algoritma u ovom rješenju podrazumijeva adekvatan API (tj. mogućnost proširenja rješenja sopstvenim modulima) ili/i dostupnost izvornog koda rješenja.

S obzirom na to da je klijent / server arhitektura iskorišćena u vidu web aplikacija koju može da karakteriše veliki broj korisnika istovremeno, performanse i konkurentni pristup su dva pitanja na koja treba obratiti pažnju pri realizaciji. Različita serverska rješenja imaju različite pristupe za povećanje performansi. Na slici broj 2 ilustrovana je klijent-server arhitektura koju je moguće iskoristiti u procesu zaštite podataka u bazama. Prikazana arhitektura se sastoji od dva servera.

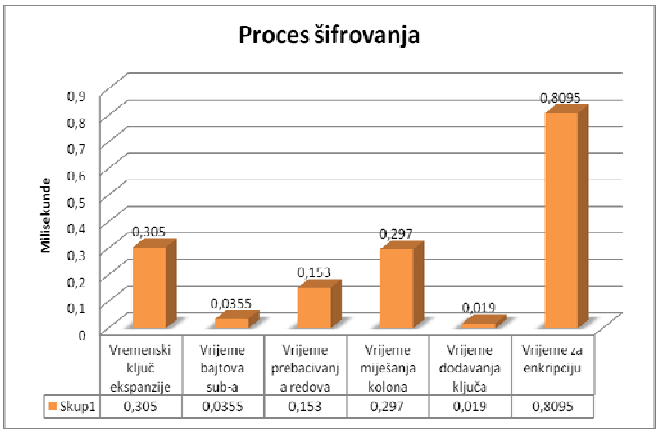
Na jedanom se nalazi baza podataka, a na drugom aplikativni server. Aplikativni server implementira PHP modul sa modulom za šifrovanje i dešifrovanje. Između ova dva servera postoji direktna komunikacija. Podaci koji se razmjenjuju su u obliku šifrata.Imajući u vidu da je PHP interpreterski jezik, performanse su znatno slabije u odnosu na prethodno analiziranu arhitekturu gdje je modul za šifrovanje realizovan u C programskom jeziku i integrisan sa bazom podataka.

Za testiranje korišten je sistem sa sljedećim karakteristikama:

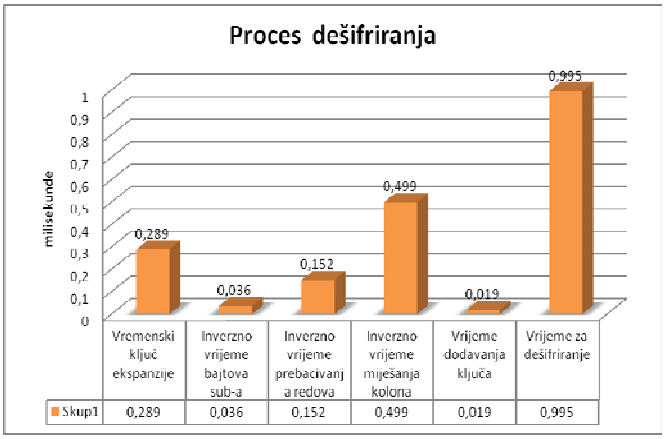
- 64 - bitni Dual - CoreAMD procesor Pentium 4,
- 8 GB RAM-a,
- Direct - Attached SCSI diskovi,
- Windows Server 2003 R2 Enterprise x64 Edition,
- MySQL Server,
- Apache Web Server.



Slika 2. Šifrovanje na aplikativnom server



Slika 3. Performanse pri procesu šifrovanja



Slika 4. Performanse pri procesu dešifriranja

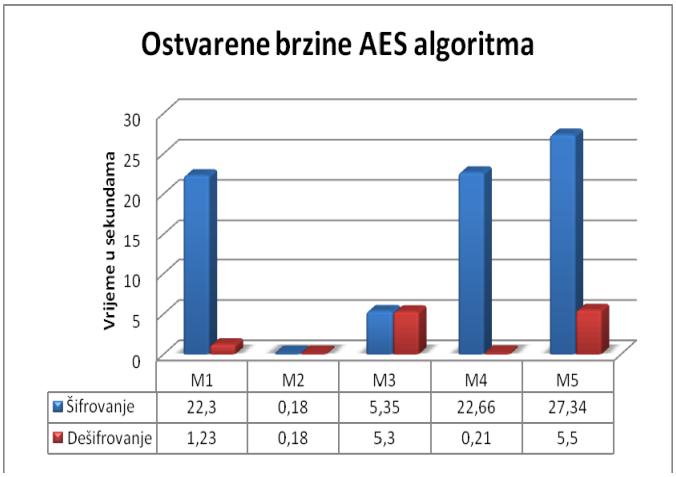
Navedene su prednosti i mane ovog koncepta zaštite:

- Prednosti:
  - podaci u komunikaciji su zaštićeni,
  - ključ se ne nalazi sa šifrovanim podacima,
  - dostupnost izvornog koda.
- Mane:
  - realizacija AES algoritma u interpreterskom jeziku (to se odražava na performanse sistema),
  - promjena ključa (proces koji zahtijeva dešifrovanje i ponovno šifrovanje kompletne baze podataka)

Ključni su vremenski resursi ili vrijeme potrebno za jedan "ciklus" algoritma. Algoritmi predstavljaju skup međusobno povezanih elementarnih struktura, za čije izvršavanje se troši značajno procesorsko vrijeme. Cilj ovog rada je bio da se provjeri koliki je uticaj softverskih realizacija algoritama za šifrovanje na opterećenost procesora. Upravo iz ovog razloga, analiziran je uticaj vremenske komponente za izvršavanje pojedinih algoritama. U daljem dijelu ovog rada prikazani su rezultati dobijeni za AES algoritam.

