DATA MASKİNG NƏDİR

Data masking, verilənlər bazasındakı (SQL-də) məlumatların gizlilik və təhlükəsizlik məqsədləri ilə qismən və ya tamamilə gizlədilmə prosesidir. Məqsəd, hassas məlumatları, məsələn, şəxsi məlumatlar (ad, soyad, ünvan, telefon nömrəsi) və ya maliyyə məlumatlarını (kredit kartı nömrəsi, bank hesabı) qorumaqdır.Data masking prosesi zamanı, məlumatlar asanlıqla tanımlanmayacaq və ya gizlədilmiş olacaq şəkildə dəyişdirilir. Buna misal olaraq, şəxsin adını "A" ilə əvəz edə bilərik, ünvanını isə tamamilə gizlədə bilərik. Bu, məlumatların təhlükəsiz bir şəkildə saxlanılmasını və təhlükəsizlik nizamlarına riayət edilməsinə kömək edir.Data masking, şirkətlər, tibbi qurumlar və digər bir çox sahələrdə məlumatların hər hansı bir formada təhlükəsiz bir şəkildə saxlanılması və idarə edilməsi üçün əhəmiyyətli bir alətdir. Bu, potensial hackerlara və ya userlərə məlumatların tam təxminləşdirilməsinin qarşısını almağa kömək edir.Data masking, məlumatların gizliliyini təmin etmək üçün əsasən iki məqsədə xidmət edir: məlumatlar üzərindəki təhlükəsizlik risklərini azaldır və test məlumatlarının hazırlanması zamanı gerçək məlumatların ifşa olunmasının qarşılıqlı törədilən hər hansı bir riskini aradan qaldırır.

DATA MASKİNG NÖVLƏRİ

Data masking mərhələli bir prosesdir və hər bir verilənlər bazası sistemində fərqli metodlarla tətbiq edilə bilər. İllər keçdikcə, SQL verilənlər bazalarının data masking funksiyalarını dəstəkləməsi üçün bir çox yeni funksiyalar və alətlər əlavə olunmuşdur. İstifadə olunan konkret metodlar və alətlər verilənlər bazası sistemindən asılıdır, lakin əsas prinsiplər yenə də eynidir.Həssas məlumatları təhlükəsizləşdirmək üçün istifadə olunan bəzi data masking növləri aşağıdakılardır:

1. Statik Data Masking: Statik data masking proseslərin, verilənlər bazasının təmizlənmiş bir kopyasını yaratmağa kömək edir. Bu proses, bir verilənlər bazasının kopyasının təhlükəsiz şəkildə paylaşılabiləcəyi bir mühitin yaradılmasını təmin edir. Tipik olaraq, bu proses, istehsal üzrə verilənlər bazasının bir ehtiyat nüsxəsini yaradır, onu müstəqil bir mühitə yükləyir, lazımsız məlumatları ləğv edir və məlumatları mask etdikdən sonra data formasinda saxlamaq olur. Mask edilmiş kopya daha sonra istifadəçiyə göndərilə bilər.
2. Dinamik Data Masking: On-the-fly masking ilə oxşardır, ancaq məlumat ikinci bir verilənlər yaddaşında saxlanılmır, əksinə, data istehsal sistemindən axın şəklində göndərilir və dev/test mühitində başqa bir sistem tərəfindən istifadə edilir.

DYNAMİC DATA MASKİNG

Dynamic data masking (dinamik data masking), verilənlər bazasında məlumatların gizlilik səviyyəsini artırmaq üçün istifadə olunan bir data masking texnikasıdır. Bu texnika, istifadəçilərə məlumatları təxminən orijinal formasında göstərməyə imkan verərkən, məlumatların gizlilik səviyyəsini saxlamağa kömək edir.Dynamic data masking, əsasən bazanın sahibi və sistem administratorları kimi gündəlik idarəçilər tərəfindən tətbiq edilir. Bu, hassas məlumatların, məsələn, sosial təhlükəsizlik nömrələri, kredit kartı məlumatları, sağlamlıq reytinqləri kimi məlumatların təhlükəsiz bir şəkildə idarə olunmasına imkan verir.Dynamic data masking əməliyyatları məlumatların istifadəçilərə çıxışı zamanı gerçəkləşdirilir. Bu texnika vasitəsilə istifadəçilər yalnız tələb olunan məlumatları görə bilərlər, lakin gizlilik səviyyəsi ilə bağlı digər məlumatlar gizlədilir və ya pərdələnir. Məsələn, bir istifadəçi əsas məlumatları (ad, soyad) görə bilər, lakin digər məlumatlar (telefon nömrəsi, ünvan) yalnız sonlu sayılar və ya yalnız ilk hərflərlə göstərilir.

Dynamic data maskingin əsas faydaları aşağıdakılardır:

1. Hassas məlumatların təhlükəsizliyini təmin etmək: Dynamic data masking, hassas məlumatların təxminən orijinal formasını göstərərək məlumatların gizliliyini və təhlükəsizliyini qoruyur.
2. İstifadəçilərin əldə etdiyi məlumatların nəzarətli olunması: Məlumat sahibləri və idarəçilər, istifadəçilərin yalnız tələb olunan məlumatlara çatmağını təmin edərək məlumatların nəzarətli olunmasını və gizliliyin saxlanılmasını təmin edir.

CODE EXAMPLES

ADD MASK TO EXSISTED TABLE/COLUMN

ALTER TABLE [TableName]

ALTER COLUMN [ColumnName] ADD MASKED WITH (FUNCTION = '[MaskingFunctions]()');

REMOVE MASK FROM EXSISTED TABLE/COLUMN

ALTER TABLE Data.Membership

ALTER COLUMN LastName DROP MASKED;

CREATE MASKED TABLE

[TableName] [DataType] MASKED WITH (FUNCTION = '[MaskingFuction]()');

CREATE TEST USER AND EXECUTE QUERY

CREATE USER [UserName] WITHOUT LOGIN;

GRANT SELECT ON SCHEMA::[SchemeName] TO [UserName];

EXECUTE AS USER = '[UserName]';

SELECT \* FROM [TableName];

REVERT;

GRANT UNMASK FOR TEST USER

GRANT UNMASK TO [UserName]

EXECUTE AS USER = '[UserName]';

SELECT \* FROM [TableName] ([CoulmName]);

REVERT;

REVOKE UNMASK TO [UserName];

GRANT UNMASK FOR TEST USER ON SPECIFIC INFO

--Grant column level UNMASK permission to User

GRANT UNMASK ON [TableName]([ColumnName]) TO [UserName]

-- Grant table level UNMASK permission to User

GRANT UNMASK ON [TableName] TO [UserName]

-- Grant schema level UNMASK permission to User

GRANT UNMASK ON SCHEMA::[Schema] TO [UserName]

GRANT UNMASK ON SCHEMA::[Schema] TO [UserName]

--Grant database level UNMASK permission to User

GRANT UNMASK TO [UserName]

REVOKE UNMASKING FOR USER

REVOKE UNMASK ON [TableName] FROM [UserName];