T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EKLENTİLER KULLANARAK VERİ KAYBINI ENGELLEME

YÜKSEK LİSANS TEZİ

Hussein AL-SANABANI

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Yrd. Doç. Dr. Murat İSKEFİYELİ**

Aralık 2016

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EKLENTİLER KULLANARAK VERİ KAYBINI ENGELLEME

YÜKSEK LİSANS TEZİ

Hussein AL-SANABANI

Enstitü Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ

Bu tez .12.2016 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Doç. Dr.	**Doç. Dr.**	**Yrd. Doç. Dr.**
Resul KARA	**Ahmet ZENGİN**	**Murat İSKEFİYELİ**
Jüri Başkanı	**Üye**	**Üye**

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

HUSSEIN AL-SANABANI

Aralık.2016

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Yrd. Doç. Dr. Murat İSKEFİYELİ'ye teşekkürlerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

DLP	: Data Loss/Leakage Prevention/Protection, Veri kaybı ve sızma engelleme / koruma
CIA	: Confidentiality, Integrity and Availability of information security Bilgi güvenliğinin gizliliği, bütünlüğü ve kullanılabilirliği
GUB	: Güvenlik, Ulaşılabilirlik ve Bütünlük
DAR	: Data-at-rest, Kaynakta duran veri
DIM	: Data-in-motion,veri akarken
DIU	: Data-in-use, very kullanılırken
ISO	: International Organization for Standardization, Uluslararası Standardizasyon Organizasyonu
IEC	: International Electrotechnical Commission, Uluslararası elektroteknik komisyonu
DoS	: Denial of Service,Hizmet Reddi
RAID	: Redundant Array of Independent Disks, Yedekli Bağımsız Diskler Dizisi
IT	: Information Technology,Bilgi teknolojisi
USB	: Universal Serial Bus, Evrensel seri veriyolu
OS	: Operating System, İşletim Sistemi
ACLs	: Access Control Lists,Erişim kontrol listeleri
IDS	: Intrusion Detection System,Saldırı tespit sistemi
IPS	: Intrusion Prevention System,Saldırı önleme sistemi
MLS	: Multilevel Security,Çok düzeyli güvenlik
CIO	: Chief information officer,Bilişim kurulu başkanı
CISO	: A Chief Information Security Officer,Baş bilgi güvenliği sorumlusu
ILP	: Information Loss/Leakage Prevention/Protection,Bilgi

	Kayıp/Sızma Engelleme/Koruma
CMF	: Content Monitoring and Filtering, İçerik İzleme ve Filtreleme
CMP	: Content Monitoring and Protection, İçerik İzleme ve Koruma
CD	: Compact Disc, Kompakt Disk
DVD	: Digital Versatile Disc or Digital Video Disc, Dijital Çok Yönlü Disk veya Dijital Video Diski
HTTP	: Hypertext Transfer Protocol, Köprü metni transfer protokolü
FTP	: File Transfer Protocol,Dosya transfer protokolü
IP	: Internet Protocol, Internet Protokolü
SSN	: Social Security Number, Sosyal Güvenlik Numarası
NDDD	: Near Duplicate Document Detection, Yakın, yinelenen döküman algılama
CPU	: Central Processing Unit, Merkezi işlem birimi
EDRM	: Enterprise Digital Rights Management, Kurumsal Dijital Haklar Yönetimi
AES	: Advanced Encryption Standard, Gelişmiş Şifreleme Standartı
RC2	: Rivest Cipher 2, Rivest Şifreleme 2
TDES	: Triple Data Encryption Standard, 3'lü Veri şifreleme standartı
RC4	: Rivest Cipher 4, Rivest Şifreleme 4
DLL	: Dynamic-Link Library, Dinamik Link Kütüphanesi
RAM	: Random Access Memory, Rastgele Eririşim Belleği
XML	: eXtensible Markup Language, Genişletilebilir İşaretleme Dili

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler:Veri kaybı engelleme, veri sızma engelleme, Şifreleme, Erişim Kontrol, Eklenti.

Bir çok organizasyon için çalışanlar tarafından farkında olmayarak veri sızıntısı oluşması büyük bir problem oluşturmaktadır. Organizasyonlar veri gizliliğini sağlamak için gün geçtikçe veri kaybı/sızıntısı önleme (DLP-Data Loss/Leakage Prevention) çözümlerini daha fazla kullanmaktadır. Şu anda, DLP çözümleri gizli verileri ayırt etmekte zorluk çekmektedir. Ayrıca, kullanıcıların gizli verileri gizli olmayan verilerden ayırt etmelerine çok az izin vermektedir. Üstelik, organizasyon çalışanlarının çalışma alanları haricinde çalışmalarına sınırlar konulmaktadır.

Bu sorunu çözmek için, veri sahiplerinin dosyanın tüm yaşam döngüsü boyunca (oluşturma, düzenleme, vb.) dosyaların gizliliğini sınıflandırarak tanımlayabilecekleri bir DLP Eklentileri modeli sunmak önemlidir. Bu model, organizyon içinde çalışanlar tarafından sınıflandırılmış dosyaların kazayla sızmasını önlemek için veri şifreleme ve erişim kontrolü gibi güvenlik önlemlerini kullanır. Bu yaklaşım, doğru kullanıcının organizasyon içindeki veya dışındaki güvenlik erişim ayrıcalığına göre doğru dosyalara erişebileceğini garanti eder. Yani sınıflandırılmış dosyaları her zaman şifrelenmiş olarak tutmak, bu dosyaları; dinlenme, hareket halinde veya kullanırken koruyacaktır.

DLP-Eklentisi, kullanıcılara dosyaların şifrelenmesi veya şifresini çözmek için herhangi bir ek prosedür eklemek zorunluluğu olmadan dosyalara doğru bir şekilde erişebilmelerini garanti edmektedir. Kullanıcının normalde olduğu gibi tek yapması gereken dosyayı açmak ve kapatmaktır. DPL-Eklentileri ile veri kaybı önleme çözümünün uygulanmasına yönelik bu yaklaşım, verilerinin korunması için Microsoft Office, pdf okuyucular, metin editörü, medya oynatıcılar ve posta uygulamaları gibi yaygın ofis uygulamalarına rahatlıkla eklenebilir. Bu amaçla, DLP-Eklentileri modellerinden bir tanesini Microsoft office Word kelime işlemci uygulamasında gerçekleştirilmiştir.

DATA LOSS PREVENTION BASED ON PLUG-INS

SUMMARY

Keywords: Data Loss Prevention, Data Leakage Prevention, Encryption, Access Control, Plugin.

Inadvertent Data leakage by insiders is considered a serious problem to many organizations. Organizations are increasingly implementing Data Leakage/Loss Prevention solutions also know as (DLP), to protect the confidentiality of their data. Currently, DLP solutions have difficulties to identify confidential data as well lack the ability to allow users to distinguish confidential from non-confidential data. Moreover, they are limited to work outside the organizations.

In order to solve this problem, it is important to introduce a DLP-Plugins model where the data owners can identify the privacy of the files during their entire lifecycle (creating, editing, etc.) by classifying them. This model uses security measures such as data encryption and access control to prevent accidental leakage of the classified files by the insiders. This approach will guarantee that the right user will have access to the correct files according to their security access privilege inside or outside the organization. By always keeping classified files encrypted this will protect them all the time and everywhere i.e. at rest, in motion, and in use.

The DLP-Plugin shall guarantee the usability for the users, so that they will be able to have the right access to the files, just in case they don't need to enforce any additional procedures to encrypt or decrypt the file. All that will be required is to simply open and close the file as they do normally. This approach to implementing data shrinkage and loss prevention solution with DPL-Plugins, can be added into the legacy applications like Microsoft Office, pdf readers, text editor, media players, and mail applications to protect their data. As an example to this DLP-Plugins model, we have built a DLP-Plugin for Microsoft office Word.

BÖLÜM 1. GİRİŞ

1.1. Geçmiş

Sayısal formdaki verilerin günümüzde kuruluşlara girip çıkma oranı çok yüksektir. Günlük olarak, tipik bir kuruluş milyonlarca e-posta mesajı gönderebilir veya alabilir, çeşitli kanallar vasıtasıyla bir kuruluş yüzlerce hatta binlerce dosyayı kaydeder ve aktarır [1]. Müşteriler, iş ortakları, yöneticiler ve hissedarlar, işletmelerin sahip oldukları hassas verilerin korunmasını beklemektedir [1]. Kurumsal veriler bir işletmenin sahip olduğu en önemli varlıklardan biridir; bu nedenle bu verilerin korunmasına büyük önem verilmelidir [2].

Veri sızıntısı, bilgi güvenliğinde istenmeyen bilgi yayılmasını işaret eder [3]. Kasıtlı veya kasıtsız olarak özel ve hasssas verileri yetkisiz kişilerle paylaşmak en ciddi güvenlik konularından biridir [4], [5]. Sızdırılmış veriler, müşteri sadakatinin ve çalışanların güveninin kaybolmasına bu durum da rekabet avantajının kaybedilmesi, siyasi krizler ve şirketin kapatılması da dahil olmak üzere bir çok zarar verebilir [2], [5].

Symantec'in yaptığı araştırmaya göre 2013'te 253 büyük kurumsal olan veri ihlali 2014'te 312 ve 2015'te 318'e ulaşmıştır. Ancak, bu ihlallere maruz kalan kişi sayısı 2013'te 552 milyon, 2014'te 348 milyon ve 2015'te 429 milyon olarak gerçekleşmiştir. Yani bu kadar kişinin kişisel bilgileri sızdırılmıştır [6]. Risk Based Security'e göre, bildirilen veri ihlalleri vakaları 2015 boyunca toplam 3.930'a ulaştı ve 736 milyondan fazla kayıt yapıldı [7]. Örnek olarak Sony firmasının Sony Playstation kullanıcılarının 77 milyon hesap bilgisi çalınmıştır ve tahminen çalınan bu bilgiler içerisinde kullanıcıların kart bilgileride bulunmaktadır [8]. Global Information Security 2015 durum raporuna göre 2014'teki veri ihlalleri 2013'e göre 38% artarak 42.8 milyona ulaşmıştır. Bu tarz olayların en büyük suçluları çalışanlar

olarak geçmektedir. Daha çok 2014 yılında, eski çalışanlar arasında veri ihlali önceki senelere göre 30%'luk artış gösterirken, mevcut çalışanlar arasında 35%'lik bir artış göstermiştir [9]. US State of Cybercrime Survey'in yaptığı ankete göre katılımcıların 32%'si içeriden gelen saldırıların dışarıdan gelen saldırılara göre daha maliyetli ve zararlı olduğunu söylemiştir [10].

Bu durum her türlü organizasyonda veri sızıntı problemini ortaya koymakta ve dolayısıyla bu problemin çözülmesi gerektiğini göstermektedir. Çözmeye yönelik ilk adım ise organizasyonların sahip oldukları verilerin gizli olduğunu anlamalı, bu verilerin nasıl yönetileceği ve yetkisiz erişimden nasıl korunacağını çözümlemesi gerekir [1]. Sonuç olarak, bu problem çözmek için çeşitli DLP çözümleri geliştirilmiştir.

1.2. Hedef

Geçerli DLP çözümlerinin çoğunda, içerik-tabanlı (kurallı ifadeler, anahtar kelimeler eşleştirme, belge parmak izi, istatistiksel analiz, vb.) veya bağlam-tabanlı (dosya türü/boyutu, gönderen, üstbilgi/meta-veri bilgisi, kaynak, hedef, vb.) denetimlerini kullanarak hassas verileri tanımlamak zordur. Çünkü hassas verilerin otomatik olarak tanımlanması güç bir durumdur ve ayrıca tüm bu teknikler çeşitli dosya türlerini ayrıştırma kabiliyetine ihtiyaç duyar. Buna ek olarak, sıkıştırılmış, şifrelenmiş veya üzerinde çok değişiklik yapıldıysa gizli verileri tanımlayamazlar [2], [11]. Dahası, DLP çözümleri, çalışanların hassas veriyi tanımlamalarına izin verme yeteneğine sahip değildir. Halbuki çalışanlar bu verinin hassaslığını ve içeriğini en iyi bilenlerdir. Çünkü bu veriyi oluşturan kişilerdir. Bununla birlikte, DLP çözümleri, çalışanları sadece kurum içinde çalışmaya zorlar.

Bu tarz problemleri çözmek için, bu çalışma Microsoft Office, pdf okuyucular, metin editörü, medya oynatıcılar ve posta gibi yaygın uygulamalara eklenecek bir DLP eklentisi modeli sunmaktadır. Bu model, verilerin içerdikleri içerik konusunda en bilgili olan veri sahiplerinin, verilerin gizliliğini tanımlamalarına imkan verir. Gizli veriler şifreleme ile her zaman korunacağından, dosyanın şifrelenmiş olması,

sıkıştırılmış olması veya üzerinde değişiklik yapılmış olması önemli değildir. Bununla birlikte, sınıflandırılmış (korunan) verilerin değiştirilmesi (düzenlenmesi) gerektiğinde, düz metin verileri kuruluşun içinde veya dışında bulunan yetkili bilgisayarlardaki yetkili kullanıcılar tarafından kullanılabilir. Bu, kuruluşun iş yeri olanaklarını genişletirken, verilerin güvenliğini garanti altına alıp kullanıcı uğraşını azaltarak daha fazla esneklik sağlayacaktır. Bunu ispatlamak için, DLP-Eklentileri modeline örnek olarak Microsoft Office Word kelime işlemcisi için bir DLP-Plugin tasarlanmış ve gerçekleştirilmiştir.

1.3. Motivasyon

CIA'in bilgi güvenliği üçlüsü gizlilik, bütünlük ve erişilebilirlik anlamına gelmektedir [12].Bu üçlü arasından tartışmamızı sadece gizlilik konusunda sınırlandırıyoruz. Tanım gereği, genellikle bilgi gizliliği, hassas bilgilerin yalnızca yetkili kullanıcılar tarafından erişildiği güvencesidir [13]. Bu görev cihaz kontrolü, şifreleme ve erişim kontrolü gibi çeşitli mekanizmalarla sağlanabilir. Kötü niyetli kurum içi çalışanlardan ve dışarıdan gelen saldırılara karşı çok miktarda kişisel veriyi güvence altına almak için bu basit önlemler kullanılmıştır [4]. Bununla birlikte, veri sızıntısını engellemenin en kolay yolu Alneyadi ve arkadaşlarına göre [3] güvenlik ilkesine ve erişim haklarına (erişim denetimi) dayanan DLP çözümü kullanılmaktadır. Çünkü bunlar, yeterince uzun süredir kullanılmakta ve iyi kurulmuş temelleri izlemektedir. Tüm bunlar, verilerin gizliliğini korumak için DLP-Eklentileri modelinde şifreleme ve erişim denetimini kullanmaya odaklanmamıza neden olmaktadır.

Websens'deki stratejik veri güvenliği çözümleri direktörü [14], [15] Lior Arbel "veri sınıflandırmak en önemli anahtar yollardan biridir DLP çözümleride bunu kullanır, bu yöntemle hangi verilerin yüksek güvenlik seviyelerine ihtiyacı var hangilerinin yok belirlenir. Ayrıca, verileri korumak için öncelikle verileri sınıflandırmak ve daha sonra bu verileri keşfetmek gerekir." demektedir. Buna dayanarak DLP-Eklentileri modelimiz, verilerin oluşturulduğu zamandan veya yaşam döngüsünün herhangi bir noktasından sınıflandırılmasına dayanır.

Iron Mountain'daki bilgi riski sorumlusu Christian Toon, etkin bir DLP uygulamasının gerçekleştirilebilmesi için insan unsurunun göz ardı edilmemesi gerektiğini vurguluyor:"Veri kaybı önleme teknolojileri eğer kullanıcılar onları kullanırsa etkili bir çözüm olabilir" demektedir [15]. Bu sebeple, hassas verilerin sınıflandırma sürecini yetkili kullanıcılara (veri sahiplerine) atanmıştır.