III. ANALIZA REZULTATA

Rezultati mjerenja prikazani su na slici 5. i u tabeli 1. Na slici 5. vidi se pad brzine šifrovanja podataka pri upisu šifrata u bazu podataka. Imajući u vidu da je za sva mjerenja korištena ista hardverska platforma i isti komunikacioni kanal (iste propusne moći) jasno je da razlog usporenja leži u brzini tvrdog diska računara na kojem se nalazi baza podataka te brzini softverske aplikacije koja je korištena. U tabeli 1. date su brojčane vrijednosti prikazane na dijagramu slike 3. (u sekundama). S obzirom da je opterećenje Intel procesora pri korišćenju svakog od algoritama bilo na maksimumu (99,9% + 0,01% za sistemske procese) to jasno ukazuje na usko grlo ovih mehanizama. Moguće je predvidjeti 2-3 puta veću brzinu korišćenjem snažnijih procesora i hard diskova veće brzine upisa.



Slika 5. Dijagram sa ostvarenim brzinama AES algoritma

Napomena: U eksperimentu su kao uzorak korišćeni stringovi dužine 300 karaktera i svako mjerenje je imalo 1000 ciklusa da bi se što bolje procijenilo opterećenje šifrovanjem velike količine podataka u što kraćem vremenskom periodu. Dijagram predstavlja 5 različitih rezultata mjerenja.

TABELA 1. REZULTATI MJERENJA

Proces	Vrijeme (s)	CPU (%)
Standardan upis/ispis nešifrovanih podataka u bazi podataka		
Upis	22.30	6
Ispis	1.23	70
Brzina AES algoritma integrisanog u bazi podataka pri šifrovanju/ dešifrovanju		
Šifrovanje	0.18	20
Dešifrovanje	0.18	20
Brzina AES algoritma integrisanog na aplikativnom serveru pri šifrovanju/dešifrovanju		
Šifrovanje	5.35	54
Dešifrovanje	5.30	54
Brzina AES algoritma integrisanog u bazi podataka pri šifrovanju/ dešifrovanju i upisu/ispisu u bazu podataka		
Šifrovanje	22.66	7
Dešifrovanje	0.21	33
Brzina AES algoritma integrisanog na aplikativnom serveru pri šifrovanju/dešifrovanju i upisu/ ispisu u bazu podataka		
Šifrovanje	27.34	54
Dešifrovanje	5.50	70

IV. ZAKLJUČAK

U današnje vrijeme se sve veći broj programskih sistema projektuje i gradi za izvođenje na globalnoj računarskoj mreži Internet. Sigurnosni mehanizmi koji se upotrebljavaju za uspostavljanje sigurnog komunikacijskog kanala zasnivaju se na primjeni metoda kriptografije kojima se jamči tajnost, izvornost i vjerodostojnost podataka koji se prenose računarskom mrežom.

Budući da se kriptografski postupci zasnivaju na poznavanju kriptografskih ključeva sudionika u komunikaciji, posebna pažnja posvećuje se postupcima sigurne razmjene tih ključeva. Najraširenij način razmjene kriptografskih ključeva je primjena infrastrukture javnih ključeva (engl. Public Key Infrastructure- PKI). Infrastruktura javnih ključeva je računarski sistem koji osigurava sigurnu razmjenu kriptografskih ključeva putem nesigurnih računarskih mreža poput mreže Internet. Infrastruktura javnih ključeva koristi digitalne vjerodajnice (engl. digital certificate) kako bi ispunila sve potrebne sigurnosne zahtjeve. Svaki sudionik infrastrukture javnih ključeva ima vlastitu digitalnu vjerodajnicu koja nepobitno dokazuje njegov identitet.

Također, možemo zaključiti da postoji značajan utjecaj softverskih realizacija algoritama za šifrovanje na opterećenost procesora.

LITERATURA

[1] A. Dujella, M. Maretić: Kriptografija, Element, Zagreb, 2007.

[2] A. J. Menezes, P. C. Oorschot, S. A. Vanstone: Handbookof Applied Cryptography, CRC Press, Boca Raton, 1996.

[3] Alan G. Konheim: „Computer Security and Cryptography“, Wiley, 2007.

[4] A. Lee, NIST SpecialPublication 800-21: Guideline for Implementing Cryptography in the Federal Goverment, National Institute of Standardsand Technology, 1999.

[5] Anne Peterson Bishop, Barbara P. Buttenfield and Nancy A. Van House: Digital Library Use: Social Practice in Design and Evaluation, MIT Press, 2003.

[6] A. Sabic, J. Azemovic: Model ofefficient Assessment System with accent on Privacy, Security and Integrationwith E-University Components, Shanghai, 2010.

[7] Application Security, "Encryption of Dataat Rest – DatabaseEncryption", White Paper

[8] B. Ibrahimpašić: Kriptografija kroz primjere, Pedagoški fakultet Bihać, 2011.

ABSTRACT

This paper presents a comparative analysis of the application of cryptographic algorithms in databases, where it was tested behavior database if applied cryptographic algorithms and proven fact as far as the application of cryptography affects the system performance. The tests were conducted in the system for managing MySQL databases.

INFLUENCE OF CRYPTOGRAPHY SYSTEM PERFORMANCE WITH AN EMPHASIS ON ENVIRONMENT MySQL

Mahir Zajmović, Siniša Minić