Büyük Hacimli Veri Tabanları İçin Bilgi Güvenliğinin Sağlanması*

Gülce Eştürk
gulce.esturk@stu.yasar.edu.tr

Bilgi güvenliği; veritabanı koruması ve veri tabanında bilgi kaybının olmaması için gereklidir. Veritabanlarında tutulan veri, matematiksel modelleri içinde barındıran bir bileşimdir.Veri tabanı güvenliği kurumsal ve/veya bireysel olarak bilgi sistemlerindeki en önemli sorunlardan biri olmaktadır. Son dönemde Veri tabanı güvenliği problemi daha da büyümüş ve kurumları ve hatta bireyleri zor durumda bırakmaya başlamıştır. Bu şekilde, güvenlik açığından dolayı oluşan kurumsal imaj kaybı, kaynak tüketimi, müşteri mağduriyeti, iş yavaşlaması ve/veya durması ve en önemlisi; veri tabanında tutulan veri ve/veya bilgilerin yetkisiz kişilerin eline geçmesiyle, üçüncü şahıslara karşı yapılacak saldırıların engellenmiş olması sağlanacaktır.

Keywords: Veritabanı Güvenlik Kriptografisi, Güvenlik ve Veritabanı Yönetimi

1.Giriş

Bilgi teknolojilerindeki gelişmeler ile birlikte kurumlar veya bireyler bir çok bilişim suçlarına maruz kalmışlardır. Bu bilişim suçlarının en önemlilerinden biri ise; veri tabanı güvenliğidir.

Veri tabanı güvenliği artık günümüz teknolojileri ile birlikte daha da önem kazanmaktadır. Şöyle ki önceden fiziksel olarak yapılan korunma tedbirleri (para, kişisel veya kurumsal bilgiler vs), günümüz teknolojileri ile birlikte yerine sanal tedbirlere (önlem) bırakmaktadırlar. Veri tabanları; korunması gereken bilgilerin olduğu her yerde, diğer bir söylemle, yüksek seviyede güvenliğin olması gereken banka, şirket, adalet, sağlık vb. kurumların veya bireylerin önemli bilgilerinin tutulduğu önemli ve en iyi şekilde korunması gereken yapılardır. Veri tabanı kullanan uygulamalar yaygınlaştıkça ve gerekli önlemler alınmadıkça, yazılım ve/veya donanım güvenlik modelleri geliştirilip kullanılmadıkça; güvenlik sorunları her geçen gün daha da artacaktır.

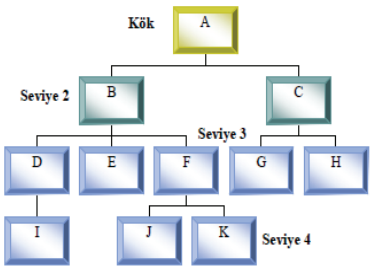
Yapılması planlanan güvenlik mimarileri ile; güvenlik açığından dolayı oluşan kurumsal imaj ve en önemlisi; veri tabanında tutulan veri ve/veya bilgilerin yetkisiz kişilerin eline geçmesiyle, üçüncü şahıslara karşı yapılacak saldırıların engellenmiş olması sağlanacaktır.

2. Veri Tabanı Modelleri

1960 yıllarında gnellikle ana bilgisayar ortamında çalışan uygulamalar tarafından kullanılmıştır. Bu model veri tabanı bilgilerini bir ağaç yapısında tutar. Kök olarak bir kayıt bulunmaktadır. Bu köke bağlı alt dallar ise; modelde alt kayıtları oluşturmaktadır. Bu şekilde veri tabanı yapısını kök ve dallardan oluşturmaktadır. Bu model yapısında ağaç yapısına benzediğinden aranacak herhengi bir bilgi için kök segmentinden aramaya başlanılmaktadır. Arama işlemi dallarda devam etmektedir. Veriye erişmek için, verinin yolunu bilmek gerekmektedir.Dezavantaj olarak; veri tabanında yapılan herhangi bir değişiklik, yolun değişmesine yol açabilir, bu da oluşturulan sistem için problem oluşturabilir. Şekil 2.1'de hiyerarşik model verilmiştir. [3][9]