Bununla birlikte, bir kurum kontrol mekanizmalarını kullanarak yani onları izleyerek ve gözetleyerek çalışanlarını yönetmeliklerine uymaya zorlayabilir. Fakat bu yaklaşımın, Edward Snowden'ın vakaları gibi birçok davada etkisiz olduğu kanıtlanmıştır [16], [17]. Ayrıca, çok kısıtlayıcı ortamlarda, bazen çalışanlar günlük işleri yapmayı rahatsız edici ve sinir bozucu bulmakta, bundan dolayı da çalışanlar alternatif yollar aramaya başlamaktadır. Dolayısıyla, kurumlar, çalışanlarına güvenmeli ve işbirliği yapmalıdır. Çünkü veri sızıntısını önlemek için tam başarılı olan bir yöntem bulunmamaktadır [16]. Başka bir deyişle, kullanıcıların bir bitlik veri sızdırmasını önleyebilecek bir DLP sistemi olsa dahi; bu sistemlerde, çalışanların aklında tuttuğu bilgileri engellemeye dair herhangi bir kontrolü yoktur. Dolayısıyla bu sistem, kullanıcıların verileri sızdırmasını asla engelleyemez. Yani kasıtlı veri sızıntısını önlemenin zor olduğu anlamına gelir ki; bu nedenle de yöntemimiz yalnızca istem dışı (kazara) veri sızıntısına odaklanmıştır.

1.4. Benzer Çalışmalar

Son yapılan incelemelerde [4], veri kaybının önlenmesine ilişkin araştırmalarda büyük bir artış olduğu görülmektedir. Veri sızıntısı ne, nerede ve nasıl korunacağına göre mevcut DLP çözümleri tarafından ele alınmiştir. Korunacak veriler olarak üç açamadaki kaynakta duran verilere (DAR-data-at-rest), hareket halindeki verilere (DIM-data-in-motion) ve kullanımdaki verilere (DIU-data-in-use) odaklanılmıştır. Korunacak yer olarak uc nokta ve merkez olarak ikiye ayrılabilir. Korunma metodu olarak sızıntıyı önleme yaklaşımları tanımlanmıştır [4].

Bir bilgisayar sisteminde gizli bilginin bir dosya sisteminde dolaşırken izlenmesine dayanan veri sızıntısı koruması (DLP) için bu [18] referansta bir teknik açıklanmıştır. Bu tekniğin temelindeki düşünce gizli olan kaynaktan gizli olmayan kaynağa aktarılan herhangi bir aktarım hedefteki güvenlik seviyesini kaynaktaki güvenlik seviyesine çıkarmaya dayanır. Bu nedenle sistem gizli bilgi sızıntılarını engellemek için tüm gizli dosyalara etiket vererek gizli bilgileri ayırt edebilir. Bazı çalışmalarda [3], [4], [19], [20] içerik etiketinden söz edilmektedir. Bu teknik, gizli dosyaları tanımlamak için etiket kullanır ve atanan etikete göre kurumsal politikalar uygular. Etiket atandıktan sonra dosya taşınsa da, kopyalansa da, farklı yada aynı tip bir dosyaya eklense de, dosya formatı değiştirilse de, içerikte büyük bir değişiklik olsa da, şifrelense de veya sıkıştırılsa da etiket kendini korur. Etiketler dosyalara; manuel olarak gizli verilerin yazarı tarafından veya otomatik olarak DLP çözümü tarafından olmak üzere iki yöntemle atanabilir. Bu teknik, dosyanın gizliliğini tanıyabilir, ancak içerdiği verilerin gizliliğini tanımaz [3].

İçerik etiketleme tekniği metodolojimize en yakın olanıdır. Çünkü gizli verilerin sınıflandırılmasını (etiketleme) dikkate almaktadır. Çalışmalarımızı farklı kılan özellik; veri sahiplerinin, hassas verileri oluşturma zamanında veya değişiklik sırasında sınıflandırarak tanımlamasıdır. Ayrıca bu gizli veriler baştdan itibaren şifrelenerek korunacak ve daima şifrelenmiş olarak kalacaktır.

Wu ve arkadaşları [5] tarafından önerilen etkin bir DLP modeli, bir dosyanın oluşturulduktan ve kaydedildikten sonra gizliliğini ve hassaslığını kontrol etmesinin aksine, kullanıcı yazarken verilerin gizliliğini ve hassaslığını izleyebilir. Bir diğer çalışmalarda [21], [22] veri sızıntısını görüntü ve ses dosyalarını kullanarak tespit etmeyi tartışır. Bu sistemin amacı, dağıtıcının (veri sahibi) hangi verileri sızdırdığını bulmak ve sızdırılmışsa; bu verileri sızdıranı (güvenilir taraf) tespit etmektir. Veri odaklı kullanım kontrol konsepti temel alınarak, Microsoft Windows işletim sistemlerinde veri kaybını önlemek için detaylı kurallarla koruma sağlamaktadırr [11].

Genel olarak; çalışmalarımızın DLP çözümlerinden farkı çözümümüzün bağımlı bir çözüm olmasıdır. Bazı uygulamaların dosyalarını korumak için hazırlanmış bir eklenti modelidir. Bu eklentiler, yanlışlıkla ortaya çıkabilecek veri sızıntılarını önlemek için veri şifreleme ve erişim kontrolü gibi uygun önleyici tedbirleri alarak olası sızıntıları oluşmadan önleyecektir. Üstelik, DLP-Eklentileri modeli hassas veriyi ayırt etmek için insan faktörünün rolüne güvenirken sadece kasıtsız (kazara) veri sızıntısına odaklanmıştır.

1.5. İşin Yapısı

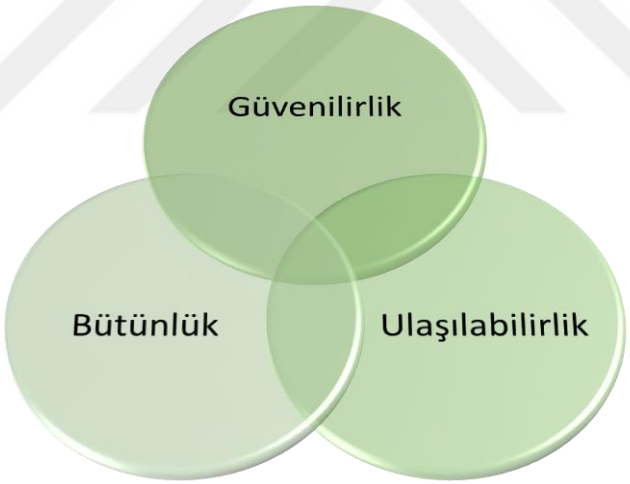
Bu tez aşağıdaki bölümlerde düzenlenmiştir::

- BÖLÜM 2: Veri güvenliği hakkında genel bilgi verir ve ardından veri kaybı/sızıntısı, veri sızıntısı türlerini ve bunları sırasıyla güncel teknolojileri kullanarak nasıl çözülebileceğini tanımlar.
- BÖLÜM 3: Veri kaybı/sızıntısını çözmenin yolları, DLP'nin veri sızıntısını gidermek için kullandığı yöntemler, DLP'nin bileşenleri ve son olarak piyasadaki DLP ürünlerinin türleri anlatmaktadır.
- BÖLÜM 4: Önerilen modeli, DLP-Eklentileri modeli tarafından kullanılan sınıflandırma yöntemini, DLP-Eklentileri bileşenlerini ve bu modelin nasıl çalıştığını açıklar.
- BÖLÜM 5: DLP-Eklentileri modelinin Performans sonuçlarını tartışır.
- BÖLÜM 6: Sonuçlar ve öneriler sunulmuştur.

BÖLÜM 2. VERİ GÜVENLİĞİ

2.1. Giriş

Veri güvenliği açısından öncelikler; güvenilirlik, ulaşılabilirlik ve bütünlüktür olarak sınıflandırılabilir. Diğer bir ismi ile Şekil 2.1.'de görüldüğü üzere GUB (Güvenilirlik, Ulaşılabilirlik ve Bütünlük) üçlüğüdür. GUB üçlüğü bize herhangi bir organizasyonda [23] veri güvenliğine odaklanmamız için bir model verir. GUB tanımlamaları ISO/IEC 1335-1:2004 standartları tarafından verilmiştir.



Şekil 2.1. GUB üçlüğü.

2.1.1. Güvenilirlik

Bilgi özelliği, yetkisiz kişilere, varlıklara veya süreçlere açık veya ulaşılabilir değildir. Verilere yetkisiz erişimin veya halka açıklığın gizliliğin kaybolmasına yol açabileceği anlamına gelir. Başka bir deyişle, gizlilik kaybı veri sızıntısıyla

gerçekleşebilir. Bunu önlemek için, şifreleme ve erişim kontrolü gibi çeşitli mekanizmaları kullanılabilir.

2.1.2. Bütünlük

Bütünlük özelliği, verilerimizin veya bölümlerinin yetkisiz olarak değiştirilmesi veya silinmesi ile veri bütünlüğünün bozulması anlamına gelir. Verilerimiz için yetkili ancak istenmeyen bir değişiklik veya silme, bütünlük kaybına neden olabilir. Verilerimizin bütünlüğünü sağlamak ve korumak için sayısal imza ve mesaj doğrulama kodu gibi çeşitli mekanizmalar kullanılabilir.

2.1.3. Ulaşılabilirlik

Yetkili bir kuruluş tarafından talep edilmesi halinde erişilebilir ve kullanılabilir niteliktir.

Bu, herhangi bir güç kaybı, hizmet reddi (DoS-Denial of Service) saldırısı, işletim sistemi veya uygulama sorunları, ağ saldırıları ve sistem hatası veya sistemin kullanılamamasına neden olan herhangi bir olayın kullanılabilirliğin kaybolmasına yol açabileceği anlamına gelir. Erişim genellikle çeşitli bağımsız güç kaynaklarının kullanımı, dağıtılmış sistem ve çoklu iletişim hatları gibi birçok mekanizma ile sağlanır.

2.2. Veri Kaybı / Sızıntısı

Veri güvenliği çalışmalarında; veri kaybı, verileri depolayan herhangi bir cihazda oluşabilir. Bu bilgisayar kullanan herkes için bir sorundur. Verilerin fiziksel veya mantıksal olarak kasıtlı olarak veya istemeden gönderildiğinde oluşur. Veri kaybı bugün kurumlarda ciddi bir sorun haline gelmiştir ve kurumler bu sorunun üstesinden gelmekle yükümlüdürler [24]. Bu sorun, veri kurtarma yazılımını kullanarak ve yedekli bağımsız diskler dizisi (RAID-Redundant Array of Independent Disks) teknolojilerini kullanan farklı bir yerde yedekleme saklama yaparak ele alınabilir.

Buna karşın, veri sızması, yetkili olmayan bir kişi tarafından bilinçli olarak veya yanlışlıkla yapılan gizli bilgilerin ifşa edilmesidir. Sızdırılan veriler, özel olabilir ve gizli olarak kabul edilirken, veri kaybı ise silme, sistem çökmesi vb. nedenlerle oluşur. Veri kaybı ve veri sızıntısı, veri ihlali olarak adlandırılabilir ve bunlardan birinin oluşması durumunda meydana gelir. Şirket ve kurumların bugün karşılaştığı en büyük korkulardan biridir [24].

Genel olarak, veri kaybı terimi; verilerin sızdırılması, kaybolması veya verilerin zarar görmesi anlamına gelir. Bu çalışmada, veri kaybı ve veri sızıntısı terimleri, hassas verilere yetkisiz erişime veya bilinçli/bilinçsız olarak (kasıtlı/kazara) duyarlı verilerin istenmeyen şekilde ifşa edilmesine işaret etmek için kullanılmaktadır.

Veri sızıntısı gizlilik için büyük bir tehdit haline gelmiştir ve son birkaç yıldır (IT-Information Technology) yöneticilerinin gündeminin en tepesinde yer almıştır. Veri sızıntısı sonucunda, bilgileri okuma, değiştirme iznine sahip olmayanların erişimi olabilir. Bilgisayar güvenlik uzmanlarının veri sızıntısını önlemek için gösterdikleri büyük çabalara rağmen, sorun halâ var olup, kuruluşlarda halâ tartışılan en önemli konudur.

Bilgi güvenliğine, saldırganlar ve kuruluşlar arasındaki bir rekabet olarak bakılabilir. Kuruluşlar, erişim kontrol mekanizmaları, güvenlik duvarları virüs tarayıcıları vb. sayaç önlemleri kullanarak bilgi varlıklarını korumaktadırlar. Ancak saldırganlar yetkisiz yollarla kurumun bilgi varlıklarına erişerek veri sızıntı sorununa yol açıyor. kurumlerde insan davranışları veri sızıntısı aracı olarak gösterildiğinden, bu davranışı engelleyen güvenlik ilkeleri uygulanmalıdır. Örneğin, kredi kartı bilgileri, kişisel finans, vergi bilgileri, hasta kayıtları vb. veriler bugünlerde çok kritik konumdadır. Daha fazla kullanıcı, daha önce hiç olmadığı kadar çok bilgiyi elektronik ortamda depolamaktadır. Kuruluşların bu hassas verilere uygun kontrol sağlamaması veri sızıntısına neden olmuş ve bunlar üzerinde büyük etkileri olmuştur. Bilgisayar güvenlik perspektifinden bakıldığında, veri sızıntısı gizlilik kaybıdır.

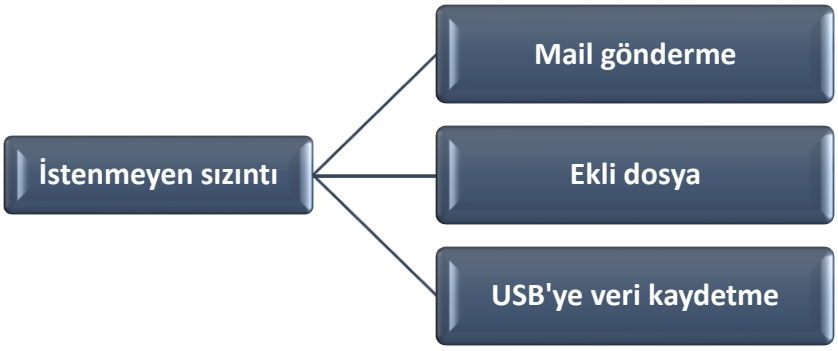
2.3. Veri Sızıntısı Türleri

Bir veri kurtarma sistemi, dahili sistemlerin ve verilerin çoğuna zaten erişimi olan bir şirketin ve diğer meşru kullanıcı personeline karşı koruma sağlamak üzere tasarlanmıştır. Kullanıcıların, sistemin koruma ve savunmalarının çoğunu geçmeleri meşrudur, çünkü bu kişilerin işlerini verimli bir şekilde yapmaları için buna ihtiyaç duyulur [4].

Tüm personel, şirketin verilerini sızdırmak istememesine rağmen istemeden sızdırdıkları birçok durum mevcuttur. Şirketin içinden gelebilecek veri sızıntısı; istenmeyen sızıntı, kötü niyetli olmayan kasti sızıntı, kötü niyetli kasti sızıntı olmak üzere üç başlıkta sınıflandırılabilir.

2.3.1. İstenmeyen sızıntı

Kasıtsız sızıntı, kötü niyeti olmayan sıradan bir kullanıcının, şirket politikasının farkında olup olmadığına bakılmaksızın, yanlışlıkla kuruluşun gizli verilerini sızdırdığı durumdur.



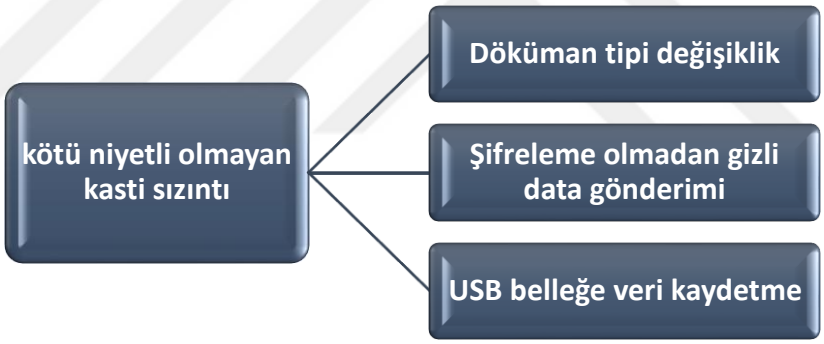
Şekil 2.2. İstenmeyen sızıntı.

Şekil 2.2.'de İstemeden sızıntıya neden olmanın olası yollarını gösterir. Kasıtsız sızıntı gerçekleştikten sonra fark edilebilir, ancak durdurmak veya geri almak için olası bir yol yoktur [25]. Örneğin, bir çalışan yanlışlıkla istenmeyen bir alıcıya veya rakibe bir yazım hatası nedeniyle bir belge ekleyen bir e-posta gönderirse bu geri

alınamaz. Buna karşın, kullanıcı kendi eylemlerinin veri sızıntısına neden olabileceğini bilmediğinde birçok durum ortaya çıkmaktadır. Örneğin, herhangi bir veri depolama alanındaki standart komutları kullanarak silinen dosyalar kolaylıkla kurtarılabilir ancak çoğu kişi bunu bilmiyor. Yanlışlıkla bir (USB-Universal Serial Bus) belleğe kopyalanan bir dosya, kullanıcıların hatasını fark ettiğinde ve yanlış araçları kullanarak sildiyse bile sızıntıya neden olabilir. Bunu yaparak, kullanıcı gerçekleşebilecek olası bir sızıntı olduğunu bilmeden doğru şekilde hareket ettiğini düşünür [25].

2.3.2. Kötü niyetli olmayan kasti sızıntı

Kasıtlı sızıntı; kasıtlı olarak ya da bilinçli olarak kötü niyeti olmayan sıradan bir kullanıcı olduğunda, kullanıcının şirket politikasının farkında olup olmadığına bakmaksızın gizli verileri sızdırdığı durumlarda ortaya çıkar.

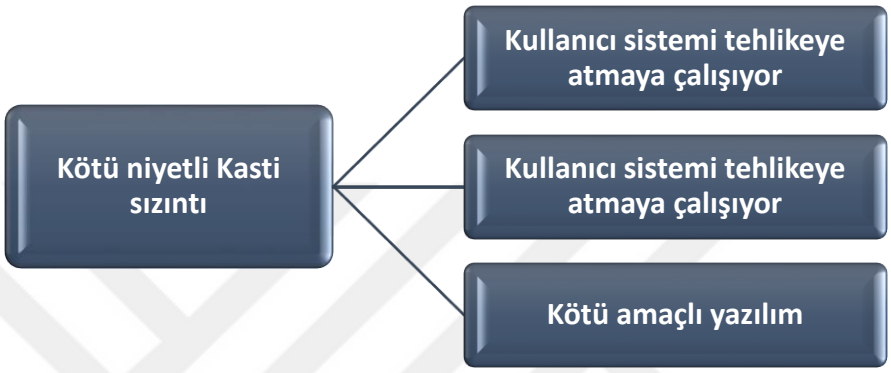


Şekil 2.3. Kasti Sızıntı (Kötü niyet olmadan).

Şekil 2.3.'te kötü amaçlı bir niyet olmadan kasten sızıntıya neden olmanın muhtemel yolunu gösterir. Bu genellikle iki durumda olur; Birincisi, kullanıcı güvenlik kurallarını atlar ve şirket politikasından haberdar edilmez. Örneğin bir kullanıcı, kişisel dizüstü bilgisayarına, kuruluştaki yönetmelik ve politikalara aykırı olduğunun hiçbir bilgisi olmaksızın evde çalışmak için bazı gizli belgeler göndermeye çalışıyor. İkincisi, kullanıcı güvenlik kurallarını ve düzenlemelerini atladığında ve şirket politikasının farkında olduğu halde organizasyon politikasına uyma ihmalinden dolayı. Örneğin, şirket gizli verileri yalnızca şifrelenerek dış iş ortaklarına gönderilmesi gerektiği yönünde bir politika varsa, aceleyle bir kullanıcı şifrelemeksizin gönderebilir.

2.3.3. Kötü niyetli Kasti sızıntı

Kasıtlı kaçak, kasıtlı olarak kişiye özel fayda sağlamak veya kuruluşa zarar vermek amacıyla kurumun gizli verilerini dışa veya bir rakibe sızdıran kötü niyetli kayıtsız kullanıcılar, saldırganlar veya zararlı yazılımlardan kaynaklanmaktadır.



Şekil 2.4. Kasti sızıntı (kötü amaçla).

Şekil 2.4.'te zararlı sızıntıya neden olmanın olası yollarını göstermektedir. Zararlı sızıntı genellikle bir kullanıcı güvenlik kurallarını ve yönetmeliklerini kasıtlı olarak atlar ve gizli verileri sızdırmaya çalışırsa oluşur. Kötü niyetli kaçaklar çok nadirdir [26]. Bu sızıntının bir örneği, bir çalışan, kişisel fayda sağlamak için kurumsal sistemden e-posta yoluyla gizli veriyi rakibe gönderdiği zaman oluşur [24].

Saldırganlar ve zararlı yazılımlar hala organizasyon için ciddi bir sorundur, çünkü gizli verileri ifşa ederek organizasyona büyük zarar verebilirler. Zararlı yazılımların çoğu, çevrimiçi bankacılık hesapları, kredi kartı, şifre vb. gibi hassas bilgileri toplamak üzere dağılımdadır.

2.4. Veri Sızıntısının Ele Alınması

Verilerin sızdırılmasıyla ortaya çıkan gizlilik kaybı, bilgi güvenliği alanında ortak bir sorundur. Bu ciddi sorunun üstesinden gelmek için, gizliliğin kaybedilmesine karşı geliştirilen birçok teknoloji vardır ve bunların çoğu sızıntıyı önlemek için

kuruluşlarda kullanılmaktadır. Bu teknolojileri ikiye bölebiliriz. İlki, dışarıdan gelen tehditlerin neden olduğu gizli verilerin sızmasını önlemeye odaklanırken, ikincisi, gizli verilerin iç tehditlerden sızmasını önlemeye odaklanmaktadır.

2.4.1. Dışarıdan veri sızması

Kuruluşları dışarıdan gelen tehditlere karşı korumak için standartlar olarak çeşitli teknolojiler kullanılmaktadır. Bu güvenlik standartları çok güçlü ve kullanışlı olsa da, yalnızca dışarıdan gelen saldırılara karşı yardımcı olabilirler [24]. Bu güvenlik ihlallerini önlemek için şu anda kullanılan bazı teknolojileri tartışacağız.

2.4.1.1. Kötü amaçlı yazılımdan koruma uygulamalar

Kötü amaçlı yazılım, bilgisayarın düzgün çalışmasını kesmek için tasarlanmış, bazen hassas bilgileri toplayan ve uzaktaki bilgisayar sistemlerine yetkisiz erişmek için kullanılan anahtar kaydediciler, casus yazılımlar, virüsler, Truva atları, solucanlar, reklam yazılımları veya arka kapılar gibi davranabilen bir yazılımdır.

Kötü amaçlı yazılımdan koruma yazılımı, bilgi işlem cihazlarını ve IT sistemlerini çeşitli kötü amaçlı yazılım (malware) türünden korumak için kullanılan bir yazılımdır [27]. Kötü amaçlı yazılımdan arındırma, işletim sisteminin (OS-Operating System) çekirdeğini veya çekirdek işlevlerini her eylemi kontrol etmek için kontrol eder ve sonra işletim sisteminin onaylanan eylemi yürütmesine izin verir veya işletim sisteminin onaylanmamış eylemi yürütmesini engeller. Başka bir deyişle; kötü amaçlı yazılım karşıtı uygulama, sistemin düzgün çalışmasını kesmesini engellemek içindir.

Kötü amaçlı yazılımlar, tarama yaparak ve imza doğrulamasının dışardan gelen tehditlere ait olmadığını kontrol ederek çalışır. Bu gerçek zamanlı ortamda çok iyi çalışır ve etkili bir şekilde zararlı yazılımları ortadan kaldırır, ancak içerideki tehditler için kötü amaçlı yazılımdan koruma uygulama (anti-malware)'in bunları işleme mekanizması yoktur.

2.4.1.2. Güvenlik duvarı

Güvenlik duvarı, önceden belirlenmiş bir kurallar dizisine [28] dayanarak gelen ve giden ağ trafiğini izleyen ve denetleyen, donanım tabanlı veya yazılım tabanlı bir ağ güvenlik sistemidir.

Ağlar, yasal iletişimlerin geçersiz kılınmasına ve yasadışı iletişimi engellemesine izin vererek, güvenlik duvarları yetkisiz erişime karşı korumaktadır. Gelen ve giden veri paketleri, güvenlik duvarından geçmesine izin verilip verilmediğini belirlemek için analiz edilir. Kuruluşlarda farklı ağ katmanlarında farklı güvenlik duvarları türleri uygulanmaktadır. Güvenlik Duvarı normalde kuruluşun ilk savunma hattıdır. Güvenli iç ağ ve güvensiz dış ağ arasındaki ayırıcı veya köprü işlevi görür. Güvenlik duvarları, genellikle (ACL-Access Control Lists)'ler olarak kısaltılan erişim kontrol listeleri gibi çalışır. ACL'ler ile olan sorun, veri paketlerinin güvenlik duvarı üzerinden geçmesine izin vermeye tamamen izin vermeleri veya reddetmeleridir. Örneğin, bir kural, belirli bir bağlantı noktasından geçen tüm giden trafiği reddetmek üzere ayarlanmışsa, bu bağlantıyı geçmek istediğiniz meşru trafik olduğunda bile, bu bağlantıyı geçen tüm bu trafiği engelleyecektir.

2.4.1.3. Saldırı tespit ve önleme sistemi

Saldırı Tespit Sistemi (IDS-Intrusion Detection System), kötü amaçlı veya şüpheli etkinlikler veya politika ihlalleri için ağ ve/veya sistem faaliyetlerini izleyen ve bir yönetim istasyonuna raporlar üreten bir cihaz veya yazılım uygulamasıdır. Saldırı tespit sistemleri öncelikli olarak olası olayların belirlenmesi, bunlar hakkında bilgilerin günlüğe kaydedilmesi ve denemelerin raporlanmasına odaklanır (örn: sinyal yoluyla uyarı verir) [29]. IDS hem bir saldırıları (organizasyonun dışından saldırılar) hem de kötüye kullanımı (organizasyon içerisindeki saldırılar) içeren olası güvenlik ihlallerini belirlemek için bir bilgisayar veya ağ içindeki çeşitli alanlardan gelen bilgileri toplar ve analiz eder [30].

Öte yandan, Saldırı önleme sistemleri (IPS-Intrusion Prevention System), ağ ve/veya sistem faaliyetlerini kötü niyetli veya şüpheli etkinlik veya politika ihlalleri için izleyen, bu etkinlikle ilgili bilgileri günlüğe kaydeden, bunları engellemek/durdurmak ve rapor etmek için kullanılan ağ güvenlik araçlarından oluşur. Saldırı önleme sistemleri, saldırı tespiti sistemlerinin uzantılarıdır, çünkü hem ağ trafiğini ve/veya kötü amaçlı etkinlik için sistem etkinliklerini izler ve bunu aktif olarak önlemeye çalışırlar. Bunu başarmak için IPS özellikle alarm gönderme, kötü niyetli paketleri bırakma, bağlantıyı sıfırlama ve/veya rahatsız edici IP adresinden trafiği engelleme gibi eylemler gerçekleştirebilir [29].

IDS/IPS'ler, güvenlik politikaları ile ilgili sorunları tanımlamak ve kişileri bu güvenlik politikalarını ihlal etmekten alıkoymak için kullanılabilir. Ancak, olası tehditleri belirlemek ve yalnızca bayrak/uyarıları izlemek veya algılanan saldırıları engellemek ve izlemek için veri kaybını önleyemezler.

2.4.2. İçeriden veri sızması

Dışarıdan veri sızması bölümünde bahsedilen teknolojilere kıyasla, bir kurumun içinden gelen tehditleri önleyici bir takım metod ve teknolojiler mevcuttur. Aşağıda içeriden gelen veri sızdırılmasına odaklanan bazı yaklaşımlardan bahsedilecektir.

2.4.2.1. Çok seviyeli güvenlik

Çok düzeyli güvenlik (MLS-Multilevel Security) modelleri, bilgiyi yalnızca gerekli izin düzeyine sahip kullanıcıların verilere erişebilecek şekilde farklı seviyelerde sınıflandırmanın bir yoludur [31]. MLS sistemlerinin ilk kullanımı, yetmişli yıllarda askeri sistemlerde paylaşılan bilginin gizliliğini desteklemek olmuştur [32].

MLS'nin askeri ortamları desteklemek için en eski haline getirilmesi Bell-LaPadula (BLP) modeliydi [33]. BLP modeli erişim kontrol politikasına bağlıydı. Bu modelde, her konu ve nesneye bir güvenlik düzeyi (etiket) atanır. Atanmış düzeyleri / etiketleri kullanarak, verilere yetkisiz erişimin engellenmesine aynı zamanda daha ayrıntılı

erişim denetimlerinin uygulanmasına izin verir. Düzeyler; dosyalar ve işlemler için Sınıflandırılmamış, Özel, Gizli ve Çok Gizli olarak sınıflandırılmıştır [32]. Bu güvenlik izinlerine dayanarak, her erişim kontrol edilir ve BLP modeli verilip verilmeyeceğine karar verir. Erişim kontrolü için iki zorunlu kurala dayanan BLP modeli:

a. Yukarıya okunamaz: Bir özne, nesnenin boşluk seviyesi ile aynı veya daha yüksekse, yalnızca nesneyi okuyabilir.
b. Aşağıya yazılamaz: Bir özne, boşluk seviyesi daha düşük veya nesnenin boşluk seviyesi ile aynıysa, bir nesneye yazabilir.

İlk kural, herhangi bir işlemin bilgiyi daha yüksek bir güvenlik düzeyinden okuyamadığı iken ikincisi hiçbir işlem daha düşük bir güvenlik düzeyine bilgi yazamayacağı anlamına gelir. Bu nedenle, hiçbir kullanıcı belgelerin güvenlik düzeyini düşürmeyi başaramaz ve bu veri sızıntısını önler. Böylece verilerin gizliliği garanti edilir. Örneğin; bir belgede güvenlik seviyesi gizli olan bir kullanıcının gizli seviyeyle kaydetmesine izin verilmiyor, çünkü gizli düzeyde olan kullanıcılar bu belgeyi okuyabilir, bu da gizliliğin ihlali anlamına gelir ve veri sızıntılarına neden olur. Şekil 2.5.'te MLS sistemindeki veri akışını göstermektedir.

Şekil 2.5. Bir MLS sisteminin güncel veri akışı [34].

2.4.2.2. Gruplar ve roller

Büyük organizasyonlarda, çoğu personel çoğunlukla az sayıda kategoriden birden fazlasına uygundur. Örneğin; normal bir organizasyonda 20 veya 40 pazarlamacı, muhasebeci, IT desteği vb. olabilir. Yalnızca birkaç düzine kişiye (güvenlik yöneticisi, IT yöneticisi, 'CIO-Chief information officer' vb.) erişim haklarını tek tek tanımlamaları gerekir. Buna göre, bir grubu bir grup insan olarak tanımlayabiliriz; bir veya daha fazla kişinin önceden belirlenmiş bazı politikaları kullanarak bir süre için üstlenebileceği sabit bir erişim izni rolü olarak tanımlayabiliriz [35]. Önceden tanımlanmış bu gruplar ve belirli personele verilen işlevsel roller, çoğu kuruluşun günümüzde mükemmel bir şekilde çalışmalarını gerçekleştirmek ve veri sızıntısını önlemek için kullandığı bir tür erişim kontrolüdür.