2.2. Ağ Model

Ağ veri modeli; tablo ve grafik

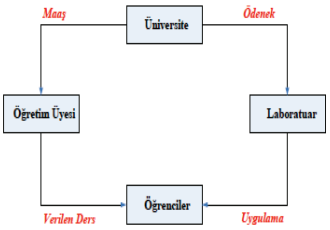


temellidir.Grafikteki düğümler veri tiplerine karşılık gelirken tablolar şeklinde temsil edilir. Grafiğin okları,

ilişkileri temsil eder ve tabloda bağlantılar olarak temsil edilir. İki ayrı veri yapılandırma aracı vardır: Kayıt tipi ve bağlantı. Kayıt tipleri; varlık tiplerini belirler. Bağlantı ise; ilişki tiplerini belirler.[2] Ağ modeli birçok yönlerden hiyerarşik modele benzemektedir. Fakat hiyerarşik yapıdan farklı olarak, ağ yapılarında bağlantı açısından herhangi bir sınırlama yoktur. Ağ veri modeli, karmaşık bir yapıya sahip olan veri ilişkilerini hiyerarşik modelin yapabildiğinden daha etkin bir şekilde gösterebilmek ve veri tabanı performansını arttırmak için geliştirilmiş yapıdır. Ağ veri modeli, düğümler arasında çoklu ilişkiler kurulamadığı için kısıtlı bir veri modelidir. [3]

2.3.İlişkisel Veri Modeli

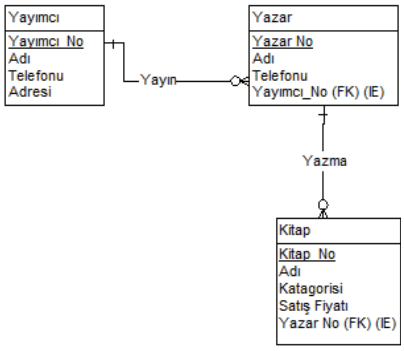
İlişkisel veri tabanı model



yapısı; verileri tablo yöntemi ile tutmayı sağlayan veri modelleme yöntemidir. Tablolar arasındaki ilişki mateamatiksel modellemelere göre oluşturulmaktadır. Tablolar satır (row) ve sütun (column) lardan oluşmaktadır. Kullanılan anahtar sistemi tablolar birbirleriyle daha kolay ilişkilendirilebilmektedir.

2.4. Nesne Yönelimli Model

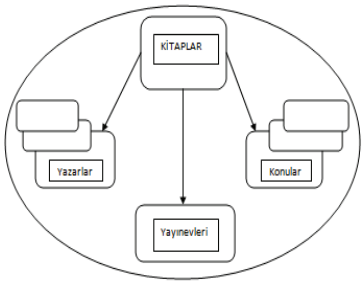
Nesne yönelimli model yapısında; veriler daha karmaşık yapılara sahiptir. Bu model yapısı diğer veri modellerine kıyasla, arama işlemleri daha hızlıdır. Veriler tek parça halinde gelmektedir. Performans açısından



değerlendirildirildiğinde nesne yönelimli model daha iyi sonuçlar vermektedir.[3][9]

3.Güvenlik Prensipleri

Security Principles temelde 3



bileşenden oluşur.

3.1. Gizlilik

Bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Gizlilik,hem kalıcı ortamlarda (disk, tape, vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur.[4][6]

3.2. Veri Bütünlüğü

Bu hizmetin amacı, veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır.

3.3. Süreklilik

Bilişim sistemleri, kendilerinden beklenen işleri gerçekleştirirken, hedeflenen bir başarım (performance) vardır. Bu başarım sayesinde müşteri memnuniyeti artar, elektronik işe geçiş süreci hızlanır. Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarı düşürücü tehditlere karşı korumayı hedefler.