2.4.2.3. Erişim kontrol listesi

Erişim Kontrol Listesi (ACL-Access Control List) erişim kontrolü kavramıdır. Bu metodoloji, erişim seviyelerini veya güvenlik açıklıklarını kullanmaz, daha ziyade bir öznenin veya nesnenin ne yapmasına izin verilip verilmediğini tanımlar [25]. Bir ACL, bir nesneye (dosya) [35] atanan bir tablo olarak düşünülebilir. Bu tablo, her kullanıcıyı ve bu belirli nesne (dosya) için erişim haklarını içerir. Tablo 2.1.'de Muhasebe Verilerinin tüm kullanıcılar için erişim hakları öğrneği gösterilmiştir:

Tablo 2.1. Erişim kontrol listesi (ACL).

Kullanıcı	Muhasebe verileri
Ali	okuma, yazma
Ahmed	yazma
Sam	okuma

ACL metodolojileri çok ince taneli erişim kurallarına izin verir çünkü bir öznenin ve bir nesnenin her etkileşimi kontrol edilebilir ve bu da veri sızıntısını önlemeye yardımcı olabilir. ACL'de, pratik olmayan tüm kullanıcıların tüm erişim haklarını atamak ve değiştirmek çok zordur. Bu nedenle, çoğu kuruluş bir önceki bölümde açıklanan Gruplar ve Roller yöntemlerini kullanmaktadır.

2.4.2.4. Yetkiler

Yetkiler, bir konunun kullanıcıya izin verilen tüm erişim haklarını içeren bir tablo olarak düşünülebilir [35]. Tablo 2.2.'deki örnekte, Sam'un yapabileceği yetkileri gösterilmektedir:

Tablo 2.2. Yetenek.

Kullanıcı	Muhasebe verisi	İşletim sistemi	Kullanıcı programı	Kişisel very
Sam	Yazma	Okuma,çalıştırma	Okuma, çalıştırma	Okuma,yazma

Yetkilerle ACL'ler gibi, tüm kullanıcılar için tüm erişim haklarını atamak da değiştirmek de zordur. Aynı nedenle, çoğu kuruluş 2'nci bölümde açıklanan Grup ve Rol yaklaşımlarını kullanmaktadır.

2.4.2.5. Veri kaybı/sızma önleme

Veri kaybını önleme, hassas verileri ön tanımlı ilkeye dayalı olarak kuruluş ağının dışına sızmasını tanımlamak, izlemek ve korumak için veri sınıflandırma, içerik ve/veya bağlam veri analizi gibi teknikleri kullanan bir çözümdür. Başka bir deyişle, DLP son kullanıcıların şirketin hassas verilerini herkese açık ağa gönderemediğinden emin olmak üzerine kuruludur.

BÖLÜM 3. VERİ KAYBI/SIZMA ÖNLEME

Kötü niyetli yetkili olmayan bir kullanıcı dahili ağa girmeye çalışırsa, Anti malware , güvenlik duvarları , İhlal tespit sistemi gibi sistemler (IDS-Intrusion Detection Systems) yada İhlal önleme sistemleri (IPS-Intrusion Prevention System) bu olayların saptanması ve engellenmesinden sorumludur. Buna rağmen bu gerçekleşir ve saldırgan bu sistemleri geçerse o zaman Veri kaybı / Sızıntı önleme (DLP-Data Loss/Leakage Prevention) adı verilen ve bu saldırganın yanı sıra, dahili ağdaki diğer kullanıcıların özel verilerini genel ağa sızdırmalarını önleyecek bir sistem var [36]. Başka bir deyişle , dışarıdan Anti malware , güvenlik duvarları İhlal tespit ve önleme sistemleri gibi bir çok farklı teknoloji mevcutken DLP sistemleri işi içeriden yapacak şekilde tasarlanmıştır [2].

3.1. DLP'nin Tanımı

Shabtai ve arkadaşları [4] 'e göre bir Veri Kaybını Önleme çözümü "gizli bilgilerin yetkisiz erişimi, kullanmasını veya iletilmesini önlemek için tasarlanmış bir sistem" olarak adlandırılmıştır. DLP, gizli verilerin içeriği ve etrafındaki içeriği derin analizi kullanarak, gizli verilere yetkisiz erişimi tespit eder ve önler [37].

Aynı zamanda DLP çözümlerini, "merkezi politikalara dayanan, dinlenme, hareket halindeki ve kullanımdaki verilerin derin içerik analizi yoluyla tanımlanması, izlenmesi ve korunması" olarak tanımlamaktadır [38]. DLP çözümleri, gizli veri sızıntısının riskini belirlemek, izlemek, korumak ve azaltmak için yardımcı olur. DLP çözümleri, yalnızca yetkili olmayan bir kullanıcının gizli verilere erişmesini tespit etmek ve caydırmak için değil aynı zamanda gizli verilerin yanlışlıkla paylaşılmasından korunması için de kullanılmaktadır [2]. Buna ek olarak, DLP kuruluşun çalışanlarını politikalarına ve düzenlemelerine uymaya zorlamak için iyi bir çözümdür.

İlk DLP çözümünün geliştirilmesi 2006 yılında başladı. Birçok güvenlik ürün gibi DLP de gelişti ve dünya çapında güvenlik endüstrisini etkilemeye başladı. Günümüzde veri sızıntısı çoğu kuruluşun karşılaştığı en büyük korkudan biridir ve DLP, hassas verilerin tanımlanması ve korunmasıyla ilgilenen [24]. CIO'Larin ve CISO'ların karşılaştıkları en kritik meselelerden biridir.

DLP, Veri Kaybı/Sızma Önleme/Koruma (DLP-Data Loss/Leakage Prevention/Protection), Bilgi Kaybı/Sızma Önleme/Koruma (ILP-Information Loss/Leakage Prevention/Protection), Kaçak Önleme, İçerik İzleme ve Filtreleme (CMF-Content Monitoring and Filtering), İçerik İzleme ve Koruma (CMP-Content Monitoring and Protection) anlamına gelir.

3.2. Sızıntı Çözme Yöntemleri

Veriyi ağ ya da uç noktalardan sızdırmanın birçok yolu vardır. Veri sızdırmanın bitiş noktasındaki yolları şöyledir: USB sürücüler, harici sürücüler, mobil cihazlar, (CD-Compact Disc)/(DVD-Digital Video Disc)'ler, yazıcılar, fakslar vs. Öte yandan ağ üzerinden sızdırmanın yolları E-posta, (HTTP-Hypertext Transfer Protocol) , anında mesajlaşma, (FTP-File Transfer Protocol), vb.

[4] 'te DLP çözümleri Veri sızmasını iki ana yöntemi kullanarak halledebilir:

a. Detektif Yöntemler: DLP çözümleri, sızıntı olaylarını tespit etmeye çalışır ve hassas verileri tanımlamak için Bağlam tabanlı (içeriğe dayalı) denetim, İçerik tabanlı (içerik farkında) denetim ve İçerik etiketi kullanarak gerçekleşen herhangi bir sızıntı oluşumunu gidermek için uygun düzeltici önlemi almaya çalışır .
b. Önleyici yöntemler: DLP çözümleri, Erişim kontrolü, Devre dışı bırakma işlevleri, Şifreleme ve Farkındalık gibi çeşitli önleyici yaklaşımları kullanarak kaçağı oluşmadan önce önler.

3.2.1. Detektif yöntemler

3.2.1.1. Bağlam-tabanlı denetim

Bağlam terimi kaynak, hedef, boyut, alıcılar, gönderen, üstbilgi / meta veri bilgisi, zaman damgaları, dosya türü, yeri, biçimi, uygulaması gibi izlenen verilerden çıkarılan bağlam bilgilerini ifade etmek için kullanılmaktadır. Kaynak/hedef (IP-Internet Protocol) adresi, kaynak/hedef portu ve başka paket öznitelikleri gibi dış filtreleme kurallarına dayalı paket filtreleme güvenlik duvarı bağlam denetim tabanlı bir sistemin örneğidir. Bağlam tabanlı DLP çözümleri, özel uygulamaların C++ dosyalarının kurum dışarısına gönderilmesini, şifrelenmiş dosyaların bloke edilmesini veya kopyalanmasını önlemektedir.

3.2.1.2. İçerik-tabanlı denetim

Bu yöntem, içeriği aşağıdaki gibi çeşitli teknikler kullanarak analiz ederek veri sızıntısını tanımlar:

a. Kurallı İfadeler ve eşleşen anahtar kelimeler

Bu yöntemler, DLP ürünleri tarafından kullanılan en yaygın tekniktir [39]. Olağan ifadelerin eşleşmesi verilen metinden bütün örüntü durumlarının tanımlanmasına ihtiyaç duyarken anahtar kelimelerin eşleşmesi verilen metinde yer alan önceden tanımlanmış anahtar kelimelerin tanımlanmasına ihtiyaç duymaktadır. Daha sonra, kredi kartı numarası, Sosyal Güvenlik Numarası (SSN-Social Security number), "gizli", "finansal rapor" vb. gibi hassas verileri tespit edebilirler. Bu yöntemler iyi bilinir, iyi tanımlanmış ve kolayca ve hızlı bir şekilde yapılandırılabilir ve DLP veri incelemesinde çok yararlı olabilir. Aksine, yüksek sahte pozitif oranlara eğilimli olup yapılandırılmamış içerik için çok az koruma sunmaktadırlar. Örneğin, gizli terimi çeşitli şekillerde, hatta gizli olmayan bağlamlarda kullanılabilir.

b. Parmak izi alma

Parmak izi, belirli bir metinden (hassas dosyalar veya veritabanı kaydı) çıkardığımız parmak izi olarak bilinen metinsel bir özellik oluşturan ve sızıntı tespiti için eşleşen tam parmak izi arayan bir yöntemdir. Bu parmak izi, bilinen belgelerin değiştirilmiş sürümleri, yinelenen doküman algılama (NDDD-Near Duplicate Document Detection), belgelerin varyantlarını algılama gibi durumları tanımlayabilir. Başka bir deyişle, dijital nesnelerin varyantlarından değişmeyenleri çıkarabilen bir tekniktir örneğin : İki belge önemli ölçüde ortak metin paylaşıyorsa, ortak parmak izlerine sahip olmalıdırlar. İki ilgisiz belgenin ortak parmak izlerine sahip olmaması için benzersiz olması gerekir.

c. Tam dosya uyumu

Bu teknik, bir dosyanın karma değerini üretir ve tam olarak bu değerle eşleşen dosyaları arar. Medya dosyaları ve metin analizinin mutlaka mümkün olmadığı diğer ikili dosyalar için çalışabilir [39]. Başka bir deyişle, yanlış pozitif oranları sıfıra yakın olan her türde çalışabilir. Ama öte yandan ufak bir değişimle kolayca bypass edebilir.

d. Kısmi belge eşleştirme

Bu teknik, eksik belgeleri veya bunların bir bölümünü diğer belgelerdeki görünüş/duruşlarla eşleştirir. Hassas belgeyi korumak için bu yöntemi kullanan DLP çözümleri, bir belgenin diğer belgelerde görülen bazı cümleleri bile algılayabilmelidir. Bu yöntem, yapılandırılmamış verileri koruyabilir ve standart ifadeler hariç tutulursa düşük oranda yanlış pozitiflik üretebilir, ancak yine de aşırı eşleme nedeniyle yüksek bir (CPU-Central Processing Unit) yükü oluşturabilir.

e. İstatistiksel analiz

Bu metotlar, veri sınıflandırılması veya spam filtrelerinde kullanıldığı gibi gizli verileri tanıyabilmek için denetim altındaki içerikleri(terimlerin oluşumu)den elde edilen istatistiksel metrikleri çıkarmanın beraberinde iş yerinde sürekli öğrenme veya yeterli veri miktarına sahip eğitim verilerini işleme yöntemlerini içeren makine öğrenmesi tekniklerni kullanmaktadır. Bu yöntem, kısmi belge eşleştirmesi gibi deterministik tekniğin bu tür veri üzerinde etkisiz olduğu durumlarda yapılandırılmamış içeriğin algılanması için etkilidir. Makine öğrenme teknikleri ve istatistiksel ölçümler mevcut en iyi yaklaşımdır.

Bu İçerik temelli denetim tekniği, çeşitli dosya türlerini ayrıştırma kabiliyetine ihtiyaç duyar ve bunların çoğu yalnızca metin içeriğine odaklanır.

3.2.1.3. İçerik etiketleme (kategoriler)

Bu yöntemde, hassas verileri içeren her dosyanın kendisine atanmış bir etiketi vardır ve atanan etikete göre bir ilke uygulanır. İçerik, diğer uygulamalar tarafından işlendiğinde bile etiketli kalır. Örneğin, hassas olarak etiketlenmiş bir pdf belge dosyası, şifrelenmiş veya sıkıştırılmış olsa dahi hassas olarak etiketlenmiş kalacaktır. Etiketler dosyalara farklı yollarla atanabilir: hassas verilerin yaratıcısı elle; içerik veya bağlam tabanlı analizleri otomatik olarak kullanarak; belirli bir konumda saklanan tüm dosyalara otomatik olarak; veya belirli uygulamalar veya kullanıcılar tarafından oluşturulan tüm dosyalara otomatik olarak eklenebilir.

3.2.2. Önleyici yöntemler

3.2.2.1. Giriş kontrolü

Erişim kontrolü, belli bir varlığın belirli bir kaynağın kullanımına izin verme veya reddetme yeteneğidir. Tanımlanmış bir politikaya göre, hassas bilgilere erişim izni

yoksa, DLP bu bilgilerin kullanımını kısıtlar, aksi halde erişim kabul edilir. DLP'yi kurumsal dijital haklar yönetimi (EDRM-Enterprise Digital Rights Management) ile entegre etmek, dokümanlara otomatik olarak erişim kontrolü sağlamak için bir yoldur.

3.2.2.2. İşlevleri devre dışı bırakma

Bu, hassas verilerin sızmasına neden olabilecek işlevleri devre dışı bırakmayı içeren önleyici bir yaklaşımdır. Örneğin, hassas içeriğe kopyalama ve yapıştırma işlemlerini kısıtlayarak, içeriği taşınabilir depolama birimine kaydederek veya ince istemcileri dağıtarak gerçekleştirilebilir.

3.2.2.3. Şifreleme

Hangi hassas verilerin şifrelenmesi gerektiğini ve bu verilerin kimlerin şifresini çözebileceğini bildiren bir ilke tanımlar. Ayrıca, yalnızca onaylı kurumsal uygulamalarla şifrelemeye izin vererek hassas verilerin kullanılmasına izin verilen uygulamaları tanımlar.

3.2.2.4. Farkındalık

Bu, kullanıcıları ve çalışanları hangi verinin özellikle hassas olduğu, kimin neye erişiminin olduğu ve bunu korumak için ne yapılması gerektiğine dair bilgilendiren bir süreçtir.

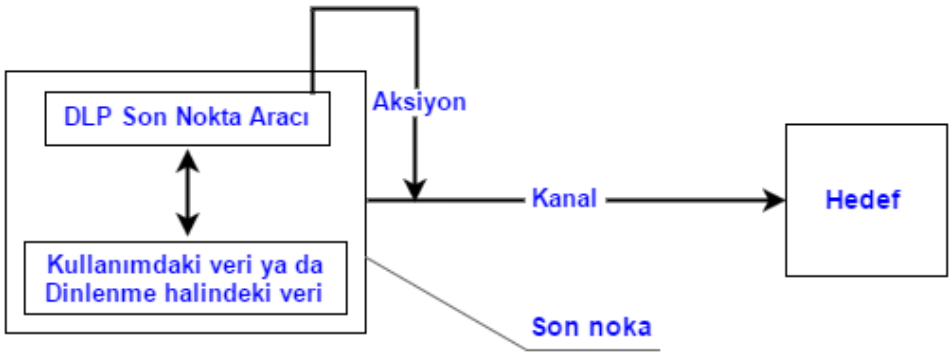
[5], [40]'e göre DLP çözümleri etkin DLP çözümleri veya etkin olmayan DLP çözümleri olarak sınıflandırılabilir. Aktif bir DLP çözümü, bir dosyanın oluşturulduğu ve kaydedildikten sonra ayrıştırılması yerine bir kullanıcı yazarken yazmanın gizli verilerini izler. Hareketsiz (içerik bilinci ve/veya içeriğe duyarlı) DLP çözümü, sızıntıyı önlemek için hareketsizken, kullanımdayken veya hareket halindeyken hassas verileri tanımlamak için içerik incelemesi ve/veya içerik analizi gerçekleştirirken, tüm dosya türlerini ayrıştırmak gerekiyor.

3.3. Veri Durumu

Tüm veri sızıntısı olaylarıyla başa çıkabilmek için bir DLP çözümü, kuruluşun verilerini tüm ömürleri boyunca izlemeli ve korumalıdır. DLP çözümleri, kullanımdaki veri (DIU-data-in-use), hareket halindeki veri (DIM-data-in-motion) ve kaynakta duran veri (DAR-data-at-rest) [4], [24], [31] gibi yaşam döngüsü boyunca üç farklı aşamada verileri değerlendirir. :

3.3.1. Kullanımdaki veri (uç nokta)

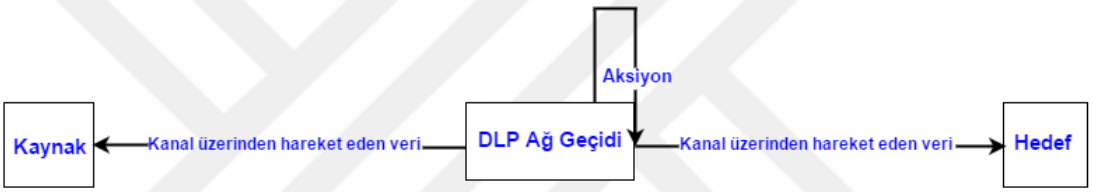
Veri kullanımı herhangi bir yazılım veya kullanıcı tarafından herhangi bir iş istasyonunda veya sunucuda kullanılan verilerdir. Bu veriler, depolama aygıtına kaydedilmeyecek geçici veriler veya depolama aygıtına kaydedilecek kalıcı veriler olabilir. DLP çözümleri, bitiş noktası aracısını, kullanıcı kullanım sırasında veya bitiş noktasındaki bir cihazdan farklı çıkış kanalları vasıtasıyla (USB sürücüler, harici sürücüler, mobil cihazlar, CD / DVD'ler, Yazıcı, faks vb.) harici cihazlara aktarırken bu verileri izleyerek etkileşime girmeye başlayan hassas verileri korumak için kullanır. Bu aracı, Gizli Verileri içeren Kopyala yapıştır ve ekran işlemleri yazdırma, Hassas verilerin USB sürücüler gibi taşınabilir depolama aygıtına aktarılması ve hassas verileri içeren faks yazdırma veya gönderme gibi etkinlikleri izleyebilirsiniz. Veri sızıntısı tespit edildiğinde, bu son nokta aracı, veri sızıntısını önlemek için kuruluş politikasına göre kopyalama ve yapıştırma işlemini engelleme gibi harekete geçecektir. Şekil 3.1. aşağıda DLP çözümünün veri kullanım durumunu nasıl ele alacağına ilişkin kavramsal görüşünü göstermektedir.



Şekil 3.1. Kullanımdaki veri.

3.3.2. Hareket halindeki veri (ağ)

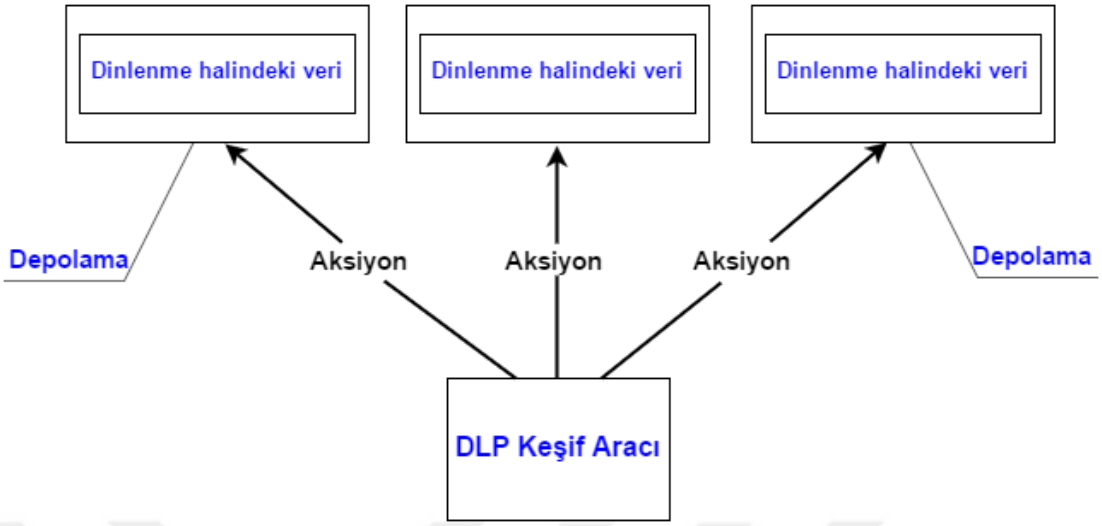
Hareket halindeki veri, organizasyon ağı üzerinden bir yerden başka bir yere dolaşan veya kuruluş ağı üzerinden İnternet üzerinden dışarıya doğru giden Veri'dir. Örneğin, çalışanların uzaktaki sunucudaki bilgilere erişmesi veya diğer takım arkadaşlarına bir e-posta göndermesi gerekir. DLP çözümleri, hassas verilerin sızıntısını tespit etmek ve hassas verilerin bu sızıntısını önlemek için organizasyonun önceden tanımlanmış politikalarına göre gereken önlemleri alabilmek için bir ağ üzerinden iletişim kanallarının dışına gönderilen verileri incelemek için kullanılır. Şekil 3.2. aşağıda DLP çözümünün hareket halindeki veri durumunu nasıl ele alacağının kavramsal görüşünü göstermektedir.



Şekil 3.2. Hareket halindeki veri.

3.3.3. Kaynakta duran veri (depolama)

Kaynakta duran verileri, sabit diskler, hafıza kartları gibi veri depolama cihazlarında depolanan, ancak aktif olarak kullanılmayan veya aktarılmayan verilerdir. DLP çözümleri içeriden yetkisiz birinin veya dahili sisteme giren bir saldırganın, durağan hassas verileri çalmasına engel olmak için kullanılır. Bu, depolama hizmetlerinde veya cihazlarda gizli verileri tanımlamak ve keşfetmek için içerik bulma mekanizmasını kullanarak, daha sonra şifreleme gibi güvenlik önlemlerini kullanarak veya kuruluş politikasına dayalı kullanıcı erişim haklarını sınırlayarak yapılabilir. Örneğin, yetkisiz bir cihazda hassas veriler bulunursa, DLP çözümleri bu verilerin yetkili bir yere taşınması, bu hassas verilerin günlüğe kaydedilmesi ve alarm verilmesi, silinmesi veya şifrelenmesi gibi işlemleri yapar. Dolayısıyla DLP, organizasyonun hassas verilerin tüm sistemde nerede dağıtıldığını bilmesine izin verebilir. Aşağıdaki Şekil 3.3. DLP çözümünün veri-dinlenme durumu üzerinde nasıl çalışacağı kavramsal görüşünü göstermektedir.



Şekil 3.3. Dinlenme halindeki veri.

3.4. DLP Eylemleri

Bir DLP eylemi, DLP yöneticisi tarafından kurulan kuruluşun ilkelerine dayanan veri sızıntısını algıladığında DLP'nin alabileceği davranıştır. The system can also log the events with information about who did it, when it happened, what it contained and what action was taken [36].

Örneğin, DLP ürünü olan MyDLP [41] tarafından gerçekleştirilen bazı işlemler aşağıda belirtilmiştir:

a. Geçiş: Verilerin iz bırakılmadan geçmesine izin verir.
b. Günlük: Geçen verilere izin verir ve olay hakkında bilgi tutar, ancak verilerin tamamını tutmaz.
c. Arşivleme: Geçen verilere izin verir ve olay ve tüm veriler hakkında bilgi tutmaya izin verir.
d. Blok: Veri aktarımını engeller ve olay hakkında bilgi tutar, ancak verilerin tamamını tutmaz.
e. Karantina: Geçen verileri engeller ve olayın ve tüm verilerin bilgisini tutar.

3.5. DLP Bileşenleri

DLP çözümünün tamamı dört ana bileşenden oluşur:

3.5.1. DLP uç nokta aracı

Bir DLP Bitiş noktası aracı, veriler kullanıcılar tarafından veya dinlenme sırasında verilerin kullanımdayken hassas verileri korumak için uç noktalara yüklenen bir yazılımdır. Bu DLP acenteleri, güncellenmiş poliçeyi almak ve gizli verilerin kaçağı olduğunda düzgün bir işlem yapmak için DLP merkezi sunucuyla iletişim kuracaklardır. Bu eylemler DLP yöneticisi tarafından tanımlanan yapılandırmalara ve ilkelere göre gerçekleşir. Bununla birlikte, bu ajanlar, alınan eylemlerin raporlarını sunucuya göndermek zorundadır. Buna ek olarak, zor şartlar altında hayatta kalmalı ve gizli veriler ağdan koptuğunda bile korunarak zararlı niyetli kullanıcılar tarafından manipüle edilmeye karşı korunmalıdır.

3.5.2. DLP ağ geçidi

Bir DLP Ağ Geçidi, ağ trafiğini izleyen ve analiz eden bir veya daha fazla sunucudur ve böylece her uç nokta, trafiğini bunun üzerinden yönlendirmek zorunda kalır. Bu sunucular, önceden tanımlı ilkeyi edinmek ve tanımlanan ilkeye göre şüpheli iletimleri engellemek veya izin vermek için uygun eylemleri tetiklemek için DLP merkezi sunucuyla iletişim kurmalıdır. Ayrıca, alınan önlemlerin DLP merkezi sunucusuna rapor gönderilmesi gerekir. Bu sunucular, önceden tanımlı ilke edinmek ve tanımlanan ilkeye göre şüpheli iletimleri engellemek veya izin vermek için uygun eylemleri tetiklemek için DLP merkezi sunucuyla iletişim kurmalıdır. Ayrıca, alınan önlemlerin DLP merkezi sunucusuna rapor gönderilmesi gerekir.

3.5.3. DLP keşif aracı

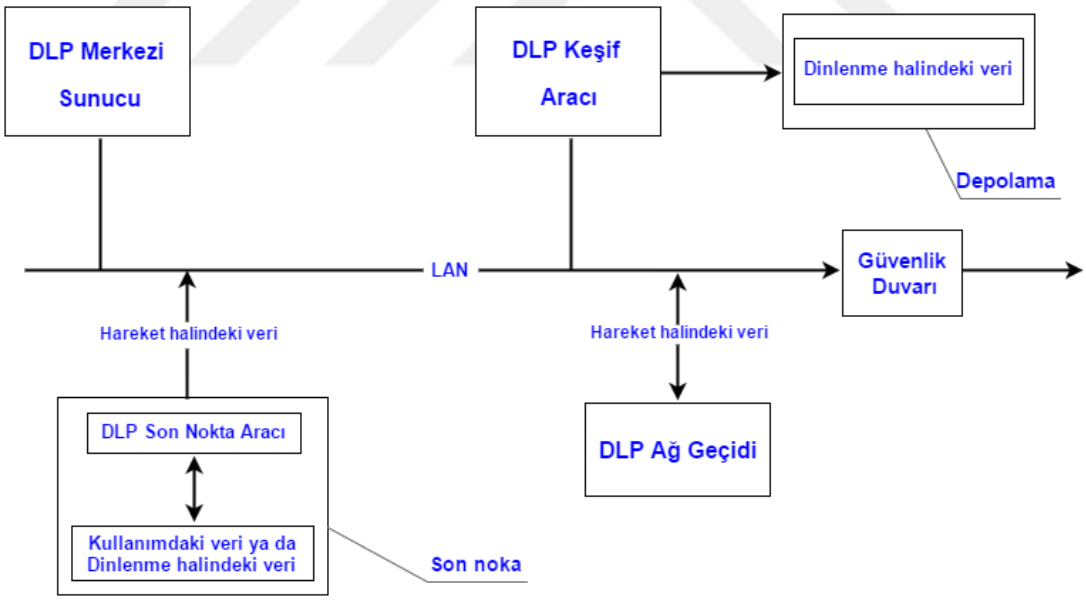
Bir DLP Keşif Aracı, dinlenmekte olan gizli verileri keşfeden, ardından silmek, şifrelemek veya güvenli bir yere taşımak gibi uygun işlemleri yapan sunucudur. Bu

keşfedici ajanlar, bu eylemlerle ilgili raporları DLP merkezi sunucusuna göndermek zorundadır. Bununla birlikte, keşfedilen süreçler DLP yöneticisi tarafından tanımlanan ilkeye ve yapılandırmalara göre programlanır ve çalışır.

3.5.4. DLP merkezi sunucu

DLP Merkezi Sunucu, kuruluşun ilkesini oluşturmak ve yönetmek için DLP yöneticisine bir yönetim konsolu sağlayacak merkezi bir sunucudur ve tüm DLP sisteminin tam kontrolünü sağlar. Bu DLP merkezi sunucu, sistem durumunun, istatistiksel sonuçların ve tüm DLP sistemi tarafından alınan tüm eylemlerin raporlarını gösterebilir.

Aşağıdaki Şekil 3.4.'te DLP sistemin tüm resmini göstermektedir ve ayrıca her veri durumunu nasıl ele alacağımızı göstermektedir: yani, kullanımdaki veri, hareket halindeki veri ve dinlenme halindeki veri.



Şekil 3.4. DLP sistemin tüm resmini göstermektedir.

3.6. DLP Ürünü Tipleri

Piyasada bulunan DLP ürünleri üç tipe bölünebilir; temsilci tabanlı, temsilcisiz ve hibritler [36].

3.6.1. Ajan tabanlı

Bir temsilci tabanlı DLP ürünü, ilkeleri ve yapılandırmaları her uç noktaya kendileriyle iletişim kurarak yayınlayacak olan DLP Merkezi Sunucu'nun her uç noktasında dağıtılan Son Nokta Aracına sahip bir üründür. Bununla birlikte, bu DLP çözümünde, ağın dışına çıkan trafiği izleyen ve analiz eden bir DLP Ağ Geçidi yok. DLP Keşif Aracı, bitiş noktasındaki hassas veriyi keşfeden Uç Nokta Aracına dahil edilmiştir.

Bu tür bir çözümün avantajı, USB sürücüler, harici sürücüler, ağ, mobil cihazlar, CD/DVD'ler, Yazıcılar, faks vb. Cihazlar için bitiş noktasının dışına çıktığı zaman verileri izlemek için son noktaya daha fazla kontrol sağlanmalarıdır.

Bu tür çözümlerin dezavantajı, bize ağ seviyesinde sınırlı kontrol sağlaması ve kuruluş ağının dışına çıkan verileri izlememesidir. Buna ek olarak, son nokta kullanıcısı tarafından tehlikeye atılabilir, müdahale edilebilir veya manipüle edilebilir.

3.6.2. Ajansız

Temsilcisiz , organizasyonun ağına giren tüm trafiği izlemek ve analiz etmek için bir veya daha fazla DLP Ağ Ağ Geçidi bulunan DLP ürününün bir başka türüdür ve bu nedenle tüm ağ trafiği bu DLP kaçamakları ile dışarı çıkmaya zorlanacaktır. Ayrıca, onları denetlemek için tüm DLP kaçışlarına ilkeleri ve yapılandırmaları yayınlayacak bir DLP Central Server da var. Bununla birlikte, bitiş noktalarında hiçbir şeyin kurulmayacağı anlamına gelen herhangi bir Son Nokta Aracısı yok. Ayrıca genellikle DLP keşif temsilcisi yoktur.

Bu çözümlerin avantajı, tüm ağ trafiğini izleyebilmeleri ve DLP Central Server tarafından kolayca kontrol edilebilmeleridir. Dahası, DLP kaçamakları güvenli

yerlere yerleştirildiğinden, son nokta kullanıcısı tarafından acente tabanına dayalı türde olduğu gibi ele geçirilemez, değiştirilemez veya manipüle edilemez.