4.Yasal Olmayan Kopyalama Tespit Sistemi Modellemesi

İçinde bulunulan bilgi çağında; bilgi güvenliği, kurumların veya bireylerin gizli olarak nitelendirdikleri bilgilerin korunmasında çok önemli bir yere sahiptir. Teknolojinin gelişmesiyle birlikte bilgiler dijital ortamda saklanmaktadır. Bu şekilde bilginin istenilen hedefe en hızlı şekilde ulaştırılması hedeflenmiştir. Akabinde bu durum kurumsal veya bireysel bazı sorunlara yol açmaktadır.

Bilgi teknolojilerindeki gelişmeler ile birlikte kurumlar veya bireyler bir çok bilişim suçlarına maruz kalmışlardır. Bu bilişim suçlarının en önemlilerinden biri ise; veri tabanı güvenliğidir. Veri tabanı güvenliği günümüz teknolojileri ile birlikte daha da önem kazanmaktadır. Şöyle ki, veri tabanında gözlenen; izinsiz kullanım, veri (bilgilerin); çalınması (=kopyalanması), ekleme yapılması, veri üzerinde değişiklik yapılması, silinmesi veya kullanılmaz hale gelmesi durumu yaratan güvenlik açığı problemleri oluşturmaktadır. Bu problemlere ek olarak, ver tabanı güvenlik problemlerinde en önemli sorunlardan biri ise; hukuksal çözüm aşamalarıdır. Herhangi bir yasal olmayan saldırıda; kurumlar veya bireyler hukuki çözüm yollarına başvurabilmektedir.

Hukuksal süreçlerin bireylere ve kurumlara olan etkilerinin minimum olması hedeflenmelidir. Bu şekilde , güvenlik açığından dolayı oluşan kurumsal imaj kaybı, kaynak tüketimi, müşteri mağduriyeti, iş yavaşlaması ve/veya durması ve en önemlisi; veri tabanında tutulan veri (bilgilerin) yetkisiz kişilerin eline geçmesiyle, üçüncü şahıslara karşı yapılacak saldırıların engellenmesi sağlanacaktır.

5. Sonuç

Kurumsal veya bireysel veri güvenliğinin aşılmasıyla oluşan; veri bütünlüğünün bozulması, erişim denetimi, gizliliğin korunamaması ve sistemlerin çalışmalarının sürdürebilirliğinin engellenmesi ve en önemlisi bu durumlara bağlı olarak hukuksal çözüm aşamalarının artmıştır. Bu şekilde kurum, birey ve ülke bazında sorunlar büyüyecek ve temel sistem bütünlüğü bozulacaktır. Oluşturulan matematiksel Yasal Olmayan Kopyalama Tespit Sistem Modeli ile kurum ve bireyler verilerini kendi kurallarına göre koruyabileceklerdir. Buna bağlı olarak da hukuksal çözüm aşamaları daha kısa sürede sonlanabilecektir.

6. Kaynakça

[1] AFSB (Air Force Studies Board). "Multilevel Data Management Security." National Academy of Sciences Report, 1983.

[2] Burns, R. "Referential Secrecy." Proc IEEE Symp on Security & Privacy, 1990, p133–142.

[3] Çelik, İ., Ünüvar, A., “Nesne Yönelimli Yaklaşımla Özellik Tabanlı Modelleme”, Mühendis ve Makine Dergisi

[4] Date, C. An Introduction to Data Base Systems, vol 1. Addison-Wesley, 1981.

[5] Date, C. An Introduction to Data Base Systems, vol.2. Addison-Wesley, 1983.

[6] Denning, D. "Commutative Filters for Reducing Inference Threats." Proc IEEE Symp on Security & Privacy, 1985, p134–146.

[7] Denning, D. "An Intrusion-Detection Model." Proc IEEE Symp on Security & Privacy, 1986, p102–117.

[8] İnternet: David Litchfield, “The Database Exposure Survey 2007”, http://regmedia.co.uk/2007/11/15/thedatabaseexposuresurvey2007.pdf (13.02.2008).

[9] Mazıbaş, M., “Operasyonel Risk Veri Tabanı Modellemesi”, Bankacılık Düzenleme ve Denetleme Kurumu, Ankara, 11-16 (2006).

[10] Stallings,W.(2012).Cryptography and Network Security(5th ed.) (p59).US:Pearson

**Bitirme projesi*