Bu çözümlerin dezavantajı, farklı çıkış kanalları vasıtasıyla USB sürücüler, harici sürücüler, CD/DVD'ler, Yazıcı gibi harici cihazlara aktarıldığında verilerin izlenmesinde yararsız olmasıdır. Çünkü izlemek için bitiş noktasına yüklenmiş hiçbir şey yok.

3.6.3. Hibrit

Hybrid, temsilci bazlı ve temsilci içermeyen DLP ürün türlerinin bir kombinasyonudur. Başka bir deyişle, DLP çözümünün dört temel bileşenini içeren, kullanımdaki verileri harekete geçirip dinlerken izleyecek ve analiz edecek eksiksiz bir DLP sistemi. Bu tip DLP ürünleri en popüler ürünlerdir.

Bu tip avantajın hem temsilci bazlı hem de temsilci içermeyen türlerinin avantajlarının bir kombinasyonu olması, hem şebeke hem de son nokta seviyelerinde daha fazla kontrol ve izleme imkanı sağladığı anlamına gelmektedir. Başka bir deyişle, bu hem ağ trafiğini hem de USB, CD/DVD ve yazıcılar gibi ortamlara dosya aktarımlarını izlemeyi mümkün kılar.

Bu tipin dezavantajı, son nokta kullanıcılarının tıpkı aracı temelli türde olduğu gibi bitiş noktaları aracısı tarafından ele geçirilebileceği, değiştirilebileceği veya manipüle edilebileceğidir.

BÖLÜM 4. ÖNERİLEN MODEL

Bu bölümde, DLP-eklentisi modelinin kullandığı sınıflandırma tekniğini, DLP-eklentisi dizayn bileşenlerini, modelin nasıl çalıştığını açıklanmaktadır.

4.1. Sınıflandırma Tekniği

Şirket kuruluşlarından, devlet kurumlarına kadar tüm kuruluşlarda bilgiler ve veriler gizlilik derecesine göre en yüksekten en alçağa doğru belirli bir kriterle sınıflandırılırlar. Bu kriter bahsi geçen bilgi ve verileri kimlerin kullanma ve dağıtım hakkına sahip olduğunu belirleyecektir [19]. Buna bağlı olarak [42]–[44] en yaygın kullanılan örnek şu şekildedir: Çok Gizli, Gizli, Gizli Kalması Gereken, Kısıtlı. Ancak her hükümet ve kuruluşun güvenlik seviyelerini belirlemek, eldeki verilerin hangi güvenlik seviyesine ait olduğunu belirlemek ve bu güvenlik seviyesiyle kimin ilgileneceğini belirlemek için kendi kuralları vardır. Sonuç olarak hem şirketler hem de hükümetler tarafından en çok kullanılan kurumsal yapının hiyerarşi (piramitsel sınıflandırma) olduğu bilinmektedir. Buna dayanarak Şekil 4.1.'de gösterilmiş olduğu gibi hiyerarşik sınıflandırma stratejisini kullanmaktayız.

Şekil 4.1. Hiyerarşik sınıflandırma stratejisini.

Verileri, Çok Gizli'den Kişisel'e doğru sıralanan beş seviyede sınıflandırdık. Birinci seviyeye (Çok Gizli) sahip kullanıcı bütün ayrıcalıklara sahip olacak ve diğer bütün güvenlik seviyelerine erişim sağlayabilecek. İkinci seviyeye sahip kullanıcı ikinci seviyeye ve bu seviyeden yüksek diğer bütün seviyelere erişim sağlayabilecek. (seviye3, 4 ve 5). Aynı şekilde üçüncü seviyeye sahip kullanıcı da bu seviyeye ve bu seviyeden yüksek diğer bütün seviyelere (seviye3, 4 ve 5) erişim sağlayabilecek. Aynı sistem 4. ve 5.seviye için de geçerli olacak. Ancak 5.güvenlik seviyesi her kullanıcı için farklılık gösterecek. 5.seviyedeki her kullanıcı kendine ait ve 5.seviye olarak sınıflandırılmış bütün verilere ulaşım sağlayabilirken, 5.seviye veriler şahsi bilgileri içerdiği için diğer kullanıcıların 5.seviyedeki verilerine erişim sağlayamayacaklar. Sunulan bu sınıflandırma modeli kuruluşların ve hükümetlerin taleplerine uyum sağlayabilir yada bunlara göre değiştirilebilecektir.

4.2. DLP-Eklentisi Bileşenleri

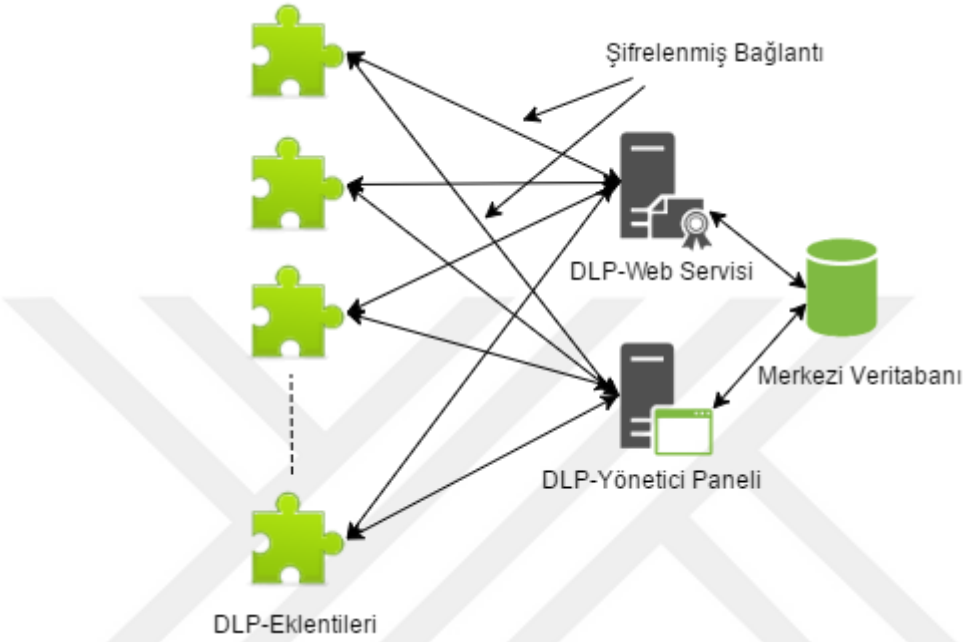
Oluşturduğumuz DLP-Eklentisi modeli üç ana bileşenden oluşmaktadır:

a. DLP-Yönetici Paneli: Kullanıcıları idare etmek için merkezi kontrol mekanizması sağlayan bir web sitesidir. Örneğin, yeni bir kullanıcı eklemek, varolan kullanıcılardan birini silmek veya belirli bir bilgisayarda varolan bir kullanıcının ayrıcalıklarını değiştirmek, vs. ve yeni bir DLP-Eklentisi eklemek yada varolan DLP-eklentisini silmek için kullanılabilir.

b. DLP-Web Servisi: Kullanıcının sahip olduğu güvenlik seviyesini öğrenerek, ona uygun şifreleme ve şifre çözme anahtarlarını şifreleme kanalı aracılığıyla DLP-eklentisine göndermek üzere hem kullanıcının hem de bilgisayarın kimliğini öğrenmeye yarayan web servisidir.

c. DLP-Eklentisi: Yetkili kullanıcıların verilerinin güvenliğini, onlar verilerini açtıklarında deşifre ederek ve kapattıklarında şifreleyerek sağlayan, kalıtsal uygulamaya eklenecek olan eklentidir. Bu DLP-Eklentisi kullanıcının kimliğini kontrol etmek ve onun güvenlik seviyesine uygun şifreleme/şifre

çözme anahtarlarını edinmek için DLP-Web Servisiyle iletişim kuracaktır. Ayrıca kullanıcıların verilerini sınıflandırmasına ve sahip oldukları güvenlik seviyesine göre verilerinin güvenlik seviyelerini düzenlemelerine yardımcı olacaktır.

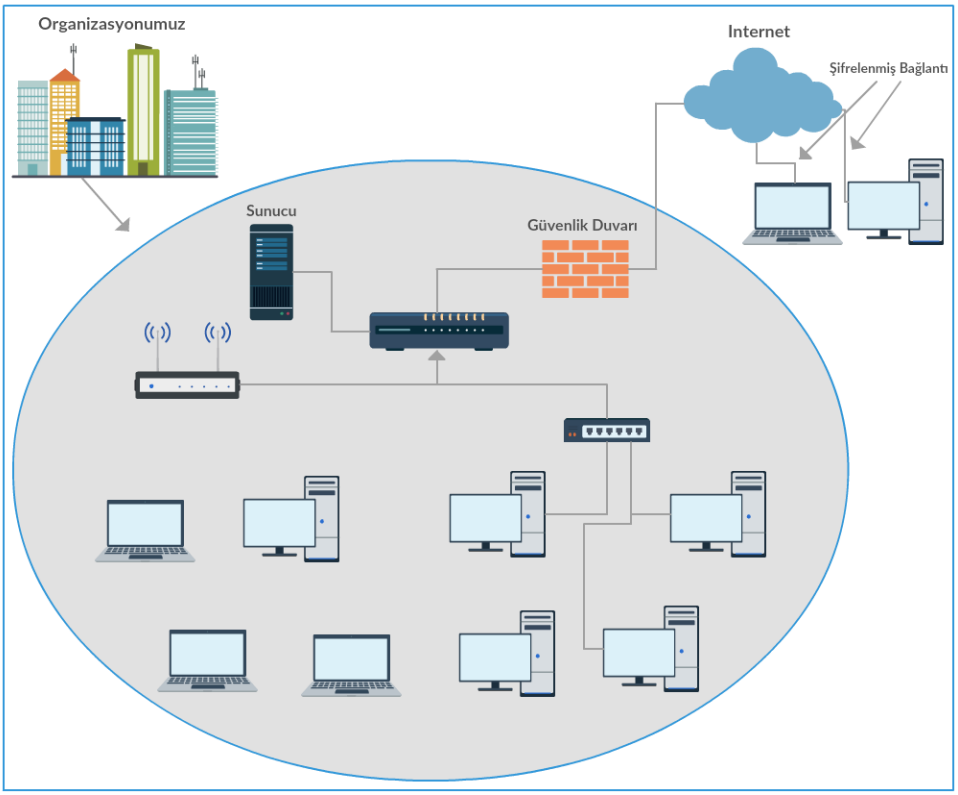


Şekil 4.2. DLP-Eklentileri bileşenleri.

Şekil 4.2.'nin yukarı göstermiş olduğu gibi birinci ve ikinci bileşenler kalıtsal uygulamalara eklenmiş olan bütün DLP-Eklentilerine bağlanacaktır, fakat üçüncü bileşenler ona eklenecek uygulamaların çeşitliliğine göre değişkenlik göstereceklerdir. Bu DLP-Eklentilerine örnek olarak Microsoft office Word için bir DLP-Eklentisi geliştirdik.

4.3. DLP-Eklentileri Modeli Çalışması (Örnek: Microsoft OfficeWord)

Şekil 4.3.'teki gibi ağ topolojisi olan bir kuruluşa sahip olduğumuzu varsayın:



Şekil 4.3. Bir kuruluşun ağ topolojisine bir örnek.

Farzedelim ki kuruluşun word belgelerini dışarıya karşı kasıtsız sızıntılardan korumak istiyoruz. Ve ayrıca bu belgelerin yetkisiz üyeler tarafından yasadışı erişime karşı güvenliğini sağlarken, aynı zamanda bu belgelerin üyeler tarafından kuruluşun içinden yada dışından kullanabilirliğini garanti ederek yasal erişim sağlamak istiyoruz.

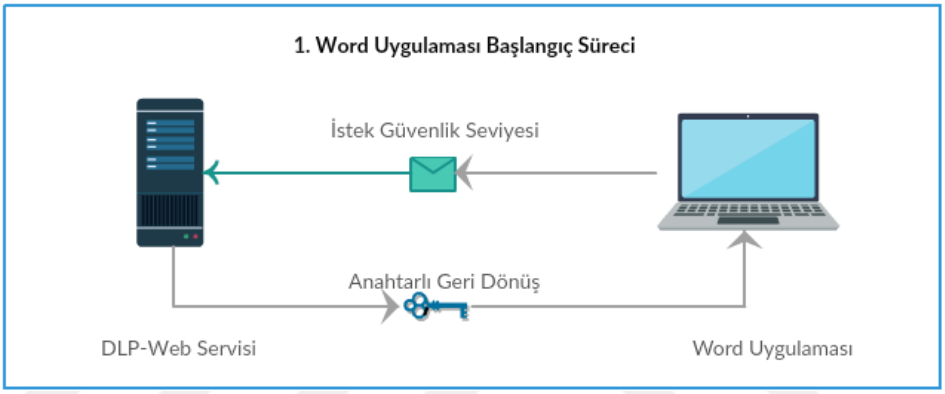
Bunu başarabilmek adına Microsoft Word uygulaması için Word belgelerini kuruluş bünyesinde çalışan üyeler tarafından yada yetkisiz kullanıcılar tarafından oluşabilecek kazara sızıntılara karşı koruyan DLP-Eklentisini oluşturduk. Modelin nasıl çalıştığını anlamak için bunu üç sürece böldük:

4.3.1. Word uygulaması başlangıç süreci

Bir Word uygulaması başlatıldığı zaman Word uygulaması içindeki DLP-Eklentisi bilgisayarı ve kullanıcı kimliğini tanımaya başlayacaktır. Kimliği edindikten sonra, DLP-Eklentisi bu kimliğe göre güvenlik seviyesini (şifreleme ve şifre çözme

anahtarlarını) edinmek için DLP-Web Servisine bağlanacaktır. Şimdi bilgisayar ayrıcalıklarını (güvenlik seviyesini) edindiğine göre uygun şifreleme ve şifre çözme anahtarlarına sahip demektir.

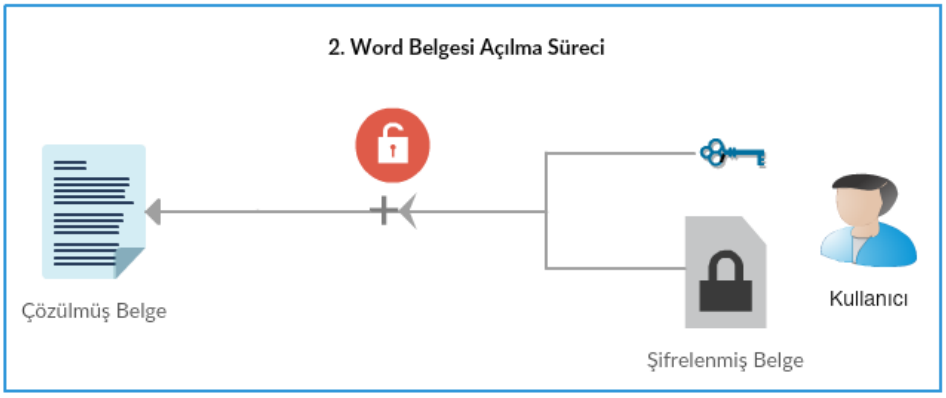
Şekil 4.4. aşağıda bilgisayarın kimliğini DLP-web servisine göndererek güvenlik seviyesi (şifreleme ve şifre çözme anahtarları) isteğinde bulunduğunu ve şifreleme kanalı vasıtasıyla güvenlik seviyesini (şifreleme ve şifre çözme anahtarları) nasıl edindiğini resmetmektedir.



Şekil 4.4. Word uygulaması başlangıç süreci.

4.3.2. Word belgesi açılış süreci

Sınıflandırılmış her belge varsayılan olarak şifrelenmiştir. Kullanıcı yukarıda açıklanan süreçten yasal şifreleme ve şifre çözme anahtarlarını edinir. Kullanıcı sınıflandırılmış belgeyi açmaya başladığı zaman DLP-eklentisi belgenin güvenlik seviyesini kontrol edecektir ve eğer bu güvenlik seviyesi kullanıcı için yasalsa DLP-Eklentisi belgeyi deşifre etmek için uygun anahtara sahiptir demektir. Böylece DLP-Eklentisi belgeyi deşifre edecek ve kullanıcı için açacaktır. Eğer güvenlik seviyesi kullanıcı için yasal değilse DLP-Eklentisi belgeyi deşifre etmek için uygun olan anahtara sahip olmadığı için belge şifrelenmiş olarak kalacaktır. Bu süreç kullanıcıya herhangi ek bir yük oluşturmadan kolayca hallolacaktır. Kullanıcı yalnızca açmak istediği belgeye çift tıklayacak ve şifre çözme süreci herhangi bir farklılık hissettirmeden arkaplanda işleyecektir. Bu süreç aşağıda Şekil 4.5.'te açıklanmıştır:

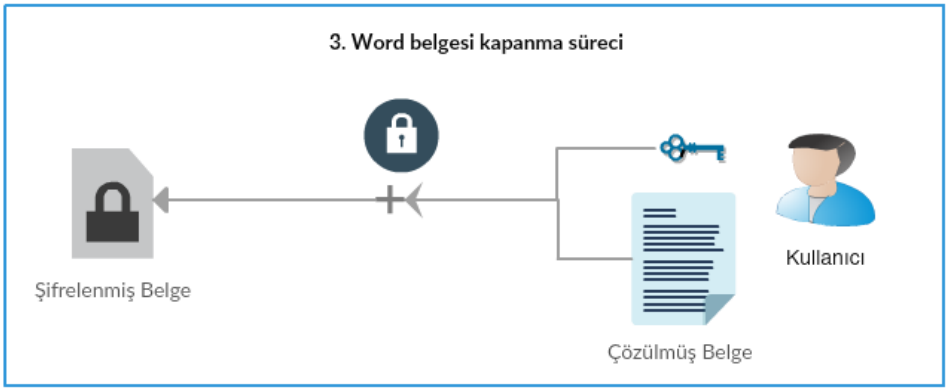


Şekil 4.5. Word belgesi açılma süreci.

4.3.3. Word belgesi kapanma süreci

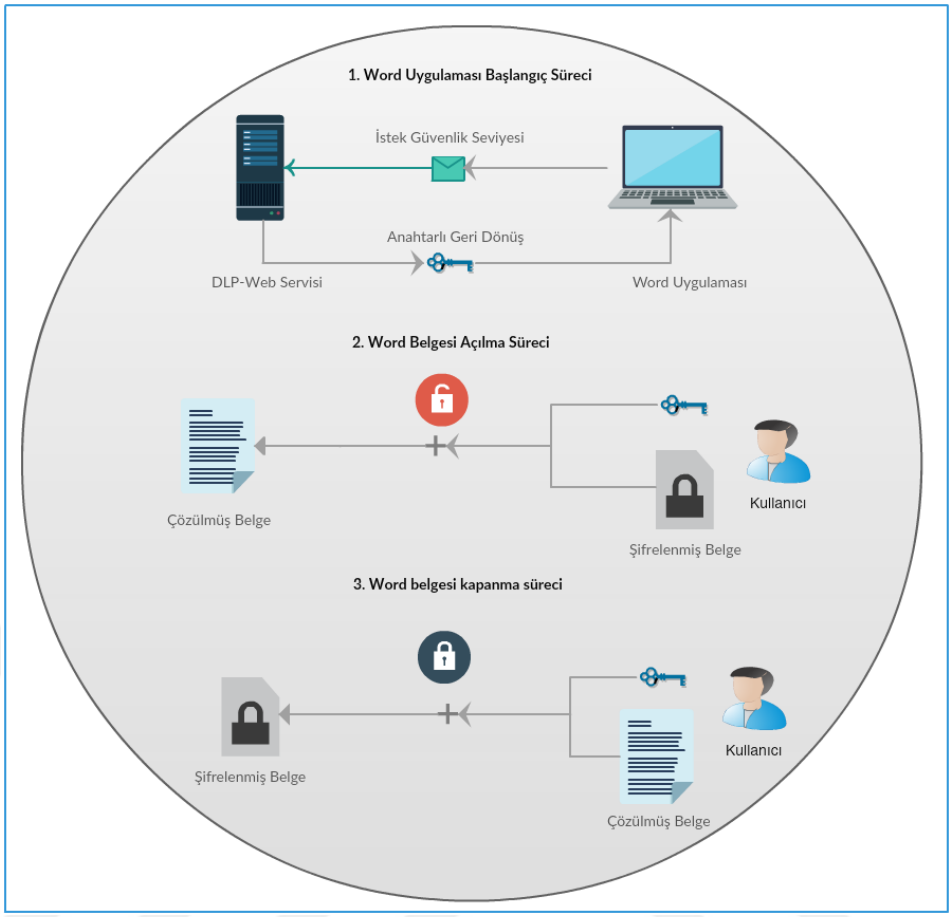
Belge açıkken kullanıcı belgesinin güvenlik seviyesini sahip olduğu herhangi bir güvenlik seviyesine dönüştürebilir.

Belgeyi kapatırken DLP-Eklentisi belgenin güvenlik seviyesine göre belgeyi şifreleyecektir. Bu süreç aşağıda Şekil 4.6.'da açıklanmıştır:



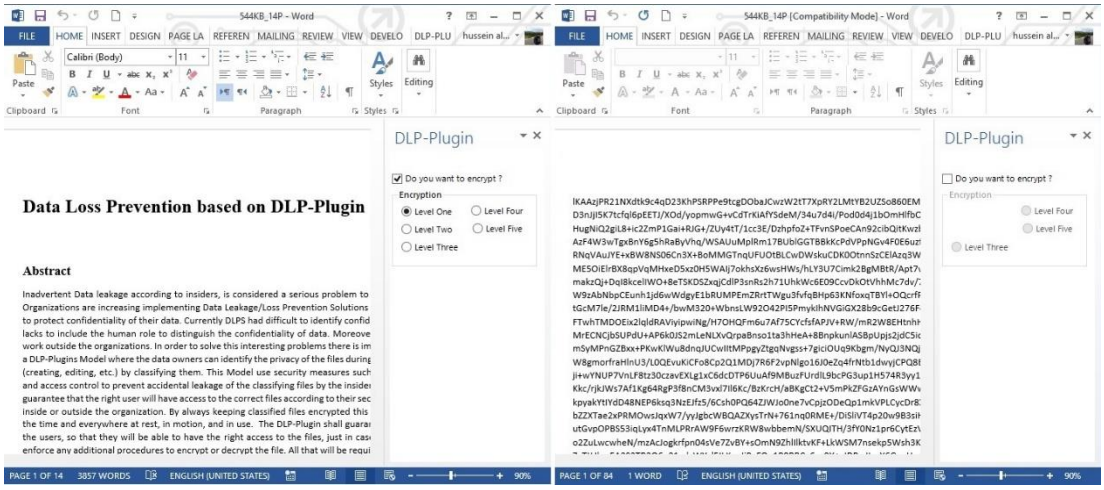
Şekil 4.6. Word belgesi kapanma süreci.

Bu üç süreç hassas verinin kuruluş dışına dikkatsizce sızmasını ve yetkisiz kullanıcılar tarafından ulaşılmasını engellemek için uygun bir koruma sağlar. Şekil 4.7. aşağıda bu üç süreci açıklamaktadır.



Şekil 4.7. DLP-Eklentileri model sürecleri.

Şekil 4.8. hem yetkisiz kullanıcı hem de yetkili kullanıcı için nasıl görüneceğini göstermektedir. Şekildeki belge Seviye-1 olarak sınıflandırılmıştır. Şeklin solundaki kullanıcı bu seviyeye sahip olduğu için yetkilidir, bu yüzden belge ona normal görünmektedir. Öte yandan şeklin sağındaki kullanıcı Seviye-1'e sahip değildir, bu sebepten yalnızca şifrelenmiş veriyi görecektir.



Şekil 4.8. Yetkili kullanıcı ve yetkisiz kullanıcı için belgenin görüntüleri.

BÖLÜM 5. DLP-EKLENTİLERİ PERFORMANSI (ÖRN: MİCROSOFT WORD)

5.1. Şifreleme

Bu bölümde, testler için kullandığımız şifreleme algoritmalarını açıklayacağız. Kullandığımız tüm şifreleme algoritmaları, hem şifreleme hem de şifre çözme işlemleri için tek bir anahtar kullandıkları anlamına gelen simetrik şifreleme algoritmalarıdır. AES, RC2, TDES, Blowfish ve Twofish'i blok şifreleme algoritmaları olarak kullandık. Ayrıca, RC4'ü bir akış şifreleme algoritması olarak kullanıyoruz.

5.1.1. AES

AES (Advanced Encryption Standard, Gelişmiş Şifreleme Standartı) simetrik bir blok şifreleme algoritmasıdır. Algoritma iki Belçikalı kriptografcı Joan Daemen ve Vincent Rijmen tarafından geliştirildi. AES hem donanım hem de yazılımda verimli olacak şekilde tasarlanmıştır. Ayrıca, 128 bitlik bir blok uzunluğunu ve 128, 192 ve 256 bitlik anahtar uzunluklarını destekler [45].

5.1.2. RC2

RC2 (Rivest Cipher 2, Rivest Şifreleme 2), simetrik bir blok şifreleme algoritmasıdır. 1987'de Ron Rivest tarafından tasarlanmış ve 64 bitlik bir blok kodudur ve 40 bit ile 128 bit (8 bitlik artışlarla) arasında anahtar boyuta sahip olabilir [46].

5.1.3. TDES

TDES (Triple Data Encryption Standard, Üçlü Veri Şifreleme Standardı), her bir veri bloğuna Veri Şifreleme Standardı (DES) şifre algoritmasını 3 kez uygulayan simetrik

bir blok şifreleme algoritmasıdır. TDES, 56, 112 ve 168 bitlik anahtar uzunluklarına sahip olabilir.

5.1.4. Blowfish

Blowfish simetrik bir blok şifre. 32 bit'den 448 bit'e kadar değişken uzunluklu anahtar alır. Blowfish 1993 yılında Bruce Schneier tarafından mevcut şifreleme algoritmalarına hızlı, özgür bir alternatif olarak tasarlandı [47].

5.1.5. Twofish

Twofish, simetrik bir blok şifre olup, 1998'de yayınlanmıştır. 128 - 256 bit arasında değişen bir anahtar boyutu alır. Twofish daha önceki blok şifreleme Blowfish ile ilgilidir.

5.1.6. RC4

RC4 (Rivest Cipher 4, Rivest Şifreleme 4), 1987'de Ronald Rivest tarafından geliştirilen ve 40 bit ila 2048 bit arasında anahtar boyuta sahip olabilen simetrik bir akış şifreleme algoritmasıdır.

5.2. Performans Testi

Uygulama sonuçları, 4 GB (RAM-Random Access Memory)'e ve Windows 10 64-bit işletim sistemi ve Microsoft Word 2013 32-bit'e sahip Intel Core i3 (2.67 GHz) işlemcisine sahip bir makineden alınır. Uygulama için C # 4.5 .NET Framework platformu kullanılır. Şifreleme algoritması uygulaması için (AES, RC2, TDES) ve (RC4, Blowfish, Twofish) için Bouncy Castle Kriptografi (DLL-Dynamic-Link Library) ve .NET Framework yerleşik Kriptografi DLL'leri kullanılır. Daha önce açıklanan her bir işlem için üç testi, bölüm 4.3'te yapıyoruz. Tüm testler 4 kere çalıştırıldı ve ortalamaları hesaplandı, her test için tablolara bakınız.

5.2.1. Word uygulamasını başlatmak için ilk test

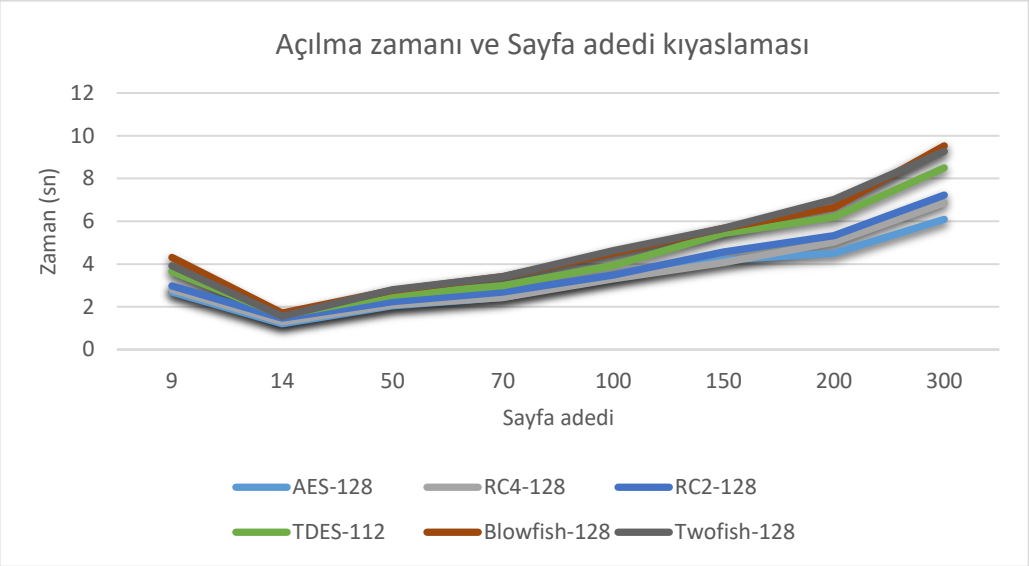
Bilgisayar kimliğini almak ve DLP-Web Servisine bağlanma süresi, internet bağlantısına bağlı olarak 0,01 saniye ile 2,0 saniye arasında değiştiği görülmüştür.

5.2.2. Dokümanın açılması için ikinci test

Tablo 5.1. Farklı dosya boyutları ve farklı şifreleme algoritmaları kullanan sayfa sayısı için dokümanın açılması ve şifresinin çözülmesi genel zamanı gösterir. Toplam süre üç katın toplamıdır. Birincisi, belgedeki şifrelenmiş verilerin okunma zamanıdır. İkincisi, düz metin ('XML-eXtensible Markup Language' dizesi) almak için şifreyi çözmenin zamanıdır. Üçüncüsü, belgeyi oluşturmak ve belgeyi açmak için XML dizesinin ayrıştırılma zamanıdır. AES, RC4, RC2, Blowfish ve Twofish'in anahtar boyutu 128 bittir ve TDES'in anahtar boyutu 112 bittir.

Tablo 5.1. Farklı dosya boyutları ve farklı şifreleme algoritmaları kullanan sayfa sayısı için belgeyi açma ve şifre çözme süresinin toplamı.

Dosya Boyutu	Sayfa adedi	AES-128	RC4-128	RC2-128	TDES-112	Blowfish-128	Twofish-128
3.45MB	9	2.695263	2.802374	2.981562	3.652868	4.309394	3.924538
544KB	14	1.204576	1.297097	1.469328	1.606416	1.703509	1.559582
847KB	50	2.050756	2.08891	2.244023	2.535857	2.759254	2.794405
1.01MB	70	2.436801	2.433337	2.696202	2.995279	3.413842	3.408304
1.60MB	100	3.377409	3.309007	3.481061	3.926474	4.511645	4.614573
1.70MB	150	4.194024	4.068522	4.567168	5.437092	5.668988	5.676459
1.77MB	200	4.501686	5.031383	5.319095	6.192539	6.639504	7.018375
2MB	300	6.088659	6.856815	7.222979	8.49772	9.526075	9.267652
Ortalama	111.6	3.318647	3.485931	3.747677	4.355531	4.816526	4.782986



Şekil 5.1. Açılma zamanı ve Sayfa adedi kıyaslaması.

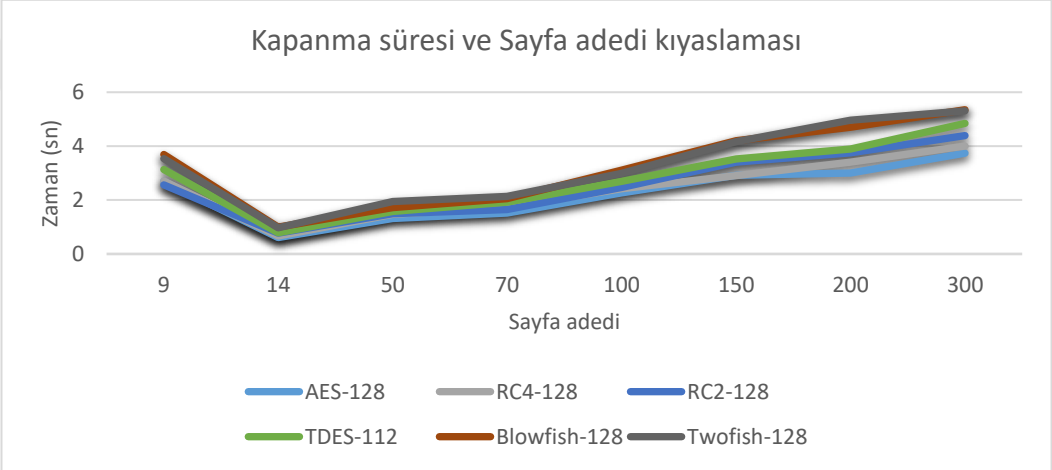
Şekil 5.1. Belge testinin açılması için Tablo 5.1.'te sunulan sonuçları özetlemektedir. Grafikte, şifrelenmiş belgenin açılma zamanının dosya boyutuna ve sayfa sayısına bağlı olduğunu görülmektedir. Sayfa sayısını veya dosya boyutunu artırmak belgenin açılış süresini artıracaktır. Test edilen şifreleme algoritmaları arasında AES'in anahtar boyutu 128 bit olan RC4 tarafından daha iyi performans gösterdiği açıkça görülebilir.

5.2.3. Belgeyi kapatmak için üçüncü test

Tablo 5.2. Belgeyi farklı dosya boyutları ve farklı şifreleme algoritmaları kullanan sayfa sayısı için kapatma ve şifreleme süresini gösterir. Toplam süre üç katın toplamıdır. İlki, belgeyi temsil eden XML dizesini okumanın zamanıdır. İkincisi, şifreli metin almak için düz metin (XML dizesi) şifreleme zamanı. Üçüncüsü belgeyi kaydetme ve kapama zamanıdır. AES, RC4, RC2, Blowfish ve Twofish'in anahtar boyutu 128 bit, TDES'in anahtar boyutu 112'dir.

Tablo 5.2. Belgeyi farklı dosya boyutları ve farklı şifreleme algoritmaları kullanan sayfa sayısı için kapatma ve şifreleme süresinin toplamı.

Dosya boyutu	Sayfa adedi	AES-128	RC4-128	RC2-128	TDES-112	Blowfish-128	Twofish-128
3.45MB	9	2.690997	2.70322	2.564246	3.130119	3.694704	3.538402
544KB	14	0.608243	0.665121	0.771921	0.785535	0.995787	0.970647
847KB	50	1.319755	1.471099	1.49678	1.571272	1.724479	1.939608
1.01MB	70	1.520164	1.730294	1.644743	1.920754	2.057411	2.136468
1.60MB	100	2.263135	2.42154	2.467695	2.697342	3.111858	2.990853
1.70MB	150	2.922747	2.90495	3.402629	3.528995	4.196691	4.167968
1.77MB	200	2.996991	3.407393	3.750937	3.88995	4.706226	4.964365
2MB	300	3.739411	4.003328	4.3916	4.844758	5.351529	5.30996
Ortalama	111.6	2.25768	2.413368	2.561319	2.796091	3.229835	3.252284



Şekil 5.2. Kapanma süresi ve Sayfa adedi kıyaslaması.

Şekil 5.2. Belgeyi kapatmak için Tablo 5.2.'de verilen sonuçları özetlemektedir. Grafikte, belgenin kapanma ve şifreleme zamanının dosya boyutuna ve sayfa sayısına bağlı olduğunu gösterir. Sayfa sayısını veya dosya boyutunu artırmak belgenin kapanış süresini artıracaktır. Belgeyi açarken olduğu gibi AES, test edilen şifreleme algoritmaları arasında 128 bit büyüklüğündeki RC4 ile daha iyi performans sergiliyor.

5.2.4. Açıklama

Kapatma süresinin, açılma süresinden daha küçük olduğunu, bunun da büyük masrafın belgeyi XML yapmak için XML çözümlemesinin bir sonucu olduğunu gösterdiğini görebiliyoruz. Genel olarak, dosyayı kapatmak için gereken zamanı yok

sayabiliriz çünkü Word uygulaması diğer işlemleri yaparken kapatma işlemi arka planda yürütülür.

İkinci ve üçüncü testlerde belgenin açılıp kapanma süresinin sayfa sayısı ve dosya boyutu ile orantılı olduğu ortaya çıktı. Sayfa sayısı veya dosya boyutu arttıkça, dokümanın açılması ve kapanma süresi, bir dizi sayfaya veya dosya boyutuna orantılı olarak artar veya tam tersi olur. Ayrıca sonuçlar, AES ve RC4 şifreleme algoritmalarının diğer algoritmalar arasında en hızlı ve uygun olduğunu göstermektedir.

BÖLÜM 6. SONUÇLAR VE ÖNERİLER

Bu araştırma, iki önleyici yaklaşımlı bir DLP-Eklentileri modelini ileri sürmektedir. Erişim kontrolü ve Şifreleme istenmeyen ve olası veri sızmalarını meydana gelmeden önce önler. Bu DLP-eklentileri modeli yetkili içeriklere (veri sahiplerine), birçok ticari DLP çözümlerinin yaptığı gibi veri içeriği ve bağlamını taramaksızın, hassas verileri tespit etme yetkisi tanır, dolaysıyla taramanın yüklediği yüksek yükten kolaylıkla kaçınır. DLP-eklentileri modeli kurum dışarısında çalışmanın daha esnek olmasını sağlar çünkü şifreli bir bağlantı ile kurum içindeki DLP-Web servisinden kullanıcının güvenlik seviyesi temin edilebilir. Ayrıca, DLP-eklentileri modeli kullancılara normal durumlarda belgeleri kullandıkları gibi sadece belgeleri açıp kapamaya benzer, belge üzerinde şifreleme ve deşifreleme işlemlerini gerektirmeyen kullanabilirliği garanti etmektedir.

Bu yaklaşımda yetkili kullancıların kasıtlı bir şekilde veri sızdırmalarının çok kolay olduğu anlaşılmıştır. Ama bilindiği üzere kasıtlı veri sızdırmanın önlenmesi imkansızdır hemde bu problem tüm DLP çözümleri için geçerlidir, bu yüzden kuruluşlar çalışanlarının kabulü ve işbirliğine güvenmelidir. Dolaysıyla, bizim DLP-eklentiler modeli çalışanların onayı ve işbirliğine güvenir ve sadece kasıtsız veri sızdırmaya odaklanır. Zaten DLP-eklentileri modeli diğer DLP çözümleri ile birlikte mükemmel çalışır.

Microsoft Office Word için DLP-eklenti modeli ve performans sonuçları amaçlanan DLP-eklenti modelinin uygulanabilir, kullanışlı ve şuanki teknolojiler ile uyumlu olduğunu gösteriyor. The implementation of DLP-Plugin for Microsoft Word and the performance results show that the proposed DLP-Plugin model is feasible, easy to use and practical using current technologies. Sonuçlar, AES ve RC4 Şifreleme algoritmalarının diğer algoritmalar arasında daha iyi olduğunu, dolayısıyla en uygun performans gösterdiğini ortaya koymuştur.

Gelecek çalışması olarak, tüm ofis belgeleri (Excel, PowerPoint, Access vb.), E-mail programları, PDF dosyaları, resimler ve video dosyaları için DLP-eklentileri modeli geliştirmeyi öneriyoruz. Bu DLP-eklentileri modelini şuanki ticari DLP çözümleri ile uyumlu bir şekilde olmasını da öneriyoruz.

KAYNAKLAR

[1] Liu, S., Kuhn, R., Data Loss Prevention, IT Prof., vol. 12, no. 2, pp. 10–13, 2010.

[2] Tahboub, R., Saleh, Y., Data Leakage/Loss Prevention Systems (DLP), in 2014 World Congress on Computer Applications and Information Systems (WCCAIS), vol. 1, pp. 1–6, 2014.

[3] Alneyadi, S., Sithirasenan, E., Muthukkumarasamy, V., A survey on data leakage prevention systems, J. Netw. Comput. Appl., vol. 62, pp. 137–152, 2016.

[4] Shabtai, A., Elovici, Y., Rokach, L., A Survey of Data Leakage Detection and Prevention Solutions. Boston, MA: Springer US, 2012.

[5] Wu , J.-S., Lee, Y.-J., Chong, S.-K., Lin, C.-T., Hsu, J.-L., Key Stroke Profiling for Data Loss Prevention, in 2013 Conference on Technologies and Applications of Artificial Intelligence, pp. 7–12, 2013.

[6] Symantec, Internet Security Threat Report, 2016.

[7] Security Risk Based, Data Breach QuickView - 2015 Data Breach Trends, https://www.riskbasedsecurity.com/2015-data-breach-quickview/., Erişim Tarihi: 11-10-2016.

[8] Arthur, C., Stuar, K., PlayStation Network users fear identity theft after major data leak, Guardian, https://www.theguardian.com/technology/2011/apr/27/playstation-users-identity-theft-data-leak., Erişim Tarihi: 01-10-2016.

[9] PwC, Managing cyber risks in an interconnected world: Key fndings from The Global State of Information Security Survey 2015, 2014.

[10] Mickelberg, K., Schive, L., Pollard, N., US cybercrime: Rising risks, reduced readiness Key fndings from the 2014 US State of Cybercrime Survey, 2014.

[11] Wuchner, T., Pretschner, A., Data Loss Prevention Based on Data-Driven Usage Control, in 2012 IEEE 23rd International Symposium on Software Reliability Engineering, pp. 151–160, 2012.

[12] Andress, J., What is Information Security?, in The Basics of Information Security, Elsevier, pp. 1–22, 2014.

[13] Guttman, B., Roback, E., An Introduction to Computer Security : The NIST Handbook, vol. SP800, no. 12, 1995.

[14] Arbel, L., Data loss prevention: the business case, Comput. Fraud Secur., vol. 2015, no. 5, pp. 13–16, 2015.

[15] Caldwell, T., Data loss prevention – not yet a cure, Comput. Fraud Secur., vol. 2011, no. 9, pp. 5–9, 2011.

[16] Hauer, B., Data and Information Leakage Prevention Within the Scope of Information Security, IEEE Access, vol. 3, pp. 2554–2565, 2015.

[17] Greenwald, G., MacAskill, E., Poitras, L., Edward Snowden: The whistleblower behind the NSA surveillance revelations, Guardian, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance., Erişim Tarihi: 11-10-2016.

[18] Petkovic, M., Popovic, M., Basicevic, I., Saric, D., A Host Based Method for Data Leak Protection by Tracking Sensitive Data Flow, in 2012 IEEE 19th International Conference and Workshops on Engineering of Computer-Based Systems, pp. 267–274, 2012.

[19] Matthee, M. H., Tagging Data to Prevent Data Leakage (Forming Content Repositories), SANS Inst., pp. 1–26, 2016.

[20] McAfee, McAfee Host Data Loss Prevention 2.2.1 Product Guide. McAfee, Inc, pp. 1–80, 2008.

[21] Dandavate, P.P., Dhotre, S.S., Data Leakage Detection using Image and Audio Files, Int. J. Comput. Appl., vol. 115, no. 8, pp. 1–4, 2015.

[22] Kale, S. A., Kulkarni, S.V., “Data Leakage Detection,” Int. J. Adv. Res. Comput. Commun. Eng., vol. 1, no. 9, pp. 668–678, 2012.

[23] Andress, J., The Basics Of Information Security: Undestanding the Fundamentals of InfoSec int Theory and Practice. 2011.

[24] Haseeb, M. A., Sethuraman, H. J., Data Loss / Leakage Prevention, Luleå University of Technology, 2012.

[25] Luft, M., Can Data Leakage Prevention Prevent Data Leakage?, University of Mannheim, 2009.

[26] Percept Technology Labs, Information Leak Prevention Accuracy and Security Tests, 2006.

[27] Rouse, M., Antimalware Definıtion, http://searchsecurity.techtarget.com/definition/antimalware., Erişim Tarihi: 07-11-2016.

[28] Rouse, M., Firewall Definıtion, http://searchsecurity.techtarget.com/definition/firewall., Erişim Tarihi: 07-11-2016.

[29] Solarflare, List of Security Terms, 2016.: http://solarflare.com/security-terms., Erişim Tarihi: 07-11-2016.

[30] Rouse, M., Definıtion Intrusion Detection (ID), http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection., Erişim Tarihi: 07-11-2016.

[31] Blasco, J., Hernandez-Castro, J. C., Tapiador, J. E., Ribagorda, A., Bypassing information leakage protection with trusted applications, Comput. Secur., vol. 31, no. 4, pp. 557–568, 2012.

[32] Anderson, R., Multilevel Security, in Security Engineering: A Guide to Building Dependable Distributed Systems PART, 2nd Edition., pp. 135–160, 2008.

[33] Bell, E., LaPadula, L., Secure Computer System: Unified Exposition and Multics Interpretation, 1976.

[34] Red Hat, Multi-Level Security (MLS), https://www.centos.org/docs/5/html/Deployment_Guide-en-US/sec-mls-ov.html., Erişim Tarihi: 07-11-2016.

[35] Anderson, R., Access Control, in Security Engineering: A Guide to Building Dependable Distributed Systems PART, 2nd Edition, Ed., pp. 93–128, 2008.

[36] Ghorbanian, S., Fryklund, G., Improving DLP system security, Faculty of Computing Blekinge Institute of Technology, 2014.

[37] Alneyadi, S., Sithirasenan, E., Muthukkumarasamy, V., Detecting Data Semantic: A Data Leakage Prevention Approach, in 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, pp. 910–917, 2015.

[38] Mogull, R., Understanding and Selecting a Data Loss Prevention Solution, 2010.

[39] Mogull, R., Understanding and Selecting a Data Loss Prevention Solution, 2007.

[40] Reed, B., Wynne, N., Magic Quadrant for Content-Aware Data Loss Prevention, 2016.

[41] MyDLP, Policy Rule Actions, https://www.mydlp.com/policy-actions/., Erişim Tarihi: 08-11-2016.

[42] DİRİ, M., GÜLÇİÇEK, M., Türkiye'de Kamu Hizmetinin Görülmesinde Kullanılmakta Olan Gizlilik Derecesi Tanımları: Uygulamadaki Sorunlar ve Çözüm Önerileri, Maliye Derg., vol. 162y, pp. 497–537, 2012.

[43] Office Cabinet UK, Government Security Classifications April 2014, pp. 1–35, 2013.

[44] Office Cabinet UK, International Classified Exchanges, no. 1–23, 2015.

[45] Aesencryption, AES encryption, http://aesencryption.net/., Erişim Tarihi: 08-11-2016.

[46] Asecuritysite, RC2, https://asecuritysite.com/encryption/rc2., Erişim Tarihi: 08-11-2016.

[47] Schneier, The Blowfish Encryption Algorithm, https://www.schneier.com/academic/blowfish/., Erişim Tarihi: 08-11-2016.

ÖZGEÇMİŞ

Huseein Al-Sanabani, 17 Temmuz 1989 yılında Sana, Yemen'de doğudu. İlk okul, orta okul ve liseyi Yemen'de 2007 senesinde tamamladı. 2007 yılında, Thamar Üniversitesi Bilişim Teknolojileri bölümünde başladığı Lisans eğitiminden 2012 yılında mezun oldu. 2012 v2 2013 yılları arasında şu üniversitede öğretmenlik yaptı. 2014 yılından bu yana Sakarya Üniversitesinde Bilgisayar ve Bilişim Mühendisliği Bölümünde Yüksek Lisans öğrencisidir.